UNIVERSIDAD NACIONAL AUTÓNOMA DE MEXICO
PROGRAMA DE POSGRADO EN DERECHO

Hacia un modelo nacional de Firma Electrónica Avanzada en la legislación mercantil

Que para optar por el grado de:

DOCTORA EN DERECHO

PRESENTA:

Lorena Pichardo Flores

Tutor: Dr. Alfredo Alejandro Reyes Krafft
FACULTAD DE DERECHO, CIUDAD UNIVERSITARIA

Ciudad México, Diciembre 2015

ÍNDICE

INTRODUCCIÓN

Existe un lenta y paulatina consolidación de la normatividad mexicana relativa al comercio electrónico y su recurso de operabilidad y seguridad: la Firma Electrónica Avanzada (FEA) desde la reforma del 29 de mayo de 2000 al Código de Comercio, el Código Civil Federal, el Código Federal de Procedimientos Civiles y la Ley Federal de Protección al Consumidor, regulación que hasta hoy no logra afianzarse por los motivos que se explican a continuación.

El marco tecno-legal de la FEA continúa inacabado, difuso, no homologado, conceptualmente diferenciado, sectorizado en los órganos de las entidades y dependencias de los poderes ejecutivo, legislativo y judicial en sus distintos ámbitos federal, estatal y municipal así como los Órganos Constitucionales Autónomos (OCA)[1]; distinciones que, además de provocar dudas, incertidumbre y contradicciones al momento de aplicar e interpretar la regulación respectiva, colocan al Derecho del Comercio Electrónico Seguro frente a marcos legales confusos y yuxtapuestos.

Entre las contradicciones más evidentes se encuentran los esquemas complejos de conservación de mensaje de datos, de digitalización de documentos que no permite su destrucción, privación de una definición del tercero legalmente autorizado (TLA), falta de confianza de los usuarios: comerciantes, Prestadores de Servicios de Certificación (PSC), autoridades y agentes certificadores, consumidores en la normatividad de la FEA.

Con ello, los beneficios que caracterizan a la FEA, las cuales se recuerdan con **A**H**ÍNCO**[2]**: A**utenticidad; **I**ntegridad; **N**o repudio y **C**onfidencialidad a través de mensajes de datos (MD), no pueden ser visibles ante la inseguridad de prestar o recibir el servicio de certificación de la FEA, especialmente de apostar a una Infraestructura de Clave Pública (Public-Key Infrastructure: PKI) en un mercado incipiente, poco demandado e insuficientemente regulado.

Ante estas vicisitudes, surgen las siguientes interrogantes:

1. ¿Deberían aplicarse distintas direcciones metodológicas para abordar el estudio de la FEA y del Derecho del Comercio Electrónico dependiendo del ámbito Nacional o Internacional?
2. ¿Es la FEA una forma de apalancar el derecho del comercio electrónico seguro?
3. ¿Cuáles son los principios jurídicos comunes en materia de comercio electrónico y la FEA?
4. ¿Cómo puede sumarse valor a la regulación actual de la FEA?
5. ¿En qué momento se puede considerar perfeccionada la voluntad de las partes contratantes en un contrato electrónico?

[1] En el artículo 6, inciso A, fracciones I y IV de la Constitución Política de los Estados Unidos Mexicanos, se hace la distinción entre los términos Órganos Autónomos Constitucionales y los Organismos Autónomos Especializados, los primeros cuyas funciones son establecer los principios, alcances y obligaciones en un ámbito de concurrencia federal, estatal así como municipal y, los segundos, cuya aplicación es aterrizar tales principios en un ámbito estatal y municipal.

[2] La palabra mnemotécnica para recordar las características de la FEA es nuestra.

6. ¿Cómo se determina el momento y el lugar de la celebración de un contrato electrónico en el ámbito nacional e internacional?
7. ¿Cuál es el ámbito territorial de ejecución de un contrato celebrado por medios electrónicos y en qué momento se considera efectuado el cumplimiento de un contrato de este tipo?
8. ¿Cuál es la ley aplicable al fondo y a la forma de un contrato electrónico seguro?
9. ¿Cuáles son las soluciones que aporta el Derecho Internacional Privado frente a los conflictos de la contratación electrónica entre diferentes Estados o Naciones?
10. ¿Qué problemas técnicos enfrenta la legislación federal mexicana de la FEA?
11. ¿Cuáles son los obstáculos que se presentan en la armonización legislativa en materia de FEA?
12. ¿Cuáles son las alternativas para lograr el uso extensivo de la FEA en el derecho del comercio electrónico nacional e internacional?
13. ¿Cuáles son las soluciones que aporta el Derecho Comparado a la regulación mexicana del comercio electrónico seguro y la FEA?

En estas condiciones, nuestra hipótesis consiste en establecer que la normatividad de la FEA en el país está tergiversada desde su elaboración, discusión y aprobación legislativa debido a una incorrecta conjugación de los elementos humanos, materiales, económicos y tecnológicos; diseminación en diversos ordenamientos jurídicos en distintas direcciones técnico-jurídicas e implementación yuxtapuestas en el sector público y privado.

De la premisa anterior, surgen varias hipótesis secundarias:

a. La actual regulación en el Derecho Mercantil Mexicano relativa a la FEA proporciona marcos legales paulatinos y escalonados que traen como efecto una pausada aplicación y obtención del máximo beneficio de la contratación electrónica segura nacional e internacional.
b. La legislación respecto al comercio electrónico y la FEA en el ciberespacio debe considerar también la aplicación de una nueva *Lex Electro-Mercatoria o Lex Info-Mercatoria.*
c. En el derecho de comercio electrónico seguro nacional, la elección de abogados expertos en Tecnologías de la Información y Comunicación (TIC) resulta la mejor vía y la mejor alternativa para resolver una *Litis.*
d. En el derecho de comercio electrónico seguro internacional, la elección de tribunales arbitrales en las cláusulas contractuales resulta la mejor opción para la resolución de controversias de manera viable y eficaz.

Bajo estos puntos de partida, el trabajo plantea los siguientes objetivos generales:

- Generar nuevas alternativas técnico-jurídicas de implementación de la FEA que abonen a su consagración nacional.
- Analizar y justificar la necesidad consagrar el marco normativo, tecnológico y práctico del Derecho del Comercio Electrónico Nacional e Internacional, en el marco de los resultados arrojados por esta investigación.

- Aunar herramientas técnico-jurídicas a través de la consideración de normas mexicanas, procesos y servicios en materia de contratación electrónica y uso de la FEA.
- Evaluar los obstáculos que presenta la aplicación de tales criterios y su eventual retroalimentación que permitan su adaptación a la contratación electrónica.
- Analizar la posible aplicación de los criterios clásicos sobre ley aplicable y jurisdicción competente en materia de contratos internacionales a los contratos electrónicos.

Por otra parte, la forma de abordar esta investigación, esto es, el marco teórico y conceptual a partir del cual encuadramos las nociones y análisis del Derecho del Comercio Electrónico seguro se basa en dos direcciones metodológicas, dependiendo del ámbito nacional o el internacional, cada uno de las cuales, a su vez, se subdividen en métodos, principios, reglas y criterios.

En este sentido, la primera dirección metodológica funda su análisis en el ámbito nacional del Derecho del Comercio Electrónico seguro y se sustenta en la pluralidad metodológica y en la interdisciplinariedad de la materia; mientras que la segunda dirección metodológica funda su análisis en el del derecho comparado del comercio electrónico seguro así como en una *Nueva Lex Electro-Mercatoria.*

En esta guisa de direcciones metodológicas, el tránsito lento de la consagración de la FEA en la legislación mercantil es amplio y su estudio se desglosa en los siguientes capítulos.

La primera unidad de este trabajo establece un amplio marco contextual normativo y tecnológico de la FEA a partir del derecho del comercio electrónico a fin de describir el estado actual del mercado, comerciantes y consumidores implicados en la contratación electrónica.

El segundo capítulo describe y analiza el marco conceptual de la configuración, formación y cumplimiento contractual electrónico sustantivo y procesal, de acuerdo de voluntades expresadas digitalmente en el ámbito nacional hasta su último acto derivado de la contratación.

El tercer capítulo aborda a la herramienta de seguridad tecnológica y jurídica del comercio electrónico, la FEA; continua con una descripción de su origen como lo es la criptografía e Infraestructura de Clave Pública.

En el capítulo cuarto se desagrega, analiza y evalúa la configuración e incorporación nacional de las soluciones técnico-jurídicas del comercio electrónico; cómo se originó, recibió e incorporó a nuestra legislación la FEA; qué modificaciones legales se requirieron para su implementación y cómo se adoptó la regulación nacional. Además, se aborda la pausada y gradual legislación de la FEA en México, su regulación comercial, tecnológica y gubernamental; así como un diagnóstico actual de su funcionamiento. De tal forma que esta sección obsequia elementos para identificar la problemática de la FEA en el derecho mercantil mexicano y prepara el terreno para para proponer soluciones en la siguiente unidad del trabajo.

En quinto capítulo se analiza la configuración técnico-jurídica de la FEA en el ámbito del Derecho del Comercio Electrónico Internacional.

En el último capítulo se realiza una propuesta sustentada en las consideraciones y alternativas que deberían considerarse o, por lo menos, evaluarse por el congresista nacional para establecer las bases de la FEA en el Derecho Comercio Electrónico en el ámbito nacional e internacional. Se exponen una serie de opciones, medidas, líneas de acción, áreas de mejora y soluciones técnico-jurídicas para una acabada consagración de la normatividad de la FEA.

Finalmente, cabe precisar dos aclaraciones. La primera consiste en que el presente estudio inicia y se justifica con el análisis del Derecho del Comercio Electrónico seguro mediante el uso de la FEA en el ámbito mercantil nacional, debido a su uso disperso y globalizado, no obstante, su análisis se extiende y retroalimenta del sector nacional (público y privado) e internacional.

La segunda precisión consiste en que a lo largo de la investigación se hace referencia continua a diversas regulaciones de la FEA por diferentes dependencias y entidades de la Administración Pública Federal (APF), órganos del Poder Judicial Federal (Suprema Corte de Justicia de la Nación, Consejo de la Judicatura Federal y el Tribunal Electoral) y Órganos y Organismos Constitucionales Autónomos, en razón de los beneficios que ofrece la retroalimentación de cada uno de estas organizaciones que regularon y gestionaron de distinta forma la FEA, a sus usuarios, titulares de certificados digitales, Prestadores de Servicios de Certificación (PSC), Autoridades y Agentes Certificadores así como a las Autoridades Certificadoras Raíz (ACR).

SIGLAS Y ACRÓNIMOS		
3D secure		*Verified by Visa* en el caso de *Visa o SecureCode* en el caso de Mastercard
3GPP		Third Generation Partnership Project
AC		Autoridad de Certificación o Autoridad Certificadora
AgC		Agentes Certificadores
AGN		Archivo General de la Nación
AMIPCI		Asociación Mexicana de Internet
AMRGSPSC		Acuerdo que Modifica las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación, reformadas publicadas el 05 de marzo de 2007.
Anteproyecto NOM-151-SCFI-2015		Anteproyecto Norma Oficial Mexicana NOM-151-SCFI-2015, Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos
APF		Administración Pública Federal
AR		Agencia Registradora
ARC		Autoridad Raíz Certificadora
ASN.1		Abstract Syntax Notation One (Notación sintáctica abstracta 1)
ATL		Above The Line:, en español: sobre la línea
B2B		Business to Business
B2C		Business to Consumer
BTL		Below The Line, en español: bajo la línea
CANIPEC		Cámara y Asociación de la Industria de Productos del Cuidado Personal y del Hogar
CCE o ECC		Criptosistema de Curvas Elípticas, en inglés Elliptic Curve Cryptography
CCiF		Código Civil Federal
CCI/ICC		Cámara de Comercio Internacional/International Chamber of Commerce
CCo		Código de Comercio
CEP		Comprobante Electrónico de Pag
CERTIFICA		Nuevo programa o software que sustituyó a SOLCEDI para integrar las nuevas disposiciones técnicas de los archivos FIEL y los Certificados Sellos Digitales (CSD) del Servicio de Administración Tributaria.
CETES		Certificados de la Tesorería de la Federación
CIEC		Clave de Identificación Electrónica Confidencial de la Clave Privada.
CIDIP		Conferencia Interamericana Especializada sobre Derecho Internacional Privado
CFD		Comprobante Fiscal Digital
CFDI		Comprobante Fiscal Digital por Internet
CFF		Código Fiscal de la Federación
CFPC		Código Federal de Procedimientos Civiles
CIDGE		Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico
CIM		Comunicaciones Integradas de Marketing
CJF		Consejo de la Judicatura Federal
CNA		Consejo Nacional de Archivos
CNBV		Comisión Nacional Bancaria y de Valores
CNSF		Comisión Nacional de Seguros y Fianzas
CNUCCIM/CISG		Convención de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías (conocida como Convención de Viena de 1980, en inglés: United Nations Convention on the International Sale of Goods: CISG).

CNUDMI/UNCITRAL		Comisión de las Naciones Unidas para el Derecho Mercantil Internacional UNCITRAL, en inglés United Nations Commission on International Trade Law.
CNUUCECI/ECC		Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales (Nueva York, 2005) o United Nations Convention on the Use of Electronic Communications in International Contracts (the *Electronic Communications Convention*: ECC)
CANIPEC		Cámara y Asociación de la Industria de Productos del Cuidado Personal y del Hogar
COFECO		Comisión Federal de Competencia
COFEMER		Comisión Federal de Mejora Regulatoria
COFEPRIS		Comisión Federal para la Protección contra Riesgos Sanitarios
CONAGO		Confederación Nacional de Gobernadores
CONAR		Consejo de Autorregulación Publicitaria
CONDUSEF		Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros
COSMEP		Código de Autorregulación y Ética Publicitaria para Productos Cosméticos
CPEUM		Constitución Política de los Estados Unidos Mexicanos
CSD		Certificado de Sello Digital
CUSF		Circular Única de Seguros y Fianzas
DDHH		Derechos Humanos
DOF		Diario Oficial de la Federación
DCP		Declaración de Prácticas de Certificación
DSA		Digital Signature Algorithm o Algoritmo de firma digital
DSS		Digital Signature Standard
DTISACG		Documento Técnico de Interoperabilidad de los Sistemas Automatizados de Control de Gestión
ECDSA		Elliptic Curve Digital Signature Algorithm
EDI		Intercambio Electrónico de Datos; en inglés, *Electronic Data Interchange*
EESSI		European Electronic Signature Standardization Initiative
ICC TERMS 2004		Cláusulas contractuales 2004 de la CCI para el comercio electrónico.
EIDA		Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal
ETSI TS		European Telecommunications Standards Institute.
ERP		Enterprise Resource Planning
FEA		Firma Electrónica Avanzada
FEC		Front End de Comunicaciones
FESE		Firma Electrónica para el Seguimiento de Expedientes
FIEL		Firma Electrónica (avanzada) del SAT, adoptada posteriormente por la Función Pública y algunas Entidades y Dependencias de la Administración Pública Gubernamental.
FIREL		Firma Electrónica Certificada del Poder Judicial de la Federación
FNTC		Fédération Nationale des Tiers de Confiance
CCI/ICC		Cámara de Comercio Internacional o International Chamber of Commerce
ICC *eTerms* 2004		Cláusulas contractuales publicadas en 2004 por la Cámara de Comercio Internacional.

ICP o PKI		Infraestructura de Clave Pública o Infraestructura de Llave Pública (Public Key Infrastructure: PKI)
IES		Infraestructura Extendida de Seguridad *o* Integrated Encryption Scheme
IETF		Internet Engineering Task Force
IFT		Instituto Federal de Telecomunicaciones
IMPI		Instituto Mexicano de la Propiedad Industrial
INAI		Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales
INCOTERMS		Términos Internacionales de Comercio o *International Commercial Terms*, elaboradas y actualizadas por la Cámara de Comercio Internacional.
InterPARES		International Research on Permanent Authentic Records in Electronic Systems
ISO		International Organization for Standardization u Organización Internacional para la Estandarización
ITFEA		Infraestructura Tecnológica de Firma Electrónica Avanzada
ITU/UIT		International Telecommunications Union/ Unión Internacional de Telecomunicaciones
LACP		Ley de Ahorro y Crédito Popular
LCS		Ley sobre el Contrato de Seguro
LEI		Legal Entity Identifier o Identificador de Entidad Jurídica
LFA		Ley Federal de Archivos
LFEA		Ley de Firma Electrónica Avanzada
LFIF		Ley Federal de Instituciones de Fianzas
LFPA		Ley Federal de Procedimiento Administrativo
LFPC		Ley Federal de Protección al Consumidor
LFPDPPP		Ley Federal de Protección de Datos Personales en Posesión de los Particulares
LFTAIPG		Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental
LGISMS		Ley General de Instituciones y Sociedades Mutualistas de Seguros
LFMN		Ley Federal de Metrología y Normalización
LGSM		Ley General de Sociedades Mercantiles
LGTOC		Ley General de Títulos y Operaciones de Crédito
LIC		Ley de Instituciones de Crédito
LISF		Ley de Instituciones de Seguros y de Fianzas
LMCE		Ley Modelo de la CNUDMI sobre Comercio Electrónico (1996)
LMFE		Ley Modelo de la CNUDMI sobre las Firmas Electrónicas (2001)
LMM		Ley Monetaria Mexicana
LNDF		Ley del Notariado del Distrito Federal
MAE		Módulo de Atención Electrónica
MD		Mensaje de Datos
MD5		Message-Digest Algorithm 5 o Algoritmo de Resumen del Mensaje 5
NARA		National Archives and Records Administration
NIP		Número de Identificación Personal
NMX-I-289		Norma Mexicana NMX-I-289-NYCE-2013: Metodología de Análisis Forense de Datos y Guías de Ejecución Information Technology (Forensic Methodology Data Analysis and Implementation Guidelines).

NMX-I-291		Norma Mexicana NMX-I-291–NYCE-2013: Digitalización Documental con Valor Agregado Information Technology (Added Value Document Digitizing).
NOM		Norma Oficial Mexicana
NOM-151		NOM-151-SCFI-2002, Prácticas comerciales-Requisitos que deben observarse para la conservación de mensajes de datos
NMX		Norma Mexicana
OECD		Organización para la Cooperación y el Desarrollo Económicos
OCA		Órganos Constitucionales Autónomos
OCSP		Protocolo de Estatus de Certificados en Línea, en inglés Online Certificate Status Protocol.
OgCA		Organismos Constitucionales Autónomos
PABI		Código de Autorregulación de Publicidad de Alimentos y Bebidas no Alcohólicas dirigidas al Público Infantil
PAC		Proveedor Autorizado de Certificación
PACCFDI		Proveedor Autorizado de Certificación de Comprobantes Fiscales Digitales a través de Internet
PACRDD		Proveedor Autorizado de Certificación de Recepción de Documentos Digitales
PGCM		Programa para un Gobierno Cercano y Moderno
PGP		Pretty Good Privacy o Privacidad Bastante Buena
PJF		Poder Judicial de la Federación
PROFECO		Procuraduría Federal del Consumidor
Protocolo SET		Protocolo de Transacción Electrónica Segura o Secure Electronic Transaction Protocol.
PSC		Prestador de Servicios de Certificación
PSI		Proveedor de Servicios de Internet
RFC		Request for Comments
RLFEA		Reglamento de la Ley de Firma Electrónica Avanzada
RMF		Resolución de Miscelánea Fiscal
RNIE		Registro Nacional de Inversiones Extranjeras
RPCSE		Registro Público de Comercio de la Secretaría de Economía
RRPG		Reglamento del Registro Público de Comercio
RCCMPSC		Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación
RGSPSC		Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación
RSA algorithm		Ron Rivest, Adi Shamir, and Leonard Adleman algorithm
RUG		Registro Único de Garantías Mobiliarias
S/MIME		Secure/Multipurpose Internet Mail Extensions
SAC		Servicios de Archivos de Confianza o *Trusted Archival Services* (TAS)
S.A.S.		Sociedad por Acciones Simplificada
SAT		Servicio de Administración Tributaria
SCJN		Suprema Corte de Justicia de la Nación
SE		Secretaría de Economía
SEGOB		Secretaría de Gobernación

SENASICA		Servicio Nacional de Sanidad, Inocuidad y Calidad Agroalimentaria
SFP		Secretaría de la Función Pública
SHA-256		Secure Hash Algorithm-256, genera un tamaño mixto de 256 bits (32 bytes) un hash casi único.
SHCP		Secretaría de Hacienda y Crédito Público
SIC		Sociedad de la Información y el Conocimiento
SIGER		Sistema Integral de Gestión Registral
SMS		Servicios de Mensajería Instantánea
SOLCEDI		Solicitud de Certificado Digital: primer plataforma del SAT para emitir solicitudes de certificado digital.
SPEI		Sistema de Pagos Electrónicos Interbancarios
SSL		Secure Sockets Layer (en español capa de conexión segura).
TE		Tribunal Electoral del Poder Judicial de la Federación
TESOFE		Tesorería de la Federación
TIC		Tecnologías de la Información y Comunicación
TLA		Tercerlo Legal Autorizado
UCC		Uniform Commercial Code
UCITA		Uniform Computer Transactions Act
UCP 600		Reglas y usos uniformes para créditos documentario 600 o Uniform Customs and Practice for Documentary Credits
UNCOCEFI		Unidad para el Control de Certificación Firmas del Poder Judicial de la Federación.
UNIDROIT		Instituto Internacional para la Unificación del Derecho Privado o *Institute for the Unification of Private Law*
UUID		Identificador Único Universal o *Universally Unique Identifier*

CAPÍTULO I. DERECHO DEL COMERCIO ELECTRÓNICO

1.1. Direcciones metodológicas para el análisis del Derecho del Comercio Electrónico.

1.1.1. Metodología para el análisis nacional del Derecho del Comercio Electrónico: La pluralidad metodológica y la interdisciplinariedad.

a) Pluralismo y sincretismo metodológico

El discurso metodológico para el estudio del derecho del comercio electrónico nacional se basa en el sincretismo metodológico al cual se accede mediante el pluralismo metodológico.

Si bien, para lograr el sincretismo se requiere el empleo del pluralismo metodológico, éste es amplio y resulta complicado fijar sus límites en razón de la generalidad y la difusión de las teorías metodológicas; no obstante debe precisarse que la pluralidad metodológica no presupone la contradicción en un cojunto de métodos.[3]

El uso del sincretismo métodológico o combinación metodológica refiere la unión de varios conceptos o teorías no armónicas sin que exista contradicciones internas, sin implicar necesariamente contradicción entre principios. En él se busca la utilización de herramientas metodológicas que complementan y ofrecen alternativas para encontrar valiosas soluciones o caminos de entendimiento, por ejemplo los tradicionales dualismos: nominalismo *vs* realismo; empirismo *vs* espiritualismo; positivismo *vs* iusnaturalismo; racionalismo *vs* visión reflexiva[4]; o bien, el propio uso del monismo teórico, como constante negación de los dualismos.

A los anteriores herramientas y caminos se integran pensamientos no dualistas pero sí complementarios, como lo son el método histórico o fenomenológico; comparatista; semiótico; deontológico o axiomático; teleológico; reductivo; exegético; dogmático (constructivismo jurídico) y sociológico (socio-económico y socio-jurídico) para el estudio nacional de Derecho del Comercio Electrónico Nacional.

b) La interdisciplinariedad.

La propuesta de la interdisciplinariedad implica la superación de la fragmentación del conocimiento técnico-jurídico que reflejan las materias y la formación de la especialización, permite el entendimiento de la diversidad y la difícil actualidad del Derecho del Comercio Electrónico.

[3] Hernández Gil, Antonio. Metodología de la ciencia del Derecho, Tomo V, 1987, Madrid, España, Ed. Espasa-Calpe, p. 577.
[4] Teubner, Gunther y Bourdieu, Pierre. La fuerza del Derecho, 2005, Bogotá, Colombia, Ed. Universidad de los Andes, 220 pp., passim.

La realidad se muestra una multidimensionalidad de causas, efectos, nexos e interrelaciones y en esa medida se obtienen distintos resultados[5], por lo cual se deben ofrecer instrumentos recíprocos como la integración, la comprensión y la extensión de la investigación.

Existen diferencias entre los niveles disciplinarios, a saber: monodisciplinar, multidisciplinar, interdisciplinar y transdisciplinar; los cuales se plasman mediante intersecciones de conjuntos.

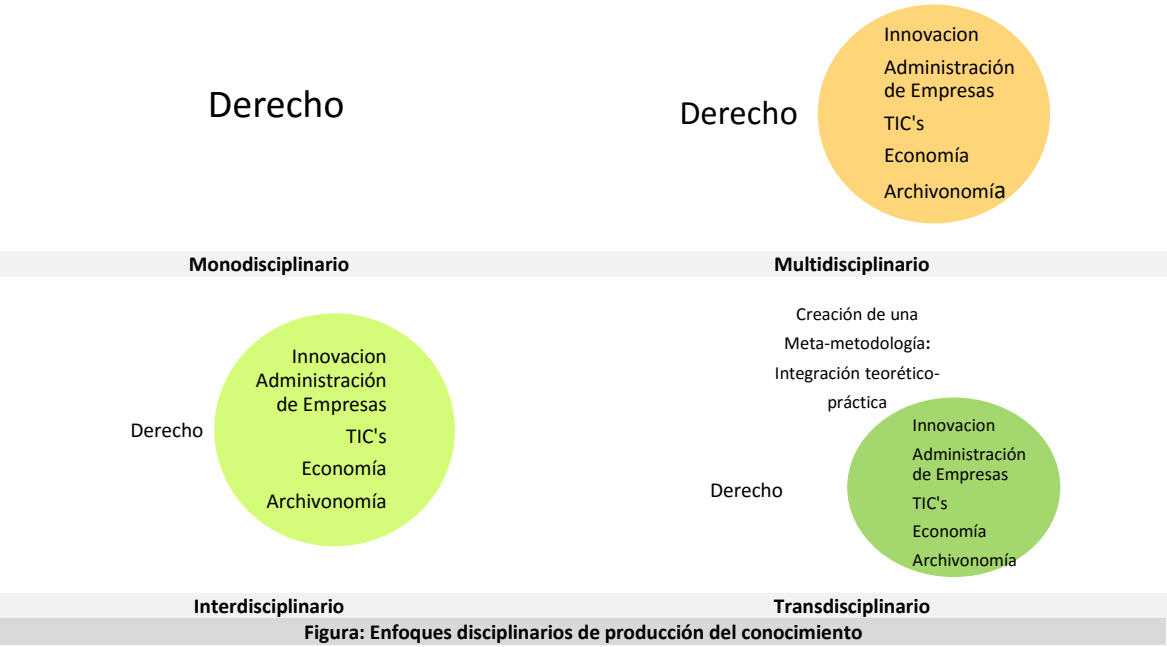
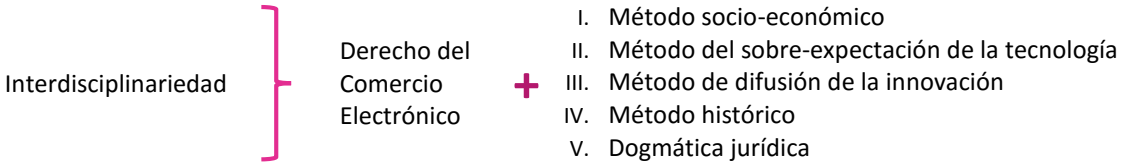


Figura: Enfoques disciplinarios de producción del conocimiento

En este trabajo nos enfocamos y seleccionamos la investigación interdisciplinaria donde la inclusión, participación e integración del conocimiento procede de diferentes análisis, definiciones, conceptos, lenguajes y puntos de partida que deben aclarase antes de iniciar la investigación; de tal forma que, cada contribución se re-estructure con el resto de las demás disciplinas para formar una unidad con significado; incluso si se llega a considerar la realización de tareas más complicadas en esta disciplina como la unidad de significado sistemático de creación de cada investigador, donde lo que solamente se comparte es la norma[6][7].

La interdisciplinariedad que se aborda en esta investigación es, por una lado: el método socio-económico, el método de la sobre-expectación de la madurez, adopción y aplicación comercial de las tecnología, y el método de difusión de la Innovación; y por el otro lado, en el área del Derecho, el método histórico y la dogmática jurídica.

[5] Para mayor información visitar la página oficial del Centro Internacional de Investigaciones y Estudios Transdisciplinarios, accesible en http://www.cietedgarmorin.org, consulta 2 de marzo de 2015.
[6] Cfr. Martínez Miguélez, Miguel. Transdisciplinariedad y Lógica Dialéctica: Un enfoque para la complejidad del mundo actual, Venezuela, accesible en http://prof.usb.ve/miguelm/transdiscylogicadialectica.html , consultada el 14 de julio de 2015.
[7] En este sentido también se pronuncia Basarab Nicolescu en La transdisciplinarité. Manifeste, 1996, Ed. Du Rocher, Mónaco, Francia. (trad.del francés, Consuelo Falla Garmilla, Escuela Nacional de Trabajo Social de la UNAM). También visible en la página oficial de "International Center for Transdisciplinary Research" (CIRET), http://ciret-transdisciplinarity.org/transdisciplinarity.php



A continuación se explica cada uno de ellos.

I) Método socio-económico de Saskia Sassen.

La visión de la socióloga neerlandesa Saskia Sassen[8] señala que cuando se realiza un *emplazamiento estratégico tecnológico* de una herramienta técnica surgirán beneficios en la competitividad, desarrollo e innovación tecnológica de una nación, pero a su falta o cuando un país no cumple con el periodo de emplazamiento de una tecnología para ponerla en práctica o uso, tal instrumento técnico, como lo es la Firma Electrónica Avanzada, esa nación ocupará el lugar de un país subdesarrollado o marginal respecto de esa tecnología.

La presencia de una tecnología vigente y en uso, en un territorio origina la creación de zonas francas industriales o de centros bancarios transnacionales, es decir de ciudades globales o mercados mundiales que concentran el poder económico, tales como Nueva York, Londres, Tokio, Paris, Fráncfort, Zúrich, Ámsterdam, Los Ángeles, Sídney, Hong Kong, Barcelona, entre otros; y últimamente participan otras ciudades incipientes como Bangkok, Taipéi, São Paolo y la Ciudad de México[9] (ver Apéndice I: Índice de Ciudades Globales en 2012).

El emplazamiento estratégico tecnológico no solo consiste en la adaptación de un producto de innovación tecnológica, sino que también integra los procesos y servicios aparejados con él, entre ellos, la normatividad que los hacen aplicables. Por ello dependiendo del producto, proceso o servicio que sea emplazado tecnológicamente, se estará ante una desigualdad en el uso de ese recurso, tal es el caso del comercio electrónico y la Firma Electrónica Avanzada en México.

Las consideraciones de Sassen se robustecen con la idea de Alain Minc, quien señala que en la tercera fase del proceso de acumulación del capital domina el capital financiero, el cual se originó para apoyar al capital industrial, pero una vez que se expandió y creció en el mercado de dinero y de capital, se independizó del capital industrial, de tal forma que actualmente el sector financiero define y controla al resto. Ante esta situación, le corresponde al juzgador equilibrar la vida económica[10].

[8] Sassen, Saskia. 2006 La ciudad global: emplazamiento estratégico, nueva frontera, del original en inglés "The Global City: Strategic Site, New Frontier", in Managing Urban Frontiers: Sustainability and Urban Growth in Developing Countries, eds. Marco Kainer, Martina Koll-Schretzenmayr, and Willy A. Schmind. Burlington, VT, Ashgate. 2005, p 35.
[9] Ibidem, p, 39.
[10] Alain Minc. www.capitalismo.net., 2001, Buenos Aires, Ed. Paidós, Colección Espacios del Saber, p. 12.

Así, frente a las innovaciones tecnológicas de Internet, el capital accionario, la expansión de los mercados de dinero y capital, la especulación con tecnología avanzada florece por arriba de la actividad productiva así como tecnológica y es más veloz que la producción de alimentos.

Luego ante esta dríada: capital accionario financiero e innovaciones tecnológicas, se suma la industria bélica, la cual sostiene la crisis estructural del capitalismo global. De tal forma que se está ante un nuevo modelo de capitalismo: la globalización, mundialización, capitalismo patrimonial o salvaje en el cual se contextualiza el comercio electrónico y la FEA.

II) Método del Ciclo de Sobre-expectación de Gartner (Gartner Hype Cycle).

El ciclo de sobre-expectación de Gartneres una curva gráfica de la madurez, adopción y aplicación comercial de una tecnología específica, que en este trabajo se adoptará para el comercio electrónico y la FEA.

El método fue elaborado en 1995 por el estadounidense Gartner a fin de investigar y analizar datos mundiales sobre la industria de las Tecnologías de la Información y Comunicación (TIC) y desde entonces es un método indispensable para describir el entusiasmo sobredimensionado de una tecnología y la decepción que ocurre en la introducción de una nueva TIC.

Todo ciclo de sobre-expectación de un mercado tecnológico se detalla en la siguiente gráfica.

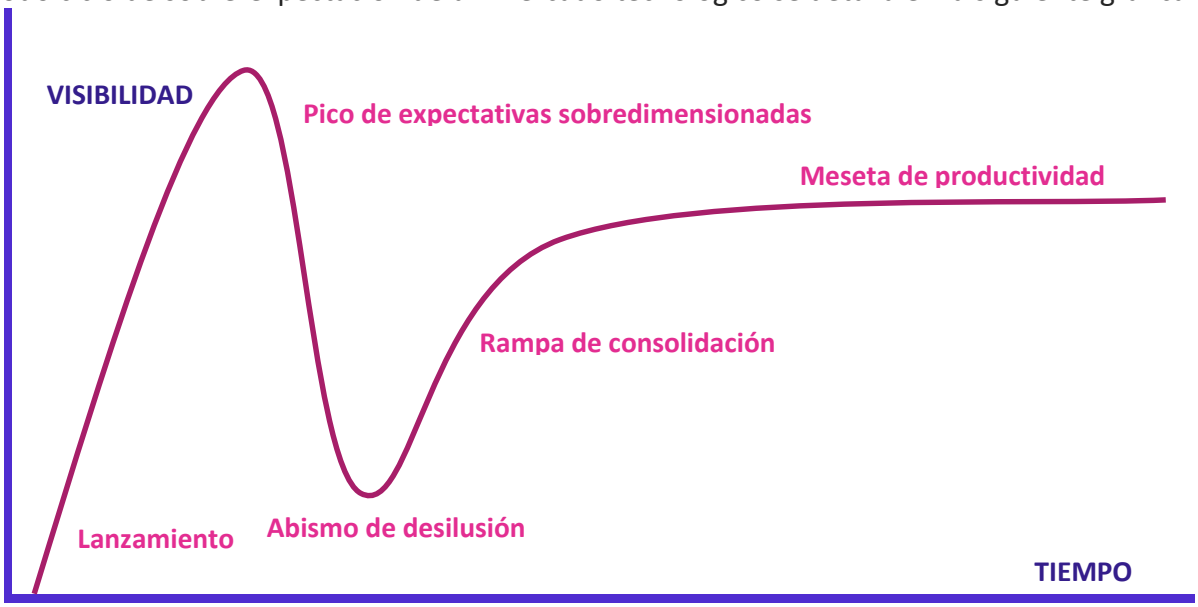


Figura del Ciclo de sobre-expectación de Gartner[11]

La figura anterior explica el ciclo de sobre-expectación tecnológica de Gartner compuesto por cinco fases:

[11] La gráfica es nuestra, retomada de las voces "Ciclo de sobreexpectación", en Wikipedia, accesible en https://es.wikipedia.org/wiki/Ciclo_de_sobreexpectaci%C3%B3n, consultado el 12 de mayo de 2015.

a) **Lanzamiento:** La primera fase de un ciclo es el *lanzamiento,* una presentación del producto o cualquier otro evento que genera interés y presencia en los medios.

b) **Pico de expectativas sobredimensionadas**: En la siguiente fase, el impacto en los medios genera normalmente un entusiasmo y expectativas poco realistas. Es posible que algunas experiencias pioneras se lleven a cabo con éxito, pero habitualmente hay más fracasos.

c) **Abismo de desilusión**: Las tecnologías entran en el abismo de desilusión porque no se cumplen las expectativas. Estas tecnologías dejan de estar de moda y en consecuencia, por lo general la prensa abandona el tema.

d) **Rampa de consolidación**: Aunque la prensa haya dejado de cubrir la tecnología, algunas empresas siguen, a través de la *pendiente de la iluminación*, experimentando para entender los beneficios que puede proporcionar la aplicación práctica de la tecnología.

e) **Meseta de productividad**: Una tecnología llega a la *meseta de productividad*, cuando sus beneficios están ampliamente demostrados y aceptados. La tecnología se vuelve cada vez más estable y evoluciona en segunda y tercera generación. La altura final de la meseta varía en función de si la tecnología es ampliamente aplicable o sólo beneficia a un nicho de mercado.

Lo deseable en la implementación de una tecnología como la FEA es transitar de la fase 4 a la fase 5 de dicho ciclo, a través de una serie de recursos y consideraciones técnico-jurídicas.

A continuación se replica el ciclo de sobre-expectación específicamente del comercio electónico en el año 2012, también elaborado por la empresa Gartner.

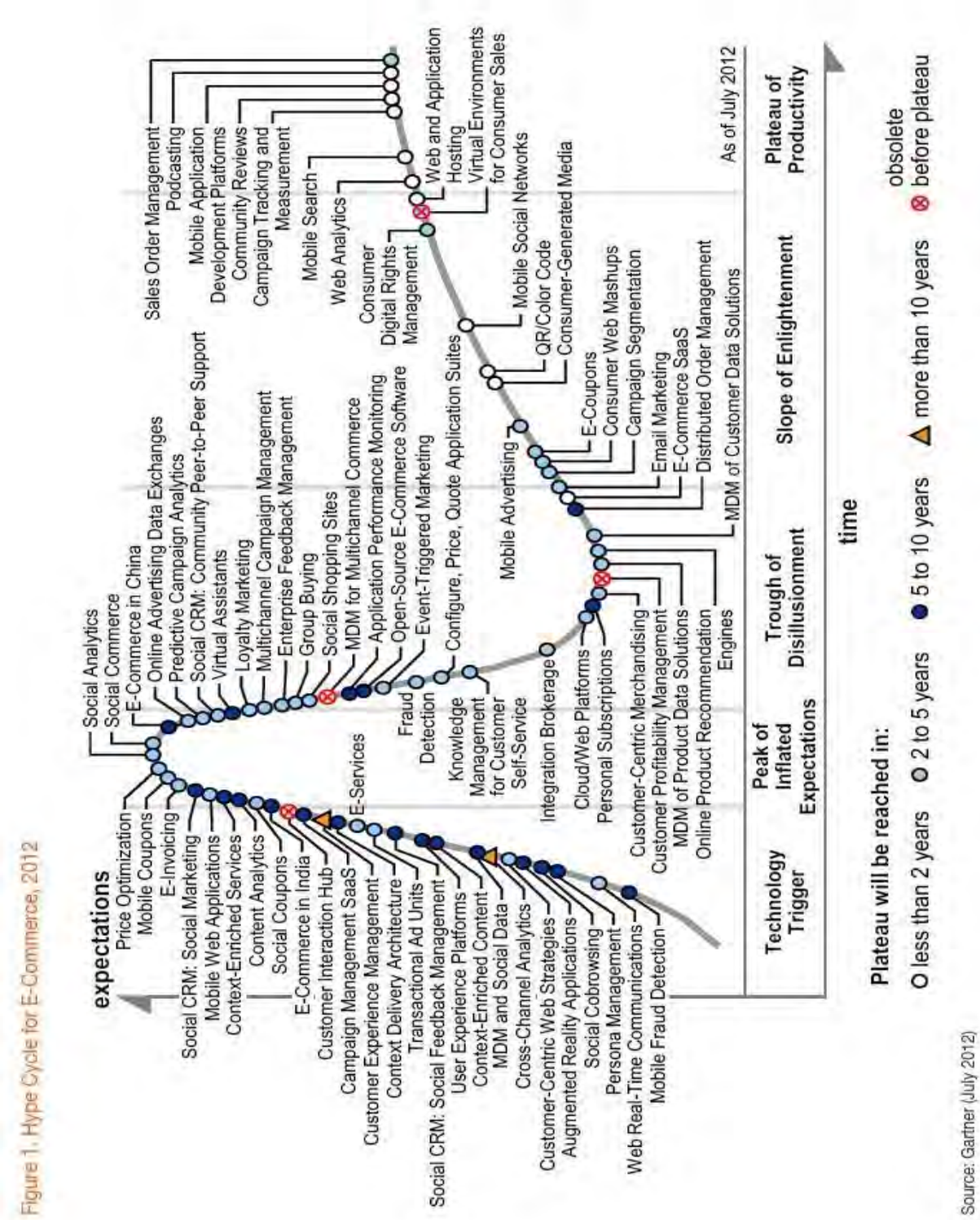


Figura del Ciclo de sobre-expectación del comercio electrónico 2012[12]

III) Método de la *Curva de Difusión de la Innovación* de Rogers

La difusión de innovaciones es una teoría sociológica que pretende explicar cómo, por qué y a qué velocidad se mueven las nuevas tecnologías (en nuestro caso la FEA) a través de las diversas culturas. La curva de difusión de la innovación explica cómo una innovación es comunicada a través de ciertos canales, a través del tiempo, miembros de un sistema social y cómo dicha tecnología es aceptada y divulgada en Internet o una red social.

La referida curva se aplicará en esta investigación para mostrar cómo México se ha insertado y comportado en la tecnología y la FEA en el comercio electrónico.

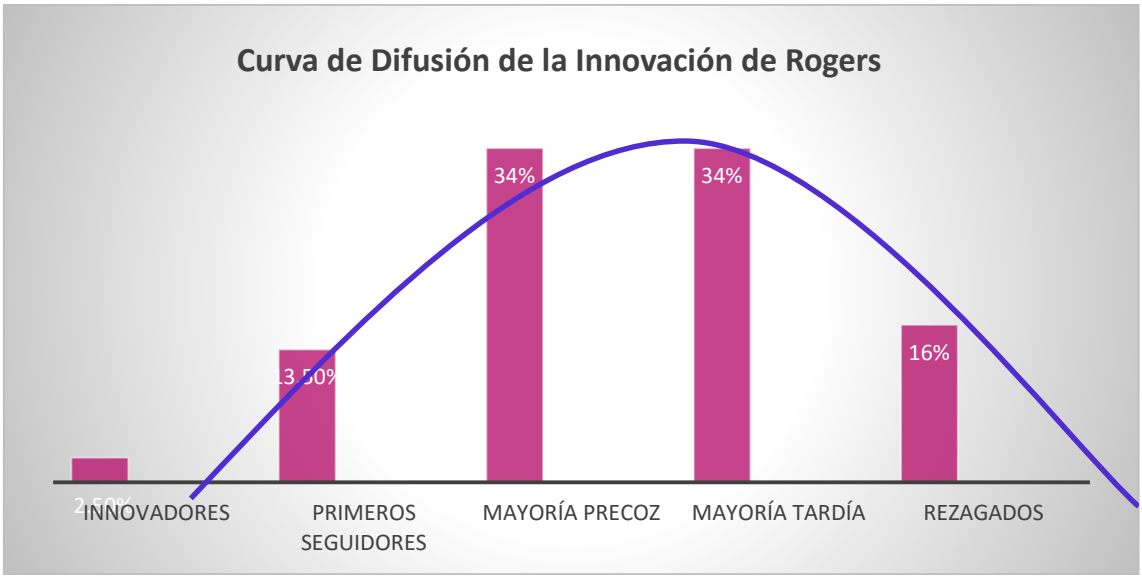


Figura: Rogers, Everett M. Adopter categorization on the basis of innovativeness, Diffusion of Innovations, 1983, USA, 3a ed., Ed. Macmillan Publishing p. 246 y ss.

IV) Método Dogmático.

Un cuarto método aplicado constantemente a lo largo de la investigación es el método dogmático a fin de profundizar en las construcciones jurídicas de los conceptos legales mediante la lógica jurídica.

IV) Método Histórico.

El quinto y último método que amerita aplicarse es el histórico.

La enunciación de métodos no es limitativa ya que a lo largo de la investigación también se ofrecen alternativas para dar nuevas soluciones jurídicas a la problemática planteada en este trabajo.

[12] Gartner Publications. Hype Cycle for E-Commerce 2013, 31 de julio 2013, Stamford, Id. number: G00252379, descarga solo accesible con pago de membresía: https://www.gartner.com/doc/2571916/hype-cycle-ecommerce-f, accesible el 2 de enero de 2015.

1.1.2. Metodología para el análisis internacional del Derecho del Comercio Electrónico: Derecho Comparado y *Nueva Lex Electro-Mercatoria.*

I) Derecho Comparado.

La globalización como proceso multidimensional integra cambios de interacciones y acuerdos sociales que impactan la magnitud, velocidad e impactan que originan las redes regionales y mundiales que abarcan sectores jurídicos, económicos, culturales, políticos y tecnológicos; por ello, se requiere profundizar en las formas en que cada país legisla figuras jurídicas que se originan y vinculan con la globalización. El método por antonomasia para llevarlo a cabo es el método de Derecho Comparado.

El Derecho Comparado es un referente de la normatividad en relación a su variedad, distinciones y posibilidades de acercamiento que existen entre los diversos sistemas jurídicos. Actulamente el derecho comparado permite la armonización y unificación progresiva de materias, por ejemplo: Derechos Humanos, Derecho al Medio Ambiente, Derecho Marítimo, Derecho internacional, Derecho Internacional Privado y Derecho del Comercio Internacional[13].

Para conocer las legislaciones e instituciones jurídicas que nos interesan introducimos la distinción de dos herramientas de equiparación y confronta del comparatista Leontín-Jean Constantinesco, la primera, la *microcomparación* y la segunda, la *macrocomparación[14]:*

> ***Microcomparación:*** *aproximación comparativa de las reglas o de las instituciones jurídicas pertenecientes a órdenes jurídicos diferentes (…) del fenómeno jurídico seccionado y reducido a sus células últimas o a sus particulares elementos.*
>
> ***Macrocomparación****: examen del fenómeno jurídico "en sus estructuras fundamentales y específicas, en su morfología características (…) que responde a fines teóricos que consisten en precisar las estructuras determinantes de los órdenes jurídicos su parentesco tipológico y fijar, en consecuencia, las familias y los sistemas jurídicos* [15]*.*

A partir del uso de estas herramientas son visibles las finalidades del Derecho Comparado, a saber[16]:

a) Mejor conocimiento del derecho nacional
b) Formación de un lenguaje jurídico internacional
c) Unificación o armonización de los ordenamientos jurídicos

---

[13] Rojas Ulloa, Milushka Felícitas. La Importancia del Derecho Comparado en el Siglo XXI, en Revista On Line del Instituto de Investigación Jurídica de la Universidad de San Martín de Porres, 2009, Perú, accesible en: http://www.derecho.usmp.edu.pe/instituto/revista/articulos/Articulo_de_Investigacion_Juridica.pdf, consulta del 22 de marzo 2015, pp. 3-5.

[14] Constantinesco, Leontin-Jean. Tratado de Derecho Comparado, Introducción al Derecho Comparado, 1981, Madrid, Ed. Tecnos., pp. 155-158.

[15] Ob. cit., p. 680. Citando a :L. J. CONSTANTINESCO, Traite de droit comparé, I y II, París, 1972-1974, passim.

[16] Rojas Ulloa, Milushka Felícitas. "La Importancia del Derecho Comparado en el Siglo XXI", en Revista On Line del Instituto de Investigación Jurídica de la Universidad de San Martín de Porres, 2009, Perú, accesible en: http://www.derecho.usmp.edu.pe/instituto/revista/articulos/Articulo_de_Investigacion_Juridica.pdf, consulta del 22 de marzo 2015, pp. 12 y 13.

d) Conocimiento de los ordenamientos jurídicos

II) *Nueva Lex Electro-Mercatoria o Lex Info-Mercatoria*

Frente a esta globalización o procesos multidimensionales de interacciones dinámicas sociales, culturales, económicos, políticos, legales, tecnológicas, se origina una *Global Village Autónoma*[17]*,* evidente que dicha mundialización trae aparejada la globalización del Derecho.

Una consecuencia de la formación de estas villas globales son la *búsqueda de una teoría global del derecho aplicable a diferentes tradiciones, culturas y órdenes jurídicos que por efecto de la globalización se han constituido en pluralismo legal.*[18]

En este contexto, el Derecho del Comercio Electrónico excede el ámbito del Derecho Mercantil Internacional convencional, lo cual se explica por el impacto de la globalización en los contratos electrónicos en el nivel internacional.

Si bien, el desarrollo del Derecho del Comercio Electrónico es una consecuencia de la adopción de las Tecnologías de la Información y Comunicación (TIC) a la teoría del negocio jurídico internacional, el Estado advierte la necesidad de regular el ciberespacio[19] y la asimilación de estas tecnologías por los contratantes y a partir de ahí surgen dos posturas que aclaran el cómo y el quién debe normar el ciberespacio.

La primer teoría o postura es la tradicionalista, que se refiere a que el Estado es el más adecuado para normar el ciberespacio pues detenta la soberanía para hacerlo toda persona debe cumplir con ciertas normas; mientras tanto, la segunda teoría es la autónoma, que se funda en que el ciberespacio es una ámbito social separado que no debe ser regulado por el derecho nacional sino por las propias reglas de los usuarios ciberespacio y que se encuentran apegadas a la *Declaración de Independencia del Ciberespacio* de 1996 de John Perry Barlow.

Es a partir de la segunda teoría de regulación del ciberespacio, la autónoma y las bases de la contratación electrónica internacional que sustentamos parte[20] de nuestro discurso metodológico, el que consiste en una Nueva *Lex Electro-Mercatoria* o Nueva *Lex-Info-Mercatoria*[21]. Lo anterior significa que el argumento de que la fuente de validez de la *Lex*

[17] Así la denoina Teubner, Gunther. Societal Constitutionalism: Alternatives to State-Centred Constitutional Theory? Oxford, 2004, Ed. Hart Publishing, p.14, accesible en: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=876941, consultado 2 de noviembre de 2015.

[18] Casados Borde, Alfonso Jesús. El Derecho Comercial y la Búsqueda de una Teoría Jurídica Global, en Revista del Posgrado en Derecho de la UNAM, Nueva época, núm. 2, julio-diciembre 2015, p. 4.

[19] El término de ciberespacio fue por primera vez utilizado en 1984 por William Gibson en su novela de ciencia ficción denominada Neuromancer y significa una alucinación consensuada que experimentan cotidianamente billones de usuarios de computadoras, como una representación gráfica de información que fluye de la computadora al sistema humano.

[20] Es parcial porque la metodología que aplicamos es un discurso basado en la pluralidad metodológica, donde la Lex Info-Mercatoria es una herramienta de análisis y solución de controversias.

[21] Ello es así porque no se refiere a la Lex Mercatoria medieval del siglo XI que se restringía a los fletes, pólizas de carga y leras de cambio en materia marinos. Lex que evidentemente se ha modernizado y evolucionado.

Mercatoria es el mismo que el de la *Lex Informática*[22]*,* lo es también para la combinación de ambas: *Lex Electro-Mercatoria.*

En este sentido, la *Lex Mercatoria* se refiere a la aparición de un derecho *no nacional* que responde a las expectativas de las negociaciones internacionales y recoge una serie de usos, costumbres y principios desarrollados por las organizaciones comerciales internacionales basados en la autonomía de la voluntad de las partes sin la participación de la normatividad interna de los Estados. Entre los instrumentos normativos que conforman la Lex Mercatoria, Labariega Villanueva[23] aduce que son:

- ***a)*** *Derecho internacional público.*
- ***b)*** *Legislación uniforme*[24]
- ***c)*** *Principios generales del Derecho*
- ***d)*** *Las normas de organizaciones internacionales*
- ***e)*** *Usos y costumbres*[25]
- ***f)*** *Contratos tipo*
- ***g)*** *Laudos arbitrales archivados*

La función de la *Lex Mercatoria* es actuar como un sistema legal supranacional que se considera autónomo para regular las transacciones comerciales internacionales así como la disertaciones en cuestiones relativas a la celebración, validez, interpretación e inejecución de las negociaciones, además de servir como complemento de los derechos positivos nacionales que le son aplicables.

Se debe precisar que hay autores que no consideran a la *Lex Mercatoria* como un cuerpo único y unificado de la ley, sino como un conjunto de leyes que varían de una industria a otra: *Lex Petrolea, Lex constructionis, Lex electrónica* y *Lex marítima*[26]*.*

Al abundar en la integración de la *Lex Mercatoria*, de acuerdo con el danés Ole Lando, es posible sistematizar sus principios[27]:

[22] Feldstein de Cárdenas, Sara Lidia (Dir.). Contratación Electrónica Internacional: Una mirada desde el Derecho Internacional Privado, 2008, 538 pp., accesible en http://www.derecho.uba.ar/investigacion/investigadores/publicaciones/feldstein-de-cardenas-contratacion-electronica-internacional-una-mirada-desde-el-derecho-internacional-privado.pdf, fecha de consulta 4 de diciembre de 2015, p. 12.

[23] Labariega Villanueva, Pedro Alfonso. "La moderna Lex Mercatoria y el comercio internacional" en Revista de Derecho Privado Núm. 26, 1998, Instituto de Investigaciones Jurídicas de la UNAM, p.53 y 54.

[24] Convención de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías, conocida como Viena 1980, así como las siglas en español CNUCCIM y el nombre en inglés como United Nations Convention on the International Sale of Goods (CISG).

[25] El caso más relevante es la codificación de los usos internacionales que regulan el transporte marítimo de mercancías, esto es los Términos Internacionales de Comercio (INCOTERMS).

[26] Doak R. Bishop, International Arbitration of Petroleum Disputes: The Development of a Lex Petrolea, 23 Y.B. com. Arb. 1131 (1998); Michael Douglas, The Lex Mercatoria and the Culture of Transnational Industry, 13 U. Miami Int'l and Comp. L. Rev. 367, 394–95 (2006).

[27] Lando, Ole "The Lex Mercatoria in International Commercial Arbitration", 34 Int'l. and Comp. L.Q., 747-748 (1985).

a. *La interpretación de los convenios con base en los siguientes principios: Pacta sunt servanda, buena fe, cortesía, equidad, verdadera intención de la partes, norma de efecto útil y regla in claris non fin interpretatio.*
b. *La presunción de la competencia profesional,*
c. *La trasparencia sustantiva en un grupo de sociedades y aplicación del efecto relativo de los contratos*
d. *El compromiso para el acreedor de una obligación ejecutada de minimizar el perjuicio*
e. *A falta de acción existirá la presunción de renuncia de las sanciones contractuales.*
f. *La obligación de cooperación entre la partes.*
g. *El ofrecimiento de la diligencia normal, útil u razonable de las partes en el cuidado de sus intereses*
h. *El equilibrio en las prestaciones contractuales.*
i. *La validez de la aceptación tácita de un contrato.*

Finalmente, entre los miembros que participan en la creación de la normatividad del derecho comercial supranacional se encuentran las siguientes organizaciones mundiales:

- Cámara de comercio internacional (CCI) o International Chamber of Commerce (ICC)
- Organización de las Naciones Unidas para el Desarrollo Industrial (ONUDI)
- Comunidad Europea (CE),
- *International Institute for the Unification of Private Law* (UNIDROIT)
- *United Nations Commission on International Trade Law* (UNCITRAL)
- *United Nations Centre on Transnational Corporations* (UNCTC)
- Fondo Europeo de Desarrollo (FED)
- Banco Mundial

Para completar la autonomía de la *Lex Mercatoria* se incluyó la figura del árbitro encargado de resolver las controversias en un medio alternativo del derecho comercial internacional, quienes por antonomasia interpretan y aplican los usos, tradiciones y costumbres comerciales internacionales lejos de los derechos positivos de los miembros de los Estados y más aún, resuelven con base en la determinación de la ley aplicable que eligieron para vincularlos.

Dichos árbitros se encuentran autorizados por el artículo 4 del *Reglamento de Arbitraje de la Cámara de Comercio Internacional* y otros como las *Reglas y usos uniformes para créditos documentario 600 o Uniform Customs and Practice for Documentary Credits* (UCP 600) vigentes en 2007 y son la sexta promulgación desde su primera vez en 1933 en que las creó la Comisión de Técnicas y Prácticas Bancarias de la Cámara de Comercio Internacional (CCI).

Retomando la idea de nuestra metodología, una Nueva *Lex Electo-Mercatoria,* es necesario definir lo que significa la *Lex Informática*[28] —también conocida como *Lex Electrónica*[29]*, Lex*

[28] Reidenberg, Joel R. "Governing Networks and Cyberspace Rule-Makin", Emory L.J.911.928. 1996, p. 929.
[29] Ver Klaus Peter Berger, The Concept of the "Creeping Codification" of Transnational Commercial Law, Center for Transnational Law (CENTRAL), University of Cologne, Germany, accesible en http://www.trans-lex.org/000004#Footnote-Inline-931c95115ba531dd2c3b935c6c262159, consultado el 25 de enero de 2015; y Nils Christian Ipsen. Private Normenordnungen als Transnationales Recht? 2009, Ed. Duncker & Humblot, Berlín, p. 104 y ss.

Networkia, y *Lex Cyberalty—,* cualquiera que sea su nombre, se trata del conjunto de usos, costumbres, principios dirigidos a los actos y negocios jurídicos celebrados a través de medios electrónicos, telemáticos o informáticos, que inició como una informatización flexible de numerosas normas de Internet así como de sus diversas comunidades y se dirige a una materialización comprensiva del control gubernamental tradicional en todo el mundo armonizada con los esfuerzos de unificación de los abogados e usuarios experimentados de Internet.

Por ende, las reflexiones en torno a la nueva Lex Electo-Mercatoria se fundan en la complementación de una *Lex Mercatoria* y *una Lex Informática* flexible y en evolución.

Una vez precisadas las direcciones metodológicas, se está en posibilidad de iniciar el análisis del marco teórico del comercio electrónico.

1.2. Comercio electrónico: concepto, tipos, ventajas y políticas internacionales.

La alteración y versatilidad generada por el comercio electrónico desde hace quince años aparece en un mundo con variaciones contractuales de alta trascendencia. Tales variaciones en la mayoría de los casos, facilitan la celebración, configuración y cumplimiento contractual electrónico en atención a la portátil y ágil infraestructura contractual, cuyo acceso se encuentra al alcance de todos y en todas partes, promueve la diversificación de la elección del usuario así como la competencia y la innovación; y en otros tantos casos, en las situaciones de desconocimiento contractual electrónico, que complican y relegan los requisitos legales que dan fluidez a la negociación contractual, como son: atender a la seguridad de las infraestructuras críticas de información, considerar sus amenazas, asegurar la protección de los datos personales de los consumidores en línea.

De ahí que con la virtualización del contrato mercantil se originen problemas que hasta hace unos años eran inconcebibles o utópicos.

Ante esta revolución de cambios tecnológicos manifestados en la contratación mercantil electrónica, se origina una virtualidad brusca y amenazante, frente a la cual se advierte una contratación con repudio, complejidad y negatividad a adoptar los soportes tecnológicos para suscribir un contrato mercantil.

Por otro lado, lentamente se adoptan reformas y adiones donde cada avance incluye una figura contractual mercantil y valores tecnológicos y legales.

En el contexto precedente se torna necesario definir la figura de comercio electrónico, de tal forma que se pueda lograr el estudio del Derecho del comercio electrónico o *electronic commerce law,* en inglés. Varias definiciones se describen en un sentido amplio (hacer negocios electrónicamente) y otras, en uno sentido restringido (concepción de los principales organismos y foros internacionales que trabajan sobre el tema, como por ejemplo: la OMC, OCDE, EITO, Unión Europea y UNCITRAL).

La concepción amplia del comercio electrónico es extensa porque abarca toda clase de transacciones electrónicas comerciales, incluyendo transferencias de fondos electrónicos, pagos con tarjeta de crédito y las actividades de infraestructura que apoyan a estas transacciones.

A esta definición se le critica por una desmedida amplitud, por no reconocer las nuevas formas de comercio electrónico (las transacciones comerciales realizadas a través de Internet), limitándose a las transacciones electrónicas en sí mismas, sin referirse al espíritu de esta clase de negocios (ciberespacio, mercado virtual, entre otros).

Entre las nociones del comercio electrónico se suelen enunciar las siguientes:

- Es hacer negocios electrónicamente.
- Son transacciones comerciales que se basen en el procesamiento y transmisión de datos digitalizados.
- Es la capacidad para compradores y vendedores de conducir negocios y/o intercambiar informaciones en tiempo real en interacciones humanas.

Mientras que la concepción restringida del comercio electrónico es propuesta por las más importantes organizaciones y foros de negocios internacionales:

La Organización Mundial del Comercio señala:

> *El comercio electrónico comprende aquellos productos que son comprados y pagados en Internet pero son entregados físicamente, y productos que son entregados bajo la forma de información digitalizada sobre Internet.*

La Organización para la Cooperación y el Desarrollo Económicos (OECD) precisa:

> *El comercio electrónico es el proceso de compra, venta o intercambio de bienes, servicios e información a través de las redes de comunicación*[30].

El Observatorio Europeo de Tecnologías de la Información (EITO), propuso en 1997 la siguiente definición:

> *El comercio electrónico es la conducción de asuntos que implican un cambio de valor a través de las redes de telecomunicaciones.*

La Unión Europea (en 1997) señala:

[30] Recomendación del Consejo de la OCDE relativa a los Lineamientos para la protección al consumidor en el contexto del comercio electrónico, 9 December 1999, trad. al español del inglés: OECD Guidelines for Consumer Protection in the Context of Electronic Commerce, Secretaría de Comercio y Fomento Industrial-Procuraduría Federal del Consumidor, México, accesible en www.oecd.org/sti/consumer/34023784.pdf, consulta del 2 de mayo de 2015.

Comercio electrónico es aquel que permite hacer los negocios electrónicamente y está fundado sobre el tratamiento electrónico y la transmisión de datos, comprendiendo textos, sonidos y video. Cubre actividades múltiples y diversas, correspondiendo al comercio de bienes y servicios, la liberación en línea de informaciones numéricas, transferencias electrónicas de fondos, actividades bursátiles electrónicas, transferencia de conocimientos electrónicos, subastas comerciales, concepción y elaboración en ingeniería, mercados en línea, mercados públicos, venta directa a los consumidores y la prestación de servicios postventa. Concierne tanto a los productos (bienes de consumo, equipo médico especializado, por ejemplo) como a los servicios (servicios de información, servicios financieros, entre otros), las actividades tradicionales. (servicios de salud, enseñanza) y actividades nuevas (centros comerciales virtuales, por ejemplo).

Ahora bien, la doctrina ofrece definiciones de autores como Gómez Vietes y Veloso Espiñeira,[31] quienes sostienen que el comercio electrónico es *la automatización mediante las tecnologías de información de los intercambios de información asociados a la compra de bienes y servicios y el pago de los mismo*s.

Otros[32] lo definen como el conjunto de actividades mercantiles que incluyen tanto actividades comerciales como acciones de mercadeo, de bienes tangibles o intangibles, siempre que éstas se produzcan por vía electrónica, sobre todo en la redes de comunicación, como es Internet.

En suma, para ellos el comercio electrónico se puede entender como cualquier forma de transacción o intercambio de información comercial (compraventas de bienes y prestación de servicios realizados entre empresarios, o bien entre empresarios y consumidores) basada en la transmisión de datos en Internet.

Nuestra definición de comercio electrónico se genera a partir de la visión *iusprivatista,* particularmente mercantil, en este sentido, el *comercio electrónico* es cualquier actividad en la que empresarios y/o consumidores ejercen una relación que operan por medios de transmisión electrónicas. Esta definición engloba distintas formas de negociación electrónica desde luego el de bienes y servicios, el suministro en línea de contenidos digitales, las transferencias electrónicas de fondos, la compra-venta de acciones, las subastas comerciales, los diseños y proyectos conjuntos, la prestación de servicios en línea, la contratación pública, la comercialización directa al consumidor, los contratos de transporte de mercaderías marítimas y aéreas[33], y los servicios de preventa y posventa[34].

---

[31] Gómez Vietes, Álvaro; Veloso Espiñeira, Manuel. Economía digital y comercio electrónico. Santiago de Compostela: EDITA Escuela de Negocios Caixa Nova-Tórculo Ediciones, S.L., p. 77.

[32] Cfr. Vasquez Callao, Enrique; Berrocal Comenarejo, Julio. Comercio electrónico. Material para Análisis. Madrid: Centro de publicaciones, Técnica, Ministerio de Fomento, 2000, p.1; GARCÍA MÁS, Francisco Javier. Comercio y firma electrónicos. Análisis Sociedad de la información. 2. ª ed. Valladolid: Edit. Lex Nova, 2004, p. 31; y GUISADO MORENO, Ángela. Formación y perfección del contrato en Internet. Madrid: Marcial Pons, Ediciones jurídicas y Sociales, S. A., 2004, p. 59.

[33] Los denominados conocimientos de embarque naviero "Airwail" y el marítimo "Bill of lading".

[34] Sobre estos ejemplos véase la Comunicación de la Comisión de las Comunidades Europeas al Consejo, al Parlamento europeo, al Comité económico social y al Comité de las regiones sobre Iniciativa europea de comercio electrónico, COM (97) 157 final, Bruselas, 16 abril 1997, págs.. 7-10, accesible en: http://eur-lex.europa.eu/procedure/ES/20320, consulta del 1 de noviembre de 2014.

Por ende, el comercio electrónico es una modalidad de comercio en la que la mediación entre la oferta así como la demanda y el perfeccionamiento de las transacciones entre ellas se realiza a través de medios digitales de comunicación, ya sea por redes abiertas o cerradas, en un mercado virtual que no posee límites geográficos ni temporales y que no tiene una ubicación determinada, porque se encuentra en el ciberespacio.

Finalmente, con las definición del comercio electrónico citadas se está en posibilidad de señalar cuáles son los mayores retos del comercio electrónico[35]:

a) *Ajustarse a los nuevos modelos de negocio.*
b) *Encontrar y capacitar a los gerentes que deberán guiar a las empresas sobre comercio electrónico los próximos años.*
c) *Detectar y sacar ventaja del entorno para integrarse en una economía global.*
d) *Fomentar la cultura de la innovación.*

1.2.1. Según cómo se realiza el contrato

Nuestra definición de comercio electrónico descrita al final del punto 1.2. abarca el *comercio electrónico directo* e *indirecto;* lo explicamos.

El *comercio electrónico directo* considera el proceso de compra-venta (oferta o policitación y aceptación) que se lleva a cabo mediante la utilización de equipos electrónicos que utilizan Internet, para la compra de un producto cualquiera, en donde el adquirente previamente observa la oferta presentada en una página web y la acepta cubriendo el precio requerido en la oferta, de tal manera que la operación de compraventa es realizada desde la página web del ofertante del producto por medio de la computadora del adquirente.[36]

Esta modalidad directa va del pedido, el pago y la entrega en línea de bienes y servicios inmateriales en mercados electrónicos mundiales, como revistas electrónicas (servicios de información especializados: bases de datos de artículos y libros digitales), software, servicios recreativos (boletos de avión, reservas de hoteles, entradas para espectáculos), música y servicios financieros.

El *comercio electrónico indirecto* considera que tanto la oferta como la solicitud de compra se realizan utilizando equipos electrónicos en línea, pero la entrega del bien ofertado así como el pago se ejecutan físicamente *off line.* Se trata de la venta a distancia en donde la oferta y la aceptación son realizadas por cualquier medio de comunicación a distancia, mediante un sistema de comunicación instrumentado por el vendedor, que para ello utiliza la página web, en la cual se presentan sus productos o servicios ofertando un precio determinado, de modo que el consumidor al aceptar la oferta elige el que necesita pero se caracteriza porque el pago

[35] Bastidas, Ma. Teresa; Novoa, Jorge y Pérez, Alfonso (coord.). La firma y la factura electrónicas: Entorno jurídico, fiscal e informático. Ed. Instituto Mexicano de Contadores Públicos (IMCP), 2004, México D.F., p. 22.
[36] Castrillón y Luna, Víctor M. Contratos mercantiles, 2011,México, Porrúa, p. 45.

del precio y la entrega del producto se llevan a cabo fuera de la página web, en un lugar físico, esto es, *off line*[37].

Esta modalidad indirecta inicia con el pedido electrónico de bienes que se entregan a través del correo o mensajería (como libros, equipo de cómputo) y depende de factores externos como la eficiencia del sistema de transporte.

1.2.2. Según los entes intervinientes

Generalmente se reconoce la existencia de cuatro modalidades de comercio electrónico muy bien diferenciadas según sus participantes[38], aunque en los últimos años se ha generalizado la tendencia de utilizar nuevos acrónimos combinados con otros para definir nuevos modelos de negocio dado la versatilidad del mercado electrónico, estos son:

a) B2B es la abreviatura de la expresión *Business to Business*: de empresa a empresa.
b) B2C es la abreviatura de *Business to Consumer*: de empresa a consumidor final.
c) B2G es la abreviatura de *Business to Government*: de Empresa a Gobierno. Consiste en optimizar los procesos de negociación entre empresas y el gobierno a través del uso de Internet.
d) C2G es la abreviatura de *Consumer to Government*: de Consumidor a Gobierno. Es la relación comercial que se establece entre una empresa y sus propios empleados.
e) C2C es la abreviatura de *Consumer to Consumer*: de Consumidor a Consumidor. Consiste en las transacciones comerciales privadas entre uno o varios consumidores que pueden tener lugar mediante el intercambio de correos electrónicos, Peer to Peer o en entornos cerrados de negocios como eBay.

1.2.3. Ventajas e inconvenientes del comercio electrónico.

Los beneficios del comercio electrónico desde el punto de vista del empresario o comerciante son:

- Presencia en Internet y, con ello, tener menores costos de entrada al mercado,
- Acceso mundial[39],
- Interactividad (sin costo telefónico y visitas al cliente),
- Difusión multimedia (que permite la integración de diferentes recursos),
- Diversificación (los productos digitalizados se pueden presentar de diversas formas para crear líneas secundarias de producto),
- Menores costos de salida (la salida del mercado es poco onerosa, como lo es la entrada),

[37] Ibídem.
[38] Rodríguez de las Heras Ballell, T. El régimen jurídico de mercados electrónicos cerrados (e-Marketplaces. Marcial Pons, 2006., p. 40 y ss.
[39] Es de destacar el ámbito mundial para las Pequeña y Mediana Empresa (PYMES) que es particularmente interesante.

- Garantía de acceso directo al cliente (contacto directo entre productores y consumidores, sin que sean necesarios los distribuidores o las redes de ventas),
- Menores costos de distribución (la separación entre el contenido y los medios de almacenamiento posibilita la eliminación de varias etapas en la cadena de distribución tradicional),
- Circuitos indirectos de ventas (los minoristas pueden utilizar la red para indicar los puntos de venta tradicionales al por mayor o al detalle),
- Mercados presegmentados (se fomenta la autosegmentación y el autoposicionamiento), Ahorro en los costos de publicidad (la simple presencia es un acto publicitario) y
- Obtención de ingresos suplementarios por la venta de espacios publicitarios.

En tanto que los beneficios del comercio electrónico desde el punto de vista del consumidor son:

- Incitación a abandonar la pasividad (el consumidor hace oír su voz y se informa más a fondo),
- Acceso significativo a la cantidad de información (los consumidores pueden recibir más información sobre el producto que quieren comprar, ya que el principal factor decisorio de un usuario de Internet es contar con la mayor información sobre un determinado producto),
- Ampliación de las opciones (mayores posibilidades de elección),
- Transparencia (se facilita el intercambio de información entre los propios consumidores), Control de precios (hace más difícil engañar al consumidor),
- Comodidad (las compras electrónicas resultan más cómodas para los consumidores), Sensibilidad a las reacciones del consumidor (los vendedores estarán atentos a las reacciones de los consumidores) y
- Carácter impersonal de las operaciones (algunos consumidores aprecian el anonimato que proporciona el comercio electrónico).

No sería acertado continuar sin mencionar varios inconvenientes e inhibidores del comercio electrónico, algunos de los cuales sí fueron subsanados al elaborarse posterior regulación sobre este tema.

Entre los inconvenientes del *e-commerce* están:

- La facilidad de uso y el acceso a esta tecnología (se requiere una infraestructura de comunicación cuyo precio es bajo, aun cuando dependa de las tarifas vigentes en cada país) y
- Incertidumbre con respecto al grado de cambio tecnológico.

Los inhibidores del comercio electrónico son:

- Mayores requerimientos de seguridad (un desarrollo adecuado del comercio electrónico, requiere que exista una mayor seguridad en los medios de pago electrónicos)
- El riesgo[40] de suplantación respecto al emisor, autor y fuente del mensaje de datos (MD) o que el MD sea alterado de forma accidental o maliciosa, durante la transmisión,
- Que el emisor del MD niegue haber transmitido el MD
- Que el destinatario niegue haberlo recibido,
- Que el contenido del mensaje sea leído por una persona no autorizada; y
- Que el requisito de fiabilidad ante la falta de calidad en las conexiones por Internet,
- El factor psicológico consiste en que los usuarios están reacios al cambio, necesitan tiempo para adaptarse a los nuevos hábitos; y pueden frustrarse cuando no le es fácil buscar un producto.

1.2.4. Políticas internacionales para el comercio electrónico.

1.2.4.1. De la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI/UNCITRAL)

El 17 de diciembre de 1966 la Asamblea General de las Naciones Unidas mediante la resolución 2205 (XXI) erige la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI, por sus siglas en español; UNCITRAL, por las siglas en inglés de *United Nations Commission on International Trade Law*) a fin de unificar y homologar criterios en materia de comercio internacional.

En su primer período de sesiones, celebrado en 1968, la Comisión adoptó nueve materias como base de su programa de trabajo, a saber:

I. La compraventa internacional de mercaderías;
II. El arbitraje comercial internacional;
III. Los transportes;
IV. Los seguros;
V. Los pagos internacionales;
VI. La propiedad intelectual;
VII. La eliminación de la discriminación en las leyes que afectan al comercio internacional;
VIII. El mandato o la representación; y
IX. La legalización de documentos.

La Comisión no ha dado curso todas estas materias, como por ejemplo, los seguros, la eliminación de la discriminación en las leyes que afectan al comercio internacional, así como el mandato o la representación y la legalización de documentos.

[40] En el aspecto técnico de los riesgos a los que se someten las comunicaciones de datos en sistemas de redes abiertos, cfr. Recomendación UIT-X.800 (1991), pág. 32-35, Anexo A: Información básica sobre seguridad en la interconexión de sistemas abiertos (ISA).

Inicialmente se asignó prioridad a los temas de la compraventa internacional de mercancías, el arbitraje comercial internacional y los pagos internacionales. Posteriormente se incorporaron al programa de trabajo otros temas, tales como los contratos de financiación del comercio, los transportes, el comercio electrónico, la contratación pública, la conciliación comercial internacional, la insolvencia, las garantías reales, la solución de controversias por vía informática y las microfinanzas[41], por lo que actualmente la clasificación es de ocho materias:

I. Compraventa internacional de mercaderías
II. Arbitraje y conciliación comercial internacionales
III. Transporte internacional de mercaderías
IV. Garantías reales
V. Insolvencia
VI. Pagos internacionales
VII. Comercio electrónico
VIII. Contratación pública y desarrollo de la infraestructura

Asimismo, la CNUDMI/UNCITRAL da cumplimiento a su mandato mediante[42]:

> *a) La coordinación de la labor de las organizaciones que realizan actividades en este campo y el estímulo de la colaboración entre ellas;*
> *b) El fomento de una participación más amplia en los convenios y las convenciones internacionales existentes y de una mayor aceptación de las leyes modelo y las leyes uniformes ya establecidas;*
> *c) La preparación o el fomento de la aprobación de nuevos convenios y convenciones internacionales**, leyes modelo** y leyes uniformes, así como el fomento de la codificación y de una aceptación más amplia de las condiciones, disposiciones, costumbres y prácticas comerciales internacionales, colaborando, en su caso, con las organizaciones que actúen en esta esfera;*
> *d) El fomento de métodos y procedimientos para asegurar la interpretación y aplicación uniformes de los convenios y las convenciones internacionales y de las leyes uniformes en el campo del derecho mercantil internacional;*
> *e) La reunión y difusión de información sobre las legislaciones nacionales y sobre la evolución jurídica moderna, incluida la jurisprudencia, en el .ámbito del derecho mercantil internacional;*
> *f) El establecimiento y mantenimiento de una estrecha colaboración con la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo;*
> *g) El mantenimiento de un enlace con otros órganos de las Naciones Unidas y con los organismos especializados que se ocupan del comercio internacional; y*
> *h) La adopción de cualquier otra medida que pudiera considerar útil para desempeñar sus funciones.*
>
> **(Énfasis añadido)**

El inciso "c)" habla de la preparación de leyes modelo, entendiéndose por estas *un texto legislativo que se recomienda a los Estados para su adopción e incorporación a su derecho interno.*

[41] Documentos Oficiales de la Asamblea General, vigésimo tercer período de sesiones, Suplemento núm. 16 (A/72/16) (1968), párrafos 40 y 48.
[42] Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, Guía de la CNUDMI: Datos básicos y funciones de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, Naciones Unidas, Viena, 2013, p. 2.

Se trata de *un medio adecuado para la modernización y armonización de las leyes nacionales si se prevé que los Estados desearán o necesitarán introducir modificaciones en el texto del modelo para ajustarlo a las necesidades de cada país, que varían en función de cada ordenamiento jurídico, o cuando no sea necesaria o conveniente una estricta uniformidad*[43].

Una de las características más relevantes de la expedición de una Ley Modelo es su flexibilidad para ser fácilmente negociable a diferencia de un texto en el que figuren obligaciones que no pueden modificarse, y por ello pueden fomentar una mayor aceptación en el caso de una ley modelo, que de una convención que regule la misma temática. No obstante, frente a esa flexibilidad para aumentar las posibilidades de alcanzar un grado satisfactorio de unificación y brindar certeza respecto del grado de unificación, se alienta a los Estados a que realicen la menor cantidad de modificaciones posible al incorporar una ley modelo a su ordenamiento jurídico interno.

Hasta hoy la CNUDMI/UNCITRAL ha expedido siete Leyes Modelo, a saber:

1. Ley Modelo de la CNUDMI sobre Arbitraje Comercial Internacional (1985)
2. Ley Modelo de la CNUDMI sobre Transferencias Internacionales de Crédito (1992)
3. Ley Modelo de la CNUDMI sobre Contratación Pública de Bienes, Obras y Servicios (1994)
4. Ley Modelo de la CNUDMI sobre Comercio Electrónico (1996)
5. Ley Modelo de la CNUDMI sobre la Insolvencia Transfronteriza (1997)
6. Ley Modelo de la CNUDMI sobre las Firmas Electrónicas (2001)
7. Ley Modelo de la CNUDMI sobre Conciliación Comercial Internacional (2002)

Las siguientes, aunque no son Leyes Modelo, son dos Convenciones también emitidas por el mismo órgano, la CNUDMI/UNCITRAL, y retroalimenta a las anteriores:

- **Convención** de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías (conocida como Convención de Viena de 1980 o en inglés: *United Nations Convention on the International Sale of Goods: CISG*)
- **Convención** Internacional sobre Utilización de las comunicaciones electrónicas en los Contratos Internacionales (Nueva York, 2005).

Además, si bien no se trata de Leyes Modelo ni de Convenciones, existen otros dos documentos de relevancia elaborados también por la CNUDMI/UNCITRAL que se relacionan constantemente con ellas:

- Recomendaciones dirigidas a los gobiernos y a las organizaciones internacionales acerca del valor jurídico de los registros de computadora (1985)

[43] Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, Guía de la CNUDMI: Datos básicos y funciones de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, Naciones Unidas, Viena, 2013, p. 15.

- Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónicas (2007)

Las últimas Leyes Modelo que ha elaborado la CNUDMI/UNCITRAL se han complementado con varias guías para su incorporación al derecho interno, en las que figura información de antecedentes y otras explicaciones para orientar a los gobiernos y legisladores en la utilización del texto, esto es, excepto las leyes citadas en los incisos "1" y "2", todas las leyes van acompañadas de guías oficiales para su incorporación al derecho interno que son más extensas. La Comisión examinó estas guías y en general las adoptó de forma conjunta con el texto de cada una de las leyes modelo.

Para ilustrar las Leyes Modelo que impactan el comercio electrónico, se debe precisar que una vez que las negociaciones comerciales por medios electrónicos desplegaron un crecimiento exponencial en los países, en 1996 se elaboró una Guía Internacional para Regular las Operaciones Comerciales Electrónicas y con ello se expidió la Ley Modelo sobre Comercio Electrónico, cuyo objeto es auxiliar y estimular a los países a legislar en la implementación legal interna de estas transacciones comerciales electrónicas. Posteriormente, en 2001, muy relacionada con la anterior ley, se expidió la Ley Modelo de la CNUDMI sobre las Firmas Electrónicas (LMFE).

La CNUDMI/UNCITRAL en el año 1985 ya había adoptado una *Recomendación sobre el Valor Jurídico de los Registros Computarizados* así como la *Recomendación sobre el Valor Jurídico de la Documentación Informática* de 1985.

Posteriormente, la Comisión expidió la Ley Modelo de la CNUDMI sobre Comercio Electrónico (LMCE) de 1996 que considera un número creciente de transacciones comerciales internacionales que se realizan por medio del intercambio electrónico de datos y por otros medios de comunicación habitualmente conocidos como *comercio electrónico*, en los que se usan métodos de comunicación y almacenamiento de información sustitutivos de los que utilizan el papel.

Los textos legislativos fundados en la Ley Modelo sobre Comercio Electrónico han sido adoptados en África del Sud (2002), Australia (1999), China (2004), Colombia (1999), Ecuador (2002), Francia (2000), India (2000), Irlanda (2000), Jordania (2001), México (2000), Nueva Zelanda (2002), Pakistán (2002), Panamá (2001), Filipinas (2000), República de Corea (1999), República Dominicana (2002), Singapur (1998), Eslovenia (2000), Sri Lanka (2006), Tailandia (2002), Venezuela (2001) y Vietnam (2005), así como también se han inspirado otras como la en las Ley Modelo en Estados Unidos *(Uniform Electronic Transactions Act* adoptada en 1999 por la Conferencia nacional de comisiones de juristas sobre la uniformización de las legislaciones de los Estados), en Canadá: *Loi uniforme sur le commerce électronique,* adoptada en 1999 por la *Conférence sur l'uniformisation des lois du Canada* y en Quebec (2001).

Años después, la CNUDMI/UNCITRAL expidió la Ley Modelo sobre Firmas Electrónicas de 2001, la cual tiene por finalidad dotar de mayor certeza jurídica al empleo de la firma electrónica.

Basándose en el principio flexible que se enuncia en el artículo 7 de la Ley Modelo sobre Comercio Electrónico se presume que toda firma electrónica que cumpla con ciertas pautas de fiabilidad técnica será equiparable a la firma manuscrita. La Ley Modelo adopta un criterio de neutralidad tecnológica para no favorecer el recurso a ningún producto técnico en particular. China (2004), México (2003), Tailandia (2001) y Vietnam (2005) han promulgado legislación basada en la LMFE.

Finalmente, el 23 de noviembre del 2005 la Asamblea General de las Naciones Unidas adoptó la Convención sobre Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales de 2005, y solicitó al Secretario General de la ONU declararla abierta para su firma. Hasta el día de hoy la han signado: República Central Africana, China, Líbano, Madagascar, Paraguay, Federación Rusa, Senegal, Sierra Leona, Singapur y Sri Lanka.

La Convención tiene la finalidad de fomentar la seguridad jurídica y la previsibilidad comercial cuando se utilicen comunicaciones electrónicas en la negociación de contratos internacionales. Además, regula la determinación de la ubicación de la parte en un entorno electrónico; el momento y lugar de envío y de recepción de las comunicaciones electrónicas; la utilización de sistemas de mensajes automatizados para la formación de contratos; y los criterios a que debe recurrirse para establecer la equivalencia funcional entre las comunicaciones electrónicas y los documentos sobre papel, incluidos los documentos sobre papel "originales", así como entre los métodos de autenticación electrónica y las firmas manuscritas.

Cuenta con veinticinco artículos, reunidos en cuatro capítulos:

- *Capítulo I. Esfera de aplicación*
- *Capítulo II. Disposiciones generales*
- *Capítulo III. Utilización de las comunicaciones electrónicas en los contratos internacionales*
- *Capítulo IV. Disposiciones finales.*

1.2.4.2. De la Organización para la Cooperación y el Desarrollo Económicos (OCDE).

La OCDE se fundó en 1961, es una institución que agrupa a 34 países miembros para promover políticas que mejoren el bienestar económico y social de las personas alrededor del mundo con un enfoque económico (analiza el desarrollo económico y los factores de tipo estructural que influyen en él).

Su trabajo se ha extendiendo a otras áreas por lo que hoy existen 14 direcciones, cada una tiene un código de 3 o 4 letras (indicado entre paréntesis) con el que se identifica su trabajo:

I. *Administración pública y desarrollo territorial (GOV)*
II. *Agricultura (AGR)*
III. *Asuntos financieros y empresariales (DAF)*
IV. *Asuntos fiscales (CTPA)*

V. *Ciencia, tecnología e industria (STI)*
VI. ***Comercio** (ECH)*
VII. *Cooperación con países no miembros (CCNM)*
VIII. *Desarrollo (DCD)*
IX. *Economía (ECO)*
X. *Educación (EDU)*
XI. *Empleo y cohesión social (ELS)*
XII. *Energía (AIE) (AEN)*
XIII. *Estadísticas (STD)*
XIV. *Iniciativa empresarial (CFE)*
XV. *Medio ambiente (ENV)*

Además, la OCDE ofrece un foro donde los gobiernos pueden trabajar conjuntamente para compartir experiencias y buscar soluciones a los problemas comunes en Comités (integrados por representantes de las administraciones nacionales de los países miembros), entender que es lo que conduce al cambio económico, social y ambiental, medir la productividad y los flujos globales del comercio e inversión, analizar y comparar datos para realizar pronósticos de tendencias y fijar estándares internacionales dentro de un rango de temas de políticas públicas.

Particularmente, el Grupo de Trabajo en Seguridad y Privacidad de la Economía Digital de la OECD, en relación con la criptografía, elaboró la *Recommendation of the council concerning guidelines for cryptography Policy (Lineamientos para Política de Criptografía),* que señala varios ocho principios a implementarse en los gobiernos, los cuales son[44]:

1. Confianza en los métodos criptográficos
2. Elección de los métodos criptográficos
3. Desarrollo de métodos criptográficos orientado por el mercado
4. Estándares para los métodos criptográficos.
5. Protección de la privacidad y datos psonales
6. Acceso legítimo
7. Responsabilidad
8. Cooperación internacional en estos asuntos.

1.2.4.3. De otros foros y organismos internacionales.

Entre dichos foros y organismos internacionales a guisa de ejemplo se mencionan los siguientes:

1. El Instituto Internacional para la Unificación del Derecho Privado o Institute for the Unification of Private Law (UNIDROIT).
2. La Cámara de Comercio Internacional o International Chamber of Commerce (CCI/ICC).

[44] OECD, Recommendation of the council concerning guidelines for cryptography Policy, de fecha 27 March 1997, C(97)62/FINAL, accesible en: http://acts.oecd.org/Instruments/ShowInstrumentView.aspx?InstrumentID=115&InstrumentPID=111&Lang=en&Book=, OECD. consultado en 15 Junio de 2015.

3. La Organización Mundial de la Propiedad Intelectual (WIPO)
4. La Conferencia de La Haya sobre Derecho Internacional Privado
5. La VI Conferencia Interamericana Especializada sobre Derecho Internacional Privado (CIDIP VI - 2002)
6. La Organización de los Estado Americanos.
7. Foro de Cooperación Económica Asia-Pacífico o Asia-Pacific Economic Cooperation (APEC)
8. International Organization for Standarization/ International Electrotechnical Commission (ISOC y IEC).

1. El Instituto Internacional para la Unificación del Derecho Privado o *Institute for the Unification of Private Law (UNIDROIT*).

Hasta ahora, ha elaborado tres versiones de los *Principios sobre los Contratos Comerciales Internacionales*: la versión de 1994, de 2004 y de 2010. Tales principios establecen reglas generales aplicables a los contratos mercantiles internacionales que debieran implementarse cuando las partes hayan acordado que su contrato se rija por ellos, o bien también pueden aplicarse cuando las partes hayan acordado que su contrato se rija por principios generales del derecho, la *Lex Mercatoria* y/o expresiones semejantes.

Se trata de principios aplicables cuando las partes no han escogido el derecho aplicable al contrato a fin de que estos lineamientos puedan ser utilizados para interpretar o complementar instrumentos internacionales de derecho uniforme e incluso complementar el derecho nacional.

2. La Cámara de Comercio Internacional o International Chamber of Commerce (CCI/ICC).
Tiene en marcha el *Electronic Commerce Project* (ECP), cuyo objetivo es definir buenas prácticas comerciales que ayuden a crear confianza en las transacciones comerciales electrónicas.

Cuenta con tres grupos de trabajo:

1) El de prácticas de comercio electrónico: Elaborar un marco regulador para los pagos del comercio electrónico,
2) El de seguridad de la información: Ha elaborado un conjunto de directrices, tituladas *General Usage in International Digitally Ensured Commerce* (GUIDEC), para aumentar la capacidad de los comerciantes internacionales de ejecutar transacciones seguras y
3) El de términos electrónicos: Que está elaborando un nuevo servicio de la CCI, que ofrecerá un depósito central para los términos jurídicos aplicables a las transacciones electrónicas.

3. La Organización Mundial de la Propiedad Intelectual (WIPO), mantiene un servidor web sobre comercio electrónico e impulsa los convenios internacionales en esta materia.

4. La Conferencia de La Haya sobre Derecho Internacional Privado ha organizado diversas conferencias y mesas redondas desde fines de la década del noventa sobre comercio

electrónico y derecho internacional privado a fin de analizar los múltiples aspectos que aquél presenta y su incidencia en las normas relacionadas con el comercio electrónico.

5. La VI Conferencia Interamericana Especializada sobre Derecho Internacional Privado (CIDIP VI - 2002) la cual adoptó una resolución a través de la cual se recomienda a los Estados Miembros de la OEA adoptar la Ley Modelo de UNCITRAL sobre Comercio Electrónico y la de Firmas Electrónicas. Asimismo, dicha conferencia aprobó la *Ley Modelo Interamericana sobre Garantías Mobiliarias* que contempla el uso de documentos y firmas electrónicas.

La CIDIP VII elaboró una lista provisional de cuatro temas:

1. Protección al consumidor,
2. Comercio electrónico,
3. Jurisdicción internacional y
4. Responsabilidad extracontractual.

El tema del comercio electrónico fue propuesto por las delegaciones de Brasil, México, Uruguay, Estados Unidos, Chile y Perú. En este contexto, se apoyó la elaboración de dos posibles instrumentos interamericanos relativos a:

a) La protección al consumidor: ley aplicable, jurisdicción y restitución monetaria (Convenciones y Leyes Modelo); y
b) Las garantías mobiliarias: registros electrónicos para implementación de la Ley Modelo Interamericana sobre Garantías Mobiliarias.

Mientras tanto quedaron pendientes los temas de comercio electrónico y responsabilidad civil.

6. Organizacíon de los Estados Americanos (OEA)

El 3 de junio de 2014 la OEA y Symantec conjuntamente presentaron el informe sobre seguridad cibernética en América Latina y el Caribe, en el marco de la XLIV Asamblea General del organismo, el informe *Tendencias en la seguridad cibernética en América Latina y el Caribe (Latin American and Caribbean Cybersecurity Trends)*[45] ilustra y analiza los últimos acontecimientos en ciberseguridad y cibercrimen en la región.

El informe incluye contribuciones de Microsoft, la Comunidad de Policías de América (AMERIPOL) y otras organizaciones como el Internet Corporation for Assigned Names and Numbers (ICANN), the Latin American and Caribbean Internet Addresses Registry (LACNIC), and the Anti-Phishing Working Group (APWG), así como la sociedad civil y otros socios del sector privado.

[45] OEA y SYMANTEC. Tendencias en la seguridad cibernética en América Latina y el Caribe (Latin American and Caribbean Cybersecurity Trends), Washington, D.C., accesible en: https://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf, consultado el 1 de diciembre de 2014, 96 p.

En él se explora diferentes aspectos relacionados con la seguridad cibernética incluyendo el incremento exponencial de las fugas de datos y tendencias como:

- Crecimiento del Ransomware[46] y Cryptolocker[47]
- Malware en cajeros automáticos
- Estafas en redes sociales
- Vulnerabilidades y riesgos en cómputo móvil
- Código malicioso (malware)
- Spam
- Spear phishing[48]

A diferencia de otros reportes de amenazas sobre vulnerabilidades cibernéticas que existen en el mercado, este informe es único ya que está enfocado en la región e incluye las perspectivas de los gobiernos de los Estados Miembros de la OEA así como información detallada sobre el panorama de amenazas cibernéticas actual obtenida de la Red Global de Inteligencia de Symantec.

7. Foro de Cooperación Económica Asia-Pacífico o Asia-Pacific Economic Cooperation (APEC)

El Foro de Cooperación Económica Asia-Pacífico (APEC) es un sitio de reunión multilateral que se integró en 1989 sin un tratado formal; por ello, sus decisiones no son vinculantes. Tiene una Secretaría General, con sede en Singapur, quien coordina el apoyo técnico y de consultoría. Cada año uno de los países miembros es huésped del foro anual.

[46] Un ransomware (del inglés ransom rescate y ware, software) es un tipo de programa informático malintencionado que restringe el acceso a determinadas partes o archivos del sistema infectado, y pide un rescate a cambio de quitar esta restricción.
[47] CryptoLocker es un malware tipo troyano dirigido a computadoras con el sistema operativo Windows que se extendió a finales de 2013. El CryptoLocker se distribuye de varias formas, una de ellas como archivo adjunto de un correo electrónico. Una vez activado, el malware cifra ciertos tipos de archivos almacenados en discos locales y en unidades de red usando criptografía de clave pública RSA, guardándose la clave privada en los servidores del malware. Realizado el cifrado, muestra un mensaje en pantalla, en el cual ofrece descifrar los archivos afectados, si se realiza un pago antes de una fecha límite (a través de Bitcoins o con vales prepagos), y menciona que la clave privada será destruida del servidor, y que será imposible recuperarla si la fecha límite expira. Si esto ocurre, el malware ofrece la posibilidad de descifrar los datos a través de un servicio en línea provisto por los operadores del malware, con un precio en Bitcoin mucho más alto. A pesar que el malware es fácilmente eliminado, los archivos permanecen cifrados, cuya clave privada se considera casi imposible de descifrar.
[48] Spear phishing es una estafa focalizada por correo electrónico cuyo único propósito es obtener acceso no autorizado a datos confidenciales. A diferencia de las estafas por phishing, que pueden lanzar ataques amplios y dispersos, el spear phishing se centra en un grupo u organización específicos. La intención es robar propiedad intelectual, datos financieros, secretos comerciales o militares y otros datos confidenciales. Por lo general, el spear phisher sabe algunas cosas sobre ti: tu nombre, tu dirección de correo electrónico, y utiliza esta información para personalizar tu ataque (el correo ya no dice "Estimado señor" sino "Hola, Pedro"). El correo puede hacer referencia a un amigo mutuo, o a algún tipo de actividad online reciente que hayas llevado a cabo. Al dar la apariencia de provenir de alguien que conoces o de una entidad confiable, es más probable que bajes la guardia y entregues la información que los estafadores están buscando.
La forma en que funciona es la siguiente: llega un correo electrónico, aparentemente de una fuente de confianza, pero en vez de eso, lleva al inadvertido destinatario a un sitio web falso lleno de malware.

Su objetivo es aprovechar la creciente interdependencia de las economías de la región a fin de crear una mayor prosperidad para los habitantes de la región, fomentando un crecimiento económico inclusivo, equitativo, sustentable e innovador.

El peso económico de APEC es muy significativo: sus 21 miembros representan 54% del PIB mundial y 44 por ciento del comercio mundial.

El foro se sostiene en tres pilares:

1. Liberalización del comercio y la inversión,
2. Facilitación para hacer negocios, y
3. Cooperación técnica

Además, la APEC promueve la transparencia y el establecimiento de mejores prácticas en los procedimientos y reglamentos relacionados con el flujo de bienes, servicios y capital en Asia-Pacífico, la región más dinámica de años recientes.[49].

Un ejemplo de logros derivados de tal cooperación se encuetran:

a) La adopción del "Marco de Privacidad de APEC"[50] en 2007, a fin de promover el comercio electrónico, reconociendo la importancia de proteger la información, sin crear obstáculos.
   En dicho documento se establece que los flujos de información son vitales para llevar a cabo negocios en una economía global, y el Marco de Privacidad de APEC promueve un acercamiento flexible a la protección de la privacidad de la información en las Economías miembros, evitando la creación de barreras innecesarias para los flujos de información.
b) El lanzamiento en 2007 de los "Sellos de Confianza" (Trustmark) por parte de AMIPCI con el apoyo de la SE y PROFECO. En 2012 existían más de 300 sitios de internet que utilizan este sello, al comprobar que cumplen con los principios de privacidad de APEC: prevenir daños, buen uso de información personal, salvaguardas de seguridad, etc., los mas significativos portadores son: Bancomer, Palacio de Hierro, Cinépolis, hasta PyMES, en sectores como comercio, turismo, finanzas, etc.

8. International Organization for Standarization/ International Electrotechnical Commission (ISOC y IEC).

ISO es una organización internacional independiente, no gubernamental, cuya Secretaría Central de ISO tiene su sede en Ginebra, Suiza y cuenta con una membresía de 161 organismos nacionales de normalización.

[49] Secretaría de Economía, Documento informativo relativo a APEC, Secretaría de Economía, México, 2012, 4 p., accesible en: http://www.economia.gob.mx/files/Documento_Informativo_APEC.pdf, consultado el 1 de enero de 2015.
[50] Secretariado de APEC, Marco de Privacidad del Foro de Cooperación Económica Asia-Pacífico, 2005, Singapur, traducción al español por la Secretaría de Economía, 39 p., accesible en https://www.sellosdeconfianza.org.mx/docs/marco_de_privacidad_APEC.pdf, consultado el 1 de febrero de 2015.

A través de sus miembros reúne a expertos para compartir conocimientos y desarrollar estrategias basadas en el consenso, el mercado Normas Internacionales voluntarias y relevantes que apoyan la innovación y aportar soluciones a los retos globales.

Tales Normas Internacionales hacen funcionar las cosas, pues dan especificaciones a nivel mundial de productos, servicios y sistemas, para garantizar la calidad, seguridad y eficiencia. Son fundamentales para facilitar el comercio internacional.

Mientras que la *International Electrotechnical Commission (IEC)* o Comisión Electrotécnica Internacional (CIE) quien prepara y publica normas internacionales para todas las tecnologías eléctricas, electrónicas y relacionadas. Estos son conocidos colectivamente como "electrotecnia". Todas sus normas internacionales se basan en el consenso y representan las necesidades de las partes interesadas clave de todas las naciones que participan en el trabajo de IEC. Cada país miembro, tiene un voto y una voz en la toma de decisiones.

Ambas organizaciones se reúnen en Comités a fin de realizar trabajos técnicos como normas para firmas electrónicas, criptografía, autenticación, certificación, y criterios para la aceptación mutua de las autoridades de certificación, terceros confiables (TTP) einfraestructura de su gestión y uso a nivel internacional.

1.2.5. Estado actual del comercio electrónico en el Mundo y en México.

1.2.5.1. Tendencias mundiales del comercio electrónico

Las tendencias y tecnologías de comercio electrónico están transformando la forma en que las empresas interactúan con los mercados, incluyendo prospectos, clientes y socios. Actualmente el interés en el comercio electrónico se ha expandido a industrias no minoristas. Las nuevas industrias invierten en capacidades del comercio electrónico tales como la manufactura o fabricación de diferentes tipos: discreta[51], de distribución, de telecomunicación y de publicación.

Las organizaciones B2C generan innovación pero en su mayoría recurren a las comunidades de los consumidores a través de software de redes sociales (como Facebook o Twitter) como una manera de relacionarse con clientes y mejorar la experiencia global de compras en línea. Por otra parte, las organizaciones de B2C capitalizan los números de teléfonos inteligentes con

[51] La manufactura discreta es la producción de artículos distintos como automóviles, muebles, juguetes, teléfonos inteligentes y aviones. Los productos resultantes son fácilmente identificables y son muy diferentes de manufactura de procesos donde los productos son indiferenciados como el petróleo, el gas natural y la sal. Por ejemplo una línea de fabricación discreta de automóviles Hyundai Motor Company en Ulsan, Corea del Sur. La fabricación discreta a menudo se caracteriza por la producción individual o de unidades por separado que pueden ser producidas en bajo volumen con muy alta complejidad o altos volúmenes de baja complejidad.

conexión a Internet. Por lo tanto, se aseguran de tener un sitio web móvil fácil de usar a través de una web móvil navegadora y para dispositivos como iOS y Android.

La Consumerización[52] (*consumerization*) presiona a las empresas para que les ofrezcan experiencias bastas y nuevas, ya que los clientes constantemente comparan cualidades y precios de productos y servicios en los sitios más populares como Google, YouTube, Yahoo, Amazon y eBay. Las empresas se amparan en las capacidades y requisitos de ventas avanzadas de sus sitios web, como la configuración de ventas, catálogos específicos para el cliente, enlaces con Intercambio Electrónico de Datos (EDI) y disposición de ambientes confiables, altamente escalables, disponibles y estables.

Desde el método de la sobre-expectación y madurez de las tecnologías del comercio electrónico de Gartner, la dinámica y complejidad anual de dicho comercio electrónico se muestra a través de varias tecnologías promocionadas en el mercado, las cuales manifestan la complejidad y la estrategias tecnológicas en el comercio electrónico.

Gartner proporciona una útil definición de comercio electrónico para analizar *el Ciclo de Sobre-expectación:*

> *Comercio electrónico es una recopilación de modelos de negocio, procesos y tecnologías que permiten las ventas en línea, servicio y marketing de B2B y el comercio B2C; facilita las transacciones través de sitios web y apoya la creación así como el desarrollo de las relaciones en línea.*

De la definición anterior se advierte que las tecnologías del comercio electrónico son fundamentales para las iniciativas clave, como la *Administración de la Relación con los Clientes*, comúnmente conocida como *Customer Relationship Management (CRM),* mejoras en los procesos, el crecimiento de las ventas, la reducción de los costos de ventas, creación de marca y entrega de valor a los consumidores y socios comerciales.

Las empresas tienen varias soluciones que ofrecer en el comercio electrónico y entre 15 a 20 puntos de integración básica para completar un proceso de negocio así como de 5 a 10 vendedores para operar. Además, algunas B2B realizan gestiones de diferentes tipos de comercio electrónico más allá de socio directo (B2B), gracias a sus capacidades en TIC y de sus redes asociadas.

De ahí que el C*iclo de sobre-expectación* brinda elementos para investigar, evaluar y priorizar las TIC que permitirán crear una experiencia única de Internet y abordar las tendencias actuales y futuras de comercio electrónico. Este ciclo de sobre-expectación del comercio electrónico aborda 65 de las TIC's más relevantes y actuales en seis áreas clave:

[52] La consumerización o consumidorización es una tendencia creciente en la cual las TIC surgen primero en el mercado del consumidor y luego se propagan hacia las organizaciones comerciales y gubernamentales. El establecimiento de los mercados de los consumidores como los impulsores primarios de la innovación en la tecnología de la información se vislumbra como un cambio grande en el ámbito de la tecnología informática.

a) *Experiencia web al Cliente*
b) *Marketing*
c) *Ventas*
d) *Servicio*
e) *Móvil*
f) *Social CRM[53] o Administración basada en la relación con los clientes.*

Ahora bien, también existen componentes funcionales del comercio electrónico que son una muestra de las formas de procesar los pedidos; gestionar muchos tipos de contenido e información de los productos; localizar productos, intercambiar datos, servicios y proveedores, así como análizar y gestionar el rendimiento general. De esta forma, las TIC's permiten a las empresas llevar a cabo cualquier tipo de comercio y dan funcionalidad a los procesos de negocio apoyados por un sitio web de comercio electrónico. Las TIC´s para el comercio electrónico incluyen:

1. *Plataformas y/o Web Cloud*
2. *Administración de derechos digitales del Consumidor (DRM)*
3. *Análisis de contenido*
4. *Redes de distribución de contenido*
5. *Arquitectura de entrega Contexto*
6. *Servicios de contexto enriquecido*
7. *Hub interacción con el cliente (CIH)*
8. *Gestión de la rentabilidad de los clientes*
9. *Gestión de pedidos distribuidos*
10. *La facturación electrónica*
11. *Detección de fraude*
12. *Portales de la empresa*
13. *La integración como servicio (IaaS)*
14. *Gestión y Administración de Datos Maestros de Clientes o Master Data Management: (MDM)*
15. *Administración de datos Maestros de productos*
16. *El video online*
17. *Visualización de la información rich*
18. *La analítica web*
19. *Web y aplicaciones de hosting*
20. *Aplicaciones web-to-print*

Finalmente y a manera de ejemplo, las actuales empresas líderes mundiales del comercio electrónico son:[54]

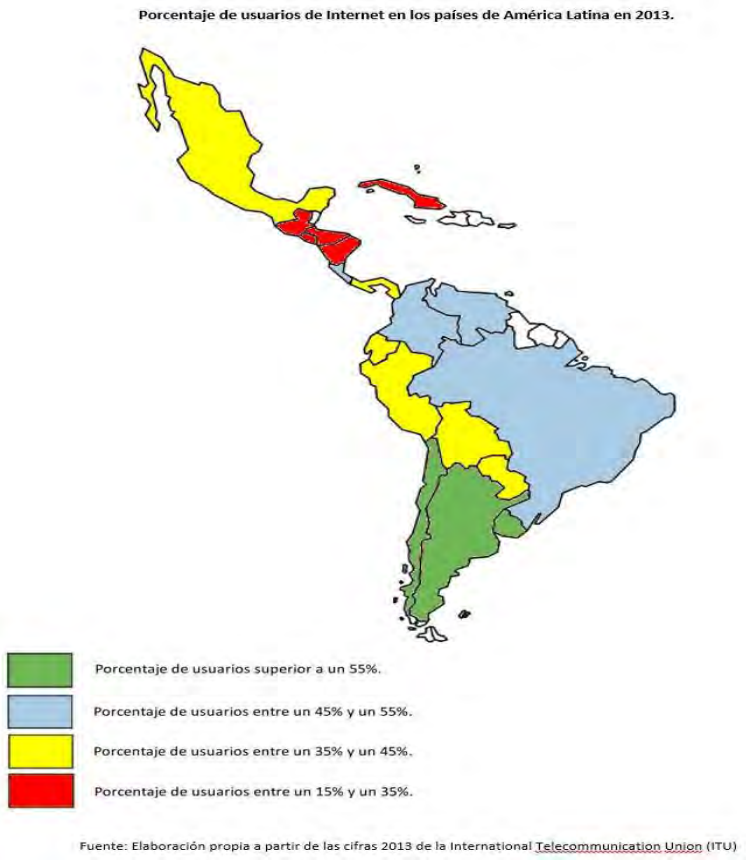
1.Amazon	5.Ovo Group	9.Tesco
2.JD.com	6.Alibaba (excepto ventas mayoristas)	10.Rakuten
3.Wal-Mart	7.Groupe Casino (Cnova)	11.Best Buy
4.eBay	8.Alibaba (excepto ventas mayoristas)	

1.2.5.2. Estadísticas relativas al Comercio Electrónico en México.

[53] "Social CRM es una filosofía y una estrategia de negocio, que se basa en el conocimiento del cliente a partir de la información transaccional y de producto, la cual se soporta en una plataforma tecnológica, reglas de negocio, procesos y características sociales, diseñado para conectar con los clientes a través de una conversación colaborativa de cara a generar un beneficio mutuo en un entorno de confianza y transparencia para los negocios. Es la respuesta de las compañías al actual control de la conversación por parte del cliente.

[54] Divante, Empresas líderes mundial de e-Commerce, en e-Commerce Trends from 2014 to 2015, accesible en: http://divante.co, consultada el 3 septiembre de 2015.

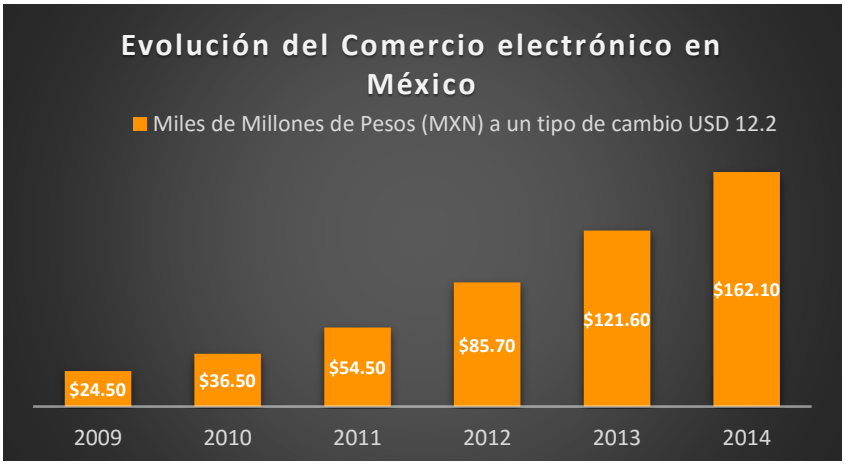
Ante todo es importante mostrar la realidad de nuestro país en una América Latina desigualmente conectada, donde la penetración de los usuarios de Internet en América Latina es baja en relación con el porcentaje de usuarios total de los países. La penetración de Internet de los principales países de América Latina se pueden repartir en 4 grupos, según su grado de penetración, como lo señala el siguiente mapa: [55]

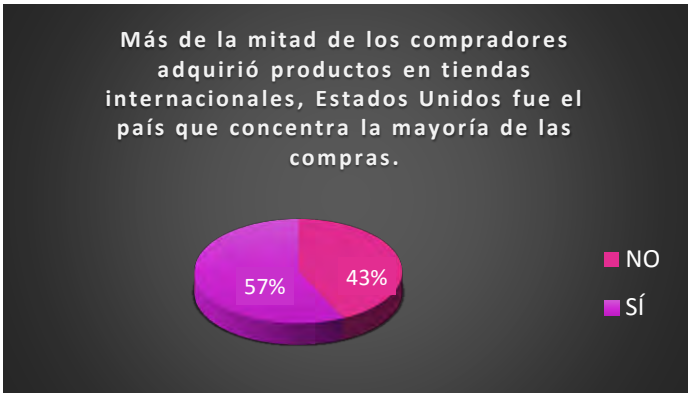


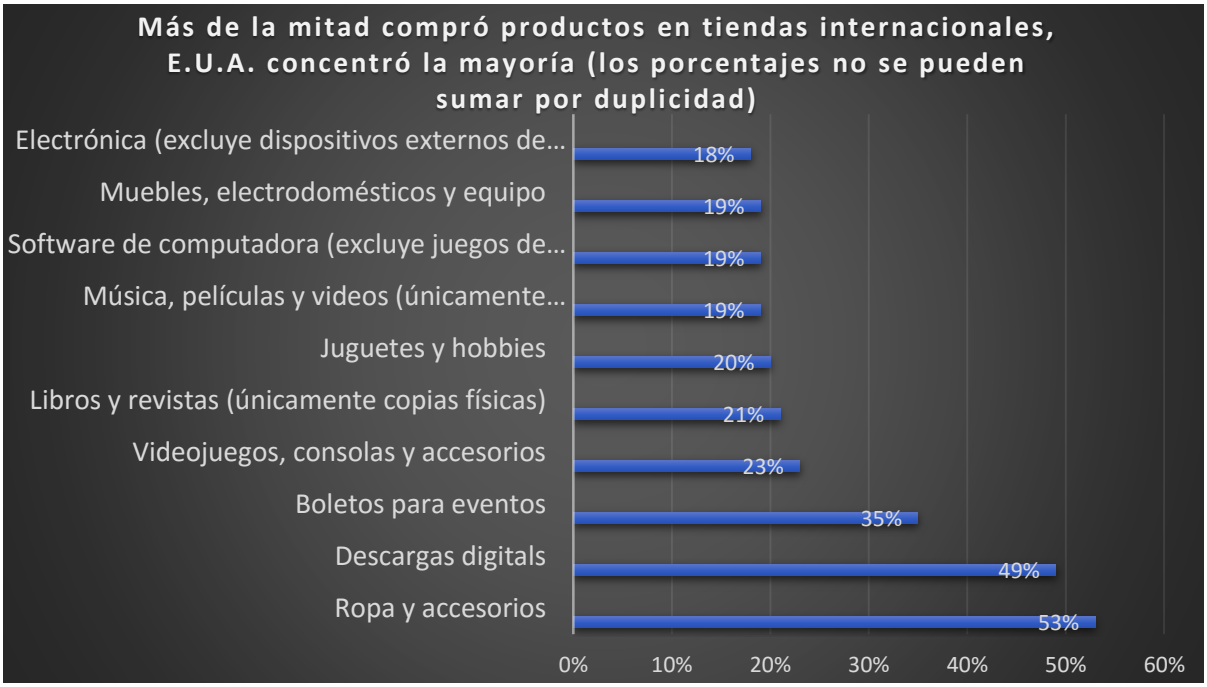
Los países menos conectados experimentan un riesgo estadísticamente menor en su amplitud que los dónde la penetración de Internet ya se encuentra avanzada por el simple efecto de un número de víctimas potenciales menor. El estar menos conectado repercute en una sobrerrepresentación de los ataques focalizados en contra de instituciones privadas y públicas. Al contrario, en países muy conectados, la población se encuentra directamente implicada en las problemáticas de seguridad y puede tener un efecto sobre las acciones llevadas a cabo a través de su comportamiento individual y de la expresión de una demanda política. Finalmente, no se debe olvidar que, en algunos países, la definición como objetivo prioritario del desarrollo de la cobertura territorial a través de infraestructuras de comunicación vinculadas a Internet – clave para la obtención de un reconocimiento internacional y político - puede ocultar límites importantes a un verdadero compromiso a favor de la calidad de estas infraestructuras y de su seguridad.

[55] Imagen que aparece en: Martin, Paul-Edouard e Instituto Español de Estudios Estratégicos, Inseguridad Cibernética en América Latina: Líneas de Reflexión para la Evaluación de riesgos, Documento de Opinión 79/2015, 24 de julio de 2015, p. 4, accesible en: http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO79-2015_InseguridadCibernetica_AmericaLatina_PaulE.Martin.pdf, consultado el 1 de agosto de 2015.

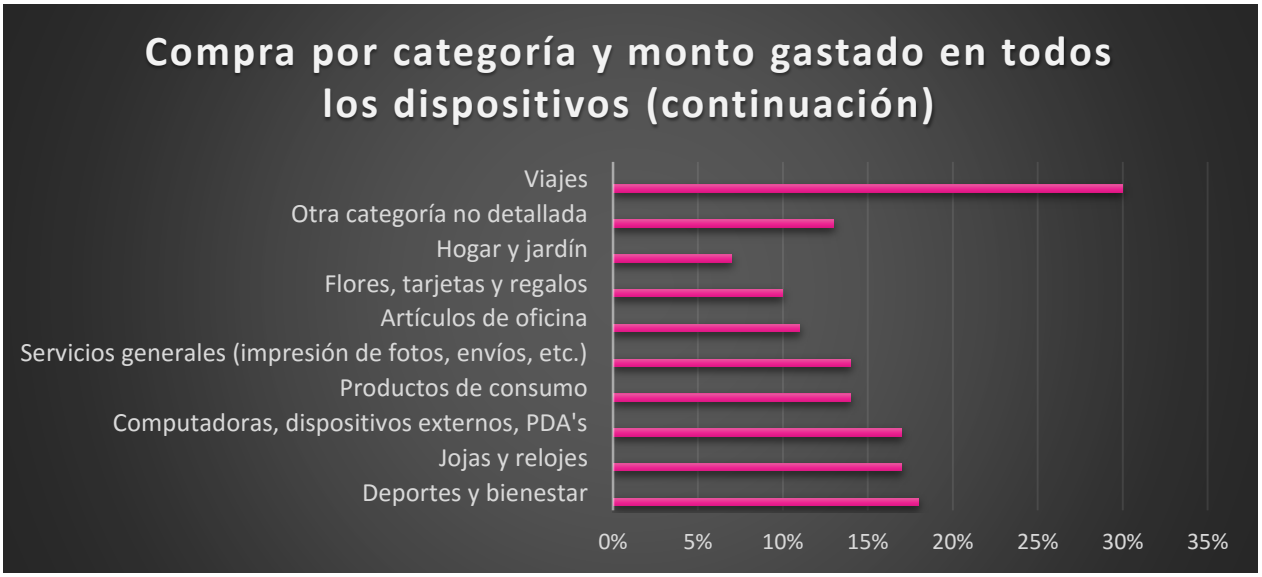
En el marco de esta penetración en Internet se inserta la evolución del comercio electrónico de acuerdo a los valores de mercado que muestra el *Estudio de Comercio Electrónico de México en 2015* de la *Asociación Mexicana de Internet, A.C. (AMIPCI)*:



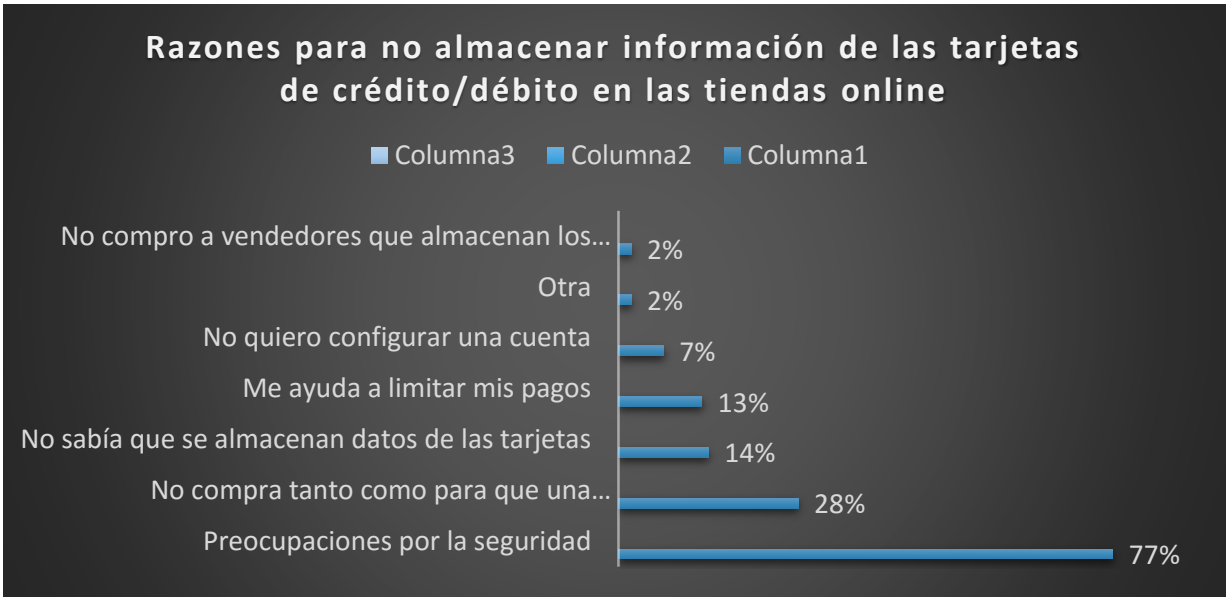




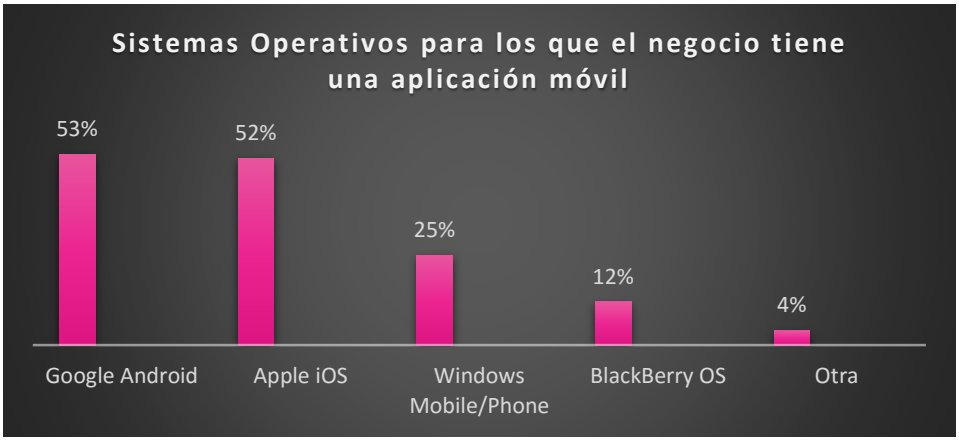
Ahora bien, tres de cada diez compradores realizaron una compra relacionada a viajes en los últimos tres meses. El gasto promedio mayor fue de MXN$ 9,284.00, casi 67% superior al promedio del resto de las categorías no relacionadas con viajes.



Los Pagos con fondeo de una cuenta bancaria (tarjeta de crédito, tarjeta de débito, PayPal, MercadoPago, SafetyPay y transferencia bancaria) dominan en México.



La preocupación acerca de la seguridad es la razón principal para no permitir guardar información en tiendas online.



Tres de cada cinco comercios tiene una aplicación móvil, la mayoría soportando tanto Android como Apple iOS.

En resumen, los hallazgos relativos al comercio electrónico en México son[56]:

- De acuerdo a la actividad de compra registrada desde Enero a Marzo de 2015, tres cuartos de los internautas mexicanos realizan compras online.
- Más de la mitad compró fuera del país durante este período.

[56] Asociación Mexicana de Internet, A.C. (AMIPCI). Estudio de Comercio Electrónico en México 2015, 10ª versión, México, D.F., accesible en: https://amipci.org.mx/estudios/comercio_electronico/Estudio_de_Comercio_Electronico_AMIPCI_2015_version_publica.pdf, consultada el 2 de diciembre de 2015.

- El volumen de compradores ha crecido fuertemente influenciado por la compra de descargas digitales desde dispositivos móviles.
- El gasto trimestral promedio en todos los dispositivos y categorías que no se relacionan a viajes fue de MXN$ 5,575.00 pesos, alrededor de MXN$ 1,860.00 pesos gastados online por mes.
- Dos tercios de los compradores utilizan un dispositivo móvil (smartphone y/o tablet) para sus compras online, frente a un tercio que utiliza exclusivamente PC/Laptop.
- A los mexicanos les gusta utilizar dispositivos móviles para un acceso a internet en cualquier lugar y por la posibilidad de utilizar la aplicación de los comercios, lo cual puede ahorrarles tiempo.
- Siete de cada diez usuarios realizaron compras desde las aplicaciones del comercio, y más de un tercio compró en las aplicaciones.
- Tres de cada cuatro ventas en línea ocurren por medio de una PC/Laptop. Las cuatro categorías principales vendidas en línea son ropa, deportes, otras categorías no enlistadas y electrónicas de consumo.
- La gran cantidad de incidencias en "otras categorías no enlistadas", indica la diversificación de la oferta del comercio electrónico.
- Por valor de ventas, sin incluir viajes, las cuatro categorías principales son electrónicos de consumo, computadoras/dispositivos periféricos/PDAs, y boletos de eventos.
- Los comercios esperan que las compras aumenten alrededor de El Buen Fin, Navidad y *HotSale.*
- Casi nueve de cada diez comercios están conscientes del *Sello de Confianza de AMIPCI*[57], pero sólo dos de cada cinco ofrece el Sello de Confianza en su sitio. Casi todos los comercios están conscientes de los eventos El Buen Fin y *HotSale.*

1.2.5.3. Factores de crecimiento del comercio electrónico en México.

De acuerdo con la *Revista Digital Forbes*, las compras móviles representaron 18% del comercio digital de México en junio de 2014, contra 12% en EUA, por ello las empresas que busquen crecimiento del comercio electrónico en México deben considerar por lo menos cinco elementos clave[58]:

a) **Personalización**: La personalización dentro del comercio electrónico permite brindar una experiencia de compra única, que puede dar como resultado un mayor volumen de ventas. En este caso es importante contar con herramientas que permitan estudiar los hábitos de compra de cada consumidor, de tal manera que podamos ofrecerles una experiencia

[57] AMIPCI en colaboración con la SE y la PROFECO expidieron el sello de confianza AMIPCI que es un distintivo único para sitios de Internet en México, que a través de un documento digital certificado, reconoce a aquellos negocios o instituciones que promueven el cumplimiento a la protección de la privacidad. Los interesados presentan una solicitud para que se lleve a cabo una verificación de la existencia del sitio, de las líneas de contacto reales así cmo de las políticas de privacidad y el compromiso a seguir su código de ética; los trámites se realizan en www.sellosdeconfianza.org.mx

[58] En este sentido, 5 Claves del Comercio Electrónico en 2015, accesible en http://www.forbes.com.mx/5-claves-del-comercio-electronico-en-2015/, 13 de enero de 2015, fecha de consulta 2 mayo de 2015.

específica, productos de acuerdo con su comportamiento o incluso recomendaciones sobre otros productos que permitan complementar su compra.

b) **Mobile commerce:** El auge de los dispositivos móviles ha dado pauta al surgimiento del comercio móvil y a que los usuarios puedan comprar en cualquier momento y lugar desde sus smartphones o tabletas. De acuerdo con datos de comScore[59], las compras móviles representaron 18% del comercio digital de México en junio de 2014, comparado con el 12% en Estados Unidos, siendo lo más comprado descargas digitales, viajes, boletos para eventos, ropa y accesorios, entre otros.
c) **Atención al cliente:** Es un factor decisivos de los consumidores a la hora de comprar en línea y que además genera confianza en el usuario.
d) **Programas de fidelidad:** Los programas de lealtad funcionan tanto en el comercio tradicional como en el digital y continúan siendo un impulso a las ventas entre los usuarios. La variante es que en el sector digital estos programas pueden ser utilizados a través de aplicaciones, redes sociales e incluso códigos QR[60].
e) **Convergencia de dispositivos:** De acuerdo con información de comScore, los internautas mexicanos utilizan diferentes dispositivos para conectarse a Internet durante todo el día (smartphones, laptops, tabletas), por lo que es importante que haya una integración de los canales de venta digital.

El comportamiento del comprador mexicano, es un factor relevante cuando se consideran que el porcentaje de acceso a Internet en los Estados de la República Mexicana va de los que cuentan con mayor acceso entre 50 y 60 por ciento de la población (Distrito Federal, Nuevo León y Sonora) a un menor acceso del 35 por ciento (Chiapas, Oaxaca, Guerrero, Veracruz o Michoacán)[61].

Básicamente, en aquellas entidades federativas, las características del comprador mexicano se encuentran estrechamente relacionadas con el impulso que se le da a los factores de crecimiento del comercio electrónico mencionados con anterioridad, de ahí que el comportamiento o conducta del consumidor nacional deban describirse para avanzar de acuerdo a ellas. Para tal efecto se caracteriza a los consumidores mexicanos[62]:

I. Compras en tienda. Los consumidores de México tienen un estilo moderno, compran más en tienda que cualquier otra región, sin embargo usan extensamente la telefonía y redes sociales para hacer compras en línea. Cuando compran con un minorista multicanal, los consumidores mexicanos tienen el nivel más alto de preferencia por las compras en tienda (45%), mientras que un 44% prefiere la compra en línea, sea a través de una laptop o teléfono inteligente.

[59] ComScore es una empresa de análisis del comportamiento de Internet.
[60] Los códigos QR son un tipo de códigos de barras bidimensionales que a diferencia de uno de barras convencional, la información está codificada dentro de un cuadrado, permitiendo almacenar gran cantidad de información alfanumérica.
[61] Belmont Vázquez, Jesús. El Cuarto Poder, accesible en http://www.cuartopoder.mx/hoyescriben/columnas/liderespoliticos-100051.html, consulta del 1 de diciembre de 2015.
[62] Cfr. ComScore, Estudio Global Revela que Compradores Mexicanos Demandan Flexibilidad, accesible en https://www.comscore.com/esl/Prensa-y-Eventos/Comunicados-de-prensa/2015/3/ESTUDIO-GLOBAL-REVELA-QUE-COMPRADORES-MEXICANOS-DEMANDAN-FLEXIBILIDAD, del 3 de Marzo de 2015, fecha de consulta: 2 de mayo de 2015.

II. Búsqueda en móviles y en línea. Contar con acceso a Internet y revisar la información de referencia acerca de un producto a través de dispositivos móviles, ha modificado el comportamiento de compra. El 44% de consumidores mexicanos usan sus teléfonos inteligentes para buscar productos antes de visitar la tienda. Asimismo, muestran el siguiente comportamiento:

a) Más del 40% utiliza sus teléfonos para comparar precios y/o revisar información adicional de los productos, cuando se encuentran en una tienda.
b) El 57% de los consumidores descargan aplicaciones móviles de sus marcas preferidas, para mantenerse al tanto de información como ventas especiales, cupones o incentivos de compra.
c) Un 70% indica que la principal razón por la que compran productos en línea en lugar del establecimiento, es porque descubrieron un mejor precio.

III. Opciones de envío. Las alternativas para la entrega al consumidor mexicano son más importantes que para el comprador de Asia, Europa y los Estados Unidos. Para envíos nacionales, 45% está dispuesto a esperar de 1 a 3 días por sus compras. Si el envío es gratis, 67% dijo que esperaría de 1 a 3 días adicionales.

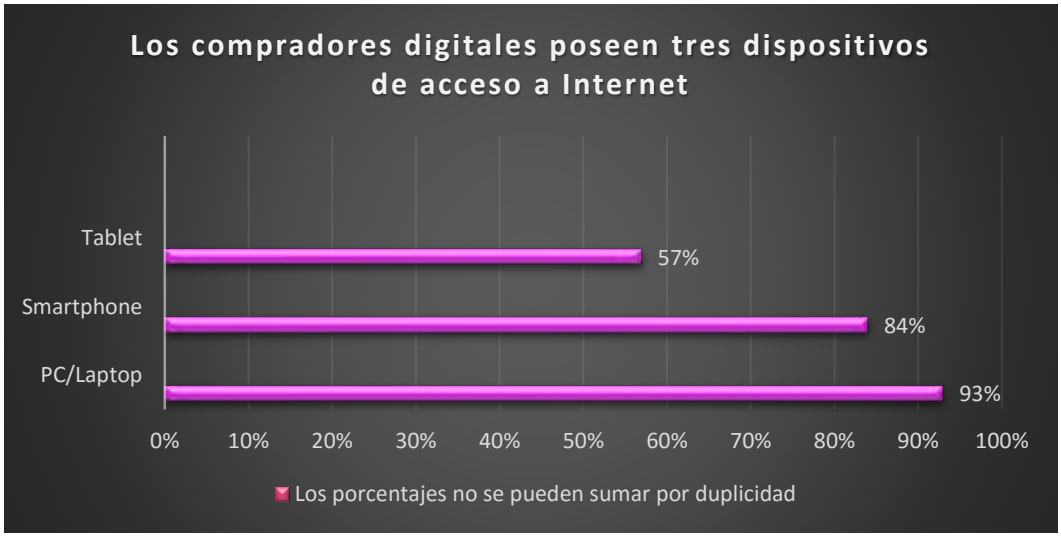
En envíos internacionales, el tiempo más seleccionado de entrega son 2 días de tránsito (25%) seguido de 3 a 5 días en tránsito (24%) y entrega del día siguiente (21%). Sin embargo, si la entrega es gratis, 54% mencionó que esperarían 5 o más días adicionales por la compra. Un proceso eficiente de entrega de los productos, es fundamental para incentivar las compras en línea, se destaca el tiempo de entrega como el factor principal (18%), seguido de la reputación del minorista (17%) y la información disponible del producto (11%).

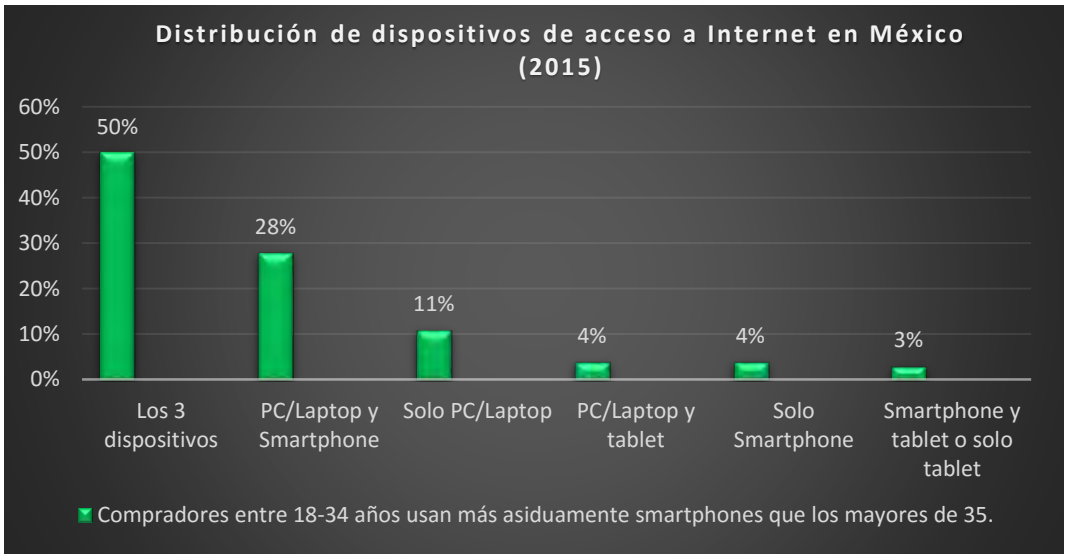
IV. Las redes sociales motivan la venta en línea. Las compras en línea a nivel mundial han sido considerablemente influenciadas por las redes sociales, especialmente en México. Tres de cada cuatro compradores y el 80% de los *millennials*[63] encuestados, afirmaron que guían sus compras a través de las redes sociales. Facebook es la plataforma social más utilizada (94%), seguida de Google + (68%), Twitter (66%) e Instagram (39%). Los minoristas y consumidores en línea aprovechan las redes sociales para publicar su opinión sobre los productos adquiridos y los procesos de compra: 92% lo hace en Facebook, 41% en Twitter; 25% en Google+; 15% en Instagram; y 6% en Pinterest.

V. Las políticas de retorno afectan las decisiones de compra. En general, los consumidores muestran estar contentos con diversos servicios disponibles de la post-compra, como notificaciones vía correo electrónico que confirman la entrega del artículo (75%), la visibilidad del proceso de envío de las compras (73%), políticas de devolución fáciles de entender (60%), y la flexibilidad de elegir la fecha de entrega del producto (55%).

[63] La Generación Millennials define a los nacidos entre 1981 y 1995, jóvenes entre 20 y 35 años que se hicieron adultos con el cambio de milenio (en plena prosperidad económica antes de la crisis). Según el reporte de Tendencias Digitales Conecta tu marca con los millennials, actualmente en Latinoamérica un 30 % de la población es Millennial y según una proyección de la consultora Deloitte, en 2025, representarán el 75 % de la fuerza laboral del mundo.

Por otro lado, las estadísticas exhibidas por AMIPCO muestran que la mitad de los compradores digitales poseen tres dispositivos de acceso a Internet: PC/laptop, Tablet y Smartphone, de la siguiente forma:





1.3. Principios generales del Derecho del comercio electrónico.

Los beneficios, inconvenientes y riesgos del comercio electrónico de los que se habló en epígrafe anterior explican la necesidad y ánimo de comprender el entorno legal, funcionamiento y dinámica del Derecho del Comercio Electrónico, la cual nos confronta con uan postura del Derecho ante la contratación electrónica.

En este contexto, a continuación se hace referencia a las reglas o principios universales del Derecho del Comercio Electrónico, a saber: equivalencia funcional de los actos comerciales electrónicos; invariabilidad del preexistente derecho comercial; neutralidad tecnológica; buena fe; y libertad contractual persistente en el entorno electrónico así como su ejercicio en el nuevo contexto tecnológico.

1.3.1. Equivalencia funcional de los actos comerciales electrónicos

La aparición del uso de transacciones por medios electrónicos y el incremento en su empleo forzó al legislador a definir cómo podía la ley o la voluntad de las partes contratantes dotar de juridicidad a las negociaciones contractuales electrónicas. Resolver este problema no fue sencillo. Un grupo de expertos juristas de la CNUDMI/UNCITRAL[64] reflexionaron y discutieron durante más de un año cuál era la "función jurídica" de los actos jurídicos electrónicos respecto de los actos jurídicos manuscritos, autógrafos o escritos.

Posteriormente, mediante la expedición de la *Ley Modelo CNUDMI sobre comercio electrónico* de 1996, las Naciones Unidas establecieron este nuevo criterio de equivalencia funcional, denominado a veces "criterio del equivalente funcional", basado en un análisis de los objetivos y funciones del requisito tradicional de la presentación de un escrito consignado sobre papel con miras a determinar la manera de satisfacer sus objetivos y funciones con técnicas del llamado comercio electrónico. Por ejemplo, ese documento de papel cumple funciones como las siguientes[65]:

a) *Proporcionar un documento legible para todos;*
b) *Asegurar la inalterabilidad de un documento a lo largo del tiempo;*
c) *Permitir la reproducción de un documento a fin de que cada una de las partes disponga de un ejemplar del mismo escrito;*
d) *Permitir la autenticación de los datos consignados suscribiéndolos con una firma; y*
e) *Proporcionar una forma aceptable para la presentación de un escrito ante las autoridades públicas y los tribunales.*

[64] El 17 de diciembre de 1966 la Asamblea General de la Organización de las Naciones Unidas estableció la CNUDMI, dándole el mandato general de fomentar la armonización y unificación progresiva del derecho mercantil internacional. Desde entonces, la CNUDMI se ha convertido en el órgano jurídico central del sistema de las Naciones Unidas en el ámbito del derecho mercantil internacional.
[65] Ley Modelo de la CNUDMI sobre Comercio Electrónico 1996 y su Guía para la incorporación de la Ley al derecho interno, Naciones Unidas, Nueva York, 1997, p. 20, epígrafe y ss.

Así, la documentación consignada por medios electrónicos puede ofrecer un grado de seguridad equivalente al del papel y, en la mayoría de los casos, mucha mayor fiabilidad y rapidez, especialmente respecto de la determinación del origen y del contenido de los datos, con tal de que se observen ciertos requisitos técnicos y jurídicos.

Ahora bien, la adopción de este criterio del equivalente funcional no debería dar lugar a que se impongan normas de seguridad más estrictas a los usuarios del comercio electrónico (con el consiguiente costo) que las aplicables a la documentación consignada sobre papel, cuestión que se verá generá más costos en un inicio pero una vez hecho el gasto, impacta posteriormente con mayores beneficios.

La equivalencia funcional se define como la función jurídica que cumple la instrumentación autógrafa respecto de cualquier acto jurídico la cual se puede cumplir con la instrumentación electrónica a través de una MD, con independencia los contenidos, dimensión, alcance y finalidad del acto[66].

Su implicación más relevante consiste en que no se puede discriminar las declaraciones de voluntad o ciencia de los mensajes de datos (MD) y, por ende, deben de surgir los efectos jurídicos con independencia del soporte en el que consten.

Además, nuestro Código de Comercio (CCo) adoptó el principio establecido en los artículos 6, 7 y 8 de la LMCE, consistente en que la equivalencia funcional se aplica a su vez en tres aspectos de la contratación electrónica:

a) Sobre el documento escrito
b) Sobre la noción de firma
c) Sobre el cumplimento del requisito legal de documentación original[67].

Está aplicación extensiva también cuenta con tres excepciones, la equivalencia no comprende[68]:

[66] Illescas Ortíz, Rafael: Derecho de la contratación electrónica, 2009, 2ª ed., Madrid, Civitas Thomson Reuters, p. 41.

[67] El segundo párrafo del artículo 210-A del Código Federal de Procedimientos Civiles, establece que cuando la ley requiera que un documento sea conservado y presentado en su forma original, ese requisito quedará satisfecho si se acredita que la información generada, comunicada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología, se ha mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y ésta pueda ser accesible para su ulterior consulta.

[68] El decreto por el que se reforman y adicionan diversas disposiciones del Código Civil para el Distrito Federal en Materia Común y para toda la República en Materia Federal, del Código Federal de Procedimientos Civiles, del Código de Comercio y de la LFPC del 29 de mayo de 2000 no es tan evidente en establecer las excepciones al principio de equivalencia funcional en los siguientes tres casos. No obstante, el citado Decreto en sus reformas al artículo 25 Código Federal de Procedimientos Civiles regula que los actos que conforme a este Código u otras leyes deban inscribirse en el Registro Público de Comercio de la Secretaría de Economía (RPCSE) deberán constar en: I.- Instrumentos públicos otorgados ante notario o corredor público; II.- Resoluciones y providencias judiciales o administrativas certificadas; III.- Documentos privados ratificados ante notario o corredor público, o autoridad judicial competente, según corresponda, o IV.- Los demás documentos que de conformidad con otras leyes así lo prevean. Finalmente, también el segundo párrafo del artículo 93 del Código de Comercio establecen los casos en que la ley dicta como requisito que cuando un acto jurídico deba otorgarse en instrumento ante fedatario público, éste y las partes obligadas podrán, a través de mensajes de datos, expresar los términos exactos en que las partes han decidido obligarse, en cuyo caso el fedatario público, deberá hacer constar en el propio instrumento los elementos a través de los cuales se

a) A los documentos públicos o notariales, salvo disposición expresa.
b) La regulación de situaciones o áreas específicas en los que la equivalencia funcional no es dable. Los motivos de excepción de la equivalencia no se encuentran en la falta de idoneidad al respecto de las operaciones sino en la necesidad de que su electrificación se lleva a cabo de un modo más complejo y exacto que el resto de los contratos. Específicamente, en el ámbito gubernamental, la Ley de FEA expedida en enero de 2012, establece en el artículo 4 que sus disposiciones no serán aplicables a los actos en que no sea factible el uso de la FEA por disposición de ley o aquéllos en que exista previo dictamen de la SFP. Asimismo, el artículo 4 y 5 del Reglamento de la Ley de FEA de marzo de 2014 establece que las dependencias y entidades de la APF podrán emitir, de manera justificada, el acto que corresponda utilizando la firma autógrafa en casos en que medie una situación de emergencia o urgencia.
c) El soporte electrónico de una declaración viciada no es reparatorio.

En suma, la equivalencia funcional se regula en dos de nuestros códigos nacionales, el primero, el Código Federal de Procedimientos Civiles (CFPC) y el segundo, el Código de Comercio (CCo) en los términos siguientes:

> ***Artículo 210-A, segundo párrafo:*** *Cuando la ley requiera que un documento sea conservado y presentado en su forma original, ese requisito quedará satisfecho si se acredita que la información generada, comunicada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología, se ha mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y ésta pueda ser accesible para su ulterior consulta*[69]*.*

Mientra que el CCo dispone:

> ***Artículo 93.*** *Cuando la ley exija la forma escrita para los contratos y la firma de los documentos relativos, esos supuestos se tendrán por cumplidos tratándose de mensaje de datos siempre que éste sea atribuible a las personas obligadas y accesibles para su ulterior consulta*[70.]

No pasa inadvertido que el principio de equivalencia funcional se aplica a cualquier firma electrónica, de acuerdo con nuestra normatividad, pues el artículo 89 del citado Código reconoce tanto a la firma autógrafa como a la firma electrónica. En este momento pudiera surgir la interrogante de si a ambas firmas se les reconoce el mismo efecto jurídico que la autógrafa ¿en qué consiste el provecho o utilidad de emplear la FEA?

La pregunta se despeja cuando se dimensiona el alcance probatorio que tiene la FEA. Gracias a que el artículo 90 bis del CCo dispuso la presunción legal a favor del destinatario de un MD que radica en la estimación de que actuó con la debida diligencia al asegurarse de la identidad del emisor del MD, que no es más que el empleo de un método de verificación que cumpla con los

---

atribuyen dichos mensajes a las partes y conservar bajo su resguardo una versión íntegra de los mismos para su ulterior consulta, otorgando dicho instrumento de conformidad con la legislación aplicable que lo rige.

[69] Último párrafo del artículo 210-A.

[70] Artículo 93.

requisitos para determinar la fiabilidad de las firmas electrónicas a que se refiere el segundo párrafo del artículo 97del multicitado Código.

En suma, el principio de equivalencia funcional a que se refiere el artículo 93 del Código citado, otorga la firma electrónica los mismos efectos y consecuencias que la firma autógrafa.

Finalmente, es con apego a este principio de equivalencia funcional, que los MD pueden tener los mismos efectos e implicaciones legales que la información y datos contenidos en papel (artículo 1298-A del CCo).

1.3.2. Invariabilidad del preexistente derecho comercial

Los principios del comercio electrónico no significan un cambio sustancial del derecho interno existente de las obligaciones y convenios, ni nacional ni internacional, cuando se da una negociación electrónica.

Por lo que las disposiciones del comercio aplicables con anterioridad son también aplicables a los casos de las negociaciones comerciales electrónicas, como ejemplo, la Ley Modelo de la CNUDMI sobre Firma Electrónica (LMFE) de 2001 establece en su primer artículo que la Ley será aplicable en todos los casos en que se utilicen firmas electrónicas en el contexto de actividades comerciales y *no derogará ninguna norma jurídica destinada a la protección del consumidor.*

Ello muestra una flexibilidad inherente a la Ley Modelo, la cual es conveniente para hacer varias modificaciones al texto uniforme antes de incorporarlo a su derecho interno.

1.3.3. Neutralidad tecnológica

Se trata de otro principio de no discriminación que se dirige a que las partes pueden acordar ciertas técnicas de soporte electrónico o exceptuarlo, en su caso, al considerar que no se excluya, restrinja o prive de efecto jurídico cualquier método para crear un MD, sistema informático, dispositivo de firma electrónica, etc.. Lo anterior indica que la forma en que se aplica una determinada tecnología no puede invocarse como única razón para denegar eficacia jurídica a una contratación electrónica. Sin embargo, no debe confundirse la eficacia con la validez jurídica de una determinada tecnología.

La forma en cómo se refiere el CCo al principio de neutralidad tecnológica es precisando que no se debe favorecer una tecnología sobre otra o bien, que no se debe obligar a los usuarios de los medios electrónicos a preferir determinada tecnología. Mientras que en el caso de la firma electrónica, implica que no se deberá favorecer a un determinado método de creación de firma electrónica respecto de otro. En este sentido el artículo 26 de ese Código refiere que no se restringirán o privará de efecto jurídico a otros medios de creación de firma electrónica.

1.3.4. Buena fe

Dado que el derecho civil constituye el derecho común de aplicación supletoria del sistema jurídico mexicano, cuando el artículo 1859 del Código Civil Federal (CCiF) establece que las

reglas del contrato son disposiciones también de los actos jurídicos, deviene indispensable profundizar en el principio orientativo y unívoco de buena fe contractual.

Los elementos que se requieren para definir la buena fe son[71]:

1) La existencia de un estado psicológico relativo a la intención de obrar honestamente, la creencia de que el otro contratante tiene la misma intención y la convicción o ignorancia de atributos o calidades de situaciones, cosas o personas.

2) La influencia de la actitud psicológica en la formación de la voluntad, y

3) La actuación conforme con el estado anímico y voluntad.

En suma, aunque la buena fe contractual no integra un elemento de validez del acto, funciona como un elemento que suple, integra y corrige el contenido del contrato en función interpretativa, esto es, participa en la estructuración de las reglas del negocio contractual, constituyéndose en una disposición más.

1.3.5. *Autonomía de la voluntad.*

La doctrina de la *autonomía de la voluntad* toma credibilidad conjuntamente con el individualismo del liberalismo económico del siglo XIX, a través de los principios del contrato social de Juan Jacobo Rousseau en el que se pregunta cómo el ser humano originalmente nace libre, pero se torna necesario consentir el "pacto social" a fin de conservar únicamente su "libertad", por ende, la "autonomía de la voluntad" consiste en reconocer que todas las obligaciones contractuales que surgen de la voluntad suprema de dos partes libres e iguales son justas en razón de que surgieron de la voluntad del ser humano.

En este orden de ideas, la generalidad de los códigos civiles de la República Mexicana reconocen y proclaman el principio del inexorable cumplimiento de la autonomía de la voluntad en los contratos, conocida con la proposición latina *pacta sunt servanda*, mientras que una escasa minoría regula el principio contrario, *rebus sic stantibus*[72] o teoría de la imprevisión, como es el caso de Jalisco, donde el consentimiento se entiende otorgado en las condiciones y circunstancias en que se celebra el contrato.

Por tanto, salvo aquellos que aparezcan celebrados con carácter aleatorio, los contratos podrán declararse rescindidos cuando por haber variado radicalmente las condiciones generales del medio en que debían tener cumplimiento, sea imposible satisfacer la verdadera intención de las partes y resulte, de llevar adelante los términos aparentes de la convención, una notoria injusticia o falta de equidad que no corresponda a la causa del contrato celebrado[73].

---

[71] Cfr. Jiménez Gómez, Juan Ricardo. El principio de la buena fe en la teoría general del contrato, en Un Siglo de Derecho Civil Mexicano. Memoria del II Coloquio Nacional de Derecho Civil Serie C, Estudios Históricos, Instituto de Investigaciones Jurídicas –UNAM, México D.F., Núm. 20, 1985, p. 191.

[72] La proposición se refiere a aquel evento que se entiende implícito en los contratos para que en el supuesto de ocurrir un evento imprevisible, que afecte gravamente al deudor para cumplir con su obligación, le permita rescindir ese contrato.

[73] Díaz Bravo, Arturo. Contratos mercantiles, 2012, México, De Iure, p. 8.

No obstante, la obligatoriedad del contrato o *pacta sunt servanda*, conforme a la cual los contratos obligan a las partes contratantes y, en consecuencia, deben cumplirse, es inherente al origen del derecho contractual. Lo anterior se funda en que el Estado ha conferido autonomía y libertad a los individuos para que autorregulen sus intereses, suscribiendo toda clase de contratos dentro de los límites que ha impuesto.

En suma, se otorgó fuerza vinculante y obligatoria a los contratos, ya que de lo contrario no existiría seguridad jurídica en la contratación, fin supremo en todo Estado de Derecho.

En tal sentido, la garantía que tienen los contratantes es que el Estado regula a través de disposiciones expresas el otorgamiento de seguridad, para que si en el futuro celebran un contrato y una de las partes no cumple con sus obligaciones, el contratante perjudicado tenga acción para exigir su cumplimiento. Por consiguiente, si dos individuos suscriben un contrato, en ejercicio de su autonomía privada y conforme a los mandatos de la buena fe, dicho contrato será obligatorio.

Una consecuencia del *pacta sunt servanda* es que la única forma de privar de efectos jurídicos al contrato será por un nuevo acuerdo, por la vía de la novación, la compensación (voluntaria), la condonación o el acuerdo de mutua terminación.

En efecto, la vigencia de tal principio no puede ser excluida por el hecho de que la libertad contractual se ejercite en un entorno electrónico, por lo que el artículo 4.1. de la LMCE 1996 dispone que:

> *Salvo que se disponga otra cosa, en las relaciones entre las partes que generan, envían, reciben, archivan o procesan de alguna otra forma mensajes de datos, las disposiciones del capítulo III podrán ser modificadas mediante acuerdo.*

Y las disposiciones del capítulo III se refieren a las relaciones contractuales de quienes contratan electrónicamente.

Nada de lo anterior implica que no existan excepciones al *pacta sunt servanda*, específicamente cuando se trata de la libertad de un negocio, entre ellas están:

a) Confidencialidad de los datos personales electrónicamente intercambiados con fines transaccionales entre el emisor y el receptor.
b) Obligaciones contraídas por el consumidor, cuando este sea una de las partes contratantes electrónicamente y su disponibilidad contractual.
c) No hay libertad empresarial respecto a quienes pueden establecerse como prestadores de servicios de certificación de firmas electrónicas.
d) Cuando no hay homologación normativa entre los Estado de la República Mexicana.

En definitiva, este principio también nombrado por nuestra legislación como el de autonomía de la voluntad, estriba en que las firmas y certificados electrónicos de firmas son de carácter

supletorio, y únicamente será aplicable en el supuesto de que los contratantes no hayan pactado con antelación u procedimiento distinto.

En el CCo fija la libertad de las partes para:

a) La verificación de la emisión y de la oportunidad de la emisión de MD (artículo 91 bis)
b) La determinación del lugar de emisión y recepción de MD; elemento principal para señalar la jurisdicción y leyes aplicables al contrato (artículo 94).
c) Acuse de recibo y mecanismos para verificarlo (artículo 92)

1.4. Elementos conceptuales del Derecho del comercio electrónico

La taxonomía consistente en la división del Derecho del comercio electrónico en elementos objetivos y subjetivos es por demás adecuada para la compresión de su naturaleza jurídica.[74]

Como elementos objetivos se consideran: el MD y documento electrónico, las normas técnicas de estructuración de MD, firmas electrónicas y/o digitales, los sistemas de información y las redes e interconexión de redes (Internet)

Mientras que como elementos subjetivos se consideran: al emisor/signatario del MD, el destinatario, los intermediarios y los prestadores de servicios de certificación de FEA.

1.4.1. Elementos objetivos.

1.4.1.1. Mensaje de datos y documento electrónico

El MD o *data message* es el componente esencial del derecho de comercio electrónico. Su antecedente en nuestro CCo es el artículo 2 de la LMCE 1996, que para los fines de esa Ley establece:

> *Por 'mensaje de datos' se entenderá la información generada, enviada, recibida o archivada o comunicada[75] por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), el correo electrónico, el telegrama, el télex o el telefax;*

Antes de realizar un análisis de lo que estatuye nuestro CCo, es relevante señalar que no toda transmisión de datos puede dar nacimiento a un acto jurídico solo las expresiones o declaraciones de voluntad realizadas para generar consecuencias jurídicas. En el caso del oferente y el destinatario, la trasmisión de datos en forma electrónica puede crear obligaciones legales.

[74] La clasificación es una aportación de Rafael Illescas Ortíz visible en su obra Derecho de la contratación electrónica, 2009, 2ª ed., Madrid, Civitas Thomson Reuters, p. 37.
[75] Es importante señalar que el término comunicación de la información no se contempla en la versión original, esto es la inglesa, de la Ley Modelo como una finalidad específica del MD. El problema se debió a un error en la aparición de la traducción a la versión al castellano y se conserva hasta hoy.

Ahora bien, el numeral 89 del vigente CCo[76] define el MD como: *la información generada, enviada, recibida o archivada por medios electrónicos, ópticos o cualquier otra tecnología*.

En esta definición la palabra *información* es utilizada de manera amplia y no literal, sino en sentido técnico o electrónico, esto es como todo aquello que puede ser sujeto de un proceso de digitalización, esto es de conversión en ceros y unos, en otras palabras se trata de todo que se transmite por vía electrónica: datos, imágenes, sonido, códigos de programas, software, bases de datos, texto, video, etc.

Esta noción de *información* trae como implicación que toda declaración comercial, pre-comercial y post-comercial efectuada por el emisor de un MD se convierte en datos constitutivos de información, ello se traduce en que no solo se considerará información las declaraciones de voluntad o jurídicas.

Un MD no es exactamente equivalente de un documento de papel pero la Ley Modelo de referencia adoptó un criterio flexible que gradúa o jerarquiza los requisitos de forma aplicables a la documentación consignada sobre papel[77], tal nivelación toma en consideración el:

1. Grado de fiabilidad,
2. Grado de inalterabilidad y
3. Grado de rastreabilidad que mejor convenga a la función que les haya sido atribuida.

Ahora bien, de la lectura de la definición de MD se advierte que la información se caracteriza por ser objeto de tratamiento de medios electrónicos, lo cual significa que solo si hay un tratamiento[78] electrónico, óptico o similar habrá declaración del emisor y ésta obtendrá la calidad de MD. Igualmente, debe darse alguno de los fines que se mencionaron con antelación: generación, envío, recepción, archivo o comunicación, para que sea un MD.

De la noción de MD se advierte que diferencia entre *medios* y *técnicas de tratamiento electrónico*, los primeros, son los medios de tratamiento en general son medios electrónicos, ópticos o similares, y los segundos, son los medios específicos de tratamiento[79] como: Intercambio Electrónico de Datos (EDI), correo electrónico, telegrama, télex o telefax. Igualmente, la Ley Modelo contempla nociones abandonadas en la cotidianidad y que ya no son considerados como tecnologías de la sociedad de la información y se atreve a incluir medios de tratamientos como el telegrama y el telefax.

[76] Hasta la última reforma publicada el 13 de junio de 2014.
[77] Ley Modelo de la CNUDMI sobre Comercio Electrónico 1996 y su Guía para la incorporación de la Ley al derecho interno, Naciones Unidas, Nueva York, 1997, p. 21, epígrafe 16 y ss.
[78] Los medios de tratamiento se diferencian de la forma de Tratamiento, esta última se refiere al uso, obtención, divulgación o almacenamiento de la información.
[79] Sobre este concepto se abunda en infra. 1.2.1.2.

Es de relevancia mencionar que el MD es siempre bilateral, esto es, hay un emisor y un destinatario a quienes les incumbe su contenido y configuración, por lo que ambas partes, previamente al empleo de MD deben poseer los medios técnicos necesarios para ingresar a su información; y generalmente, la resolución de usar los medios electrónicos para llevar a cabo una relación contractual corresponde al emisor, quien debe conocer que capacidades técnicas tienen el destinatario o el tercero por cuenta de este.

Una excepción a ello podría ser que ambas partes contractualmente y de manera autógrafa decidan a futuro emplear MD.

De acuerdo a las consideraciones anteriores, el MD no será tal si no presenta la bilateralidad tecnológica, este es el caso de cualquier información o documentación digitalizada fuera de una negociación o llegada después de la negociación, el mismo caso sucede con el *back up*[80] de un MD realizado por el emisor, o bien la contabilidad electrónica de un comerciante que tampoco sería un MD dada la carencia de un destinatario.

En México, la reforma del 29 de mayo de 2000 tuvo como consecuencia práctica la forma de acreditar que un MD era emitido realmente por quien se ostentaba como emisor, y luego, la manera de acreditar que el MD fue recibido por el destinatario.

Del análisis de los artículos 90 y 91 del CCo, se presume que un MD es del emisor si fue enviado usando medios de identificación (NIP[81], contraseñas o claves) o por un sistema de información programado por el emisor, o en su nombre, para que opere automáticamente; mientras que para determinar el tiempo en que se recibió el MD se señaló el momento en que ingrese en el sistema de información designado por el destinatario; o, cuando no se designó un sistema de referencia, el momento en que el destinatario obtenga dicha información. De tal forma que el artículo 1298-A del Código citado reconoció como medio de prueba a los MD a través de una presunción *iuris tantum* (salvo prueba en contrario) al evaluar la fuerza probatoria de estos, estimando primordialmente la fiabilidad del método en que aquellos fueron generados, archivados, conservados o comunicados.

En este orden, quedó precisada en la legislación mexicana la paternidad de los MD y su reconocimiento como prueba; no obstante, restaba definir la forma de acreditar que los medios de identificación efectivamente pertenecían al emisor; la manera en que el sistema de información fue programado por el emisor; qué métodos técnicos son fiables para la generación, conservación, archivo o comunicación los medios de generación; así como la forma de acreditar que los MD no fueron alterados; de ahí, la reforma del 29 de agosto de 2003 exclusiva al CCo, cuyo objeto fue modificar el reciente agregado capítulo I, del título segundo denominado "Mensaje de Datos", así como la incorporación del: *Capítulo II: de las Firmas (incluyendo a la FEA); Capítulo III: de los Prestadores de Servicios de Certificación*; y *Capítulo IV: Reconocimiento de Certificados y Firmas Electrónicas Extranjeras.*

[80] Es la copia de seguridad de uno o más archivos informáticos, que se hace, generalmente, para prevenir posibles pérdidas de información.
[81] En inglés, Personal Identification Number (PIN).

Finalmente, para que un mensaje de datos consignados en contratos pueda considerarse legalmente válido, se debe asegurar que la información en él contenida cuente con ciertas características, a saber: integridad, atribución y accesibilidad[82].

a) Integridad: Se desagrega en dos aspectos:

   i) Fiabilidad del método para generarla, comunicarla, recibirla o archivarla.
   ii) No alteración de la información contenida en él, la garantía de la conservación de los MD es de acuerdo a la *Norma Oficial Mexicana NOM-151-SCFI-2002: Prácticas comerciales: Requisitos que deben observarse para la conservación de Mensaje de Datos* (NOM-151).

b) Atribución: La manera en que las partes adquieren derechos y obligaciones en el contrato por ser quienes aseguran ser y expresan su voluntad libre de vicios y ello se hace a través de una firma electrónica o digital.

c) Accesibilidad: Que la información del MD del contrato pueda estar disponible al *usuario* para su ulterior consulta, acompañada de las dos características citadas (integridad y atribución). Los *usuarios* de estos MD pueden ir desde el emisor, receptor, juez, auditor, autoridades y todas aquellas personas que estén relacionadas con el MD. La forma en que se puede presentar es previa certificación de atribución e integridad por el PSC.

1.4.1.2. Norma técnica de estructuración de Mensajes de Datos

Los mensajes de datos pueden transmitirse entre sistemas de información de variadas formas y criterios, los más conocidos son: el correo electrónico, el *Intercambio Electrónico de Datos*[83] (*Electronic Data Interchange, EDI, por sus siglas en inglés)* y el MD bancarios SWIFT (*Society for Worldwide Interbank Financial Telecommunications).*

El *Intercambio Electrónico de Datos* fue la primera norma técnica de estructuración de MD en el comercio electrónico, surgió en los 80's[84] y permite la interacción de información estructurada, confiable, rápida, actualizada entre un sistema de origen, contenida en un formato estándar, a fin de que luego sea reconocida por una computadora para su procesamiento y almacenamiento en una computadora receptora.

Las normas técnicas de estructuración de MD se basan en la realización de transacciones comerciales de forma automatizada y en el intercambio de formatos normalizado de órdenes de compra, venta y pago realizadas de computadora a computadora, dentro de comunicaciones

[82] El recurso nemotécnico sugerido es, por sus vocales: **I**nd**A**g**A**r: **I**ntegridad, **A**tribución y **A**ccesiblidad.
[83] El articulo 2.2. y 2.3. del Modelo Europeo de Acuerdo de Intercambio Electrónico de Datos (EDI) del 19 de octubre de 1994 define al EDI como el intercambio electrónico de datos es la transferencia electrónica, Bastidas, Ma. Teresa; Novoa, Jorge y Pérez, Alfonso (coord.). La firma y la factura electrónicas: Entorno jurídico, fiscal e informático. Ed. Instituto Mexicano de Contadores Públicos (IMCP), 2004, México D.F., 295 pp.
[84] EDI es conocido como el embrión de e-business.

sectoriales y generalmente a través de redes cerradas así como de valor añadido cuyo uso es proporcionado por los proveedores de servicios.

Las transacciones tradicionales vía EDI requieren generalmente una larga fase de preparación y negociación entre las partes implicadas, para establecer los protocolos técnicos y administrativos y los acuerdos que les serán aplicables. Implica relaciones comerciales duraderas con cierto volumen de operaciones entre partes próximas, que son empresas muta y recíprocamente conocidas y dignas de confianza, pues sólo este tipo de relación justifica los altos costos de puesta en funcionamiento del EDI[85].

> *Un ejemplo claro de este proceso de intercambio de información electrónica, se presenta en la industria automotriz, donde la armadora solicita al proveedor de componentes cierta información comercial que ambos han realizado con alguna periodicidad en un fomento especial que sólo es manejado por la industria automotriz, a la cual, el proveedor deberá respetar. Sin embargo, el formato con el cual el proveedor almacena su información no es compatible con el primero, lo cual lo obligará a pasar su información a un medio electrónico con el formato solicitado y enviarlo a la armadora, que bajará esta información a su sistema, el cual lo reconocerá de inmediato. Esto facilitará la conciliación de operaciones entre ambos, agilizando por una parte, los procesos de pagos, compras y planeación de la producción entre otros; y, por el otro, mejorando los procesos de cobros, pedidos y producción haciéndolos más eficientes en sus procesos comerciales, sin importar el tamaño de empresa que tenga uno u otro[86].*

La importancia de una norma técnica radica en que tanto el iniciador como el destinatario acuerdan conformar sus MD de acuerdo a una forma estructurada de información convenida, donde tales normas técnicas no son más que programas informáticos que configuran un estándar en la forma de los mensajes a fin de eficiente procesos, esto generalmente se utiliza de empresario a empresario, en negocios B2B.

Frente a este tipo de transacciones se encuentran las normas que utilizan los empresarios frente a consumidores en negocios B2C, donde las normas técnicas le son impuestas al consumidor en su desconocimiento, ya que este ni siquiera llega a conocer el programa de computo o software que requiere para llevar a cabo una negociación comercial.

En cualquiera de los casos citados, la norma técnica implica que las partes adquieren la responsabilidad instrumental de contar con un medio definido para cumplir y se ha de comportar con diligencia de acuerdo al uso de la norma de referencia. A esta obligación se suma el efecto de que una norma técnica además de cerrar el entorno jurídico y comercial para el intercambio de datos, también excluye todas lo que no formen parte de dicha norma.

---

[85] Martínez Nadal, Apol·lònia : Comercio electrónico, firma digital y autoridades de certificación, 2001, 3ª ed., Madrid, Civitas, p.32.

[86] Arredondo Barrera, Luis. H, et al. “Los negocios electrónicos por Internet”, en Bastidas, Ma. Teresa; Novoa, Jorge y Pérez, Alfonso (coord.). La firma y la factura electrónicas: Entorno jurídico, fiscal e informático. Ed. Instituto Mexicano de Contadores Públicos (IMCP), 2004, México D.F., p. 65.

1.4.1.3. Firma Electrónica y Firma Digital

En principio, deben realizarse observaciones terminológicas relativas a firma electrónica y firma digital, podemos adelantar que se entide por firma digital a la Firma Electrónica Avanzada.

Internacionalmente, la forma en que se denomina una firma es muy relevante, pues desde un principio, se ha distinguido entre los términos firma electrónica y firma digital en las leyes alrededor del mundo.[87]

La primera ley sobre firma digital fue dictada en los en Estados Unidos bajo el nombre de *Utah Digital Signature Act*, publicada en mayo de 1995 por el Estado de Utah. En ella, se hacía referencia a la firma digital como FEA, la única diferencia es que en aquella no se reconocía la neutralidad tecnológica. A partir de ahí le sucedieron a siguientes regulaciones:

- La Guía de Firmas Digitales, elaborada por *American Bar Association* en agosto de 1996.
- *La Uniform Electronic Transactions Act*, emitida el 15 de agosto de 1997 por la Conferencia Nacional de Comisionados sobre Derecho Estatal Uniforme pero aprobada hasta el 30 de julio de 1999.
- *Electronic Signatures in Global and National Commerce Act,* emitida el 30 de junio de 2000, en vigor el 1º de octubre de 2000.
- *Uniform Computer Information Transactions Act*, aprobada el 4 de agosto de 2000 y desde ahí, se ha ido adoptando por los diversos estados de la Unión Americana.

Globalmente la denominación de firma digital es símil de FEA y se apoya en el empleo del método de criptografía[88] asimétrica o Infraestructura de Clave Pública (ICP) o Public Key Infrastructure en inglés (PKI) como forma de autenticación; mientras la designación de firma electrónica se refiere a las firmas que utilizan un identificador electrónico como forma de autenticación pero sin hacer uso de la ICP[89].

Ahora bien, la firma digital no debe ser confundida con la imagen digitalizada de una firma manuscrita o con una firma escrita en un bloc o *pad* electrónico. Por este motivo, en este trabajo se denominará a la firma digital y FEA indistintamente y a la firma electrónica a la que se refiere el uso internacional[90].

Para la Directiva 1999/93/CE de la Unión Europea[91] la firma electrónica es la firma digital, pero sí diferencia entre firma electrónica y la FEA, a través de las siguientes definiciones:

[87] Cfr. Wells, Thomas O. Electronic and Digital Signatures: In Search of a Standard. IT Professional, IEEE Educational Activities Department, (May-June 2000), 24-30 p.
[88] En el tema de criptografía se abundará en el capítulo tercero.
[89] Masse, David G. Economic modelling and risk management in public key infraestructura, versión 3.0, april 15, 1997, pág. 26, también consultable en http://masse.org/rsa97/index.html, fecha de acceso: 4 de noviembre de 2014.
[90] Atreya, Paine, Burnett, Hammond, Starrett y Wu, Digital Signatures. 2002, McGraw-Hill, Osborne, p. 4.
[91] Véanse los artículos 2.1 y 2.2 respectivamente de la Directiva 1999/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999 por la que se establece un marco comunitario para la firma electrónica, Diario Oficial de las Comunidades Europeas 19. 1. 2000.

Firma Electrónica: *Son los datos en forma electrónica ajenos a otros datos electrónicos o asociados de manera lógica con ellos, utilizados como medio de autenticación;*

Firma Electrónica Avanzada*: Es la firma electrónica que cumple los requisitos siguientes:*

a) Estar vinculada al firmante de manera única;
b) Permitir la identificación del firmante;
c) Haber sido creada utilizando medios que el firmante puede mantener bajo su exclusivo control;
d) Estar vinculada a los datos a que se refiere de modo que cualquier cambio ulterior de los mismos sea detectable;

Se debe precisar que esta Directiva 1999/93/CE de la firma electrónica es complementada con la Directiva 2000/31/CE relativa a ciertos aspectos jurídicos de los servicios de la sociedad de la información, particularmente del comercio electrónico en el mercado interior (libre circulación y libertad de establecimiento), la cual fue aprobada por la Unión Europea el del 8 de junio de 2000; con ella se equiparan a la contratación tradicional con la que es por medios electrónicos y se crea un marco general de tipo flexible, donde los Estados miembros gozan de una gran libertad de transposición de esta Directiva.

Nuestra legislación mercantil, en particular, el segundo párrafo del artículo 89 del CCo, considera a la firma digital o FEA como una especie de la firma electrónica y establece como otra firma a la FEA. Mientras que la *Norma Oficial Mexicana NOM-151-SCFI-2002, Prácticas comerciales-Requisitos que deben observarse para la conservación de mensajes de datos* (NOM-151) precisa que la firma digital es la FEA y la firma electrónica es una firma electrónica:

Código de Comercio:
Artículo 89. *Firma electrónica avanzada o fiable:*
(…)
En aquellas disposiciones que se refieran a ***firma digital****, se considerará a ésta como una especie de la Firma Electrónica.*

(énfasis añadido)

NOM-151-SCFI-2002:
Firma digital: *A la* ***firma electrónica*** *que está vinculada al firmante de manera única, permitiendo así su identificación, creada utilizando medios que aquél pueda mantener bajo su exclusivo control, estando vinculada a los datos a que se refiere de modo que cualquier cambio ulterior de los mismos sea detectable. La firma digital es una especie de firma electrónica que garantiza la autenticidad e integridad y la posibilidad de detectar cualquier cambio ulterior.*

(Énfasis añadido)

Firma electrónica: *A los datos en forma electrónica consignados en un mensaje de datos, o adjuntados, o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que dicho firmante aprueba la información recogida en el mensaje de datos. La firma electrónica establece la relación entre los datos y la identidad del firmante.*

En suma, ambas regulaciones establecen que la FEA (o firma digital) es una figura, y la firma electrónica es otra.

Por otra parte, el siguiente elemento conceptual objetivo que nos ocupa se relaciona con la seguridad y privacidad en la contratación mercantil: la firma electrónica, que es el elemento conceptual objetivo que se caracteriza por generar esa confianza como una certeza material jurídica; así lo advierte la CNUDMI en la Ley Modelo sobre Firma Electrónica de 2001, al considerar que:

> *Por **'firma electrónica'** se entenderán los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para **identificar** al firmante en relación con el mensaje de datos e indicar que el firmante **aprueba** la información recogida en el mensaje de datos;*
>
> ***(énfasis añadido)***

De la noción anterior se obtienen dos elementos de la firma electrónica, el primero es que una firma electrónica es una cierta tecnología que permite la **identificación**[92] de una persona, y segundo, que el signatario **aprueba o atribuye** su conformidad con la información ahí contenida, esto es, se conoce la persona que emite la declaración y se fija una certeza de que lo ahí contenido es voluntad del signatario.

Además, algunas empresas ofrecen firmas electrónicas que cumplen con una función adicional: codificar o cifrar el MD firmado a fin de que solo su destinatario pueda saber el MD que incluye.

Entonces, son cuatro las funciones de la firma electrónica:

a) Autenticación: Función de identificación y atribución del mensaje y de la información contenida en el mensaje.
b) Integridad respecto de la evidencia de apertura o alteración del mensaje entre el momento de su emisión firmada y el de su llegada a su destinatario; el MD no podrá ser modificado.
c) No repudio en origen: el emisor no puede negar haber enviado el mensaje.
d) Confidencialidad. Solo el emisor y el receptor pueden leer el mensaje.

Conviene precisar que generalmente cuando se habla de identificación de una persona en las transacciones electrónicas se refiere a ella como autenticación. No obstante, el término autenticación tiene sentidos ambiguos, en Estados Unidos de América es usado predominantemente para referirse a la identificación del signatario y este es el significado que prevalece. En cambio en Europa, el término es usado en relación a la verificación de la firma[93].

Existen una variedad de firmas electrónicas que se utilizan diariamente en el comercio electrónico. La forma más conocida y fácil de crear es aceptar un contrato dando un *clic* en "sí"

[92] Desde el punto de vista tecnológico, toda firma electrónica tiene como objeto el lograr la identificación de una persona, o su autenticación. Existen documentos que además de poder ir firmados por una persona, deben acreditar ser auténticos. Un sello estampado en un documento, por ejemplo, no es una firma; sin embargo, realiza en el documento una función de autenticación.

[93] Atreya, Paine, Burnett, Hammond, Starrett y Wu, Digital Signatures. 2002, McGraw-Hill, Osborne, p.3-5.

en un icono de computadora[94]. Otra forma consiste en que un individuo puede contratar con la firma de un e-mail y su nombre, incluso escribiendo una “X” o produciendo un sonido musical.

En la actualidad, un método común de crear una firma válida es el método de "secretos compartidos", este proceso implica el uso de contraseñas o números de tarjetas de crédito para evidenciar la intención de concluir una transacción. Por ejemplo, alguien podría comprar un disco de ópera y después de introducir su número de tarjeta de crédito tanto para pagar como para manifestar su intención de obligarse en la contratación[95].

En este sentido se puede clasificar las firmas electrónicas como firmas numéricas[96] y firmas biométricas. Como ejemplo de las firmas numéricas se encuentran la firma que se escribe con un lápiz especial en la pantalla de una computadora o en una *handheld*, el uso de Números de Identificación Personal (NIP) y versiones digitalizadas de firmas manuscritas.

La firma biométrica, es un método más complejo de firma de un contrato consistente en que la autenticación opera mediante muestreo y retención electrónica de una característica fisiológica de un usuario, permite la identificación de una persona por sus características físicas, de tal forma que cada que un usuario invoca el procedimiento de autenticación, la característica se mide de nuevo y se compara con el perfil que se tiene en el muestreo. La tecnología biométrica de autenticación puede identificar a una persona a través del reconocimiento de una huella dactilar, firma, voz o iris.

Una firma digital es por antonomasia es la FEA y requiere para su uso la generación de un par de claves privada y pública que por lo general te ofrece un Prestador de Servicios de Certificación (PSC) con los servicios de certificación de dicha firma[97]. Ese tipo de prestador puede crearla a través de una Infraestructura de Clave Pública (ICP) pues representa un tercero de confianza que comprueba y verifica la identidad de la persona que solicita el par de claves. Este tipo de firma se abordará a profunidad en el capítulo III.

---

[94] Harris Ominsky, Oops! I Just Clicked My Life Away, The Legal Intelligencer, July 26, 2000. Empresas como Amazon utilizaron de manera comercial los “clics” antes de la expedición de la primera regulación armonizada y general para todos los Estados Unidos de América respecto de la firma electrónica. Hasta antes de la llegada de E-Sign Act, Amazon sólo confiaba que frente a un conflicto las leyes estatales promulgadas sobre e firma electrónica asumiría el riesgo de que los tribunales federales o estatales le hicieran cumplir estos contratos. En otras palabras, Amazon no tenía ninguna indicación clara de que un “clic” del consumidor en el icono "Acepto" o "sí" obligarían a ambas partes a cumplir con los términos de un contrato.

[95] Stern, Jonathan E. The Electronic Signatures in Global and National Commerce Act, Berkeley Technology Law Journal, Volume 16, Issue 1 Article 21, January 2001, p. 5 y ss.

[96] De conformidad con la Ley Modelo de Firmas Electrónicas, las firmas electrónicas “numéricas” se crean y verifican utilizando la criptografía. Estas firmas utilizan la “criptografía de clave pública”, la cual generalmente emplea funciones algorítmicas para generar dos “claves” diferentes, pero que matemáticamente se relacionan entre sí. Una de esas “claves” se utiliza para crear una firma numérica o transformar datos en una forma aparentemente ininteligible, y la otra para verificar una firma numérica o devolver el mensaje a su forma original.

[97] Las claves públicas y privadas se hacen a través de la composición de complejos algoritmos matemáticos que disfrazan los mensajes de datos. Incluso, los algoritmos más comunes para la codificación se basan en grandes números primos que una vez que se multiplican entre sí para producir un nuevo número es virtualmente imposible determinar cuáles fueron los dos números primos que crearon ese nuevo número más grande, y no obstante se conocida la calve pública de un firmante, para verificar sus firmas, no podrían descubrir la clave privada del firmante y utilizarla para falsificar firmas digitales.

1.4.1.4. Sistemas de Información

La LMCE de 1996 establece que se entenderá por "sistema de información*" todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos.* La misma definición la recoge nuestro CCo, en el artículo 89 del *Título Segundo: Del Comercio Electrónico,* Capítulo I: *De los Mensajes de Datos.*

El concepto puede definirse mejor sin la repetición de la noción de sistema y en cambio usar las palabras medio o instrumento electrónico, *para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos.* Lo importante de la idea de los sistemas informáticos es que abarcan diversidad de instrumentos electrónicos y redes sin ser relevante su nivel o avance tecnológico, no obstante deben de contar con tres características:

a) Recuperabilidad de los MD,
b) Fiabilidad de los MD y
c) Control de los MD,

a) Recuperabilidad de los MD. El artículo 91 del CCo dispone que el momento de recepción de un MD se determinará como sigue:

> *I. Si el Destinatario ha designado un Sistema de Información para la recepción de Mensajes de Datos, ésta tendrá lugar en el momento en que **ingrese** en dicho Sistema de Información;*
> *II. De enviarse el Mensaje de Datos a un Sistema de Información del Destinatario que no sea el Sistema de Información designado, o de no haber un Sistema de Información designado, en el momento en que el Destinatario **recupere** el Mensaje de Datos, o*
> *III. Si el Destinatario no ha designado un Sistema de Información, la recepción tendrá lugar cuando el Mensaje de Datos **ingrese** a un Sistema de Información del Destinatario.*
> *Lo dispuesto en este artículo será aplicable aun cuando el Sistema de Información esté ubicado en un lugar distinto de donde se tenga por recibido el Mensaje de Datos conforme al artículo 94.*
> ***(Énfasis añadido)***

b) Fiabilidad de los mensajes de datos. El primer y último párrafo del artículo 97 del CCo dispone que:

> *Cuando la ley requiera o las partes acuerden la existencia de una Firma en relación con un MD, se entenderá satisfecho dicho requerimiento si se utiliza una Firma Electrónica que resulte apropiada para los fines para los cuales se generó o comunicó ese MD (…) Lo dispuesto en el presente artículo se entenderá sin perjuicio de la posibilidad de que cualquier persona demuestre de cualquier otra manera la **fiabilidad** de una Firma Electrónica; o presente pruebas de que una Firma Electrónica no es fiable.* ***(Énfasis añadido)***

c) Control de los MD. El artículo 93 del CCo dispone que *Cuando la ley exija la forma escrita para los actos, convenios o contratos, este supuesto se tendrá por cumplido tratándose de MD, siempre que la información en él contenida se mantenga íntegra y sea accesible para su ulterior consulta, sin importar el formato en el que se encuentre o represente.* Mientras que

el siguiente artículo 93 bis del mismo Código dispone que *cuando la ley requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho respecto a un MD: (…) II. De requerirse que la* ***información sea presentada****, si dicha información puede ser mostrada a la persona a la que se deba presentar.*

(Énfasis añadido)

En suma, todo sistema de información debe contar con las siguientes características para el tratamiento de los MD: **R**ecuperabilidad, **F**iabilidad y **C**ontrol de los MD (el recurso nemotécnico sugerido en razón de sus consonantes es: RFC).

1.4.1.5. Redes e Interconexión de Redes (Internet)

Toda red es un conjunto de sistemas de información, tomando en consideración que las redes de transmisión de datos comunican entre sí a varios sistemas de información de las partes contratantes se debe tener presente que estas no son de la propiedad de los sujetos contratantes y que tampoco se hallan bajo su control sino que lo están generalmente por las empresas de telecomunicaciones, por lo que en este sentido debe atenderse a la normatividad nacional en materia de telecomunicaciones, la cual otorga un trato distinto a cada tipo de red y sistema de información.

En este contexto, es de relevancia hacer notar que cuando existan problemas de seguridad en la configuración del comercio electrónico, el artículo 3 de la *Ley Federal de Telecomunicaciones y Radiodifusión* publicada el 14 de julio de 2014, no define como un sistema de información a la red de telecomunicaciones, a la red pública de telecomunicaciones ni a la red de telefonía pública; no obstante, identifica al sistema de información con dos de sus conceptos de redes: la red de acceso público (abierta) y la red acceso privado (cerrada).

Artículo 3.(…)
LVII: Red (privada) de telecomunicaciones: *sistema integrado por medios de transmisión, tales como canales o circuitos que utilicen bandas de frecuencias del espectro radioeléctrico, enlaces satelitales, cableados, redes de transmisión eléctrica o cualquier otro medio de transmisión, así como, en su caso, centrales, dispositivos de conmutación o cualquier equipo necesario.*
LVIII: Red pública de telecomunicaciones: *red de telecomunicaciones a través de la cual se explotan comercialmente servicios de telecomunicaciones. La red no comprende los equipos terminales de telecomunicaciones de los usuarios, ni las redes de telecomunicaciones que se encuentren más allá del punto de conexión terminal.*

En este sentido las redes son un tercero que participa en el comercio electrónico y que participa en la seguridad y secreto de los MD diligenciados a través de redes sin importar si son abiertas o cerradas ambos son sujetos de responsabilidad.

1.4.2. Elementos subjetivos

Los elementos subjetivos integran las partes intervinientes en la contratación electrónica, desde el precontrato hasta el cumplimiento de la negociación. Los elementos son:

- Emisor o Iniciador del MD o, en su caso, Firmante,
- Destinatario,
- Intermediarios
- Prestadores de Servicios de Certificación (PSC)

1.4.2.1. Emisor del mensaje de datos.

El artículo 89 del CCo define al "emisor" *como:*

> *Toda persona que, al tenor del MD, haya actuado a nombre propio o en cuyo nombre se haya enviado o generado ese mensaje antes de ser archivado, si éste es el caso, pero que no haya actuado a título de Intermediario.* Mientras que la noción de "firmante" establecida es: *la persona que posee los datos de la creación de la firma y que actúa en nombre propio o de la persona a la que representa.*

Conviene precisar las características y funciones de emisor[98]:

a) El emisor o iniciador es la persona física o moral que envía o genera un MD. Su perfil puede implicar hasta dos tipos de actitudes:

   - Originar y/o enviar un MD: Significa redactarlo previo a su envío o bien empleando una redacción automática del MD por medio de un agente electrónico sometido al control del iniciador[99].
   - Envío del MD: Es la acción electrónica necesaria para proceder a la expedición del mismo hacia su destinatario cuyo resultado se genera cuando el MD entra en el sistema de información que no esté bajo el control del emisor o persona que lo represente.

b) La identidad del iniciador debe deducirse del texto del propio MD y no de un documento distinto, en consecuencia el cumplimento de este requisito se logra cuando en el MD conste una firma electrónica, sea o no fiable, reconocida o avanzada y no existe otra forma diferente de conseguir que en el MD se identifique literalmente su iniciador y, por ende, ello será un elemento categórico para calificar la fuerza probatoria del MD (y más aún, el tipo de firma electrónica que sea adjuntada determinará el grado probatorio del MD).
c) El emisor o iniciador actuará por su cuenta, lo mismo aplica para el representante de la persona física o moral que expide el MD.
d) Habrá emisor o iniciador aun cuando el documento electrónico elaborado tenga un destinatario que no se relacione con la esfera jurídica de la persona física o moral del propio iniciador. Esta situación se clarifica en los casos en que se llevan a cabo contratos de

[98] Cfr. Illescas Ortíz, Rafael: Derecho de la contratación electrónica, 2009, 2ª ed., Madrid, Civitas Thomson Reuters, p. 121.
[99] Infra "2.4.1. Declaración de voluntad por sistemas informáticos expertos o de inteligencia artificial".

suministro *just in time*[100] en empresas como los frabricantes de comida rápida, Wal-Mart, los vendedores de computadora o Sears, que se llevan a cabo a través de actos electrificados sin destinatarios identificados, por lo que en estos casos habrá que hacer uso de la analogía parcial de estos documentos electrónicos que solicitan el abastecer o proveer de ciertos bienes o productos para asimilarlos con los MD.

e) El hecho de archivar un MD no convierte en emisor al individuo que decide archivarlo:[101]
   - El emisor suficientemente identificado es criterio determinante de la atribución a su persona del MD y su contenido.
   - El emisor posee la voluntad determinante de la aplicación y las modalidades del acuse de recibo del MD.
   - El iniciador y su conducta *ad hoc* son determinantes de la fijación exacta del lugar de la expedición del MD.

1.4.2.2. Destinatario.

El destinatario es la contraparte (o *addresee* en inglés). La noción que aparece de él en el artículo 89 de nuestro CCo es una copia de la LMCE 1996 y así lo define:

> *Persona designada por el emisor para recibir el Mensaje de Datos, pero que no esté actuando a título de Intermediario con respecto a dicho Mensaje*.

Existen dos componentes que configuran al destinatario del MD:

a) No basta la designación como destinatario en el MD, esto deja fuera a los intermediarios. Como excepción de los intermediarios, cuando se expiden MD destinados a la generalidad o se trata de ofertas *ad incertain personam o invitatio ad offerendum*, también denominadas *spam* (ofertas sin destinatario nombrado), no se configura la figura de destinatario, independientemente de que el caso sea valorado al tenor de su contenido.

b) Es obligación del emisor identificar de modo electrónico a su destinatario, es decir, debe poseer la dirección electrónica del destinatario y esta contenga el sistema de información para la recepción del MD; mientras que el destinatario está obligado a cumplir con una aptitud de atención y cuidado, ello lo compromete a mantener el equipo y dirección ofrecidos en estado operativo para la recepción del MD además de comprometerlo a revisarlos periódicamente y con la precisión que requiera el caso. Así también, le responsabiliza de aplicar el método de determinación de la procedencia del MD convenido, y cuando así lo hayan convenido, de acusar recibo.

[100] Las ventas al detalle empezaron a transformarse durante la década de los 80. Wal-Mart fue la pionera al iniciar la aplicación de sistemas Justo a Tiempo (Just in Time), en sus entregas, que fueran utilizados por los japoneses en sus industrias con tanto éxito. Con estos sistemas se consigue entregar productos en el momento exacto requerido y en la cantidad precisa. Sears de Canadá adoptó estas prácticas como un gran paso para la formación de grupos multifuncionales, que simplifican los procesos de pedido, recibo y pago por compras; de esa manera se reduce en forma radical el tiempo entre el pedido y la recepción.
[101] Ver los aspectos que se vinculan directamente con el emisor en los Artículos 13.1, 14.1, 15.1 y 15.4 de la LMCE.

1.4.2.3. Intermediarios.

El artículo 2, inciso e) de la "*Ley Modelo de la CNUDMI sobre Comercio Electrónico y su Guía para su incorporación al* derecho interno con el nuevo artículo 5 aprobado en 1998" define la figura de "intermediario" lo siguiente:

> *(…) en relación con un determinado mensaje de datos, se entenderá toda persona que,* ***actuando por cuenta de otra****, envíe, reciba o archive dicho mensaje o preste algún otro servicio con respecto a él.*
>
> ***(Énfasis añadido)***

1.4.2.4. Prestadores de Servicios de Certificación

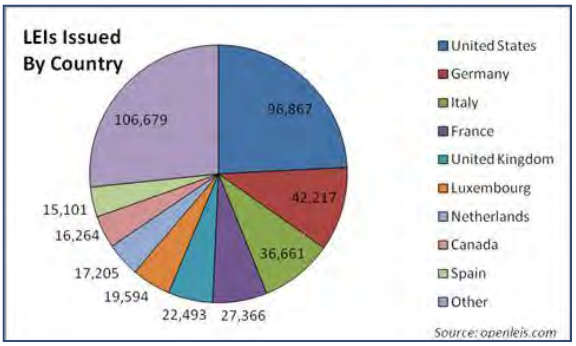
Hemos dicho ya que la FEA o firma digital requiere para su uso un par de claves, una privada y una pública[102] que por lo general se compran a un PSC, el cual es un tercero de confianza que comprueba y verifica la identidad de la persona que solicita el par de claves.

Existen los siguientes servicios de verificación de identidad basados en certificados digitales que lleva a cabo un PSC:

a) El proceso de verificación de identidad de personas y empresas cuando solicitan la FEA por primera vez, es una de los elementos más sólidos en el proceso de firma electrónica.
b) Actualmente existen esfuerzos internacionales para contar con estándares para la identificación de empresas, basados en procesos locales robustos y confiables.Uno de dichos esfuerzos es el conocido como Legal Entity Identifier (LEI) a través del cual se identifica a una empresa a nivel internacional y que pueda ser consultado a través de mecanismos en línea en cualquier parte del mundo. El identificador de entidad legal (LEI) es un código alfanumérico de 20 caracteres para identificar de forma única entidades jurídicamente independientes que se dedican a las transacciones financieras.

Legal Entity Identifier[103]**:** 261700WQICZMR9SKZA31
Legal Name: Pearl Hotels ZC 2013 Trust
Legal Address: C/O The Trust Company (Australia) Limited, Level 12 Angel Place, 123 Pitt Street, Sydney, 2000

Información de Global Financial Markets Association[104]



[102] Es relevante recalcar que las claves públicas y privadas se hacen a través de la composición de complejos algoritmos matemáticos que disfrazan los mensajes de datos. Sobre este tema se abundará en el punto siguiente.

[103] Caso real reproducido de la página web: http://www.lei-lookup.com/#!record;lei=261700WQICZMR9SKZA31;from=0, consultada el 2 de enero de 2016.

[104] Visible en http://www.gfma.org/initiatives/legal-entity-identifier-(lei)/legal-entity-identifier-(lei)/, consultada el 2 de marzo de 2015.

Para apoyar estos esfuerzos internacionales, en México se pordría aprovechar la infraestructura ya desarrollada por el SAT y usar el Registro Federal de Contribuyentes (RFC) así como el proceso de identificación de la FIEL.

Retomando el tema de los PSC, sus responsabilidades pueden abarcar el siguiente espectro:

a) Responsabilidad contractual y extracontractual, según el caso.
b) Responsabilidad objetiva, por culpa o negligencia.
c) Responsabilidad con inversión de la carga de la prueba al determinarse que habrá de ser el PSC quien ha de demostrar que actuó con la diligencia debida.

CAPÍTULO II. CONFIGURACIÓN, FORMACIÓN Y CUMPLIMIENTO CONTRACTUAL ELECTRÓNICO MEXICANO.

2.1. Supletoriedad sustantiva y adjetiva del Código de Comercio.

Los contratos en el sistema jurídico mexicano tienen un matiz consensual y formal, cuya razón de ser es que la configuración contractual electrónica se funda en dos regímenes: el primero, el régimen supletorio adjetivo del CCo mexicano, que a su vez se cimienta en el régimen general el derecho civil o común; el segundo, el régimen especial del derecho mercantil.

En este sentido Pina Vara expone que:

> *(…) mientras el derecho civil regula las relaciones jurídicas privadas en general, el derecho mercantil reglamenta una categoría particular de relaciones, personas y cosas: aquellas a las que la ley otorga la calidad de mercantiles*[105].

Por tal razón son limitadas las disposiciones respecto a las obligaciones y contratos mercantiles que contiene el CCo pero que el CCiF regula, de ahí que en aquél no exista una definición de obligación mercantil; no obstante, el propio artículo 2[106] y 81[107] del código mercantil[108] refiere que son aplicables a las obligaciones mercantiles la legislación civil, sólo cuando el CCo no disponga al respecto y no lo contradiga.

Del mismo modo, el derecho común es declarado regulación supletoria por el artículo 2º de la Ley General de Títulos y Operaciones de Crédito (LGTOC)[109].

Lo anterior no implica que el derecho mercantil sea inmutable pues, en algunos casos, la normatividad civil se adecúa al campo mercantil, dado que el derecho comercial no debe desligarse tampoco del acto de comercio, ni olvidar su carácter federal.

Dicha adecuación se vincula con la existencia de un amplio campo de actos mixtos que por su doble carácter poseen un elemento relacionado con el comercio y otro con el civil. Tal es el supuesto del contrato de compra-venta que puede ser civil para una de las partes y mercantil

---

[105] Vara, Pina. Derecho Mercantil Mexicano, 2005, 30ª ed., Porrúa, México, p. 5.

[106] Artículo 2o.- A falta de disposiciones de este ordenamiento y las demás leyes mercantiles, serán aplicables a los actos de comercio las del derecho común contenidas en el Código Civil aplicable en materia federal.

[107] Artículo 81.- Con las modificaciones y restricciones de este Código, serán aplicables a los actos mercantiles las disposiciones del derecho civil acerca de la capacidad de los contrayentes, y de las excepciones y causas que rescinden o invalidan los contratos.

[108] Artículo 2º de la Ley General de Títulos y Operaciones de Crédito:
Los actos y las operaciones a que se refiere el artículo anterior, se rigen:
I.- Por lo dispuesto en esta Ley, y en las demás leyes especiales, relativas; en su defecto,
II.- Por la Legislación Mercantil general; en su defecto,
III.- Por los usos bancarios y mercantiles y, en defecto de éstos,
IV.- Por el Derecho Común, declarándose aplicable en toda la República, para los fines de esta ley, el Código Civil del Distrito Federal.

[109] Independientemente que la les especial (LGTOC) deroga la ley general (CCo).

para la otra, toda vez que hasta antes de las reformas del 4 de enero de 1989 al artículo 1050[110] del CCo, en los conflictos suscitados entre las partes de una relación contractual, si la parte demanda fuera quien celebró el acto de comercio y la otra parte lo realizó como uno de naturaleza civil, sería procedente la vía mercantil; en tanto que si la parte demandada fuera quien celebró el acto civil, sería procedente la vía civil.

Sin embargo, después de las reformas del 4 de enero de 1989, todas las controversias derivadas de un acto mercantil, donde para una de las partes tenga naturaleza comercial y para la otra tenga naturaleza civil, se regirán por lo estatuido en las leyes mercantiles (artículo 1050 del CCo) [111]. Un caso de expeción es el contrato mercantil con garantía hipotecaria porque está regulado por una ley especial, la Ley de Instituciones de Crédito donde si demanda la institución de crédito es procedente la vía civil hipotecaria en razón de que las instituciones de crédito deben estar en posibilidad de ejercer la vía hipotecaria para hacerla efectiva ante el incumplimiento de la obligación principal que garantiza, pues de lo contrario se harían nugatorios los derechos de ejecución relativos al no encontrarse estatuido en la legislación mercantil un juicio que permita válidamente la ejecución de la garantía hipotecaria[112].

Ahora corresponde describir cómo funciona el régimen legal supletorio adjetivo, sobre su facilidad y claridad debe agradecerse al legislador, pues además de destacarlo en el artículo 1050 del CCo, lo complementa con los artículos 1049, 1051, 1052, 1053 y 1054[113] de dicho ordenamiento, para concluir que en todo caso la ley procesal supletoria será el CFPC.

Regulación procesal civil que expresamente estatuye que son juicios mercantiles los que tienen por objeto ventilar y decidir las controversias que, conforme a los artículos 4, 75 y 76 deriven de actos comerciales. Tal es el caso de la procedencia de la vía ordinaria mercantil tratándose de arrendamiento de inmuebles destinados a actividades comerciales siempre que se verifiquen para fines de especulación comercial. En sentido opuesto se da la improcedencia de la vía mercantil pero en el caso de arrendamiento de inmuebles entre comerciantes, pues aunque las partes que intervienen en el arrendamiento son comerciantes, si estos no realizan una especulación comercial con la renta del inmueble, no se imputa como un acto de especulación comercial, y por ende, se sujetará al Código de Civil.

---

[110] Artículo 1050.- Cuando conforme a las disposiciones mercantiles, para una de las partes que intervienen en un acto, éste tenga naturaleza comercial y para la otra tenga naturaleza civil la controversia que del mismo se derive se regirá conforme a las leyes mercantiles.

[111] Para más ejemplos sobre actos mixtos, véase Díaz Bravo, Arturo. Contratos mercantiles, 2012, México, Ed. De Iure, p. 4.

[112] Véase tesis: XIV.2o. J/13, Semanario Judicial de la Federación y su Gaceta, Novena Época, Tribunales Colegiados de Circuito, Tomo VI, Agosto de 1997, pág. 513, Jurisprudencia(Civil), de rubro: "CONTRATO MERCANTIL CON GARANTÍA HIPOTECARIA, CELEBRADO POR UNA INSTITUCIÓN DE CRÉDITO. VÍA MERCANTIL O HIPOTECARIA OPTATIVA (ARTÍCULO 72 DE LA LEY DE INSTITUCIONES DE CRÉDITO)."

[113] El artículo 1054 dice: En caso de no existir convenio de las partes sobre el procedimiento ante tribunales en los términos de los anteriores artículos, salvo que las leyes mercantiles establezcan un procedimiento especial o una supletoriedad expresa, los juicios mercantiles se regirán por las disposiciones de este libro y, en su defecto, se aplicará supletoriamente el Código Federal de Procedimientos Civiles y en caso de que no regule suficientemente la institución cuya supletoriedad se requiera, la ley de procedimientos local respectiva.

2.2. Contrato de comercio electrónico como fuente de obligaciones mercantiles.

La definición de obligación de Borja Soriano[114]:

> *(…) relación jurídica entre dos personas, en virtud de la cual una de ellas, llamada deudor, queda sujeta para otra, llamada acreedor, a una prestación o a una abstención de carácter patrimonial, que el acreedor puede exigir del deudor.*

Donde patrimonio es el conjunto de derechos y obligaciones susceptibles de valoración económica, y los derechos que conforman el patrimonio son los derechos reales[115] y personales.[116]

> *"Ciertos hechos de la naturaleza que el derecho, al relacionarlos con los seres humanos, les atribuye ciertas consecuencias jurídicas. Pues bien esos hechos humanos y los naturales son fuente general y primordial más amplia de donde brotan las obligaciones",* decía Ernesto Guitiérrez y González, para quien las fuentes de las obligaciones son el hecho jurídico en su doble visión de acto y hecho jurídico.

La visión estricta que muestra el libro cuarto, primera parte, título primero del CCo habla de las fuentes de las obligaciones, las cuales son:

1) Contrato (abarca desde el artículo 1792 hasta el 1859). Para hablar de contrato es necesario establecer que es un conveio, lo cual lo define el artículo 1792 cómo: "es el acuerdo de dos o más personas para crear, transferir, modificar o extinguir obligaciones". Posteriormente, el artículo 1793 define al contrato cómo: "los convenios que producen o transfieren las obligaciones y derechos". El código define lo que es el convenio en lato sensu, y también su división que es el contrato, aquí vemos que parte de la teoría francesa del acto jurídico.

2) Declaración Unilateral de voluntad (abarca desde el artículo1860 hasta el artículo 1881). El artículo 1860 por su parte define a la declaración cómo: "el hecho de ofrecer al público objetos en determinado precio, obliga al dueño a sostener su ofrecimiento", lo cual viene a complementar el artículo 1861, el cuál afirma: "el que anuncios u ofrecimientos hechos al público se comprometa a alguna prestación en favor de quien llene determinada condición o desempeñe cierto servicio, contrae la obligación de cumplir lo prometido".

3) Enriquecimiento ilegítimo (abarca desde el artículo 1882 hasta el artículo 1895). Dichos artículos señalan varias hipótesis de Enriquecimiento ilegítimo o ilícito, hemos de citar dos ejemplos. En el artículo 1883 dice: "cuando se reciba alguna cosa que no se tenía derecho de exigir y que por error ha sido indebidamente pagada, se tiene obligación de restituirla. También en el artículo 1885 que dice: si el que recibió la cosa con mala fe, la hubiere enajenado a un

[114] Borja Soriano, Manuel. Teoría general de las obligaciones, 11. ed., 2001, México, Ed. Porrúa, p. 89.
[115] Derecho real es aquel cuyo titular puede ejercerlo, hacerlo valer, frente a cualquier persona, respecto de una cosa.
[116] Derecho personal o de obligación, es el que una persona tiene para exigir a otra determinada, una prestación, un hecho o una abstención.

tercero que tuviere también mala fe, podrá el dueño reivindicarla y cobrar de uno u otro los daños y perjuicios".

4) Gestión de negocios (abarca desde el artículo1896 hasta el artículo 1909). El código civil no define la gestión de negocios, sin embargo es menester definirla como: "el que sin mandato y sin estar obligado, voluntariamente se encarga de un asunto de otro por su ausencia o cualquier otra causa, y conforme a los intereses del dueño del negocio". Al hablar del negocio, se hace alusión a un negocio jurídico**.**

5) Actos ilícitos (abarca desde el artículo 1910 hasta el 1934 BIS).
El artículo 1910, específica en que momentos se habla de un acto ilícito, no específica ni entra en detalles. El cual dice: "el que obrando ilícitamente o contra las buenas costumbre cause daño a otro, está obligado a repararlo…".

6) Riesgo profesional (abarca el artículo 1935 hasta el 1937). Habla acerca de la relación entre los patrones y los trabajadores, designando a los patrones como responsables de los accidentes del trabajo, de allí brota la obligación.

El suma, el contrato de comercio electrónico, forma parte de las seis fuentes de las obligaciones mercantiles de acuerdo con el CCiF, a saber: 1) los contratos 2) la declaración unilateral de voluntad, 3) el enriquecimiento ilegítimo, 4) la gestión de negocios, 5) el acto ilícito y 6) riesgo profesional (aunque el CCiF no enuncia en algún capítulo, la Ley es otra fuente).

1. *Contrato*
2. *Declaración unilateral de voluntad.*
3. *Enriquecimiento ilegítimo y su apéndice pago de lo indebido.*
4. *Gestión de negocios.*
5. *Hechos ilícitos.*
6. *Responsabilidad objetiva.*
7. *Le ley.*

Siendo así de evidente importancia la noción de obligaciones, es necesario recurrir a la ley supletoria civil aplicable pues se ha dicho que el derecho mercantil es principalmente, derecho de las obligaciones[117].

Así, los artículos 1792[118] y 1793[119] del CCiF, establecen que el contrato es una especie del género convenio, donde el contrato es un acuerdo de voluntad por el cual se producen o transfieren obligaciones o derechos y, por convenio es un acuerdo por el cual se modifican o extinguen las obligaciones. Aun con esta clara distinción el CCo se refiere indistintamente a convenio y contrato.

[117] Malagarriga, Carlos C.: Tratado elemental de derecho comercial, 3. ed.., 1963, Buenos Aires, Argentina, p. 47.
[118] El artículo 1792.- Convenio es el acuerdo de dos o más personas para crear, transferir, modificar o extinguir obligaciones.
[119] Artículo 1793.- Los convenios que producen o transfieren las obligaciones y derechos, toman el nombre de contratos.

No resulta trivial precisar que el contrato mercantil electrónico también se constituye de tres elementos esenciales del contrato civil:

1) el consentimiento,
2) el objeto y
3) la solemnidad, en los casos exigidos por la ley[120].

Mientras sus elementos de validez son:

1) la capacidad,
2) la ausencia de vicios en el consentimiento,
3) la licitud en el objeto, motivo o fin del acto y,
4) la forma en los casos en los que sea requerida por la ley [121]

Por lo que a la integración del consentimiento se refiere en la contratación mercantil, de inicio se presenta la oferta y para que el contrato se perfeccione debe recaerle una aceptación, donde la oferta será una declaración unilateral de voluntad hasta en tanto el aceptante no remita su aceptación; no obstante y dado que este tema es trascendental, será tratado en el apartado 2.4.

Por otra parte, en cuanto a las modalidades de los contratos electrónicos, no será una sorpresa el señalar que a los contratos mercantiles electrónicos le son aplicables las modalidades de las obligaciones civiles pero con ciertos bemoles, en atención a las reglas de las modalidades que se presumen en materia mercantil, pero no en la materia civil y viceversa; lo mismo sucede con los significados de algunos términos, que para el CCo representan algo distinto que para el CCiF.

Particularmente vamos a detallar las siguientes modalidades: solidaridad, onerosidad, moneda de pago, cláusula de ajuste, cláusula penal, término y mora, oferta o propuesta, aceptación, lugar de pago, especie y calidad, la adhesión mercantil, la prescripción y la caducidad y el pacto en exclusiva.

Ello independientemente de los contratos típicos y atípicos que se puedan realizar en materia mercantil, dentro de los nominados o típicos se consideran: el contrato de comisión, depósito mercantil, contrato de préstamo, compraventa, contrato de suministro y contrato estimatorio, contrato de transporte, contrato de seguro, contrato de fianza, contrato de edición, contrato de reporto, contrato bancario de depósito, descuento de créditos en libros, contrato de cuenta corriente, contrato de crédito habitación o avío y refaccionarios, contrato de prenda, contrato

[120] El artículo 1794 del CCiF.- Para la existencia del contrato se requiere: I. Consentimiento; II. Objeto que pueda ser materia del contrato.
[121] Artículo 1795 del CCiF.- El contrato puede ser invalidado:
I. Por incapacidad legal de las partes o de una de ellas;
II. Por vicios del consentimiento;
III. Porque su objeto, o su motivo o fin sea ilícito;
IV. Porque el consentimiento no se haya manifestado en la forma que la ley establece.

de fideicomiso, contrato de arrendamiento financiero, contratos bursátiles, contrato de asociación en participación y el contrato de franquicia.

2.3 Modalidades del contrato mercantil electrónico

La primer modalidad a tratar es la solidaridad en las obligaciones mercantiles, la cual se presume, a diferencia las que regula la materia civil que en su artículo 1988 señala que debe especificase cómo queda obligado el deudor. En este sentido un codeudor mercantil se obliga solidariamente porque el comercio requiere seguridad ante el pago del deudor, no obstante dicha presunción no se precisa específicamente, sistemáticamente el artículo 4 de la LGTOC junto con el 7 y 21 de la Ley General de Sociedades Mercantiles (LGSM).

Ahora bien, en cuanto a la modalidad de la moneda de pago, el contrato es ley entre las partes, por ende, se puede estipular fijando la moneda que los contratantes decidan, no obstante, que las obligaciones mercantiles se deban pagar en moneda nacional de acuerdo con el artículo 7 de la Ley Monetaria Mexicana (LMM).

Por lo que refiere al cumplimiento de las obligaciones mercantiles, el término es distinto que en el derecho civil, pues en esta área puede o no establecerse por el contratante, en cambio en la mercantil, se exige cumplir en un plazo el contrato, de hecho, lo más rápido posible. Asimismo, tampoco se concederán ningún plazo de gracia o cortesía, lo que sí sucede en el derecho civil. En el artículo 83 del CCo, las obligaciones que no tuvieren término prefijado por las partes o por las disposiciones de este Código, serán exigibles a los diez días después de contraídas, si sólo produjeren acción ordinaria, y al día inmediato si llevaren aparejada ejecución, salvo en el préstamo que lo regula el artículo 360, que será después de 30 días siguientes a la interpelación.

En cuanto al retardo en el cumplimiento de una obligación mercantil o mora, no es necesaria la interpelación del acreedor, sino que los efectos de la morosidad se dan al día siguiente del vencimiento del plazo. Sin embargo, el deudor puede probar que dicho retardo de la prestación es por causas ajenas y nadie está obligado al caso fortuito de acuerdo con el artículo 2111 del CCiF. Ahora, la consecuencia de la mora es la imposición de indemnización por los daños y perjuicios ocasionados de acuerdo con el artículo 2104 de este mismo ordenamiento. Como efectos de la morosidad, el artículo 85 establece que en el cumplimiento de las obligaciones mercantiles comenzarán, en los contratos que tuvieren día señalado para su cumplimiento por voluntad de las partes o por la ley, al día siguiente de su vencimiento; y en los que lo tengan, desde el día en que el acreedor le reclamare al deudor, judicial o extrajudicialmente ante escribano o testigos[122].

Hemos dicho ya que la oferta es una declaración unilateral de voluntad, que debe persistir hasta que sea aceptada o rechazada, pero a fin de que esta oferta obligue al proponente a celebrase,

[122] Cfr. Vara, Pina. Derecho Mercantil Mexicano, 2005, 30ª ed., Porrúa, México, p. 202 y ss.

debe hacerse de acuerdo a los términos prescritos, deberá incluir requisitos de forma y contenido, como lo son objeto, precio, duración.

La duración de la oferta (o propuesta) no es indefinida, debe fijarse un término, el cual puede ser convencional o legal, de acuerdo al CCiF, que en los artículos 1804 a 1810 establece que toda persona que propone a otra la celebración de un contrato, fijándole un plazo para aceptar, queda ligada por su oferta hasta la expiración del plazo; pero cuando la oferta se haga a una persona presente, sin fijación de plazo para aceptarla, el autor de la oferta queda desligado si la aceptación no se hace inmediatamente.

La misma regla se aplicará a la oferta hecha por teléfono o a través de cualquier otro medio electrónico, óptico o de cualquier otra tecnología que permita la expresión de la oferta y la aceptación de ésta en forma inmediata. Pero cuando la oferta se haga sin fijación de plazo a una persona no presente, el autor de la oferta quedará ligado durante tres días, además del tiempo necesario para la ida y vuelta regular del correo público, o del que se juzgue bastante, no habiendo correo público, según las distancias y la facilidad o dificultad de las comunicaciones.

La aceptación se realiza mediante una expresa declaración o por la propia ejecución. Se consideran requisitos de la aceptación, su claridad, donde se muestre que el destinatario de la oferta la acepto en todos sus términos, la aceptación de la oferta debe dirigirse al oferente, nunca a persona distinta. En este sentido, existe la aceptación expresa y tácita que regula el artículo 1803 del CCiF, el consentimiento será expreso cuando la voluntad se manifiesta verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos, y el tácito resultará de hechos o de actos que lo presupongan o que autoricen a presumirlo, excepto en los casos en que por ley o por convenio, la voluntad deba manifestarse expresamente.

Pero cualquiera que sea la forma de aceptación, debe ser lisa y llana, es decir, no se admite condición del aceptante, porque se le consideraría una nueva propuesta[123], además de que en ese momento el ofertante quedaría libre de su compromiso respecto de la oferta[124].

Ante la correspondencia de la oferta y la aceptación, el contrato se perfecciona. En el trabajo que nos ocupa, aquí aparece el punto más importante, el perfeccionamiento del contrato mercantil puede ser entre **presentes** y entre **ausentes.**

De conformidad con el artículo **1805** de CCiF, la oferta sin plazo entre **presentes** es aceptada **inmediatamente,** en caso de que no sea así, queda desvinculado el oferente[125]. De conformidad con el artículo **1806** de CCiF, si la oferta se hace olvidando señalar un plazo a una persona **ausente,** el oferente queda obligado a sostenerla durante tres días, más el tiempo necesario para ida y vuelta regular del correo público, o del que se juzgue bastante, no habiendo correo

[123] Vásquez Del Mercado Cordero, Óscar. Contratos mercantiles, 14. ed., 2006, México, Porrúa, p. 158 y 159.
[124] Véase articulo 1810 del CCiF.
[125] Véase artículo 1805 del CCiF.

público, según las distancias y la facilidad o dificultad de las comunicaciones. Esta noción evidentemente ya quedó en desuso, aunque sigue vigente.

En paralelo, el artículo 80 del CCo, dispone que los contratos celebrados por medios electrónicos, ópticos o de cualquier otra tecnología, quedan perfeccionados desde que se reciba la aceptación de la propuesta o las condiciones con que ésta fue modificada, el artículo 56 de la Ley Federal de Protección al Consumidor (LFPC), se establece que las ventas a domicilio se perfeccionan 5 días a partir de la firma, entre tanto el contrato puede revocarse.

Cuando se habla de la forma en material legal, en México se cuenta con un sistema equilibrado entre formalismo y consensualismo, pues para la celebración de un contrato no se requiere forma alguna a menos que la legislación disponga una forma particular.

La forma no es más que el medio requerido por los ordenamientos para la manifestación de la voluntad de los contratantes, se refiere a la creación del negocio jurídico, porque la ley la requiere para su validez. Aunque el artículo 78 y 79 del CCo, indiquen que en las convenciones mercantiles cada uno se obliga en la manera y términos que aparezcan que quiso obligarse, sin que la validez del acto comercial dependa de la observancia de formalidades o requisitos determinados, sí hay excepciones:

a) Los contratos que con arreglo a las leyes deban reducirse a escritura o requieran formas o solemnidades necesarias para su eficacia; y
b) Los contratos celebrados en país extranjero en que la ley exige escrituras, formas o solemnidades determinadas para su validez, aunque no las exija la ley mexicana.

Además agrega, que en uno y otro caso, los contratos que no llenen las circunstancias respectivamente requeridas, no producirán obligación ni acción en juicio.

En lo que concierne al lugar de pago, el artículo 86 del CCo detalla que las obligaciones mercantiles deben cumplirse en el lugar determinado en el contrato o, en aquél que según la naturaleza del negocio o la intención de las partes debe considerarse adecuado al efecto, por consentimiento de aquellas o arbitro judicial.

Cuando se fija en dónde debe cumplirse el contrato, la parte obligada habrá de hacerlo de la manera señalada. Ahora bien, el artículo 1104 del ordenamiento citado, dispone que salvo lo dispuesto en el artículo 1093[126] en el orden en que un juez es competente es la siguiente: el del lugar que el demandado haya designado para ser requerido judicialmente de pago; el del lugar designado en el contrato para el cumplimiento de la obligación; y el del domicilio del demandado. Si tuviere varios domicilios, el juez competente será el que elija el actor.

[126] Artículo 1093.- Hay sumisión expresa cuando los interesados renuncien clara y terminantemente al fuero que la ley les concede, y para el caso de controversia, señalan como tribunales competentes a los del domicilio de cualquiera de las partes, del lugar de cumplimiento de alguna de las obligaciones contraídas, o de la ubicación de la cosa. En el caso de que se acuerden pluralidad de jurisdicciones, el actor podrá elegir a un tribunal competente entre cualquiera de ellas.

Tratándose de personas morales, para los efectos de esta fracción, se considerará como su domicilio aquel donde se ubique su administración.

Si en el contrato no se precisó la especie y calidad del objeto que ha de entregarse, no podrá exigírsele al deudor otra cosa que la entrega de mercancías de especie y calidad media, aunque cuando el obligado cuente con objetos o mercancías de mayor calidad[127]. Y cuando se refiere a calidad y especie deben de poder ser precisadas en sus medidas o nivel o calidades.

La cláusula penal en los contratos mercantiles es muy particular de la materia, se da cuando existe incumplimiento de una de las partes y se regula por el artículo 1949 del CCiF. El perjudicado podrá escoger entre exigir el cumplimiento o la resolución de la obligación, con el resarcimiento de daños y perjuicios en ambos casos. También se podrá pedir la resolución de las obligaciones aún después de haber optado por el cumplimiento, cuando éste resultare imposible. Pero a ello debe añadirse lo dispuesto por el artículo 88 del CCo, que establece que en el contrato mercantil en que se fijare pena de indemnización contra el que no lo cumpliere, la parte perjudicada podrá exigir el cumplimiento del contrato o la pena prescrita; pero utilizando una de estas dos acciones, quedará extinguida la otra. Frente a esta posición mercantil, el derecho civil establece una pena de acuerdo al artículo 1846, para ejercitar la acción para exigir el cumplimiento de la obligación o el pago de la pena, pero no ambos; a menos que aparezca haber estipulado la pena por el simple retardo en el cumplimiento de la obligación, o porque ésta no se preste de la manera convenida.

Por último, la prescripción en los contratos mercantiles se refiere a la falta de acción por el titular de los derechos que de ellos surgen. En este sentido el CCo establece de los artículos 1039 a 1042, que los términos fijados para el ejercicio de acciones procedentes de actos mercantiles, serán fatales, sin que contra ellos se dé restitución. La prescripción mercantil negativa se contará desde el día en que la acción pudo ser legalmente ejercitada en juicio.

La prescripción se interrumpirá por la demanda u otro cualquier género de interpelación judicial hecha al deudor, por el reconocimiento de las obligaciones, o por la renovación del documento en que se funde el derecho del acreedor. Así también, empezará a contarse el nuevo término de la prescripción en caso de reconocimiento de las obligaciones, desde el día que se haga; en el de renovación desde la fecha del nuevo título; y si en él se hubiere prorrogado el plazo del cumplimiento de la obligación, desde que éste hubiere vencido.

2.4. Declaración de voluntad electrónica

Antes del 29 de mayo de 2000 no existía señalamiento respecto a si la manifestación de voluntad expresada en medios electrónicos era considerada realizada entre personas presentes o entre ausentes; no obstante, la forma de solucionar dicha laguna era asemejar dicha manifestación electrónica de la voluntad a una expresada por teléfono, cuya implicación consistía en que el consentimiento era otorgado entre personas presentes y conforme a esta

[127] Véase el artículo 87del Código de Comercio.

regla se procedía a aplicar el entonces Código Civil para el Distrito Federal en Materia Común y para toda la República en Materia Federal.

Además, si llegado el caso daba inicio un juicio donde el oferente de un bien o servicio en Internet recibía una aceptación por parte del destinatario por esa mismo vía electrónica, el instrumento para acreditar la transacción electrónica y determinar tanto la fecha como la forma del perfeccionamiento del contrato era con la impresión de las comunicaciones efectuadas a través de Internet o de su correo electrónico, lo que implicaba que el juzgador, de conformidad con el artículo 1205 del CCo debía evaluar la naturaleza de dichas impresiones; como resultado de tal valoración, el juez aplicaba la tesis de rubro: *Documentos simples. Conforme al Código de Comercio anterior a la reforma de veinticuatro de mayo de mil novecientos noventa y seis, son las impresiones que se afirma provienen de páginas de Internet*[128] ; lo que significaba que las impresiones provenientes de correos electrónicos o Internet no eran consideradas como documentos privados, pues no figuraban en originales y, por ello, el juzgador para corroborarlo, debía de tener ofrecidos otros elementos como confesionales, testimoniales u otros materiales de convicción.

Antes de la citada reforma del 29 de mayo de 2000, el CCiF establecía que la comunicación por medios electrónicos era considerada realizada entre ausentes, a menos que se haga a través de mensajería instantánea o chat[129] como: Yahoo! Messenger, Hangouts (antes Google Talk), Facebook Messenger, Skype, Line, Telegram y Whatsapp; pero después del 29 de mayo de 2000, el artículo 1805[130] del CCiF definió que la comunicación por medios electrónicos era considerada entre realizada entre presentes.

En este sentido debe atenderse también a que el artículo 1806 CCiF señala:

> *Cuando la oferta se haga sin fijación de plazo a una persona no presente, el autor de la oferta quedará ligado durante tres días, además del tiempo necesario para la ida y vuelta regular del correo público, o del que se juzgue bastante, no habiendo correo público, según las distancias y la facilidad o dificultad de las comunicaciones.*

Mientras que el artículo 80 del CCo precisa que:

> ***Artículo 80.-*** *Los convenios y contratos mercantiles que se celebren por correspondencia, telégrafo, o mediante el uso de medios electrónicos, ópticos o de cualquier otra tecnología, quedarán perfeccionados desde que se reciba la aceptación de la propuesta o las condiciones con que ésta fuere modificada.*

[128] Véase Semanario Judicial de la Federación y su Gaceta, Tomo XV, Febrero de 2002, Material Civil, Novena Época, Página: 806.

[129] Requiere el uso de un cliente de mensajería instantánea que realiza el servicio y se diferencia del correo electrónico.

[130] Artículo 1805.- Cuando la oferta se haga a una persona presente, sin fijación de plazo para aceptarla, el autor de la oferta queda desligado si la aceptación no se hace inmediatamente. La misma regla se aplicará a la oferta hecha por teléfono o a través de cualquier otro medio electrónico, óptico o de cualquier otra tecnología que permita la expresión de la oferta y la aceptación de ésta en forma inmediata.

Las anteriores precisiones en la reforma realizada por los legisladores provocó muchos disentimientos entre los doctrinarios y abogados, la cual se vio reflejada en la postura que cada uno tomaba al elegir uno de los sistemas o teorías que consideran un momento distinto para el perfeccionamiento del consentimiento respecto de personas no presentes, a saber:[131]

- **I.** Teoría de la declaración.- En cuanto el destinatario de la oferta se entera de la misma y mediante cualquier signo, declara, que acepta la oferta, aunque el oferente aún no esté enterado de la respuesta.
- **II.** Teoría de la expedición.- Cuando el destinatario de la oferta declara y expide al oferente su respuesta y sale de su control (sistema adoptado por el CCo antes de la reforma del 29 de mayo de 2000)
- **III.** Teoría de la recepción.- El contrato queda formado en el momento el oferente recibe la respuesta del aceptante, esto es, desde que la aceptación está a su disposición (sistema adoptado por el CCiF y el CCo desde la reforma del 29 de mayo de 2000)
- **IV.** Teoría de la información.- Cuando el oferente tiene pleno conocimiento, se informa, de la respuesta del aceptante.

El CCiF simpatiza con la teoría de la **recepción** cuya regulación se fija en el artículo 1807: *El contrato se forma en el momento en que el proponente reciba la aceptación, estando ligado por su oferta, según los artículos precedentes.* Por el contrario, el artículo 80 del CCo antes del Decreto de reformas del 29 de mayo de 2000, concordaba con la teoría de la **expedición** y posteriormente, esto es después del multicitado decreto de reformas se siguió la teoría de la **recepción:**

> ***Artículo 80 (antes del 29 de mayo de 2000):*** *Los contratos mercantiles que se celebren por correspondencia, quedarán perfeccionados desde que se* ***conteste*** *aceptando la propuesta o las condiciones con que ésta fuera modificada (Teoría de la expedición).*
>
> ***Artículo 80 (después del 29 de mayo de 2000)****: Los convenios y contratos mercantiles que se celebren por correspondencia, telégrafo, o mediante el uso de medios electrónicos, ópticos o de cualquier otra tecnología, quedarán perfeccionados desde que se reciba la aceptación de la propuesta o las condiciones con que ésta fuere modificada (Teoría de la recepción).*

Según el maestro Acosta Romero, el vigente artículo 80 del CCo se funda en la **teoría de recepción** como lo venía haciendo el artículo 1807 del CCiF pues anteriormente, el mismo artículo se basaba en la **teoría de la expedición** como forma en que el aceptante manifestaba su consentimiento. La finalidad de tan acertada reforma es otorgar certeza del momento en que se perfeccionan los contratos electrónicos, y con ello, la seguridad de su validez, de tal forma que se pueda saber en qué momento quedó expresado el consentimiento.

En este sentido, es escasa la jurisprudencia elaborada por nuestros tribunales federales, excepción hecha de los casos de rubros: *Contratos mercantiles celebrados a distancia y pedidos*

[131] Gutiérrez y González, Ernesto. Derecho de las obligaciones, 14ª ed., 2002, México, Ed. Porrúa, p. 285 y ss.

por teléfono[132] *y Contratos mercantiles celebrados por correspondencia. Su perfeccionamiento*[133].

La declaración de voluntad electrónica se traduce en el MD o documento electrónico con diferentes composiciones[134] y métodos de firma electrónica y/o digital del iniciador y destinatario respectivamente.

El acuerdo o responsabilidades comunicadas mediante el MD puede ser unilateral o bilateral, donde los efectos jurídicos de la declaración de voluntad son idénticos a los generados por una que se realizó de manera escrita.

Actualmente las ofertas públicas de venta de productos o servicios pueden efectuarse también por estos medios electrónicos, la declaración unilateral de la voluntad (oferta) constituye una de las fuentes de las obligaciones dispuestas por el CCiF, específicamente en el artículo 1860, que establece que le ofrecimiento al público de objetos en determinado precio, obliga al oferente a sostenerlo; incluso, el numeral 1805 del mismo ordenamiento determina que cuando la oferta se realice por conducto de medios electrónicos sin fijar un plazo para aceptarla, el autor de ella queda desligado si la aceptación no se hace inmediatamente. Mientras que en el supuesto del comercio en línea, quedarán desvinculados de su oferta, si la persona que ingresa al sitio web en línea no emite su aceptación en forma inmediata.

> ***Artículo 1805.-*** *Cuando la oferta se haga a una persona presente, sin fijación de plazo para aceptarla, el autor de la oferta queda desligado si la aceptación no se hace inmediatamente. La misma regla se aplicará a la oferta hecha por teléfono o a través de cualquier otro medio electrónico, óptico o de cualquier otra tecnología que permita la expresión de la oferta y la aceptación de ésta en forma inmediata.*
>
> ***Artículo 1860.-*** *El hecho de ofrecer al público objetos en determinado precio, obliga al dueño a sostener su ofrecimiento.*

No pasa inadvertida la forma en que la Ley Modelo CNUDMI de Comercio Electrónico incorporó en su artículo 13 normas sobre la atribución de los MD, su representación en un entorno electrónico y responsabilidad derivada de las conductas ilícitas o negligentes relacionadas con ellos, dichas normas se limitan a seis reglas:

> ***Artículo 13.*** *— Atribución de los mensajes de datos*
> ***1)*** *Un MD proviene del iniciador si ha sido enviado por el propio iniciador.*
> ***2)*** *En las relaciones entre el iniciador y el destinatario, se entenderá que un mensaje de datos proviene del iniciador si ha sido enviado:*
> *a) Por alguna persona facultada para actuar en nombre del iniciador respecto de ese mensaje; o*

[132] Véase Semanario Judicial de la Federación, Volumen 73, Cuarta Parte, Séptima Época, Página: 19.
[133] Véase Semanario Judicial de la Federación, Volumen 63, Cuarta Parte, Séptima Época, Página: 18.
[134] Aunque el más conocido es EDI, en este punto se incluyen todo tipo de formas de mensaje de datos que sirvan para el intercambio de información industrial, comercial, financiera, médica, administrativa, fabril o cualquier otro tipo similar de información estructurada.

b) Por un sistema de información programado por el iniciador o en su nombre para que opere automáticamente.
***3**) En las relaciones entre el iniciador y el destinatario, el destinatario tendrá derecho a considerar que un **mensaje de datos proviene del iniciador, y a actuar en consecuencia,** cuando:*
a) Para comprobar que el mensaje provenía del iniciador, el destinatario haya aplicado adecuadamente un procedimiento aceptado previamente por el iniciador con ese fin; o
b) El mensaje de datos que reciba el destinatario resulte de los actos de una persona cuya relación con el iniciador, o con algún mandatario suyo, le haya dado acceso a algún método utilizado por el iniciador para identificar un mensaje de datos como propio.
***4)** El párrafo 3) no se aplicará:*
a) A partir del momento en que el destinatario haya sido informado por el iniciador de que el mensaje de datos no provenía del iniciador y haya dispuesto de un plazo razonable para actuar en consecuencia; o
b) En los casos previstos en el inciso b) del párrafo 3), desde el momento en que el destinatario sepa, o debiera saber de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que el mensaje de datos no provenía del iniciador.
***5)** Siempre que un mensaje de datos provenga del iniciador o que se entienda que proviene de él, o siempre que el destinatario tenga derecho a actuar con arreglo a este supuesto, en las relaciones entre el iniciador y el destinatario, el destinatario tendrá derecho a considerar que el mensaje de datos recibido corresponde al que quería enviar el iniciador, y podrá actuar en consecuencia. El destinatario no gozará de este derecho si sabía, o hubiera sabido de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que la transmisión había dado lugar a algún error en el mensaje de datos recibido.*
***6)** El destinatario tendrá derecho a considerar que cada mensaje de datos recibido es un mensaje de datos separado y a actuar en consecuencia, salvo en la medida en que duplique otro mensaje de datos, y que el destinatario sepa, o debiera saber de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que el mensaje de datos era un duplicado.*

En cuanto a la primera regla que se cita en el párrafo precedente, se considera que la relevancia de la regla de procedencia primaria en materia de atribución de un MD radica en que un contacto nuevo, por primera vez, envía un MD, el cual es una representación fiel de la regla fijada en el mundo escrito y oral en que las obligaciones tienen fuerza de ley.

Respecto a la segunda pauta, que reza que en las relaciones entre el iniciador y el destinatario, se entenderá que un MD proviene del iniciador si ha sido enviado: a) por alguna persona facultada para actuar en nombre del iniciador respecto de ese mensaje; o b) por un sistema de información programado por el iniciador o en su nombre para que opere automáticamente; el destinatario tiene derecho a considerar que el MD proviene del iniciador cuando haya aplicado adecuadamente un procedimiento de comprobación del origen del mensaje cuya aceptación haya sido otorgada por el iniciador. A propósito del método que haya sido utilizado por el iniciador, el tercero o intermediario o el propio destinatario, lo relevante es que exista un método aceptado por el iniciador expresa o tácitamente y que hubiera habido una comprobación efectuada por el destinatario. En este respecto, la confirmación imputa al destinatario el derecho a actuar en relación al contenido del MD, lo mismo sucede cuando se le imputa al iniciador.

En cuanto a la tercera regla, en las relaciones entre el iniciador y el destinatario, el destinatario tendrá derecho a considerar que un MD proviene del iniciador, y a actuar en consecuencia, cuando: a) Para comprobar que el mensaje provenía del iniciador, el destinatario haya aplicado adecuadamente un procedimiento aceptado previamente por el iniciador con ese fin; o b) El MD que reciba el destinatario resulte de los actos de una persona cuya relación con el iniciador, o con algún mandatario suyo, le haya dado acceso a algún método utilizado por el iniciador para identificar un MD como propio. En suma, en sentido contrario desde el momento en que el destinatario haya sido informado por el iniciador de que el mensaje no proviene de él, le exige a aquel a suspender toda actuación derivada; la interrupción será a partir de que transcurrió el plazo razonable a partir de que el destinatario tuvo conocimiento del repudio del MD. No obstante, las gestiones dirigidas por el destinatario en relación con el MD antes de ser informado de su repudio, crean efectos jurídicos entre las partes y obligan al iniciador como al destinario del falso MD; siempre que sean coherentes con el asunto y su asignación.

Respecto a la cuarta norma, el párrafo 3) no se aplicará:

a) A partir del momento en que el destinatario haya sido informado por el iniciador de que el MD no provenía del iniciador y haya dispuesto de un plazo razonable para actuar en consecuencia; o
b) En los casos previstos en el inciso b) del párrafo 3), desde el momento en que el destinatario sepa, o debiera saber de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que el MD no provenía del iniciador.

Semejante similitud debe ser adoptada en los casos en que la información absurda o incoherente de la atribución de un MD es otorgada al destinatario por un intermedio o un tercero confiable vinculados de alguna forma con la circulación del MD incoherente o absurdo.

En cuanto a la quinta regla, siempre que un MD provenga del iniciador o que se entienda que proviene de él, o siempre que el destinatario tenga derecho a actuar con arreglo a este supuesto, en las relaciones entre el iniciador y el destinatario, el destinatario tendrá derecho a considerar que el MD recibido corresponde al que quería enviar el iniciador, y podrá actuar en consecuencia. El destinatario no gozará de este derecho si sabía, o hubiera sabido de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que la transmisión había dado lugar a algún error en el MD recibido. Lo anterior se traduce en que cuando el iniciador reconoce la procedencia de un MD con posterioridad a su recepción por el destinatario y cuyo contenido muestra equivocaciones, la norma presume un vínculo entre el iniciador y el contenido del MD. Aquí se está sujetando a la teoría del error en la formación del negocio jurídico, quien lo genera asume sus efectos, donde los errores que se revelen han de ser objetivos, con ello se habla de una problema de redes, estándares tecnológicos o computadoras, en razón de que la manifestación de un error subjetivo del iniciador del mensaje de datos no se produce en la práctica en atención a que el iniciador se encuentra a distancia.

Respecto al sexto y último precepto, el destinatario tendrá derecho a considerar que cada MD recibido es un MD separado y a actuar en consecuencia, salvo en la medida en que duplique

otro MD, y que el destinatario sepa, o debiera saber de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que el MD era un duplicado. También existe la posibilidad de que se genere una multiplicidad de MD, quizás una duplicación de MD, cuya similitud en el contenido reflejen que son contrataciones electrónicas autónomas y distintas unas de otras. Este caso es un supuesto de error por medio del cual el destinatario tendrá derecho a considerar que cada mensaje de datos recibido es uno separado y por ende, actuar en consecuencia. Es evidente que este supuesto requiere de una actitud diligente por parte del iniciador al momento de enviar un MD, esto es, tanto de prevenir que el envío duplicado de mensajes como la precisión de que existe la intención (por algún motivo) de enviar por duplicado algún mensaje.

2.4.1. Declaración de voluntad por sistemas informáticos expertos o de inteligencia artificial.

Cuando se pone en marcha un sistema informático experto, un consumidor o un proveedor pueden perfeccionar negocios jurídicos. La respuesta de una computadora de un sistema informático experto forma parte de la voluntad del usuario y realmente existe una voluntad manifestada, a continuación detallamos el por qué.

La inteligencia artificial o un sistema informático experto permite que una máquina pueda simular los procesos de razonamiento que caracterizan al cerebro humano, de tal forma que recoge el conocimiento y lo emplea para emular el proceso de intelectual humano, tales como el juicio o sus criterios para decidir determinadas situaciones, la forma en que lo hace es a través de la automatización del proceso de toma de decisiones.

Un sistema experto consta de los siguientes elementos: una base de conocimientos, un motor de inferencia y un procedimiento de diálogo con el usuario[135], cada uno se describen así:

> ***1) la base de conocimiento****- equivale a la memoria humana, en el sentido de que almacena toda la información disponible para realizar el proceso deductivo.*
> ***2) el motor de inferencia-*** *reproduce las operaciones lógicas necesarias -algoritmos- para llegar a las conclusiones deseadas frente a un problema concreto.*
> ***3) El procedimiento -o interfase- de diálogo con el usuario****, consiste en el medio comunicacional a través del cual el sistema recibe información de parte de los sujetos, tanto sobre la base de conocimientos como sobre los procesos lógicos a realizar, formula preguntas necesarias para afinar sus resultados y finalmente entrega la información obtenida como resultado de la actividad informática.*

El acto de voluntad determinante es la activación del sistema, la cual concreta la voluntad expresada en el momento de la programación del sistema, que se encuentra latente en el programa, lo que origina que desde el momento que el contratante da por bueno el sistema y lo activa, convalida cualquier futuro proceso del sistema que actúe fiel a su programación y sin errores.

---

[135] Hess Araya, Christian. 2001. "Inteligencia artificial y Derecho", Revista Electrónica de Derecho Informático. N° 39. Ed. Vlex,http://vlex.com/redi.

Ejemplos típicos en la vida diaria del uso de estos sistemas expertos informáticos se muestra con las empresas que emiten órdenes de compra o con los corredores de bolsa que programan sus sistemas para comprar las acciones y venderlas en momentos en que suban o bajen de precio[136]

En la contratación realizada por computadoras a través de tales sistemas la voluntad de las partes se lleva a cabo en dos momentos: en la elaboración del programa y en la fase de comunicación o de transmisión de la voluntad[137], normalmente, un sistema experto no requiere confirmación de la ejecución de la orden en el momento que constate el cumplimiento de las condiciones predefinidas y, subsiguientemente, podrá emitir de manera independiente la orden que significará el perfeccionamiento del contrato.

El método precedente conforma la expresión de una voluntad, pero puede haber sido formulada en términos tan amplios y su ejecución rodeada de circunstancias tan extraordinarias a la decisión, que costará ver cumplidas en el proceso de adopción y transmisión decisional informático las condiciones que se exigen a la voluntad como elemento de validez en la teoría del negocio jurídico.

En cuanto al cumplimiento de la voluntad como requisito de validez del contrato mercantil hecho por medio de sistemas expertos se aplica una visión de responsabilidad y en la admisión del riesgo por el iniciador o destinatario respecto del consentimiento contractual, y por ende, de una autodeterminación y de la autorresponsabilidad. Sin embargo, dicha explicación se vuelve vana cuando nos referimos al CCiF, el cual regula que el consentimiento será expreso cuando la voluntad se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos.

Por ello, nos parece más relevante referirnos a que una persona que decide contratar por medio de un sistema experto debe, con su voluntad, asumir las consecuencias del negocio que activa, sobre todo si se considera que los riesgos de tal proceso también pueden ser perfectamente acotados mediante instrucciones que pueden entregarse al mismo programa informático como, por ejemplo, en el caso que hemos propuesto de compra y venta de acciones en la bolsa electrónica, señalándose al sistema: Nunca adquirir arriba del precio X o nunca vender por debajo del precio Y, sin previa consulta al usuario. De ese modo ante circunstancias de mercado que el mismo sistema pudiera percibir como anormales pediría confirmaciones personalizadas al sujeto cuya voluntad ha de declarar.

---

[136] Pinochet Olave, Ruperto. Los sistemas informáticos expertos de toma de decisiones y la voluntad como elemento de validez del contrato electrónico, Revista Ius et Praxis v.9 n.2, p p. 161-184, Talca (Chile), 2003, disponible en: http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-00122003000200005&lng=es&nrm=iso, accedido en 20 enero 2015.

[137] Carrascosa, Valentín, Pozo; Ma. A., Rodríguez, E.P. La Contratación Informática: El Nuevo Horizonte Contractual. Los Contratos Electrónicos e Informáticos, 1999, Granada: Segunda Edición, Editorial Comares, p. 15.

Actualmente, las partes contratantes que acuerdan mediante tecnologías lo hacen en mejores circunstancias de las que eran posibles en la contratación tradicional, ello debido a que tales técnicas permiten un conocimiento mayor, más rápido y más barato de las diversas variables que pueden afectar el proceso de toma de decisiones.

2.5. Representación electrónica.

Las actuaciones típicas que se pueden presentar en materia de representación electrónica son por lo menos tres:

a) Acción del iniciador de un MD por medio de un representante
b) Acción como parte de los procesos de formación y ejecución contractual de un sistema informático experto o de inteligencia artificial.
c) Acción de intermediación, jurídica y no electrónicamente entendida, en operaciones electrónicas.

Es preciso mencionar, que en el primer caso, el jurídicamente responsable de la acción del iniciador de un MD por medio de un representante, es la persona en cuyo nombre se actuó y a quien se le atribuirán los efectos jurídicos, independientemente de que exista un iniciador material que lo generó y envió. El caso más emblemático es el de los representantes de las personas morales.

No se finaliza este apartado sin antes hacer referencia a programación de la intervención de sistemas informáticos expertos, de inteligencia artificial o agentes electrónicos inteligentes, a efecto de que automáticamente de generen o den respuesta a MD, lo que generalmente es tergiversado como una actuación en “representación” del iniciador, motivo por el cual este no será nunca un tema de una representación jurídica, sino un conjunto de instrucciones dirigidas a los sistemas de información cuyas actividades automáticas se le atribuyen a las personas responsables de instruir su gestión y ejecución. A mayor abundamiento, el acto de programación del sistema experto por parte de la persona física en cuya espera de control actúa, no es importante a efectos de la perfección del contrato electrónico suscrito, sino la respuesta del sistema informático a las condiciones de la oferta y demanda de dicho contrato.

2.6. Consentimiento: acuse de recibo y confirmación.

Si bien el consentimiento se forma por una policitación u oferta y por la aceptación de la misma, éste también es un elemento esencial del contrato, por lo que la falta de dicho elemento provocará la nulidad absoluta o inexistencia del contrato mercantil. De ahí que el CCo deba contar con dos normas específicas, una para el consentimiento realizado a través del empleo de los medios electrónicos, y la otra, para el momento en que este se tiene por perfeccionado.

En este contexto, el consentimiento se perfecciona cuando el emisor del MD recibe la contestación de la aceptación de la oferta, por lo que cuando se realice una oferta a través de

medios electrónicos, sin fijación de plazo para aceptarla, el oferente quedará desvinculado de la misma si la aceptación no se hace inmediatamente. Así, en un primer instante se origina cuando el destinatario contesta en forma inmediata, en tanto que el segundo instante se genera cuando el oferente recibe la aceptación.

Esos dos instantes determinan la aplicación del artículo 91 del CCo, que establece que la aceptación de la oferta tendrá lugar:

> *I. En el momento en que ingrese en el Sistema de Información designado por el emisor;*
> *II. De enviarse el MD a un Sistema de Información del Destinatario que no sea el Sistema de Información designado, o de no haber un Sistema de Información designado, en el momento en que el Destinatario recupere el MD, o*
> *III. Si el destinatario no ha designado un Sistema de Información, la recepción tendrá lugar cuando el MD ingrese a un Sistema de Información del Destinatario.*

A propósito de la recepción de la aceptación, también existe el acuse de recibo de los MD regulado por el numeral 92 de la normatividad en comento pero sólo es aplicable cuando lo hayan acordado así las partes; por tanto, el acuse no es un requisito que fija el Código para el perfeccionamiento del consentimiento, sin embargo, si fue pactado así, se estimará que el MD que contiene la oferta no ha sido enviado, en el caso de que no se hay recibido el acuso respectivo.

El efecto jurídico de la recepción de MD realizado por el emisor que no acordó la solicitud de acuse de recibo, hacen que la no aceptación o contestación de la oferta en el plazo señalado presumen su rechazo, ello con fundamento en el artículo 1805 del CCiF; en tanto que la consecuencia legal de la recepción de MD realizado por el emisor con acuerdo de acuse de recibo, hacen que la falta de respuesta o recepción sea considerada como no enviada.

Aquí lo trascendente del asunto, si el emisor recibió el acuse de recibo del destinatario, se presume que éste último ha recibido el MD; como corolario, en este instante, el destinatario deberá manifestar en forma inmediata si acepta o no la oferta hecha, pues el citado acuse de recibo del destinatario no significa forzosamente que acepto la oferta, por lo que puede consentir la oferta en otro momento.

Ahora, si bien la confirmación de recibo es piedra angular de la contratación electrónica al marcar el momento de entrada de los MD a sus destinatarios, no auxilia en determinar en qué términos fue recibido y acusado un MD, esto es, si llegó a su destinatario y si fue alterado antes de su llegada al destinatario, es aquí donde se subraya la utilidad de la FEA.

La pertinencia del acuse de recibo es más de certeza jurídica y se funda en la declaración expresa del destinatario; ello implica, que frente a situaciones fraudulentas, tanto el iniciador como el destinatario tendrán la oportunidad separada en tiempo para comprobar el origen y atribución del MD atribuido.

A nivel probatorio, el acuse de recibo preconstituye prueba judicialmente porque el acuse de recibo es otro MD y posee un soporte electrónico.

En cambio y a propósito de la confirmación se trata de una diligencia que puede ser solicitada por el destinatario al iniciador a fin de que el mensaje sea reiterado en forma repetida y que no exista incertidumbre de la procedencia, asignación y que no es un MD ocasional que se reproduce. Así, a falta de confirmación cuando ésta ha sido acordada previamente, permite a la contraparte considerar como no atribuible a dicha persona física o moral, el MD no confirmado. En este contexto, las reglas a las que se somete el acuse de recibo tienen cabida a la confirmación.

2.7. Formación del contrato electrónico: Policitación, publicidad y spam

La contratación electrónica permite que un usuario acceda a los sitios web que le interesen a fin comprar un producto o servicio en línea, cuando se encuentra en uno de ellos, tiene conocimiento de las condiciones integras del contrato cuya oferta ve firme en la página web. En tal hipótesis nos encontramos ante una oferta ***ad incertam personam*** (a persona indeterminada), porque los términos esenciales de la contratación son puestos a su disposición y acceso. También se puede presentar el caso de que tales condiciones no sean accesibles en el sitio web, por lo que se estará en presencia de una ***invitatio ad offerendum*** (invitación a contratar) que incita al destinatario a realizar ofertas, las que podrán o no ser aceptadas por el oferente inicial además conlleva a la inversión de la posición de las partes a la hora de emitir una oferta de contrato[138], porque una vez que el iniciador difunde una invitación de esta clase, queda en espera de la formulación de propuestas vinculantes de contrato por parte de los destinatarios de la primera.

No obstante, también existe una diferencia entre la **oferta al público** y la oferta ***ad incertam personam*****,** la cual radica en que aun cuando las dos son una modalidad de ofertas dirigidas a una generalidad indeterminada de sujetos desconocidos por el oferente, las primeras fueron creadas para ser recibidas por la generalidad de la colectividad, mientras que las segundas se remiten a un grupo de miembros, lo que hace que se distingan *por el carácter más o menos indeterminado de los sujetos destinatarios. La diferencia es más que cualitativa, cuantitativa ,* como sucede en el caso de las comunicaciones comerciales[139].

En una gran mayoría de casos, la contratación electrónica es resultado de una serie de ofertas, donde la visión publicitaria es parte de esta oferta.

El derecho que todavía no tenía una inmersión del entorno digital, regula de la misma manera al ámbito electrónico, incluso considerando que los medios de comunicación ahora son un

[138] Sánchez del Castillo, Vilma. La Publicidad en Internet: régimen jurídico de las comunicaciones electrónicas, 2006, Ed. La ley, España, p. 62 y 63.
[139] Cuadrado Pérez, Carlos. Oferta, aceptación y conclusión del contrato. Bolonia. Publicaciones del Real Colegio de España, 2003, pág. 152.

abanico diferente, pues varían desde los info-comerciales[140] hasta Internet, lo que ha evolucionado la manera de elaborar la publicidad. No podemos negar que resulta preocupante que en la medida en que incrementa la apertura comercial electrónica, se transforman las estructuras de mercado del dominio de proveedores/productores a la apertura de posibilidades de consumo y publicidad.

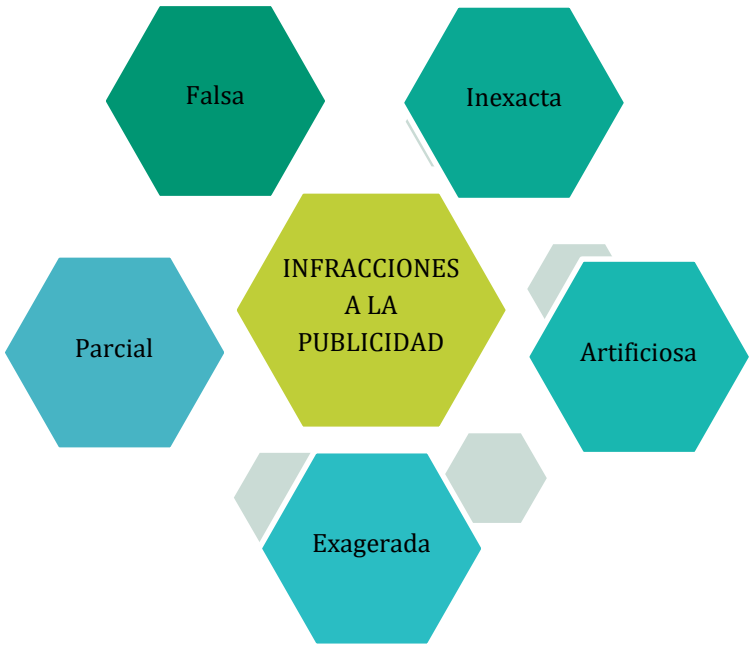
No obstante, los principios de publicidad en México se encuentran el artículo 32[141] de la LFPC, su redacción genera un sin número de posibles interpretaciones subjetivas y discrecionalidades que no permiten navegar en la certeza jurídica, tales como ¿Cómo se induce al error o confusión en la publicidad?, ¿si la información es verdadera, por qué se pudiera considerar falsa, artificiosa o tendenciosa?

Básicamente, las respuestas se encuentran y desglosan en los siguientes principios de la publicidad que se encuentran en dicho articulado.

- **a)** La publicidad debe ser congruente con las características o especificaciones establecidas en el producto o servicio,
- **b)** La publicidad no debe causar confusión ante su uso o atributos (ser orientadora y educativa)
- **c)** La publicidad no debe engañar,
- **d)** La publicidad no debe atentar o poner en riesgo la seguridad, integridad física o mental y la dignidad de las personas,
- **e)** La publicidad debe contener información comprobable.

[140] Los infomerciales en su gran mayoría son un programa de televisión normal donde la teleaudiencia suele recibir poca o nula información del hecho de que el programa es en realidad un comercial. Los infomerciales están diseñados para solicitar una respuesta directa que es específica y cuantitativa y es, por tanto, una forma de mercadeo de respuesta directa. Se emiten normalmente fuera de las horas pico, como durante el día o la madrugada (generalmente entre las 2 y 6 de la mañana). Más información véase: Electronic Retailing Association, accesible en http://www.retailing.org/

[141] "**Artículo 32.** La información o publicidad relativa a bienes, productos o servicios que se difundan por cualquier medio o forma, deberán ser veraces, comprobables y exentos de textos, diálogos, sonidos, imágenes, marcas, denominaciones de origen y otras descripciones que induzcan o puedan inducir a error o confusión por engañosas o abusivas.
Para los efectos de esta ley, se entiende por información o publicidad engañosa o abusiva aquella que refiere características o información relacionadas con algún bien, producto o servicio que pudiendo o no ser verdaderas, inducen a error o confusión al consumidor por la forma inexacta, falsa, exagerada, parcial, artificiosa o tendenciosa en que se presenta.
La información o publicidad que compare productos o servicios, sean de una misma marca o de distinta, no podrá ser engañosa o abusiva en términos de lo dispuesto en el párrafo anterior.
La Procuraduría podrá emitir lineamientos para el análisis y verificación de dicha información o publicidad a fin de evitar que se induzca a error o confusión al consumidor, considerando el contexto temporal en que se difunde, el momento en que se transmite respecto de otros contenidos difundidos en el mismo medio y las circunstancias económicas o especiales del mercado."



De lo anterior, se afirma que la información contenida en la publicidad debe garantizar que no confunda o induzca al error a los consumidores, que sus términos y condiciones estén siempre al alcance del consumidor y, que no omita información relevante para la toma de una decisión por parte del consumidor.

Por su parte, la Procuraduría Federal del Consumidor (PROFECO), organismo para la defensa de los derechos del consumidor en México; establece criterios y elementos para el análisis de la publicidad en nuestro país, entre ellos están:

1) Realizar un análisis integral y armónico de la publicidad, sin descomponer sus partes integrantes.
2) No limitar contenido creativo, ni emitir juicios relacionados con su diseño o elaboración.
3) Contexto temporal en que se difunde y consumidores receptores de la publicidad.
4) Protección a consumidores vulnerables: niños, adultos mayores y enfermos (art. 76 bis, fracción VII de la LFPC)

Además, en el análisis de la publicidad los funcionarios públicos de la PROFECO atienden diversos principios y criterios tales como: la legalidad, el análisis integral, la no limitación de la creatividad o diseño, la verificación de que la información no induzca al error o engaño, la protección de los consumidores vulnerables, la transparencia y la protección de la información y la corresponsabilidad. Con esta forma de analizar y verificar, la Procuraduría cumple con el objetivo de disminuir la asimetría de información entre consumidores y proveedores, así como evitar riesgos para el consumidor, y con esto lograr equidad, certeza y seguridad jurídica en las relaciones de consumo.

Lamentablemente, sobresalen los retos del dinamismo del comercio electrónico como son la necesidad de determinar las nuevas modalidades de la publicidad; determinar la responsabilidad e identificación del anunciante; indicar los mayores recursos técnicos-científicos en el análisis y verificación de la publicidad, y sobre todo, extender la capacitación que deben tener los funcionarios encargados de supervisar la publicidad en medios electrónicos.

No obstante, la actividad de la PROFECO no se encuentra aislada de otras entidades y dependencias del gobierno, pues existen cuando menos cuatro entidades gubernamentales que además de la Procuraduría contienen regulación sobre la publicidad y que colaboran sistemáticamente respecto al bienestar del consumidor, entre ellas, la Comisión Federal para la Protección contra Riesgos Sanitarios (COFEPRIS), Comisión Federal de Competencia (COFECO) y el Servicio Nacional de Sanidad, Inocuidad y Calidad Agroalimentaria (SENASICA). Pues aun cuando es evidente la preponderancia de las facultades de la PROFECO en el área de protección a los derechos del consumidor en materia de ofertas y publicidad, también lo son las funciones de verificación, de imposición de medidas precautorias en materia de información y publicidad; exceptuando las materias de servicios regulados por leyes financieras (autofinanciamiento, casas de empeño), los servicios profesionales, las sociedades de información crediticia, la publicidad en materia sanitaria, y publicidad electoral); no son de menor valor las facultades concurrentes de la PROFECO con las siguientes autoridades:

1. Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF)
2. Comisión Federal para la Protección contra Riesgos Sanitarios (COFEPRIS)
3. Secretaría de Gobernación (SEGOB)
4. Instituto Mexicano de la Propiedad Industrial (IMPI)

El ejemplo más claro de la concurrencia de facultades entre dos autoridades lo representa el caso del control sanitario de ciertos productos que realiza la COFEPRIS, y al mismo tiempo, el control comercial que realiza la PROFECO.

Asimismo, en materia de publicidad, la Procuraduría cuenta con la función de gestión punitiva (inmovilizaciones, sellos, venta de productos de temporada, visitas de verificación), de promoción, supervisión de precios y divulgación de las causas de salud, seguridad y ecología así como de reivindicación del cumplimiento de las normas de etiquetado, de las Normas Oficiales Mexicanas (NOM's) en materia de salud, seguridad y ecología (retiro de productos milagro[142] y/o con riesgos, señalados por las autoridades). Un ejemplo de lo anterior, es que en el año 2012, el 70%[143] de las actividades administrativas llevadas a cabo por la PROFECO se dirigió

[142] Los productos milagro no cuentan con un concepto unívoco a pesar de ser un problema mundial, pero se caracterizan por generar daños a la salud y al patrimonio de los consumidores, afectan la sana competencia.
[143] Jiménez Paz, Aarón. Criterios y evaluación de la publicidad engañosa en la labor de la PROFECO, Seminario el derecho a la información de los consumidores y la publicidad responsable, IIJ-UNAM-PROFECO, 16 y 17 de mayo de 2012, accesible en: http://www.consumidor.gob.mx/wordpress/wp-content/uploads/2012/05/presentacionAaronJimenez.pdf, fecha de consulta enero de 2015.

sancionar por infracciones a la normatividad publicitaria, es decir, por presentar publicidad engañosa o abusiva e infringir alguno de los siguientes artículos: 7[144], 7bis[145], 32[146], 34[147], 38[148] y 48[149] de la LFPC.

En concordancia con lo anterior, las facultades de la Procuraduría en materia de regulación de la publicidad consisten en requerimientos de información, procedimientos por infracciones a la ley, medidas precautorias (artículos 35[150], 25 bis[151] de la LFPC), exhortos, medidas de apremio

---

[144]"**Artículo 7.-** Todo proveedor está obligado a informar y respetar los precios, tarifas, garantías, cantidades, calidades, medidas, intereses, cargos, términos, plazos, fechas, modalidades, reservaciones y demás condiciones conforme a las cuales se hubiera ofrecido, obligado o convenido con el consumidor la entrega del bien o prestación del servicio, y bajo ninguna circunstancia serán negados estos bienes o servicios a persona alguna."

[145] "**Artículo 7 Bis.-** El proveedor está obligado a exhibir de forma notoria y visible el monto total a pagar por los bienes, productos o servicios que ofrezca al consumidor.

Dicho monto deberá incluir impuestos, comisiones, intereses, seguros y cualquier otro costo, cargo, gasto o erogación adicional que se requiera cubrir con motivo de la adquisición o contratación respectiva, sea ésta al contado o a crédito."

[146] "**Artículo 32.** La información o publicidad relativa a bienes, productos o servicios que se difundan por cualquier medio o forma, deberán ser veraces, comprobables y exentos de textos, diálogos, sonidos, imágenes, marcas, denominaciones de origen y otras descripciones que induzcan o puedan inducir a error o confusión por engañosas o abusivas.

Para los efectos de esta ley, se entiende por información o publicidad engañosa o abusiva aquella que refiere características o información relacionadas con algún bien, producto o servicio que pudiendo o no ser verdaderas, inducen a error o confusión al consumidor por la forma inexacta, falsa, exagerada, parcial, artificiosa o tendenciosa en que se presenta.

La información o publicidad que compare productos o servicios, sean de una misma marca o de distinta, no podrá ser engañosa o abusiva en términos de lo dispuesto en el párrafo anterior.

La Procuraduría podrá emitir lineamientos para el análisis y verificación de dicha información o publicidad a fin de evitar que se induzca a error o confusión al consumidor, considerando el contexto temporal en que se difunde, el momento en que se transmite respecto de otros contenidos difundidos en el mismo medio y las circunstancias económicas o especiales del mercado."

[147]"**Artículo 34.-** Los datos que ostenten los productos o sus etiquetas, envases y empaques y la publicidad respectiva, tanto de manufactura nacional como de procedencia extranjera, se expresarán en idioma español y su precio en moneda nacional en términos comprensibles y legibles conforme al sistema general de unidades de medida, sin perjuicio de que, además, se expresen en otro idioma u otro sistema de medida."

[148]"**Artículo 38**.- Las leyendas que restrinjan o limiten el uso del bien o el servicio deberán hacerse patentes en forma clara, veraz y sin ambigüedades."

[149] "**Artículo 48.-** En las promociones y ofertas se observarán las siguientes reglas:

I. En los anuncios respectivos deberán indicarse las condiciones, así como el plazo de duración o el volumen de los bienes o servicios ofrecidos; dicho volumen deberá acreditarse a solicitud de la autoridad. Si no se fija plazo ni volumen, se presume que son indefinidos hasta que se haga del conocimiento público la revocación de la promoción o de la oferta, de modo suficiente y por los mismos medios de difusión, y

II. Todo consumidor que reúna los requisitos respectivos tendrá derecho a la adquisición, durante el plazo previamente determinado o en tanto exista disponibilidad, de los bienes o servicios de que se trate."

[150]"**Artículo 35.-** Sin perjuicio de la intervención que otras disposiciones legales asignen a distintas dependencias, la Procuraduría podrá:

I. Ordenar al proveedor que suspenda la información o publicidad que viole las disposiciones de esta ley y, en su caso, al medio que la difunda;

II. Ordenar que se corrija la información o publicidad que viole las disposiciones de esta ley en la forma en que se estime suficiente, y

III. Imponer las sanciones que correspondan, en términos de esta ley.

Para los efectos de las fracciones II y III, deberá concederse al infractor la garantía de audiencia a que se refiere el artículo 123 de este ordenamiento.

Cuando la Procuraduría instaure algún procedimiento administrativo relacionado con la veracidad de la información, podrá ordenar al proveedor que en la publicidad o información que se difunda, se indique que la veracidad de la misma no ha sido comprobada ante la autoridad competente."

[151] "**Artículo 25 Bis.** La Procuraduría podrá aplicar las siguientes medidas precautorias cuando se afecte o pueda afectar la vida, la salud, la seguridad o la economía de una colectividad de consumidores:

I. Inmovilización de envases, bienes, productos y transportes;

(artículo 25[152] LFPC) y sanciones económicas (128 bis[153] de la LFPC) así como de clausura (128 ter[154]).

Es evidente que la gestión de la Profeco trasladada al ámbito del comercio electrónico, particularmente, en Internet es inasequible o inalcanzable, dada la amplitud y nivel

---

II. El aseguramiento de bienes o productos en términos de lo dispuesto por el artículo 98 TER de esta Ley;
III. Suspensión de la comercialización de bienes, productos o servicios;
IV. Ordenar el retiro de bienes o productos del mercado, cuando se haya determinado fehacientemente por la autoridad competente que ponen en riesgo la vida o la salud de los consumidores;
V. Colocación de sellos e información de advertencia, y
VI. Ordenar la suspensión de información o publicidad a que se refiere el artículo 35 de esta Ley.
Las medidas precautorias se dictarán conforme a los criterios que al efecto expida la Procuraduría y dentro del procedimiento correspondiente en términos de lo dispuesto en el artículo 57 y demás relativos de la Ley Federal sobre Metrología y Normalización; así como cuando se advierta que se afecta o se puede afectar la economía de una colectividad de consumidores en los casos a que se refiere el artículo 128 TER o cuando se violen disposiciones de esta ley por diversas conductas o prácticas comerciales abusivas, tales como: el incumplimiento de precios o tarifas exhibidos; el condicionamiento de la venta de bienes o de servicios; el incumplimiento de ofertas y promociones; por conductas discriminatorias y por publicidad o información engañosa. En el caso de la medida precautoria a que se refiere la fracción IV de este precepto, previo a la colocación del sello e información respectiva, la Procuraduría aplicará la medida a que se refiere el artículo 25, fracción I, de esta ley, salvo el caso de que se encuentre en riesgo el principio señalado en la fracción X del artículo 1 de la presente ley. Tales medidas se levantarán una vez que se acredite el cese de las causas que hubieren originado su aplicación. En su caso, la Procuraduría hará del conocimiento de otras autoridades competentes la aplicación de la o las medidas a que se refiere este precepto.
Los proveedores están obligados a informar de inmediato a las autoridades si determinan que alguno de sus productos puede implicar riesgos para la vida o la salud de los consumidores."

[152] **Artículo 25.-** La Procuraduría, para el desempeño de las funciones que le atribuye la ley, podrá aplicar las siguientes medidas de apremio:
I. Apercibimiento;
II. Multa de **$231.42** a **$23,142.38**;
III. En caso de que persista la infracción podrán imponerse nuevas multas por cada día que transcurra sin que se obedezca el mandato respectivo, hasta por **$9,256.95**, y
IV. El auxilio de la fuerza pública.

[153] **Artículo 128 Bis.** En casos particularmente graves, la Procuraduría podrá sancionar con clausura total o parcial, la cual podrá ser hasta de noventa días y con multa de **$138,854.28** a **$3´887,919.91**.
Las violaciones a lo establecido en el artículo 32 que se consideren particularmente graves conforme a lo establecido en el artículo 128 Ter de esta ley, serán sancionadas con la multa establecida en el párrafo anterior o bien con multa de hasta un 10% de los ingresos brutos anuales del infractor obtenidos por la comercialización del bien o los bienes, productos o servicios contenidos en la publicidad respectiva, correspondiente al último ejercicio fiscal en que se haya cometido la infracción, en caso de reincidencia.

[154] **Artículo 128 Ter.-** Se considerarán casos particularmente graves:
I. Aquellos en que de seguir operando el proveedor, se pudieran afectar los derechos e intereses de un grupo de consumidores;
II. Cuando la infracción de que se trate pudiera poner en peligro la vida, la salud o la seguridad de un grupo de consumidores;
III. Aquellas infracciones que se cometan en relación con bienes, productos o servicios que por la temporada o las circunstancias especiales del mercado afecten los derechos de un grupo de consumidores;
IV. Aquellas conductas que se cometan aprovechando la escasez, lejanía o dificultad en el abastecimiento de un bien o en la prestación de un servicio;
V. Cuando se trate de productos básicos de consumo generalizado, como alimentos, gas natural o licuado de petróleo, gasolina o productos sujetos a precio máximo o a precios o tarifas establecidos o registrados por la Secretaría o por cualquiera otra autoridad competente;
VI. Cuando la información o publicidad relacionada con algún bien, producto o servicio que pudiendo o no ser verdadera, induzcan a error o confusión al consumidor por la forma falsa, exagerada, parcial, artificiosa o tendenciosa en que se presente;
VII. La reincidencia en la comisión de infracciones a los artículos señalados en el artículo 128 de esta ley, y
VIII. Aquellas que vulneren los derechos contemplados en el Título Segundo de la Ley para la Protección de los Derechos de Niñas, Niños y Adolescentes.

transfronterizo del mismo. Por ello en este sentido resultan idóneas las alianzas y sinergias de los agentes del mercado, ello permite una colaboración ampliada de protección al consumidor.

Por ello, se estima por demás conveniente, una autorresponsabilidad en materia publicitaria por parte del consumidor digital, que se rija por principios básicos de las relaciones de consumo en materia de información adecuada y la protección del consumidor frente a la publicidad engañosa. A esta visión, la secunda la tendencia creciente de trabajar con y generar esquemas de auto-regulación en los diversos sectores de productos y servicios, actualmente existen los casos de éxito del *Código de autorregulación de Publicidad de Alimentos y Bebidas no Alcohólicas dirigidas al Público Infantil* (PABI)[155] y *Código de Autorregulación y Ética Publicitaria para Productos Cosméticos* (COSMEP) elaborado por de la Cámara y Asociación de la Industria de Productos del Cuidado Personal y del Hogar (CANIPEC) y del Consejo de Autorregulación Publicitaria (CONAR), lo mismo está sucediendo con las bebidas alcohólicas y las leyendas ecológicas.

Si bien, desde el contexto de la protección del consumidor, la regulación no responde al dinamismo y evolución del comercio electrónico así como los distintos vehículos de comunicación donde se hace publicidad, también las empresas y comercios se encuentran dando respuesta más rápida que la regulación jurídica, con respecto a la especialidad de los productos y servicios que ahora exige a las empresas o negocios[156] proveer un servicio más expedito y eficiente de entrega de productos[157], el incremento de pagos móviles o a través de smartphones[158] y finalmente, un consumidor selectivo, exigente y discriminante. Lo anterior es así, porque hoy en día, las empresas deben de atender a nuevas formas de publicitarse, pues ahora se ven afectadas por las comunicaciones integradas de marketing (CIM), donde los tipos de publicidad van de la denominada *Above The Line (*ATL: acrónimo de las iniciales en inglés) o *sobre la línea*, la cual se distingue por utilizar medios publicitarios convencionales con inversiones elevadas de dinero a fin de llegar a una audiencia más amplia y lograr el mayor número de impactos, ya que se sirve de los medios masivos (televisión, radio, prensa escrita, revistas, vallas), donde, los contenidos son muy cuidados ya que además de ser vistos por el segmento objetivo, son vistos por otros como menores de edad, ancianos, adolescentes, grupos étnicos y religiosos con diversas creencias. En contraste con este tipo de publicidad, se encuentra la denominada *Below The Line* (BTL: acrónimo de las iniciales en inglés) o bajo la

[155] El código se puede descargar de http://www.promocion.salud.gob.mx/dgps/descargas1/programas/codigo_pabi.pdf, última fecha de consulta: 16 mayo 2015.

[156] Nos referimos al tipo de productos y servicios que no se adquieren en tiendas departamentales o de autoservicio, sino que se realizan a través de plataformas electrónicas específicas como Amazon o eBay.

[157] Con el retail tradicional había una ventana de entregas de dos días, en e-commerce tienes que entregar en 24 o 48 horas máximo. Ahora se manejan la distribución bajo un modelo similar al de mensajería. Ver http://www.antad.net/index.php/publicaciones/antad-informa/antad-informa/item/20421-comercio-electr%C3%B3nico-pone-a-prueba-log%C3%ADstica-de-empresas

[158] Los pagos móviles aumentan 46%, el doble que el comercio electrónico con 15 mil mdp en 2014, representan 15% del e-commerce en México. La penetración de los smartphones y tablets en el país acelera su crecimiento. Para 2015 se estima que el gasto móvil aumente 39%, frente al 19% del e-commerce. (Fuente: El Financiero/Ciudad de México/ Distrito Federal/Empresas, P 36, 06:01/12/12/2014) En los últimos cuatro años, el mercado de smartphones creció a un ritmo anual de 70 por ciento. Actualmente hay en el mercado mexicano cerca de 44 millones 150 mil smartphones, los cuales representan 49 por ciento de la telefonía celular total, según datos de The Competitive Intelligence Unit.

línea, la cual utiliza formas no masivas de comunicación con altos niveles de creatividad e innovación dirigidas a segmentos de mercado específicos. Finalmente, ambas son utilizadas como complementos una de otra[159].

Por ello, se reafirma la relevancia de dos derechos del consumidor en el ámbito publicitario: a) el derecho a la información de los consumidores y b) derecho a la protección de la vida, salud, seguridad así como la economía de la colectividad. En relación con el primero se explica la obligación que nace para el negocio de generar publicidad responsable, más aun en un entorno digital.

Este tipo de derecho atribuye al consumidor la responsabilidad de evaluar lo que compra y en qué condiciones lo hace, entre ellas, dudar de lo que *"suena demasiado bueno"* para ser verdad; tener presente que lo que se ofrece en la publicidad debe ser cumplido; identificar y poner atención a las restricciones y condiciones que aplican los negocios sobre un producto o servicio; buscar en las letras más pequeñas o acústicamente insonoras, en las voces que se difunden más rápidamente; leer la publicidad de abajo hacia arriba; buscar el monto total a pagar incluyendo impuestos; etc. Pero sobretodo, es un derecho del consumidor a conocer y a tomar decisiones racionales en materia de consumo y competencia, ello nivela el flujo de asimetría informativa[160].

En respuesta la idea anterior, se aduce como respuesta el proyecto de centros de monitoreo de medios de comunicación electrónicos, impresos, internet, alternos y cine en materia de consumo de productos y servicios, la cual no es una noción nueva, no obstante, la existencia de lineamientos para el monitoreo a no es todavía una realidad en México, sólo lo es en materia electoral dado el constante en interés político en el tema[161].

En cuanto a la responsabilidad civil en materia de publicidad, debemos recordar que esta se puede presentar derivado de varias situaciones: por un hecho ilícito, por incumplimiento de contrato o por falta a un deber jurídico, se pueden determinar diversas indemnizaciones o la reparación del daño; o bien, promover acciones colectivas.

El caso más frecuente es la responsabilidad civil en materia de publicidad por un hecho ilícito dada en Internet o en un establecimiento comercial, la cual requiere acreditar elementos de la responsabilidad civil:

1) La conducta: una acción u omisión;
2) La antijuricidad: contrario a la ley, reglamento, moral y buenas costumbres.
3) Culpabilidad: dolo o culpa (engaño, falta de claridad).

---

[159] Philip Kotler, Kevin Lane Keller (2006). Marketing Management, 14 ed., 2012, New Jersey, Prentice Hall, pp. 474-502.
[160] Cfr. García Sais, Fernando, Derecho de los consumidores a la información. Una aproximación a la publicidad engañosa en México, Ed. Porrúa-ITAM, México, 2007, págs. 44-71.
[161] Lineamientos para el monitoreo a medios de comunicación electrónicos, impresos, internet, alternos y cine, previo al inicio del periodo de precampañas electorales, para el proceso electoral 2014-2015, accesible en la página oficial del Instituto Electoral del Estado de México, www.ieem.org.mx

4) Daño: que sea resarcible y cierto.

Generalmente, la primer forma de reparar el daño es cumpliendo con la oferta, la promoción, actividad, servicio, condiciones o garantías ofrecidas; si esta no es la forma viable, queda la recisión del contrato, con el correspondiente pago de daños y perjuicios; como tercera opción esta la reintegración de la prestación; y la última, es el retiro de la mercancía del mercado.

Ahora corresponde atender al tratamiento legal del ***spam.*** El spam representa una molestia que abarca perdidas tanto económicas como materiales, se trata de mensajes no solicitados, con remitente desconocido, de carácter publicitario, enviado en cantidades masivas, logrando perjudicar de varias formas al receptor, y que tiene por fin el ánimo de lucro. Se debe aclarar que el spam únicamente se refiere a las comunicaciones publicitarias no solicitadas a través de medios electrónicos, pues existen otras formas de comunicaciones no deseadas como el *junk mail*, que no necesariamente tiene una finalidad comercial y el *mail bombing,* que es el que intencionalmente se envía para bloquear una cuenta de correo electrónico.

El sujeto activo del spam es denominado *spammer(s)* cuya finalidad es obtener cuentas electrónicas verdaderas (no importa donde tienen que buscar, ya que la diversidad que existe es muy amplia), al obtenerlas enviarán la mayoría de las veces publicidad muy tentativa y atractiva o peor aún causar daño de cualquier tipo (principalmente económico) al receptor final. El problema que acarrea esta actividad es que dicha población está creciendo en razón de la facilidad con que se puede comprar un listado enorme de direcciones electrónicas válidas,

El spam básicamente se caracteriza por ser:

a) **Masivo:** esta característica es algo distintiva con estos correos electrónicos no solicitados, ya que un solo mensaje de publicidad es enviado a una cantidad enorme de emails, el fin de esta acción es que mientras más destinatarios reciban esta información, implica mayor ganancia, aunque sólo la mínima parte sean víctimas.
b) **Anónimo:** el mayor porcentaje de los mensajes electrónicos cuyo contenido es de spam, su verdadero origen es mediante remitentes falsos, o de contactos conocidos (pero con una dirección errónea), esto sucede porque la finalidad es hacer que el destinatario final caiga en el engaño, la trampa y así abrir dichos mensajes.
c) **No solicitado:** muchas veces recibimos mensajes legítimos, esto es porque al formar parte o darnos de alta en algún foro, un grupo de noticias o información de nuestro interés, estaremos recibiendo información constantemente de las novedades de dichas páginas (esto sucede por aceptar su recepción), pero muchas ocasiones son enviados a la bandeja de Spam y en realidad son legítimos. Simplemente si nosotros no hemos pedido información de cualquier género, pero sobretodo de publicidad, no tenemos por qué recibirla.
d) **Publicitario:** es atraer la atención del usuario final, es decir, cuando por alguna razón hemos abierto un mensaje con estas características y no lo borramos de inmediato, aplican distintas técnicas por ejemplo: ofertas insuperables de artículos de marcas prestigiosas;

artículos cura-todo; viajes a precios realmente tentativos, son muchas las técnicas para engañar fácilmente (adelante veremos más información al respecto).

e) **Falta de legislación nacional e internacional vigente:** Por este motivo muchos de los ilícitos informáticos quedan impunes, al no tener una ley especializada en la materia, también quedan absueltos de pena los sujetos activos, aunque su actuar sea doloso.
f) **Fin de lucro**: la finalidad de que el Spam sea masivo, es por la sencilla razón, de que algún porcentaje de los sujetos que accedan a los medios informáticos, caigan en el engaño y así obtener ganancias, que ocasionan grandes pérdidas económicas a nivel mundial.

Existe una noción imprecisa en cuanto al campo de aplicación del spam, si bien es cierto que en el lugar en donde se presenta con un mayor porcentaje es a través del correo electrónico, también existen los siguientes lugares en que se puede presentar:

a) **Teléfonos móviles:** Se presta mediante Servicios de Mensajería Instantánea (SMS) y se encuentra en
b) **Mensajería instantánea *spim*** (acrónimo en inglés de SPam over Instant Messaging), una forma de correo basura que llega a través de los populares programas de mensajería instantánea, también conocidos como chats (MSN de Microsoft, Yahoo! Messenger o AOL Messenger, entre otros).
c) **Spit** (spam sobre telefonía IP): Al contrario que la telefonía tradicional, los usuarios de VoIP no serán contactados digitando un número a la vez. Con la ayuda de VoIP, los distribuidores de spit podrán hacer llegar su mensaje a miles de usuarios simultáneamente, de la misma forma que los usuarios de correo electrónico reciben actualmente el spam.
d) **Grupos de noticias**: Se utilizan **parEa** poder opinar sobre un tema en común con algunas otras personas, que pueden ser miembros de dicho servicio y por lo tanto dar su punto de vista en el mismo, hay que mencionar que la mayoría de las veces es de carácter público y cualquiera puede comentar ya sea a favor o en contra, también existen grupos privados para empresas estos son más serios en cuanto a la dinámica.
e) **Foros:** Esta clase de spam es realmente muy extraña ya que la mayoría prefiere mantener el anonimato, pero aquí generalmente los mismos usuarios hacen una constante referencia, sobre algún enlace que por lo general no tiene relevancia con el tema en comento.
f) **Blogs**: Incluye sitios web de debates, discusiones mismas que son abiertas para todos aquellos a quienes les interese, su finalidad es hablar al respecto y compartir nuestras opiniones en una temática de cualquier índole e interés.

Frecuentemente los temas sobre los que se dirige un *spam* son los relacionados con artículos novedosos, de marcas reconocidas mundialmente, pero con un atractivo descuento que es difícil no querer, lo interesante es que dicho mensaje de publicidad cumple su primer objetivo, el cual es dar *click* sobre éste para acceder al link que muchas de las veces aparenta ser un sitio oficial, para que el usuario no desconfié en ningún momento y otorguemos información confidencial sobre nuestras cuentas bancarias, datos personales sin darnos cuenta de los motivos que tienen al tenerlos en su poder.

Son varios los efectos producidos por culpa del spam, llega a ocasionar el llamado "tráfico de correo electrónico" en la red, esto es porque se envían y reciben más correos de esta índole, a comparación con los mails que en verdad son legítimos, causan una saturación en el servicio.

El primordial emisor de spam en el mundo es Estados Unidos, seguido por el Asia (países como Vietnam, Corea, China). Mientras que en México, el spam como tal no se encuentra regulado como delito en ninguna de las leyes mexicanas hasta el momento, no obstante, la transmisión de los datos de los usuarios a estas bases de envío sí constituyen una violación a la LFPC, en su artículo 76 bis[162] ya que rompen el acuerdo entre el usuario y los proveedores.

El artículo 76 bis establece además que el proveedor tiene prohibido difundir la información a otros proveedores ajenos a la transacción, a menos que el propio consumidor lo apruebe y que deberá brindar seguridad y confidencialidad sobre los datos proporcionados (ver el artículo 6 de la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP).

Por otro lado, en el mismo artículo se establece que *el proveedor respetará la decisión del consumidor en cuanto a la cantidad y calidad de los productos que desea recibir, así como la de no recibir avisos comerciales* .

En caso de que el usuario compruebe que tus datos fueron traspasados por un proveedor, o que dicho proveedor continúa mandando avisos comerciales se puede acudir ante la PROFECO para levantar una denuncia.

2.8. Perfeccionamiento del contrato.

[162] **Artículo 76 Bis.-** Las disposiciones del presente Capítulo aplican a las relaciones entre proveedores y consumidores en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología. En la celebración de dichas transacciones se cumplirá con lo siguiente:
I. El proveedor utilizará la información proporcionada por el consumidor en forma confidencial, por lo que no podrá difundirla o transmitirla a otros proveedores ajenos a la transacción, salvo autorización expresa del propio consumidor o por requerimiento de autoridad competente;
II. El proveedor utilizará alguno de los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por el consumidor e informará a éste, previamente a la celebración de la transacción, de las características generales de dichos elementos;
III. El proveedor deberá proporcionar al consumidor, antes de celebrar la transacción, su domicilio físico, números telefónicos y demás medios a los que pueda acudir el propio consumidor para presentarle sus reclamaciones o solicitarle aclaraciones;
IV. El proveedor evitará las prácticas comerciales engañosas respecto de las características de los productos, por lo que deberá cumplir con las disposiciones relativas a la información y publicidad de los bienes y servicios que ofrezca, señaladas en esta Ley y demás disposiciones que se deriven de ella;
V. El consumidor tendrá derecho a conocer toda la información sobre los términos, condiciones, costos, cargos adicionales, en su caso, formas de pago de los bienes y servicios ofrecidos por el proveedor;
VI. El proveedor respetará la decisión del consumidor en cuanto a la cantidad y calidad de los productos que desea recibir, así como la de no recibir avisos comerciales, y
VII. El proveedor deberá abstenerse de utilizar estrategias de venta o publicitarias que no proporcionen al consumidor información clara y suficiente sobre los servicios ofrecidos, en especial tratándose de prácticas de mercadotecnia dirigidas a la población vulnerable, como los niños, ancianos y enfermos, incorporando mecanismos que adviertan cuando la información no sea apta para esa población."

El contrato electrónico se perfecciona mediante el consentimiento expreso o tácito[163] de los contratantes manifestado por el concurso de la oferta y la aceptación sobre la cosa y la causa que han de constituir el contrato, ello implica que su perfeccionamiento se dará hasta que exista el acuerdo de voluntades, el cual puede darse de manera gradual en el caso del comercio electrónico de empresa a empresa, de conformidad con sucesivas ofertas y contraofertas, pues en el caso de empresa a consumidor es más simple el acuerdo de voluntades.

El perfeccionamiento del contrato mercantil se perfecciona de acuerdo al código civil y mercantil, los cuales determinan el momento en que se reúne el consentimiento de este tipo de contratos y con ello se está en posibilidad de resolver sobre las siguientes circunstancias[164]:

- **a)** Para determinar la ley aplicable en caso de conflicto de leyes en el tiempo y lugar;
- **b)** Para apreciar si las partes son capaces;
- **c)** Para determinar la fecha de la transmisión del riesgo en caso de que se pierda la cosa objeto del contrato.
- **d)** Para señalar el inicio del plazo de ejercicio o prescripción de ciertas acciones de nulidad o rescisión.
- **e)** En caso de quiebra, para saber si el contrato fue celebrado dentro del periodo sospechoso.
- **f)** En relación a la revocación de la oferta, mientras el contrato no se perfeccione, puede revocarse por muerte del oferente o por declaración de su voluntad.

En primer caso, esto es, la determinación del momento y lugar en que el concurso de voluntades se produce, y en el comercio electrónico comprende dos situaciones:

- **I)** Cuando los contratantes se encuentran en lugares diferentes,
- **II)** El que esos lugares radiquen en jurisdicciones distintas.

De acuerdo con Rafael Illescas[165], existen tres situaciones que, a su vez, impactan el perfeccionamiento de los contratos electrónicos:

- **i)** La pertinencia y efectos de un acuerdo previo entre las partes, que conduzca las ulteriores transacciones electrónicas.
- **ii)** La determinación del derecho sustantivo aplicable dada su modalidad de contrato entre ausentes.
- **iii)** Las especialidades en la aplicación de dicho derecho sustantivo resultantes del previo acuerdo de negociación entre las partes que serán transmitidas electrónicamente mediante MD emitidos y recibidos a través de los sistemas informáticos de los contratantes.

[163] Este punto se aborda a cabalidad en el punto: "4.2. Código de Comercio, Código Civil Federal y Código Federal de Procedimientos Civiles", de este trabajo.
[164] Rojina Villegas, Rafael. Derecho Civil Mexicano, 4ª ed,1981, México, Porrúa, p. 276.
[165] Illescas Ortíz, Rafael: Derecho de la contratación electrónica, 2009, 2ª ed., Madrid, Civitas Thomson Reuters, p. 249

Con anterioridad a sucesivas, frecuentes, cuantiosas transacciones electrónicas, es pertinente elaborar un acuerdo para determinar el momento de la fijación de la perfección del contrato, a través de un acuerdo marco que considere los lineamientos básicos para futuras negociaciones en soporte electrónico.

En cuanto a la determinación del derecho sustantivo aplicable dada su modalidad de contrato entre ausentes, implica atender a si es un contrato de naturaleza estrictamente mercantil (o mixta: civil-mercantil) o internacional.

Para calificar una compraventa mercantil como internacional se requiere aplicar una interpretación a contrario *sensu* del artículo 2 de la Convención de Viena sobre Compraventa Internacional de Mercaderías[166] (CNUCCIM en español o CISG en inglés), la cual regula aspectos sustanciales del contrato más utilizado del comercio internacional que establece:

> ***Artículo 2**. La presente Convención no se aplicará a las compraventas:*
> ***a)** de mercaderías compradas para uso personal, familiar o doméstico, salvo que el vendedor, en cualquier momento antes de la celebración del contrato o en el momento de su celebración, no hubiera tenido ni debiera haber tenido conocimiento de que las mercaderías se compraban para ese uso;*
> ***b)** en subastas;*
> ***c)** judiciales;*
> ***d)** de valores mobiliarios, títulos o efectos de comercio y dinero;*
> ***e)** de buques, embarcaciones, aerodeslizadores y aeronaves;*
> ***f)** de electricidad.*

En esta definición se advierte que desde un principio queda fuera del campo internacional los contratos civiles o domésticos, las subastas, las compraventas judiciales, de valores mobiliarios, títulos o efectos de comercio y dinero, de buques, embarcaciones, aerodeslizadores y aeronaves y electricidad. Por lo que el perfeccionamiento del contrato de acuerdo a la CNUCCIM, que es parte de la legislación mexicana y por ende aplicable, se produce de conformidad a los artículos 18.2, 15.1 y 24 de la CNUCCIM.

> ***Artículo 15**. 1) La oferta surtirá efecto cuando llegue al destinatario. (…)*
> ***Artículo 18.** (…)*
> *2) La aceptación de la oferta surtirá efecto en el momento en que la indicación de asentimiento llegue al oferente. La aceptación no surtirá efecto si la indicación de asentimiento no llega al oferente dentro del plazo que éste haya fijado o, si no se ha fijado plazo, dentro de un plazo razonable, habida cuenta de las circunstancias de la transacción y, en particular, de la rapidez de los medios de comunicación empleados por el oferente. La aceptación de las ofertas verbales tendrá que ser inmediata a menos que de las circunstancias resulte otra cosa.*
> ***Artículo 24.** A los efectos de esta Parte de la presente Convención, la oferta, la declaración de aceptación o cualquier otra manifestación de intención "llega" al destinatario cuando se le comunica verbalmente o se entrega por cualquier otro medio al destinatario personalmente, o en su establecimiento o dirección postal o, si no tiene establecimiento ni dirección postal, en su residencia habitual.*

[166] Elaborada en el seno de la Comisión de Las Naciones Unidas para el derecho mercantil Internacional. Viena, 11 de abril de 1980.

Es conforme a estos tres lineamientos que la llegada de la respuesta con la aceptación de la oferta es elemento determinante de la perfección del contrato. Asimismo, la "llegada" de la oferta al destinatario, la declaración de aceptación o cualquier otra manifestación de intención es cuando se le comunica verbalmente o se entrega por cualquier otro medio al destinatario personalmente, o en su establecimiento o dirección postal o, si no tiene establecimiento ni dirección postal, en su residencia habitual. En igual sentido, todo MD integrante del proceso de formación del contrato entre ausentes produce efectos al momento de su llegada a su destinatario, por ende, los contratos mercantiles electrónicos internacionales dentro del derecho mexicano requieren de la llegada de la voluntad al destinatario del MD, por lo que no resulta relevante en qué momento se tuvo conocimiento de él o en qué momento se emitió. Sin embargo, siempre que se cumpla con la obligación objeto del contrato por parte del ofertado o contraofertado se traduce en aceptación, por lo que en ese instante se produce el perfeccionamiento del contrato.

En este sentido, al abordar los bemoles de la aplicación del derecho sustantivo derivadas del previo acuerdo de negociación entre las partes, implica que debe tomarse en cuenta la participación de cuatro elementos que pueden localizarse en jurisdicciones diferentes del negocio:

1) Sistema de información,
2) Proveedor de Servicios de Internet (PSI)
3) Iniciador del MD
4) Destinatario del MD

Es pertinente señalar, antes de desagregar estos cuatro puntos, que estos elementos se desprenden del reconocimiento que hace el artículo de la 15 LMCE 1996, de la dificultad de la determinación del tiempo y el lugar cuando se emplean comunicaciones electrónicas pues los usuarios del comercio electrónico y otros medios de comunicación se comunican de un Estado a otro sin percatarse de la ubicación de los sistemas de información por medio de los cuales se efectúa la comunicación.

Algunas consideraciones deben establecerse en orden al derecho sustantivo aplicable:

- **A.** Momento de expedición del MD.
- **B.** Momento de recepción del MD

A. Respecto al momento de expedición del MD, el artículo 15.1 de la Ley CNUDMI:

> ***Artículo 15. —*** *Tiempo y lugar del envío y la recepción de un mensaje de datos.*
> *1) De no convenir otra cosa el iniciador y el destinatario, el mensaje de datos se tendrá por expedido cuando entre en un sistema de información que no esté bajo el control del iniciador o de la persona que envió el mensaje de datos en nombre del iniciador.*

Del numeral anterior se advierte que hay dos requisitos para que ocurra el envío de un MD:

a) Que el mensaje entre en un sistema de información distinto del sistema de información en el que ha sido generado: no basta por tanto que haya salido de éste último sistema sino que es necesario que salga del mismo y en otro sistema.
b) Que el sistema en el que el MD entra no esté bajo control del iniciador o de su representante sino, que, por consiguiente, quien ejerza el control sobre el sistema de información en el que el MD entra sea bien directamente el destinatario del MD o un tercero. Ello sucede cuando en su recorrido, por muy rápido que sea, el MD necesite recorrer redes, atravesar nudos y ser objeto de otros servicios de teletransmisión prestados por terceros, generalmente Proveedores de Servicios de Internet.

En este sentido, se aprecian dos nociones que trascienden en el significado de la expedición del MD: el de ***control*** *y el de* ***entrada***.

En el caso de ***control*** se trata de un MD que entra en un sistema de información no controlado por su iniciador es un MD que ha comenzado el trayecto hacia su destinatario sin que pueda la llegada y recepción ser evitada por el iniciador. La ignorancia o mal funcionamiento de los intermediarios y sus sistemas podrían evitar la recepción.

En tanto que la noción ***entrada*** permite comprender el uso de llegada de un MD en un sistema de información distinto de aquel momento en que puede ser procesado en ese sistema de información, esto es, cuando se hace accesible a su destinatario. En este sentido, la entrada coincide con la disponibilidad del MD para ser procesado en un sistema de información distinto del de su iniciador, lo cual difiere de su procesamiento (descifrado, impresión, reenvío, etc.)

Cuando el párrafo 1) del artículo 15 de esa Ley Modelo de la CNUDMI de Comercio Electrónico 1996, dispone que un MD se considerará **expedido** a partir del momento en que entre en un sistema de información que no esté bajo el control del iniciador, el concepto "**expedición"** se refiere al comienzo de la transmisión electrónica del MD, donde la expedición se produce cuando el MD llega al sistema de información del destinatario, la expedición según el párrafo 1) y la recepción según el párrafo 2) son simultáneos, excepto cuando el MD se expida a un sistema de información del destinatario que no sea el sistema designado por el destinatario con arreglo al inciso a) del párrafo 2) .

B. Respecto al momento de recepción del MD se afirma que corresponde con el momento de entrada de tal MD en el sistema de información de su destinatario. El lineamiento lo establece el artículo 15.2) de la de la Ley CNUDMI.

> ***Artículo 15. —*** *Tiempo y lugar del envío y la recepción de un mensaje de datos*
> *(…)*
> *2) De no convenir otra cosa el iniciador y el destinatario, el momento de recepción de un mensaje de datos se determinará como sigue:*
> *a) Si el destinatario ha designado un sistema de información para la recepción de mensajes de datos, la recepción tendrá lugar:*

i) En el momento en que entre el mensaje de datos en el sistema de información designado; o
ii) De enviarse el mensaje de datos a un sistema de información del destinatario que no sea el sistema de información designado, en el momento en que el destinatario recupere el mensaje de datos;
b) Si el destinatario no ha designado un sistema de información, la recepción tendrá lugar al entrar el mensaje de datos en un sistema de información del destinatario.

El *quid* del asunto es determinar de manera precisa en qué sistema de información tiene entrada el MD. Existen cuatro situaciones que complican la fijación del momento de entrada[167]:

- **I.** Indicación en particular de un sistema de información. Lo cual corresponde con la disponibilidad para el procesamiento del MD por el sistema de información.
- **II.** No indicación en particular de un sistema de información por el destinatario. Se considerará que existe entrada cuando el MD entre en un sistema de información del destinatario.
- **III.** Envío de MD a sistema de información no indicado por el destinatario. En esta situación no existirá jurídicamente entrada del MD en el sistema de información.
- **IV.** Envío de un MD a un sistema de información no indicado por el destinatario aun cuando este se encuentra bajo control del destinatario. En este caso únicamente existirá entrada del MD si el destinatario recupera el MD a partir del sistema de información no indicado pero por él controlado, en esta hipótesis el momento de la entrada será el de la recuperación y accesibilidad y no el de llegada al sistema de información no indicado aun cuando éste este bajo control del destinatario.

Además y de manera separada a las situaciones anteriores, las comunicaciones digitales posibilitan que se presente un caso más, consistente en que un sistema de información en el que entra un determinado MD se localice en ubicación distinta a aquel en el que se tiene por recibido el MD, ello deriva en que exista un lugar de envío y un lugar de recepción.

Ahora, el párrafo 2) del artículo 15 de la Ley Modelo al precisar el momento de recepción de un MD, señala que cuando el destinatario designa unilateralmente un determinado sistema de información para la recepción de un mensaje (en cuyo caso el sistema designado puede o no ser un sistema de información del destinatario), y el mensaje llega a un sistema de información del destinatario que no es el sistema designado. En este caso, la recepción tendrá lugar cuando el destinatario recupere el MD. Agrega que el *sistema de información designado* será el sistema que una parte haya designado específicamente, por ejemplo, en el caso en que una oferta estipule expresamente el domicilio al cual se debe enviar la aceptación.

En cuanto a la noción de "entrada" en un sistema de información, utilizado para definir tanto la expedición como la recepción de un MD. Este entra en un sistema de información desde el momento en que puede ser procesado. Si bien es cierto que dentro de la Ley Modelo no existe pronunciamiento respecto a si dicha entrada puede ser en un sistema de información artificial, lo cierto es que los usos comerciales y la propia legislación mexicana le dan cabida.

[167] Illescas Ortíz, Rafael: Derecho de la contratación electrónica, 2009, 2ª ed., Madrid, Civitas Thomson Reuters, pp. 258-259.

Un MD no habría de considerarse expedido si simplemente ha llegado al sistema de información del destinatario, pero sin conseguir entrar en él.

2.8.1. Lugar de perfección del contrato.

Tanto LMCE 1996 como la CNUCCIM de 11 de abril de 1980 coinciden en que el lugar de llegada o recepción de MD debe corresponder con el lugar del establecimiento de su destinatario, mientras que, el de emisión debe concordar con el del establecimiento del iniciador[168].

La anterior consideración, es una respuesta inmediata a la interrogante de cuál será el lugar de perfección del contrato en el caso de que no se ha pactado entre las partes un lugar en específico, pues siendo el supuesto que exista un convenio entre las partes -lo que evitaría muchos problemas-, estas podrían citar el lugar de ubicación donde se encuentra el sistema de información. Lo cierto es que la carencia de contrato marco o convenio previo entre las partes establece la aplicación del derecho sustantivo que resulte aplicable.

El lugar de recepción de un MD el párrafo 4) del multicitado artículo 15, plantea que frecuentemente un sistema d*e* información del destinatario en el que se recibe o recupera el MD no se halla bajo la misma jurisdicción que el destinatario, razón por la cual debe garantizarse que el lugar en que se encuentra el sistema de información no sea el elemento determinante, y que haya un vínculo razonable entre el destinatario y lo que se considere el lugar de recepción, y que el iniciador pueda determinar fácilmente ese lugar. Asimismo, este párrafo incluye la noción de la "operación subyacente", como las operaciones subyacentes efectivamente realizadas y previstas. Las referencias a "establecimiento", "establecimiento principal" y "lugar de residencia habitual" se introdujeron en el texto para homologarlo con el numeral 10 de la CNUCCIM.

En este sentido el fin del párrafo aludido es incluir una diferencia entre el lugar considerado de recepción y el lugar al que haya llegado realmente el MD en el momento de recepción a que se refiere el párrafo 2)[169].

2.8.2. Los mercados electrónicos cerrados o canales de ventas de *e-marketplaces*

Los mercados electrónicos cerrados o *e-marketplaces* son conocidos como mercado en sitios web que reúnen una gran cantidad de compradores y vendedores internacionalmente, los cuales ofertan y demandan productos de manera virtual y el acuerdo de voluntades se genera sólo entre aquellos que han accedido al entorno cerrado que el mercado establece y donde, solo es posible generalmente, negociar las condiciones relativas al precio, cantidad, calidad, plazo y modo de entrega, y el resto de las cláusulas del convenio deriva de una aceptación de condiciones generales de adhesión, ejemplo de ellos son: Amazon, eBay y Mercado Libre. Una de las principales ventajas de los *e-marketplaces* es que permiten a personas que no

[168] Illescas Ortíz, Rafael: Derecho de la contratación electrónica, 2009, 2ª ed., Madrid, Civitas Thomson Reuters, pp. 261.
[169] CNUDMI, Ley Modelo de la CNUDMI sobre Comercio Electrónico 1996 y su Guía para la incorporación de la Ley al derecho interno, Naciones Unidas, Nueva York, 1997, p. 59.

necesariamente se dedican al comercio, ofrecer sus productos por Internet sin necesidad de contar con una página web propia, ni de mayores conocimientos en diseño web.

El acceso a un *e-marketplace* se configura por medio de un contrato que debe ser requisitado por el solicitante con el administrador del mercado denominado "contrato de acceso", "de uso" o "de pertenencia". Dicho contrato es un contrato de adhesión con condiciones generales, lo que significa que el solicitante no tiene capacidad de redacción ni de negociación de las condiciones que regulan el acceso y la pertenencia al mercado y que su decisión se reduce a aceptar la oferta, *take-or-leave-it*, que efectúa el administrador a través de su sitio web, lo anterior asegura la uniformidad en el acceso de todos los participantes. [170]

Dentro el clausulado se encuentra la relativa al lugar en el que se perfecciona el contrato, que normalmente es la ubicación en que se encuentra establecido el administrador del *e-marketplace* criterio que puede ir en contra de todo lo dicho en los subtítulos precedentes. No obstante, la Unión Europea regula este tipo de mercados por ser mercados susceptibles de configuración de Proveedores de Servicios de Internet, mientras el CCo de nuestro país no menciona nada al respecto, lo que implica que lo deja al arbitrio de las partes y en particular, del usuario de este tipo de plataformas, lo que desde el punto de vista de la protección del consumidor deja en un estado de preocupación bajo el pretexto legal de que al comercio electrónico se le aplican las mismas reglas que el comercio tradicional o presencial, sin considerar que las ofertas que ahí se configuran, la publicidad y un procedimiento de gestión y reclamación custodiado desde otro país, lo que torna problemáticas las negociaciones.

2.8.3. Elementos de existencia y validez en la perfección del contrato: capacidad de las partes y error electrónico:

Los artículos 1794 y 1795 del CCiF establecen los elementos de existencia y validez de los contratos, entre los cuales, se citan dos que merecen especial atención, el primero se refiere a la incapacidad de las partes y, el segundo, el error como vicio de consentimiento en la contratación.

En cuanto a la acreditación de la capacidad y personalidad de las partes, en México no existe una inscripción de la persona física o moral comerciante que cuente con un sitio web comercial que oferte productos y servicios al público cibernauta, cuya anotación correspondería en principio al Registro Público de Comercio de la Secretaría de Economía (RPCSE)[171], razón por la

[170] Cfr. Rodríguez de las Heras Ballell, Teresa, "El régimen jurídico de los mercados electrónicos cerrados (e-Marketplaces): Contrato de Acceso (desde la perspectiva de los participantes)", en E-business de eMarket Services España, Agosto 2006, p.4, accesible en http://www.emarketservices.es/FicherosEstaticos/auto/0806/Libro%20Teresa-rev1-participantes_22051_.pdf

[171] Menos aun existen en los Registros Públicos de la Propiedad y de Comercio del Distrito Federal o de las Entidades Federativas. Por ejemplo, en el caso del Gobierno de la Ciudad de México, un comerciante debe cumplir con el requisito de llenar los siguientes formatos.

1) Sistema electrónico de avisos y permisos de establecimientos mercantiles de la Secretaria de Desarrollo Económico del DF (SI@PEM) es el medio Único de registro para que las personas físicas o morales puedan presentar sus avisos, solicitudes de permiso, registros o autorizaciones para la apertura y funcionamiento de un establecimiento mercantil en el Distrito Federal.

cual la forma de saber si la apertura de un negocio está supervisada por la entidad gubernamental correspondiente, deriva de que haya sido constituido como establecimiento mercantil físico no virtual, ello implica que contará con todos los documentos necesarios para ello: permiso de uso de suelo, aviso de declaración de apertura de establecimientos mercantiles, licencia de funcionamiento (en caso de venta de productos alimenticios, bebidas alcohólicas), anuncio exterior e inscripción al registro federal de contribuyentes, en el caso de la creación de una sociedad mercantil se debe contar también con un alta ante la Secretaría de Economía (SE). Trámites que son elementos seguridad jurídica que se traducen en la certeza que tiene un consumidor en el ámbito comercial.

Esta idea de certeza jurídica para el consumidor se ve avalada por los documentos inscribibles en el RPCSE que exige el artículo 25 de CCo:

I.- Instrumentos públicos otorgados ante notario o corredor público;
II.- Resoluciones y providencias judiciales o administrativas certificadas;
III.- Documentos privados ratificados ante notario o corredor público, o autoridad judicial competente, según corresponda, o
IV.- Los demás documentos que de conformidad con otras leyes así lo prevean.

Lo anterior es así, porque en países de la Unión Europea se ha extendido el requisito de solicitar un registro en línea de los negocios que administran y oferten en sitios web comerciales, particularmente en España, el artículo 3 de la Instrucción de la Dirección General de los Registro y el Notariado de 17 de febrero de 1998 (BOE no. 50 de 27 de febrero de 1998), solicita que las personas morales realicen tal registro, además de que obliga a que se inscriban sentencias o resoluciones que inhabiliten un comercio electrónico y no virtual también, ello permite que un consumidor pueda llevar a cabo consultas electrónicas sobre el sitio web con el que quiere realizar una contratación electrónica, no obstante, este no es el caso de las personas físicas con actividad comercial, pues ello no es un requisito, independientemente de lo deseable que es contar con un sistema electrónico que permita conocer su capacidad para obrar en actividades comerciales.

Por otra parte, la falta de capacidad de actuar suele tolerarse por la contraparte en aras a la celeridad y al volumen de negocios, sin embargo, tanto en el CCo como en la Ley de FEA, tener una firma digital implica que un prestador de servicios de certificación ya comprobó la capacidad de actuar de las partes, pues a su falta no otorgaría su reconocimiento consistente en un certificado.

En cuanto al error informático es una situación dudosa cuando se presenta, en atención a la facilidad entre las partes de comprobar electrónicamente la voluntad emitida en un MD, si se tiene presente el principio del acuse de recibo y de la confirmación del MD por ambas partes. En este sentido el numeral 14.1. de la Convención de las Naciones Unidas sobre la Utilización

2) Certificado de uso de suelo
3) Capacidad de aforo (capacidad de atención y espacio del establecimiento mercantil)
4) Autorización de seguridad y operación

de las Comunicaciones Electrónicas en los Contratos Internacionales (Nueva York, 2005), define al error en las comunicaciones y señala una solución supletoria para este.

> *1. Cuando una persona física cometa un error al introducir los datos de una comunicación electrónica intercambiada con el sistema automatizado de mensajes de otra parte y dicho sistema no le brinde la oportunidad de corregir el error, esa persona, o la parte en cuyo nombre ésta haya actuado, tendrá derecho a retirar la parte de la comunicación electrónica en que se produjo dicho error, si:*
> *a) La persona, o la parte en cuyo nombre haya actuado esa persona, notifica a la otra parte el error tan pronto como sea posible después de haberse percatado de éste y le indica que lo ha cometido; y si*
> *b) La persona, o la parte en cuyo nombre haya actuado esa persona, no ha utilizado los bienes o servicios ni ha obtenido ningún beneficio material o valor de los bienes o servicios, si los hubiere, que haya recibido de la otra parte.*
> *2. Nada de lo dispuesto en el presente artículo afectará a la aplicación de regla de derecho alguna que regule las consecuencias de un error cometido, a reserva de lo dispuesto en el párrafo 1.*

El anterior artículo exhibe una postura unilateral pues dispone que el error podrá devolver el bien o servicio si cumple con las dos inicios señalados.

2.9. Administración electrónica del contrato de tracto sucesivo.

Las variaciones contractuales a que puede sujetarse un contrato incluyen diferentes situaciones e incidentes durante la vigencia de ellos, como lo son los actos preparativos de ciertos contratos o en los que se realizan durante una duración en prolongada, muchas transacciones concernientes al mismo, este es el caso del contrato de depósito, bursátil, bancario, de transporte y de seguro.

Existen tres supuestos que se pueden dar en contrataciones de larga duración[172]:

1) *La validez de los actos que se generaron como actos manuales o verbales y que después podrían ser migrados a soporte electrónico,*
2) *Las diferentes actividades susceptibles de ser realizadas por la partes como gestiones, contabilidad y operaciones contractuales.*
3) *La electronificación de los sucesivos actos de ejecución y novación de así como los preparatorios de ellos, con ello hacemos alusión a la suscripción de garantías, adelantos y deducciones, ampliaciones de plazo de subcontratación y penalidades*.

De las tres hipótesis, la tercera hipótesis reviste especial importancia porque ni el uso del documento electrónico ni de la FEA se restringen sólo a la perfección o formación del contrato sino también a una cantidad significativa de actos electronificables de ejecución contractual, algunas de tracto sucesivo, otras como actos de gestión, administración, cumplimiento o novación contractuales, que por su importancia y efectos entre las partes y frente a terceros se

[172] Illescas Ortíz, Rafael: Derecho de la contratación electrónica, 2009, 2ª ed., Madrid, Civitas Thomson Reuters, p. 287.

tornan trascendentales en la contratación electrónica, en razón de que la propia regulación de la FEA establece el principio de equivalencia funcional entre el MD y el documento en soporte de papel.

Además, el artículo 11 de la *Ley Modelo CNUDMI sobre comercio electrónico* de 1996, refiere:

> ***Artículo 11.*** *— Formación y validez de los contratos*
> *1) En la formación de un contrato, de no convenir las partes otra cosa, la oferta y su aceptación podrán ser expresadas por medio de un mensaje de datos. No se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación un mensaje de datos.*
> *2) Lo dispuesto en el presente artículo no será aplicable a: [...].*

Podría marcar una dirección de la equivalencia funcional, esto es, solo a la formación y validez de los contratos, y no así a la electronificación de otro tipo de actos, ello queda subsanado con la regulación mexicana de la FEA, que establece el principio de equivalencia funcional entre el MD y el documento en soporte de papel.

Las implicaciones que citamos en relación a la electronificación de los actos sucesivos de ejecución y novación, se esclarecen con el ejemplo del contrato de seguro de tracto sucesivo, el cual, tan sólo, se caracteriza por las siguientes operaciones escritas y por ende, electronificables:

I. Modificación de póliza,
II. Adiciones a la póliza,
III. Documento de cobertura provisional de la póliza,
IV. Declaración de riesgo,
V. Declaración de alteración de riesgo,
VI. Rescisión del contrato,
VII. Modificación del contrato,
VIII. Declaración de siniestro,
IX. Dictamen de daños asegurados,
X. Declaración de alimento de pólizas flotantes o de abono,
XI. Declaración de alimento de pólizas en seguro de grupo,
XII. Certificado de seguro,
XIII. Resolución de seguro de vida,
XIV. Designación de beneficiaros y su revocación,
XV. Petición de rescate,
XVI. Petición de reducción,
XVII. Cesión de póliza,
XVIII. Pignoración de póliza, etc.

Imaginemos que si se ha producido el siniestro y sobrevienen numerosas comunicaciones derivadas de la reclamación del asegurado o beneficiario, se incluirá la valoración de peritos sobre los daños del siniestro hasta la indemnización.

Un caso similar es el contrato de transporte de mercancías, que es el único caso de contratos especiales que regula el artículo 16 de la Ley Modelo CNUDMI sobre comercio electrónico de 1996:

> ***Artículo 16. —*** *Actos relacionados con los contratos de transporte de mercancías Sin perjuicio de lo dispuesto en la parte I de la presente Ley, el presente capítulo será aplicable a cualquiera de los siguientes actos que guarde relación con un contrato de transporte de mercancías, o con su cumplimiento, sin que la lista sea exhaustiva:*
> *a) i) indicación de las marcas, el número, la cantidad o el peso de las mercancías;*
> *ii) declaración de la índole o el valor de las mercancías;*
> *iii) emisión de un recibo por las mercancías;*
> *iv) confirmación de haberse completado la carga de las mercancías;*
> *b) i) notificación a alguna persona de las cláusulas y condiciones del contrato;*
> *ii) comunicación de instrucciones al portador;*
> *c) i) reclamación de la entrega de las mercancías;*
> *ii) autorización para proceder a la entrega de las mercancías;*
> *iii) notificación de la pérdida de las mercancías o de los daños que hayan sufrido;*
> *d) cualquier otra notificación o declaración relativas al cumplimiento del contrato;*
> *e) promesa de hacer entrega de las mercancías a la persona designada o a una persona autorizada para reclamar esa entrega;*
> *f) concesión, adquisición, renuncia, restitución, transferencia o negociación de algún derecho sobre mercancías;*
> *g) Adquisición o transferencia de derechos y obligaciones con arreglo al contrato.*
>
> ***Artículo 17.*** *— Documentos de transporte*
> *1) Con sujeción a lo dispuesto en el párrafo 3), en los casos en que la ley requiera que alguno de los actos enunciados en el artículo 16 se lleve a cabo por escrito o mediante un documento que conste de papel, ese requisito quedará satisfecho cuando el acto se lleve a cabo por medio de uno o más mensajes de datos.*
> *2) El párrafo 1) será aplicable tanto si el requisito en él previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que no se lleve a cabo el acto por escrito o mediante un documento.*
> *3) Cuando se conceda algún derecho a una persona determinada y a ninguna otra, o ésta adquiera alguna obligación, y la ley requiera que, para que ese acto surta efecto, el derecho o la obligación hayan de transferirse a esa persona mediante el envío, o la utilización, de un documento, ese requisito quedará satisfecho si el derecho o la obligación se transfiere mediante la utilización de uno o más mensajes de datos, siempre que se emplee un método fiable para garantizar la singularidad de ese mensaje o esos mensajes de datos.*
> *4) Para los fines del párrafo 3), el nivel de fiabilidad requerido será determinado a la luz de los fines para los que se transfirió el derecho o la obligación y de todas las circunstancias del caso, incluido cualquier acuerdo pertinente.*
> *5) Cuando se utilicen uno o más mensajes de datos para llevar a cabo alguno de los actos enunciados en los incisos f) y g) del artículo 16, no será válido ningún documento utilizado para llevar a cabo cualquiera de esos actos, a menos que se haya puesto fin al uso de mensajes de datos para sustituirlo por el de documentos. Todo documento que se emita en esas circunstancias deberá contener una*

declaración a tal efecto. La sustitución de mensajes de datos por documentos no afectará a los derechos ni a las obligaciones de las partes.
6) Cuando se aplique obligatoriamente una norma jurídica a un contrato de transporte de mercancías que esté consignado, o del que se haya dejado constancia, en un documento, esa norma no dejará de aplicarse a un contrato de transporte de mercancías del que se haya dejado constancia en uno o más mensajes de datos por razón de que el contrato conste en ese mensaje o esos mensajes de datos en lugar de constar en un documento.
7) Lo dispuesto en el presente artículo no será aplicable a: [...].

El estudio los artículos anteriores, dejan ver la cantidad y variedad de comunicaciones y gestiones de trasportes pactados entre cargador, transportista, consignatario e incluso con terceras personas cesionarias de los derechos derivados del contrato

2.10. Los terceros y los derechos contractuales generados electrónicamente.

En razón de que en los contratos se realizan estipulaciones en favor de tercero y que la estipulación hecha a favor de éste hace que adquiera el derecho de exigir del promitente la prestación a que se ha obligado, estos derechos también son incluidos en las contrataciones mercantiles electrónicas.

En este contexto y de conformidad con el artículo 1870 del CCiF, el derecho de tercero nace en el momento de perfeccionarse el contrato, salvo la facultad que los contratantes conservan de imponerle las modalidades que juzgue convenientes, siempre que éstas consten expresamente en el referido contrato; por ende, ello implica que los derechos o sus resultas patrimoniales de esos contratos que pudieran ejercitarse y transmitirse a terceras personas (cesionarios) por parte de sus titulares (cedentes), también pueden tener un destino contractual electrónico. Los casos tradicionales, son: el endoso de títulos, los seguros pactados por cuenta de terceros, cuyo cumplimiento se efectuaría como una gestión del contrato de tracto sucesivo y los contratos de transporte tanto nacional como internacional.

De conformidad con el artículo 22 del CCo cuando, conforme a la ley, algún acto o contrato deba inscribirse en el Registro Público de la Propiedad o en registros especiales para surtir efectos contra terceros, su inscripción en dichos registros será bastante.

Las dependencias y organismos responsables de los registros especiales deberán coordinarse con la SE para que las garantías mobiliarias y gravámenes sobre bienes muebles que hayan sido inscritos en dichos registros especiales puedan también ser consultados a través del Registro Único de Garantías Mobiliarias (RUG), en los términos que establezca el Reglamento del Registro Público de Comercio (RRPG).

2.10.1. Estipulación a favor de tercero.

Basta mencionar que la estipulación a favor de tercero, no es más que un contrato a favor de tercero, gracias al cual los contratantes acuerdan otorgar a una persona, que no es una de las

contratantes, uno, varios o la totalidad de los derechos que el contrato genera. Los elementos, más no requisitos, que la conforman son básicamente cuatro:

1. No hay una forma específica de contrato a favor de tercero,
2. El tercero que se beneficia no debe otorgar su aceptación para la adquisición del derecho objeto de estipulación.
3. En caso de producirse la aceptación del beneficiado no se somete a formalidad, pues solo es una declaración unilateral de voluntad.
4. La notificación de la aceptación al contratante que la estipuló por parte del beneficiario, impide la revocación de la estipulación en su contra. El lugar que el beneficiario adquiere de la estipulación y la comunicación sobre la aceptación hacen que sea oponible frente a terceros.

Así como los cuatro elementos anteriores no son requisitos, la electronificación del contrato a favor de tercero, tampoco lo es, en realidad, la eficacia depende de comunicación entre el beneficiario y el promitente.

2.10.2. Cesión de derechos contractuales.

Nuestro CCiF reconoce la transmisión de tres tipos de obligaciones: la cesión de derechos, la cesión de deudas y la subrogación.

El primer supuesto está regulado del artículo 2029 al 2050 del Código y establece que habrá cesión de derechos cuando el acreedor transfiera a otro los que tenga contra su deudor. El acreedor puede ceder su derecho a un tercero sin el consentimiento del deudor, a menos que la cesión esté prohibida por la ley, se haya convenido no hacerla o no la permita la naturaleza del derecho.

El deudor no puede alegar contra el tercero que el derecho no podía cederse porque así se había convenido, cuando ese convenio conste en el título constitutivo del derecho.

En la cesión de crédito se observarán las disposiciones relativas al acto jurídico que le dé origen (artículos 2033 a 2055 del CCi).

La cesión de un crédito comprende la de todos los derechos accesorios como la fianza, hipoteca, prenda o privilegio, salvo aquellos que son inseparables de la persona del cedente. Los intereses vencidos se presume que fueron cedidos con el crédito principal.

La cesión de créditos civiles que no sean a la orden o al portador, puede hacerse en escrito privado que firmarán cedente, cesionario y dos testigos. Sólo cuando la ley exija que el título del crédito cedido conste en escritura pública, la cesión deberá hacerse en esta clase de documento.

Cuando no se trate de títulos a la orden o al portador, el deudor puede oponer al cesionario las excepciones que podría oponer al cedente en el momento en que se hace la cesión. Si tiene contra el cedente un crédito todavía no exigible cuando se hace la cesión, podrá invocar la compensación con tal que su crédito no sea exigible después de que lo sea el cedido. Finalmente, para que el cesionario pueda ejercitar sus derechos contra el deudor, deberá hacer a éste la notificación de la cesión, ya sea judicialmente, ya en lo extrajudicial, ante dos testigos o ante notario. (Artículos 2033, 2035 y 2036).

En tanto, el CCo establece en sus artículos 389, 390 y 391 las cesiones de créditos no endosables y señala que los créditos mercantiles que no sean al portador ni endosables, se transferirán por medio de cesión. La cesión producirá sus efectos legales con respecto al deudor, desde que le sea notificada ante dos testigos y contra terceros a partir de su inscripción en la Sección Única del RUG del Registro Público de Comercio. Salvo pacto en contrario, el cedente de un crédito mercantil responderá tan solo de la legitimidad del crédito y de la personalidad con que hizo la cesión.

En este sentido, reviste especial importancia la notificación electrónica donde se acepta la estipulación de tercero, en atención a que el deudor quedará obligado para con el beneficiario en razón de tal notificación, y desde que tenga lugar no se reputará pago legítimo sino el que se hiciere a éste. Por lo que el pago del derecho con el deudor, que será el único obligado en relación con el acreedor notificado.

No es discutible la electronificabilidad de cualquier transferencia electrónica así como tampoco lo es la trascendencia de la comunicación que se haga de esta, a menos que se haya estipulado entre la partes lo contrario, como por ejemplo que la misma se haga sin que medien MD, dado que los alcances de la electronificabilidad son amplios de acuerdo a las disposiciones de nuestro CCo.

2.10.3. Electronificación de títulos valores.

Partiendo del hecho de que los títulos valor son regulados por la Ley de Mercado de Valores (LMV) y los títulos de crédito por la Ley General de Títulos y Operaciones de Crédito (LGTOC), esto es ninguno es regulado por el CCo. Ambos títulos son parte del comercio electrónico en general. Por ello, precisamos las diferencias entre los títulos valores y títulos de crédito, sobretodo porque la electronificación de los segundos no se encuentra aún regulada en México[173].

Los títulos de crédito son documentos que tienen incorporado un derecho económico en el texto del mismo, que a decir de la propia LGTOC son los documentos necesarios para ejercitar el derecho literal que en ellos se consigna y son exclusivamente los documentos señalados en esta ley.

[173] Ver el caso de Colombia.

Las características de los títulos de crédito son la circulación, la incorporación de un derecho; la literalidad (que obliga al deudor en los términos del documento); la autonomía (que da al documento un valor intrínseco); la legitimación (que consiste en que el tenedor del documento debe detentarlo legalmente).

Las clases de títulos de crédito son:

1) letra de cambio,
2) cheque,
3) pagaré y
4) certificados bursátiles y los certificados de participación.

Por su parte, los títulos valores, son una obligación de pago de una entidad privada o pública, que tiene un contenido económico sujeto al vencimiento y una tasa de interés o de rendimiento sujeta a una determinada Ley y de acuerdo a la fluctuación económica del mercado, podría decirse que son una especie de los títulos de crédito pero se diferencia de estos en que son documentos que no están destinados a circular, sino que sirve exclusivamente para identificar quien tiene derecho a exigir la prestación que en éste se consigna; ejemplos de ellos son: las acciones de empresas, los certificados de vivienda, los certificados de entidades fiduciarias, los certificados de depósito de los almacenes generales de depósito, cetes, petrobonos, entre otros.

De conformidad con la reforma del 10 de enero de 2014 a la LMV, el artículo 282 estableció que los títulos valores objeto de depósito en instituciones para el depósito de valores, podrán ser representados en títulos múltiples o en un solo título que amparare parte o la totalidad de los valores materia de la emisión y del depósito. Tales títulos podrán emitirse de manera electrónica en forma de MD con FEA de acuerdo con lo establecido en el CCo y de conformidad con las disposiciones de carácter general que emita el Banco de México, que comprendan, entre otros aspectos, los títulos que podrán emitirse utilizando medios electrónicos, así como las características específicas y de seguridad que deberán reunir para tales efectos. Además, los títulos que se encuentren emitidos en medios impresos, podrán sustituirse de manera electrónica en los términos del presente párrafo de conformidad con las disposiciones de carácter general que emita el Banco de México.

Se debe recordar que los títulos valores han sido medios de circulación del crédito relevantes en el comercio[174] y son una creación del tráfico mercantil. Actualmente existe un avance en varios países en materia de circulación crediticia donde los derechos de crédito de circulación autónoma ya no son representados en papel, lo cual facilita las transacciones.

Si bien es cierto que los medios computaciones han sido de gran utilidad para permitir la circulación crediticia, el uso de las TIC no es sinónimo de desmaterialización de los títulos valor.

[174] En voz Gustav Radbruch: “El comerciante crea su propio Derecho allí donde la ley calla”. Ver: Introducción a la ciencia del Derecho, Madrid, 1930.

La inmediatez y seguridad jurídica en la circulación de títulos valores no son las únicas ventajas de su electrificación; Gómez Diez menciona 3 beneficios:

> *1) Económicas: permiten al inversionista comprar y vender en un mínimo tiempo y evitan distorsiones en el precio generadas por la demora en la entrega de los certificados emitidos o bien producidas por el ahorro de costes de transacción.*
> *2) De control: permiten recibir la información sobre las transacciones de valores en el mercado secundario en tiempo real y posibilitan el control de todos los títulos emitidos por un mismo emisor.*
> *3) Jurídicas: se reduce la posibilidad del fraude, al crear mayor seguridad jurídica, y puede darse la verificación automática de su contenido y validez.* [175]

El autor colombiano citado[176], en relación con los títulos valor aborda varias situaciones sobre la desmaterialización de la letra de cambio:

> 1. La desmaterialización del título valor en su emisión y en la sucesiva incorporación de derechos.
> 2. La desmaterialización de la circulación.
> 3. La acreditación del título valor y sus derechos: la acreditación de la regular circulación y el ejercicio de la acción cambiaria.

La problemática de estas tres situaciones se basa en que a falta de acción cambiaria, no tiene razón de ser los títulos valores electrónicos.

La desmaterialización no se ha desarrollado en el abanico de títulos valores, no obstante, en Inglaterra ya se planteó el cheque electrónico. Le corresponde a los doctrinarios estudiar la compatibilidad de estas nuevas figuras con la teoría tradicional de los títulos y operaciones de crédito, de qué manera afecta la desmaterialización a las características comunes de los títulos valores, la cual posiblemente requiera una reformulación terminológica[177] y plantear iniciativas de reforma.

Es loable la regulación respecto a la circulación electrónica de títulos valores en Colombia a través de la figura de depósito centralizado de títulos y los valores representados por anotaciones en cuentas, como forma de circulación de títulos valores de conformidad con el artículo 2.14.2.15 del Decreto 3960 del 25 de octubre 2010; el cual establece en el *Libro 14: Normas aplicables a los depósitos centralizados de valores*, el cual reza lo siguiente:

---

[175] Gómez Díez, José Luis. El título valor electrónico: especial referencia a la letra de cambio electrónica y la actuación notarial, 2009, Mallorca, en Títulos valores electrónicos, por la Dirección General de Investigación del Ministerio de Educación y Ciencia, p. 102.
[176] Ibídem, p. 102.
[177] En tal sentido pronuncia Musitani, Alfredo, Desmaterialización de títulos valores, 2006, Revista Argentina de Derecho Empresario, No. 5, accesible en : http://www.ijeditores.com.ar/articulos se.php?idarticulo=42143&print=2, consulado el 2 de febrero de 2015.

Artículo 2.14.2.1.5. Custodia y administración de títulos valores e instrumentos financieros. *Los depósitos centralizados de valores podrán custodiar y administrar valores, títulos valores de contenido crediticio, de participación, representativos de mercancías e instrumentos financieros que no se encuentren inscritos en el* ***Registro Nacional de Valores y Emisores -RNVE****-, ya sea que se emitan o negocien localmente o en el exterior, previa solicitud del emisor o su mandatario, del administrador de la emisión, del custodio en el exterior o del depositante directo local o extranjero, en la forma y condiciones que señale el reglamento del depósito centralizado de valores. Esta actividad se ejercerá con estricta observancia de las normas cambiarias y tributarias aplicables.*

Parágrafo. *Las disposiciones del presente Libro relativas a la* ***anotación en cuenta*** *serán aplicables en lo pertinente a los títulos valores de contenido crediticio o de participación, que reciban en custodia tales depósitos. En este caso, se entenderá que la entrega y/o endoso de los títulos valores se efectuará mediante la* ***anotación en cuenta*** *siempre que, en relación con el endoso, la orden de transferencia que emita el endosante cumpla con los requisitos pertinentes establecidos en la Ley. Los títulos valores indicados en este parágrafo conservaran todos los derechos, acciones y prerrogativas propias de su naturaleza, consagradas en la legislación mercantil.*

(Énfasis añadido)

La "Anotación en Cuenta" considera con varios principios e implicaciones jurídicas, a saber:

Principio	Implicaciones jurídicas[178]
Prioridad	Una vez que se realiza un registro no puede practicarse ningún otro respecto de los mismos valores o derechos que obedezca a un hecho producido con anterioridad en lo que resulte opuesto o incompatible con dicho registro
Tracto sucesivo	Los registros sobre un mismo derecho anotado deberán estar encadenados cronológica, secuencial e ininterrumpidamente, de modo que quien transmite el valor o derecho aparezca previamente en el registro
Rogación	Para realizar cada registro se necesita solicitud previa del titular del valor o derecho registrado o de la entidad competente y autorizada para tal fin.
Buena fe	Quien aparezca como titular de un registro se presumen como legitimo titular del valor o del derecho al cual se refiere el respectivo registro.
Fungibilidad	Los titulares de registros que se refieran a valores o derechos que hagan parte de una misma emisión y tengan iguales características, serán legítimos titulares de tales valores en la cantidad correspondiente, y no de unos valores o derechos especificados individualmente

Jurídicamente, la trascendencia de la electronificación de los títulos valor consiste en agilizar los flujos de inversión tanto internacionales como nacionales, con motivo de la circulación

[178] Nelson Remolina Angarita, Comercio electrónico en Colombia: regulación y tendencias, VI Congreso de Prevención del Fraude y Seguridad, Asobancaria, Bogotá, octubre 25 de 2012, diapositiva 24, accesible en: http://r.search.yahoo.com/_ylt=A86.J74X0N5Wam0Agpjv8wt.;_ylu=X3oDMTByaDNhc2JxBHNlYwNzcgRwb3MDMQRjb2xvA2dxMQR2dGlkAw--/RV=2/RE=1457471639/RO=10/RU=http%3a%2f%2fwww.asobancaria.com%2fportal%2fpage%2fportal%2fEventos%2feventos%2fcongreso_fraude_seguridad_2012%2fTab5%2fNelson%2520Remolina.pdf/RK=0/RS=9WGU9iaeBrkFgpJe3jDvy3VCabM-, consultado el 3 de marzo de 2015.

expedita de tales valores, donde la legitimación atiende al momento y forma en que se registró en el sistema informático del receptor o en la forma en que lo hayan acordado las partes así como en la confianza que se le tiene al suscriptor, la cual atiende a la certidumbre o seguridad que el propio suscriptor otorga y ha ido construyendo en el ámbito comercial en que se desenvuelve.

No se puede dejar de señalar que desde luego, uno de los grandes beneficios es que se disminuyen los costos de transacción.

2.11. Cumplimiento contractual: transferencia electrónica de fondos y compensación.

Si se considera que la declaración de la voluntad abre un abanico de distintos momentos dentro marco del perfeccionamiento del contrato por vía electrónica, ello implica transitar el camino donde inician las negociaciones *precontractuales, contractuales y postcontractuales*, esto es, hasta el cumplimiento de la voluntad de las partes.

En este proceso, la documentación contractual se torna muy especial; la representación de las partes en el ambiente digital se diversifica, es decir, puede transitar desde el acuse de recibo de los MD; las incorporaciones por referencia o las cláusulas fuera del propio documento electrónico; la dinámica contractual es bastante singular y las modalidades requieren especial estudio como son la cesión de derechos derivados del contrato, los tipos de contratos, las formas de cumplimiento o imposibilidad de cumplir con él, generan medios innovadores de resolver las obligaciones, así como también los medios de pago y compensación en ambiente de los sistemas electrónicos .

Ahora bien, toda obligación se extingue por medio de alguna de las siguientes cuatro figuras: la compensación; la confusión de derechos; la remisión de deudas o la novación. Particularmente y de acuerdo con el artículo 2062 del Capítulo I del Título Cuarto del CCiF denominado “Efectos de las Obligaciones”, el pago o cumplimiento es la entrega de la cosa o cantidad debida, o la prestación del servicio que se hubiere prometido.

Es relevante apuntar que en estricto sentido, mínimo se pueden presentar dos supuestos en el cumplimiento del contrato: uno al inicio y al finalizar el contrato, casos que se traducen en:

a) El cumplimiento las obligaciones por medios electrónicos.
b) La extinción de las obligaciones por medios electrónicos.

Lo anterior, precisa considerar que en el cumplimiento de las obligaciones, la seguridad en la operativa de pago mediante tarjeta de crédito o débito en el comercio electrónico es vital.

En cuanto al cumplimiento del pago bajo la seguridad requerida en los medios electrónicos, el artículo 54 LFPC prevé que cuando el cobro o cargo por un bien o servicio se haga en forma automática al recibo telefónico, o a una cuenta de tarjeta de crédito o a otro recibo o cuenta que le lleven al consumidor, el proveedor y el agente cobrador deberán advertir esto al

consumidor en forma clara, ya sea en la publicidad, en el canal de venta o en el recibo. Lo mismo se aplica a aquellos casos en que la compra involucre el pago de una llamada de larga distancia o gastos de entrega pagaderos por el consumidor.

Por último, debemos señalar que el uso del *Sistema de Pagos Electrónicos Interbancarios* (SPEI) es un sistema desarrollado y operado por el Banco de México que permite al público en general realizar en cuestión de segundos pagos electrónicos, también llamados transferencias electrónicas, a través de la banca por internet o de la banca móvil. Este sistema permite transferir dinero electrónicamente entre cuentas de depósito de los bancos de manera casi instantánea.

Sobre el valor probatorio del SPEI, los tribunales federales ya se han pronunciado en el siguiente tenor:

> ***SISTEMA DE PAGOS ELECTRÓNICOS INTERBANCARIOS (SPEI). CONSTITUYE UN ELEMENTO DE PRUEBA EN TÉRMINOS DEL ARTÍCULO 1205 DEL CÓDIGO DE COMERCIO[179].*** *De conformidad con lo dispuesto en el artículo 1205 del Código de Comercio, son admisibles como medios de prueba todos aquellos elementos que puedan producir convicción en el ánimo del juzgador acerca de los hechos controvertidos o dudosos. De ahí que el Sistema de Pagos Electrónicos Interbancarios, denominado SPEI, por sus siglas, desarrollado por el Banco de México, y adoptado por la banca comercial para la transferencia de dinero entre sus clientes, sea reconocido como un medio de prueba en términos de lo dispuesto en el citado numeral, si reúne los requisitos exigidos al efecto. Así, para que dichos instrumentos surtan efectos convictivos, es menester que satisfagan los siguientes requisitos: a) la especificación de la persona que transfiere el dinero desde su cuenta; b) el nombre del beneficiario, o sea, la persona que recibe el dinero de esa transferencia; c) el banco emisor que lleva la cuenta del ordenante; d) el banco receptor; e) el monto de la transferencia; y, f) la "CLABE" interbancaria del beneficiario, que debe constar de dieciocho dígitos, o bien su número de tarjeta de débito, que invariablemente consta de dieciséis dígitos; con el fin de identificar debidamente el pago realizado a través de dicho sistema.*
>
> ***TRANSFERENCIA BANCARIA VÍA SPEI. SU VALOR PROBATORIO[180].*** *El Sistema de Pagos Electrónicos Interbancarios (SPEI), fue desarrollado por el Banco de México, Banco Central de la Nación y la Banca Comercial, para permitir a los clientes de bancos enviar y recibir transferencias electrónicas de dinero. Sistema complejo del que destaca que para poder llevar a cabo este tipo de transacciones, los usuarios deben completar toda aquella información fidedigna que identifique ampliamente no sólo a la parte que abona y a la que recibe, sino que proporciona un número de referencia de hasta 7 dígitos, un identificador llamado clave de rastreo, de hasta 30 posiciones alfanuméricas que llevan como finalidad la rápida identificación del pago realizado, el monto del abono, así como la fecha y hora en que se realiza. Dicha seguridad se encuentra basada en mensajes firmados digitalmente para lo cual los participantes usan certificados digitales y las claves de las personas autorizadas, los que se obtienen de acuerdo con las normas*

[179] Décima Época, Tribunales Colegiados de Circuito, Semanario Judicial de la Federación y su Gaceta, Libro XIII, Octubre de 2012, Tomo 4, Tesis aislada en materia civil: II.2o.C.6 C (10a.), página: 2804.

[180] Décima Época, Tribunales Colegiados de Circuito, Gaceta del Semanario Judicial de la Federación, Libro 16, Marzo de 2015, Tomo III, tesis aislada en materia civil: I.3o.C.162 C (10a.), página: 2546

de la Infraestructura Extendida de Seguridad (IES), del Banco de México. Luego, toda vez que dichos pagos contienen el mismo tipo de firma digital que se requiere para llevar a cabo el pago de impuestos, derechos y que han sido analizados por nuestro Máximo Tribunal y se les concede valor diverso a los documentos privados pues, incluso, con relación a la firma electrónica, la Segunda Sala de la Suprema Corte de Justicia de las Nación, en la tesis 2a. XCVII/2007, publicada en la página seiscientos treinta y ocho del Tomo XXVI, del mes de agosto de dos mil siete, correspondiente a la Novena Época del Semanario Judicial de la Federación y su Gaceta, de rubro: FIRMA ELECTRÓNICA AVANZADA. EL HECHO DE QUE EL CÓDIGO FISCAL DE LA FEDERACIÓN NO ESTABLEZCA SU DEFINICIÓN NO VIOLA LA GARANTÍA DE LEGALIDAD., estableció que su finalidad es identificar al emisor de un mensaje como su autor legítimo, como si se tratara de una firma autógrafa, con lo que se garantiza la integridad del documento produciendo los mismos efectos que las leyes otorgan a los documentos con firma autógrafa y tienen el mismo valor probatorio.

CAPÍTULO III. RECURSO PARA LA CONTRATACIÓN ELECTRÓNICA SEGURA: FIRMA ELECTRÓNICA AVANZADA

3.1. Firma: concepto, clases y efectos.

La firma puede ser un nombre, apellido o título, que una persona escribe de su propia mano en un documento, para darle autenticidad o para expresar que aprueba su contenido[181]; aunque basta con que el concepto de firma incluya cualquier signo que individualice al ser humano y muestre la voluntad, independientemente de si tal(es) signo(s) puede(n) ir de un monosílabo hasta un largo número de caracteres alfanuméricos, garabatos o líneas en diversas direcciones.

Por su parte, la Suprema Corte de Justicia de la Nación (SCJN) define la firma como:

> *(…) los caracteres, signos o nombre que use o estampe determinada persona en un documento para obligarse a responder del contenido de ese documento o para hacer constar que ha recibido alguna cosa*[182]

Esta concepción es muy cercana a la naturaleza jurídica de la firma autógrafa, en este sentido el artículo 204 del CFPC identifica a la Firma con la *"subscripción*", precisando que "*hace plena fe de la formación del documento por cuenta del subscriptor (*...)", lo que significa que la firma hace prueba que en dicho documento se encuentra expresa la voluntariedad del subscriptor o firmante; por ende, al firmarse un documento, el subscriptor se está haciendo responsable de su contenido en lo particular.

En suma, se entiende que la firma autógrafa no requiere reproducir solo el nombre de la persona o sus apellidos, sino basta que sea la forma constante en la que un individuo manifiesta su ánimo de adherirse a un postulado que está por escrito o indicar su consentimiento en el contexto de que se trate.

La variedad de firmas van desde la autógrafa[183], el facsímil, la mecánica, la suscrita por personas físicas y morales hasta otras elaboradas con diversas herramientas. No obstante, la firma autógrafa ha sido la más usada y conocida hasta hoy.

Ante la imposibilidad de que un suscriptor pueda estampar su firma autógrafa, el legislador creó tres figuras que toman en consideración la dificultad, inconveniente u obstáculos que hacen que no sea factible signar de manera autógrafa, tales figuras son:

- **(i)** Huella digital
- **(ii)** *Firma a ruego*

[181] Real Academia Española. (2001). Diccionario de la lengua española (22.a ed.). Consultado en http://www.rae.es/rae.html
[182] Véase Informe 1959, tesis aislada de la Tercera Sala, Sexta Época, página: 100, de rubro: "Reconocimiento de Firma para Preparar la Acción Ejecutiva Mercantil".
[183] Infra 3.1.2. Firma electrónica frente a la firma autógrafa.

(iii) *Facsímil o máquina de firma*

(i) Huella digital. *Como acertadamente lo señala el profesor Orgaz, implica que quien pone su impresión digital al pie de una escritura regularmente es persona que no sabe firmar, y, por tanto, que no sabe leer. ¿Cómo podría suponer la ley, en estas condiciones, que el otorgante ha querido realmente las declaraciones de Derecho que contiene el documento? La firma tiene ojos, la impresión digital es ciega*[184]*.*

De lo anterior, se advierte que una persona que es incapaz de leer y escribir puede ser fácilmente inducida al error por medio de engaños, obligándose con su huella digital a responsabilidades muy diversas a las que realmente quiera. No obstante, esta forma de firmar es una disposición del artículo 1834 del CCiF, la cual se ha vuelto de empleo frecuente, al encontrar la huella digital y la firma a ruego constantemente para autenticar los documentos privados. Por ende, si bien este tipo de firmas (digital y a ruego) no son pruebas indiscutibles, sí pueden ser puntos importantes a valorarse en un litigio; de tal forma que se podrían utilizar dos apreciaciones:

- En caso de que la huella digital sea reconocida voluntariamente, puede comparársele a una confesión, pero si no es reconocida, el Juez que tenga conocimiento de que el suscriptor era analfabeta, le leerá la información a éste además de incluir un peritaje dactiloscópico.

- En caso de que se compruebe que quien uso su huella digital tiene capacidad para leer y escribir y que es auténtico, puede llegar a comparársele a la firma, sino no se prueba engaños o inducciones físicas o morales para hacerlo. Por ello, todo analfabeta no debería suscribir actos jurídicos sino en forma pública, careciendo de eficacia aquellos documentos privados en los que estampen su huella digital, aunque puedan en última instancia, llegar a constituirse en medios de pruebas en el litigio.

La propuesta indicada para dar respuesta a las consecuencias de que se generan por la imposibilidad de que un analfabeta exprese realmente su voluntad, consiste en que para no negar que los analfabetas contraten en forma privada, el legislador debe crear un trámite eficiente cuya tramitación sea de bajo precio en atención a que generalmente los analfabetas son individuos de escasos recursos económicos que no podrían pagar los honorarios de un notario público por lo que una alternativa sería habilitar a los Jueces de primera instancia de las diversas materias del Derecho, a fin de que otorguen fe de este tipo de contratos ante la constatación de la comparecencia de las partes interesadas y los testigos de conocimiento de las mismas, leyéndoles a todos ellos el contenido del documento, para que una vez realizado esto se proceda a recabar la firma de las partes intervinientes que puedan hacerlo y a la impresión de su huella digital de las que se encuentren impedidas para firmar parcial o totalmente.

[184] Orgaz, Alfredo. "Valor de la impresión digital en los documentos no firmados", en Estudios de Derecho Civil, 1948, Topográfica Editora Argentina, Buenos Aires, pp. 208-233.

La huella digital es prueba de quien la estampó es la persona que otorgó el consentimiento y no otra, presumiéndose su voluntariado al imprimir su huella digital, siendo indubitable su validez a menos que se demuestre presión moral para el otorgamiento del acto. Actualmente, en los casos en que varios documentos oficiales tales como credenciales para votar expedidas por el Instituto Nacional Electoral, visas al extranjero, pasaportes, licencias de conducir y actas del registro civil, se ha exigido que se suscriba la firma autógrafa así como también se grave la huella digital; cuyo efecto legal es que otorgue un aumento de la autenticidad al documento en razón de que convergen el consentimiento- firma autógrafa- y su identificación personal -huella digital- que dan al documento respectivo el carácter de inequívoco e innegable.

(ii) *Firma a Ruego.*

La *Firma a Ruego* para reemplazar la inscripción de la autógrafa de quien no puede o no sabe hacerlo; no define sus elementos o cómo debe ser otorgada en diferentes supuestos.

El *rogado* permite que un individuo diferente al incapacitado, acceda a firmar por éste a su ruego, sin importar que sea o no parte interviniente en el acto instrumentado correspondiente; asimismo, el impedido, es aquella persona que por un inconveniente permanente (el no saber firmar o una falta de habilidad persistente irreparable) o transitoria por inhabilidad física recuperable, no puede firmar.

En el ejercicio legal y en la normatividad, el rogado debe estampar su firma en razón de que ésta será prueba irrefutable de que intervino en el acto correspondiente.

En materia Civil se permite que cuando alguna de las personas que deba firmar no pueda o no sepa hacerlo, lo haga otra "a su ruego", imprimiendo en el documento la huella digital del que no firmó como lo señala el numeral 1834 del CCiF.

> ***Artículo 1834.-*** *Cuando se exija la forma escrita para el contrato, los documentos relativos deben ser firmados por todas las personas a las cuales se imponga esa obligación.*
> *Si alguna de ellas no puede o no sabe firmar, lo hará otra a su ruego y en el documento se imprimirá la huella digital del interesado que no firmó.*

En este sentido, ni requiere que participe en el acto un funcionario investido de fe pública ni tampoco obliga a hacerlo por un medio por el cual se pueda corroborar que el que no firmó pidió efectivamente a otra persona que firmara "a su cargo". Los contratos privados frecuentemente se llevan a cabo frente a dos testigos quienes podrían dar fe de que el que no firmó pidió a otro que firmara a su ruego, pero nuevamente lo que se vuelve discutible es que los testigos pudieran pactar con otros inducir a error al imposibilitado o coaccionarlo para que estampe su huella.

Otro elemento discutible es que el propio imposibilitado se valga de las anteriores consideraciones para tratar de refutar en juicio lo que antes contrató con absoluto conocimiento de causa y razón, o sea que para ambas partes resulta peligroso contratar cuando alguna de ellas esté impedida para firmar temporal o permanentemente.

Ahora bien, en el derecho público la intervención de un funcionario investido de fe pública otorga una formalidad al acto correspondiente, ya que éste constatará el pedimento que haga el imposibilitado para que otra persona firme a su ruego; asimismo, excluirá la posibilidad de que no sepa aquél del contenido del documento respectivo, ya que es una obligación la lectura del mismo por parte del fedatario.

Por otra parte, al respecto a los efectos jurídicos de la firma, los artículos 204 y 206 del CFPC establecen que inscribir en un documento, obra de arte o en un escrito, de palabras o signos que emplea su autor para identificarse, tienen el efecto jurídico respecto de las obras de arte, de identificar a la persona que los suscribe, aun cuando el texto no haya sido escrito, en todo, ni en parte por ésta.

> ***Artículo 204****.- Se reputa autor de un documento privado al que lo suscribe, salvo la excepción de que trata el artículo 206. Se entiende por subscripción la colocación, al pie del escrito, de las palabras que, con respecto al destino del mismo, sean idóneas para identificar a la persona que subscribe. La subscripción hace plena fe de la formación del documento por cuenta del subscriptor, aun cuando el texto no haya sido escrito ni en todo ni en parte por él, excepto por lo que se refiere a agregados interlineales o marginales, cancelaciones o cualesquiera otras modificaciones contenidas en él, las cuales no se reputan provenientes del autor, si no están escritas por su mano, o no se ha hecho mención de ellas antes de la subscripción.*
>
> ***Artículo 206.-*** *Se considera autor de los libros de comercio, registrados domésticos y demás documentos que no se acostumbra subscribir, a aquél que los haya formado o por cuya cuenta se hicieren. Si la parte contra la cual se propone un documento de esta naturaleza no objeta, dentro del término fijado por el artículo 142, ser su autor, ni declara no reconocer como tal al tercero indicado por quien lo presentó, se tendrá al autor por reconocido. En caso contrario, la verdad del hecho de que el documento haya sido escrito por cuenta de la persona indicada, debe demostrarse por prueba directa, de acuerdo con los capítulos anteriores de este título. En los casos de este artículo y en los del anterior, no tendrá valor probatorio el documento no objetado, si el juicio se ha seguido en rebeldía, pues entonces es necesario el reconocimiento del documento, el que se practicará con sujeción a las disposiciones sobre confesión, y surtirá sus mismos efectos, y, si el documento es de un tercero, la verdad de su contenido debe demostrarse por otras pruebas.*

La firma cohesiona la identificación de aquel que está suscribiendo un documentos y la presunción de que éste vale en cuanto está signado y si no está firmado, no tiene ninguna validez. Esta visión la comparte la SCJN[185] y el artículo 103 de la Ley del Notariado del Distrito Federal (LNDF).

> ***Artículo 103.-*** *Cuando ante un Notario se vayan a otorgar diversas escrituras, cuyos actos sean respecto de inmuebles con un mismo antecedente de propiedad, por tratarse de predios resultantes de porciones mayores o de unidades sujetas al régimen de propiedad en condominio, se seguirán las reglas establecidas en el artículo anterior, con las excepciones siguientes:*

[185] Véase Semanario Judicial de la Federación, Registro: 272907, tesis aislada de la Tercera Sala, Sexta Época, página: 73, Rubro: "Escritos Sin Firmar (Contestación De La Demanda)."

I.- *En un primer instrumento, que se llamará de certificación de antecedentes, a solicitud de cualquiera de las partes, el Notario relacionará todos los títulos y demás documentos necesarios para el otorgamiento de dichos actos;*
II.- *En las escrituras en que se contengan éstos, el Notario no relacionará ya los antecedentes que consten en el instrumento indicado en la fracción anterior, sino sólo se hará mención de su otorgamiento y que conforme al mismo quien dispone puede hacerlo legítimamente; describirá sólo l inmueble materia de la operación y citará el antecedente registral en el que haya quedado inscrita la lotificación en los casos de fraccionamiento, o la constitución del régimen de propiedad en condominio, cuando se trate de actos cuyo objeto sean las unidades del inmueble antecedente;*
Así como los relativos a gravámenes o fideicomisos que se extingan;
III.- *Cuando la escritura de la notificación o constitución del régimen de propiedad en condominio se haya otorgado en el protocolo del mismo Notario ante quien se otorguen los actos sucesivos, dicha escritura hará los efectos del instrumento de certificación de antecedentes. Surtirá también esos efectos la escritura en la que por una operación anterior consten en el mismo protocolo los antecedentes de propiedad de un inmueble, y*
IV.- *Al expedir los testimonios de la escritura donde se contengan los actos sucesivos, el Notario deberá anexarles una certificación que contenga, en lo conducente, la relación de antecedentes que obren en el instrumento de certificación respectivo.*

3.1.1. Firmas en las distintas ramas jurídicas

El alcance de las firmas incrementa o disminuye según la rama del Derecho de que se trate, de tal forma que si se atiende a una firma de un testamento público abierto, implica que es un requisito de forma, ya que su ausencia no provoca la nulidad absoluta del acto, en atención a que ha participado en él un funcionario investido de fe pública; evidentemente, tal situación no ocurre en el testamento ológrafo, en el que la firma es un elemento esencial, por lo que a su falta es causa de nulidad absoluta.

En tales condiciones, la trascendencia o relevancia de las ramas del Derecho permiten establecer el siguiente catálogo de firmas autógrafas[186]:

- **a)** Firma en el Derecho Civil.
- **b)** Firma de las instituciones de crédito frente al cliente: Ley de Instituciones de Crédito.
- **c)** Firma en títulos de crédito: Ley de Títulos y Operaciones de Crédito.
- **d)** Firma en títulos de crédito emitidos en serie: Ley de Títulos y Operaciones de Crédito y Ley General de Sociedades Mercantiles.
- **e)** Firma en materia de finanzas: Ley Federal de Instituciones de Seguros y Fianzas
- **f)** Firma en pólizas de seguros: Ley Federal de Instituciones de Seguros y Fianzas así como Ley Federal de Contrato de Seguros.

3.1.1.1. Firma en el Derecho Civil.

[186] Esta taxonomía fue complementado con algunos elementos de la lista que describe Miguel Acosta Romero y Julieta Arelí Lara Luna en: Nuevo derecho mercantil, 1. ed., 2000, México, Porrúa, p. 542-552.

Como se comentó en el párrafo precedente, la firma en el derecho civil tiene sus propios alcances. Atendiendo al ejemplo citado sobre el testamento, existen otras variantes del testamento como el público cerrado, donde la firma también es un elemento esencial de validez, solo que a diferencia del testamento ológrafo, y en concordancia con el público abierto, puede ser estampada por otra persona que lo haga a ruego del testador, cuando éste se encuentre impedido de hacerlo. Luego, dispone el artículo 1530 del CCiF que *los que no saben o no pueden leer, son inhábiles para hacer testamento cerrado .*

Ahora, la alternativa aquí sería que el parlamentario requiriera en cualquier documento en que se contengan manifestaciones de voluntad, la firma de persona o personas que lo suscriban, o en su defecto, de sus representantes legales, estableciendo qué nulidad se generaría en su ausencia, ya que es evidente que la ausencia de firma no debe tener los mismos efectos en todos los casos, basta con citar la fracción V, del numeral 162 de la LNDF que señala:

> ***Artículo 162.-*** *El instrumento o registro notarial sólo será nulo:*
> *(…)*
> ***V.-*** *Si no está firmado por todos los que deben firmarlo según esta Ley, o no contiene la mención exigida a falta de firma;*

Por lo que hace a esta fracción, nuestra opinión se dirige en el sentido de que el instrumento gozará de nulidad relativa en atención a que lo esencial es el consentimiento del suscriptor en comparecencia ante el Notario y de quienes testifican esa declaración de voluntad ante dicho Notario, pues no debe sujetarse a la existencia de todas las firmas de los que deben hacerlo según el Código.

3.1.1.2. Firma de las Instituciones de Crédito.

La variedad de operaciones de crédito van de los depósitos bancarios de dinero, aceptación de préstamos y créditos; emisión de bonos bancarios; emisión de obligaciones subordinadas; constitución de depósitos en instituciones de crédito y entidades financieras del exterior; expedición de tarjetas de crédito con base en contratos de apertura de crédito en cuenta corriente; asunción de obligaciones por cuenta de terceros, con base en créditos concedidos, a través del otorgamiento de aceptaciones, endoso o aval de títulos de crédito, así como de la expedición de cartas de crédito; operaciones con valores; promoción de la organización y transformación de toda clase de empresas o sociedades mercantiles y suscribir y conservar acciones o partes de interés en las mismas; operación con documentos mercantiles por cuenta propia; operaciones con oro, plata y divisas, incluyendo reportos sobre estas últimas; expedición de cartas de crédito previa recepción de su importe, hacer efectivos créditos y realizar pagos por cuenta de clientes; fideicomisos, mandatos y comisiones; recepción de depósitos en administración o custodia, o en garantía por cuenta de terceros, de títulos o valores y en general de documentos mercantiles; actuaciones como representante común de los tenedores de títulos de crédito; servicio de caja y tesorería relativo a títulos de crédito, por cuenta de las emisoras; llevar la contabilidad y los libros de actas y de registro de sociedades y empresas; desempeñar el cargo de albacea; desempeñar la sindicatura o encargarse de la

liquidación judicial o extrajudicial de negociaciones, establecimientos, concursos o herencias; encargarse de hacer avalúos que tendrán la misma fuerza probatoria que las leyes asignan a los hechos por corredor público o perito; adquisición los bienes muebles e inmuebles necesarios para la realización de su objeto y enajenarlos cuando corresponda, celebración de contratos de arrendamiento financiero y adquirir los bienes que sean objeto de tales contratos; realización de operaciones derivadas, sujetándose a las disposiciones técnicas y operativas que expida el Banco de México, en las cuales se establezcan las características de dichas operaciones, tales como tipos, plazos, contrapartes, subyacentes, garantías y formas de liquidación; operaciones de factoraje financiero; emisión y poner en circulación cualquier medio de pago que determine el Banco de México; intervención en la contratación de seguros para lo cual deberán cumplir con lo establecido en la Ley General de Instituciones y Sociedades Mutualistas de Seguros (LGISMS) y en las disposiciones de carácter general que de la misma emanen.

Los artículos 48 Bis 5, sexto párrafo, 52, 57 y 72 bis de la Ley de Instituciones de Crédito (LIC) no sólo disponen como requisito para la validez de operaciones bancarias y de crédito, el de la firma, sino también, las instituciones de banca múltiple e instituciones de banca de desarrollo adaptaron rápidamente los cambios a través del reconocimiento normativo de las autorizaciones, instrucciones y comunicaciones de actos por medios electrónicos, ópticos o de cualquier otra tecnología que previamente convengan las partes además de la tradicional firma autógrafa.

> ***Artículo 48 Bis 5.-*** *Las instituciones de crédito están obligadas a realizar las acciones conducentes para que sus clientes puedan dar por terminados los contratos de adhesión que hubieren celebrado con las mismas en operaciones activas y pasivas, mediante escrito en el que manifieste su voluntad de dar por terminada la relación jurídica con esa institución. Los clientes podrán en todo momento celebrar dichas operaciones con otra institución de crédito. En estos casos será aplicable lo previsto en el tercer párrafo de este artículo respecto de los plazos para transferir los recursos respectivos y dar por terminada la operación una vez recibida la solicitud respectiva del cliente.*
> *(…)*
> *Las solicitudes, autorizaciones, instrucciones y comunicaciones a que se refiere este artículo podrán llevarse a cabo por escrito con* ***firma autógrafa*** *o a través de medios electrónicos, ópticos o de cualquier otra tecnología que previamente convengan las partes, siempre y cuando pueda comprobarse fehacientemente el acto jurídico de que se trate.*
> ***Artículo 52.-*** *Las instituciones de crédito podrán pactar la celebración de sus operaciones y la prestación de servicios con el público mediante el uso de equipos, medios electrónicos, ópticos o de cualquier otra tecnología, sistemas automatizados de procesamiento de datos y redes de telecomunicaciones, ya sean privados o públicos, y establecerán en los contratos respectivos las bases para determinar lo siguiente:*
> ***I.*** *Las operaciones y servicios cuya prestación se pacte;*
> ***II.*** *Los medios de identificación del usuario y las responsabilidades correspondientes a su uso, y*
> ***III.*** *Los medios por los que se hagan constar la creación, transmisión, modificación o extinción de derechos y obligaciones inherentes a las operaciones y servicios de que se trate.*
> *Cuando así lo acuerden con su clientela, las instituciones podrán suspender o cancelar el trámite de operaciones que aquélla pretenda realizar mediante el uso de equipos o medios a*

que se refiere el primer párrafo de este artículo, siempre que cuenten con elementos suficientes para presumir que los medios de identificación pactados para tal efecto han sido utilizados en forma indebida.
(…)
El uso de los medios de identificación que se establezcan conforme a lo previsto por este artículo, en sustitución de la ***firma autógrafa,*** *producirá los mismos efectos que las leyes otorgan a los documentos correspondientes y, en consecuencia, tendrán el mismo* ***valor probatorio.*** *La instalación y el uso de los equipos y medios señalados en el primer párrafo de este artículo se sujetarán a las reglas de carácter general que emita la Comisión Nacional Bancaria y de Valores, sin perjuicio de las facultades con que cuenta el Banco de México para regular las operaciones que efectúen las instituciones de crédito relacionadas con los sistemas de pagos y las de transferencias de fondos en términos de su ley. (…)*

Artículo 57.- *Los clientes de las instituciones de crédito que mantengan cuentas vinculadas con las operaciones a que se refieren las fracciones* ***I y II del artículo 46*** *de esta Ley podrán autorizar a terceros para que hagan disposiciones de efectivo con cargo a dichas cuentas. Para ello, las instituciones deberán contar con la autorización del titular o titulares de la cuenta. Tratándose de instituciones de banca múltiple, éstas además deberán realizar los actos necesarios para que en los contratos en los que se documenten las operaciones referidas, se señale expresamente a la o las personas que tendrán derecho al pago de las obligaciones garantizadas a que se refiere la Ley de Protección al Ahorro Bancario.*
(…) Las autorizaciones, instrucciones y comunicaciones a que se refiere este artículo podrán llevarse a cabo por escrito con ***firma autógrafa*** *o a través de* ***medios electrónicos, ópticos o de cualquier otra tecnología*** *que previamente convengan las partes.*

Artículo 72 Bis.- *Los clientes de las instituciones de crédito que tengan celebrados contratos de apertura de crédito en cuenta corriente, a los que se refiere la fracción VII del artículo 46 de esta Ley, podrán autorizar a dichas instituciones o a proveedores que se realice el pago de bienes y servicios con cargo a la cuenta que corresponda a dicho contrato.*
(…) Las autorizaciones, instrucciones y comunicaciones a que se refiere este artículo podrán llevarse a cabo por escrito con ***firma autógrafa*** *o a través de medios electrónicos, ópticos o de cualquier otra tecnología que previamente convengan las partes.*

(Énfasis añadido)

En suma, la firma en el derecho bancario tiene matices particulares que la distinguen de la firma en general; sin embargo, le continúan siendo aplicables las caracterísitas de la firma autógrafa.

3.1.1.3. Firma en Títulos de Crédito.

En cuanto a los títulos de crédito y tomando en consideración que son los documentos necesarios para ejercitar el derecho literal que en ellos se consignan cuyas características son la incorporación, legitimación, autonomía y dicha literalidad; el abanico de títulos va desde el endoso, letra de cambio, aval, protesto, pagaré, cheque, los certificados de participación así como de depósito, el bono en prenda hasta los bonos bancarios y sus cupones, conforme al artículo 63 de la LIC.

Del análisis de los artículos 8, fracción II y 11 en concordancia con el 29, fracción II; 76, fracción VII; 85, párrafo segundo; 111, 170, fracción VI; 176, fracción VI; 203, 210, fracciones X y XI; 228, fracciones III y XI; 231, fracción II; 232, fracción V, de la LGTOC, se advierte que la firma autógrafa es un requisito indispensable para los títulos de crédito así como también para aquellos actos en que se relacionen con los mismos, ya sea como obligados directos, en vía de regreso, por aval, por endoso, o por alguna otra situación en que se exija la firma en esos documentos. Lamentablemente, las obligaciones en materia de títulos de crédito aun estilan el uso mercantil de la firma manuscrita, la cual no puede ser substituida por una firma electrónica o digital.

De tal forma que para el caso de una persona que no pueda o sepa firmar, requerirá que un tercero firme el título de crédito a su nombre, tomando en cuenta los siguientes

i. Tratándose de persona física que no sepa o no pueda escribir, un fedatario deberá otorgar un poder a una tercera persona para que éste firme los títulos de crédito.

ii. Tratándose de una persona física o moral la representación para otorgar o suscribir títulos de crédito se confiere mediante poder inscrito debidamente en el Registro de Comercio; y por simple declaración escrita dirigida al tercero con quien habrá de contratar el representante. En tanto que los administradores o gerentes de sociedades o negociaciones mercantiles se reputan autorizados para suscribir letras de cambio a nombre de éstas, por el hecho de su nombramiento.

> ***Artículo 8o.-*** *Contra las acciones derivadas de un título de crédito, sólo pueden oponerse las siguientes excepciones y defensas:*
> ***I.-*** *Las de incompetencia y de falta de personalidad en el actor;*
> ***II.-*** *Las que se funden en el hecho de no haber sido el demandado quien* ***firmó*** *el documento;*
> ***III.-*** *Las de falta de representación, de poder bastante o de facultades legales en quien subscribió el título a nombre del demandado, salvo lo dispuesto en al artículo 11;*
> ***IV.-*** *La de haber sido incapaz el demandado al suscribir el título;*
> ***V.-*** *Las fundadas en la omisión de los requisitos y menciones que el título o el acto en él consignado deben llenar o contener y la ley no presuma expresamente, o que no se hayan satisfecho dentro del término que señala el artículo 15;*
> ***VI.-*** *La de alteración del texto del documento o de los demás actos que en él conste, sin perjuicio de lo dispuesto en el artículo 13;*
> ***VII.-*** *Las que se funden en que el título no es negociable;*
> ***VIII.-*** *Las que se basen en la quita o pago parcial que consten en el texto mismo del documento, o en el depósito del importe de la letra en el caso del artículo 132;*
> ***IX.-*** *Las que se funden en la cancelación del título, o en la suspensión de su pago ordenada judicialmente, en el caso de la fracción II del artículo 45;*
> ***X.-*** *Las de prescripción y caducidad y las que se basen en la falta de las demás condiciones necesarias para el ejercicio de la acción;*
> ***XI.-*** *Las personales que tenga el demandado contra el actor.*
>
> ***Artículo 9o.-*** *La representación para otorgar o suscribir títulos de crédito se confiere:*
> ***I.-*** *Mediante poder inscrito debidamente en el Registro de Comercio; y*

II.- *Por simple declaración escrita dirigida al tercero con quien habrá de contratar el representante.*
En el caso de la fracción I, la representación se entenderá conferida respecto de cualquier persona y en el de la fracción II sólo respecto de aquella a quien la declaración escrita haya sido dirigida.
En ambos casos, la representación no tendrá más límites que los que expresamente le haya fijado el representado en el instrumento o declaración respectivos.

Artículo 11.- *Quien haya dado lugar, con actos positivos o con omisiones graves, a que se crea, conforme a los usos del comercio, que un tercero está facultado para suscribir en su nombre títulos de crédito, no podrá invocar la excepción a que se refiere la* ***fracción III del artículo 8o****. contra el tenedor de buena fe. La buena fe se presume, salvo prueba en contrario, siempre que concurran las demás circunstancias que en este artículo se expresan.*

Artículo 29.- *El endoso debe constar en el título relativo o en hoja adherida al mismo, y llenar los siguientes requisitos:*
I.- *El nombre del endosatario;*
II.- La firma del endosante o de la persona *que suscriba el endoso a su ruego o en su nombre;*
III.- *La clase de endoso;*
IV.- *El lugar y la fecha.*

Artículo 76.- *La letra de cambio debe contener:*
I.- La mención de ser letra de cambio, inserta en el texto del documento;
II.- La expresión del lugar y del día, mes y año en que se suscribe;
III.- La orden incondicional al girado de pagar una suma determinada de dinero;
IV.- El nombre del girado;
V.- El lugar y la época del pago;
VI.- El nombre de la persona a quien ha de hacerse el pago; y
VII.- La firma del girador o de la persona que suscriba a su ruego o en su nombre.

Artículo 85.- *La facultad de obrar en nombre y por cuenta de otro no comprende la de obligarlo cambiariamente, salvo lo que dispongan el poder o la declaración a que se refiere el artículo 9o. Los administradores o gerentes de sociedades o negociaciones mercantiles se reputan* ***autorizados*** *para suscribir letras de cambio a nombre de éstas, por el hecho de su nombramiento. Los límites de esa autorización son los que señalen los estatutos o poderes respectivos.*

Artículo 111.- *El aval debe constar en la letra o en hoja que se le adhiera. Se expresará con la fórmula por aval, u otra equivalente, y debe llevar la firma de quien lo presta. La sola firma puesta en la letra, cuando no se le pueda atribuir otro significado, se tendrá como aval.*

Artículo 170.- *El pagaré debe contener:*
I.- La mención de ser pagaré, inserta en el texto del documento;
II.- La promesa incondicional de pagar una suma determinada de dinero;
III.- El nombre de la persona a quien ha de hacerse el pago;
IV.- La época y el lugar del pago;
V.- La fecha y el lugar en que se subscriba el documento; y
VI.- La firma del suscriptor o de la persona que firme a su ruego o en su nombre.

Artículo 176.- *El cheque debe contener:*
I.- La mención de ser cheque, inserta en el texto del documento;
II.- El lugar y la fecha en que se expide;
III.- La orden incondicional de pagar una suma determinada de dinero;
IV.- El nombre del librado;
V.- El lugar del pago; y
VI.- La firma del librador.

Artículo 203.- *Los cheques de viajero serán precisamente nominativos. El que pague el cheque deberá verificar la autenticidad de la* ***firma del tomador****, cotejándola con la firma de éste que aparezca certificada por el que haya puesto los cheques en circulación.*

Artículo 210.- *Las obligaciones deben contener:*
I.- *Nombre, nacionalidad y domicilio del obligacionista, excepto en los casos en que se trate de obligaciones emitidas al portador en los términos del primer párrafo del artículo anterior.*
II.- *La denominación, el objeto y el domicilio de la sociedad emisora;*
III.- *El importe del capital pagado de la sociedad emisora y el de su activo y de su pasivo, según el balance que se practique precisamente para efectuar la emisión;*
IV.- *El importe de la emisión, con especificación del número y del valor nominal de las obligaciones que se emitan;*
V.- *El tipo de interés pactado;*
VI.- *El término señalado para el pago de interés y de capital y los plazos, condiciones y manera en que las obligaciones han de ser amortizadas;*
VII.- *El lugar del pago;*
VIII.- *La especificación, en su caso, de las garantías especiales que se constituyan para la emisión, con expresión de las inscripciones relativas en el Registro Público;*
IX.- *El lugar y fecha de la emisión, con especificación de la fecha y número de la inscripción relativa en el Registro de Comercio.*
X.- La firma autógrafa de los administradores de la sociedad, *autorizados al efecto, o bien la firma impresa en facsímil de dichos administradores, a condición, en este último caso, de que se deposite el original de las firmas respectivas en el Registro Público de Comercio en que se haya registrado la sociedad emisora.*
XI.- La firma autógrafa del representante común de los obligacionistas, o bien la firma impresa en facsímil de dicho representante, a condición, en este último caso, de que se deposite el original de dicha firma en el Registro Público de Comercio en que se haya registrado la sociedad emisora.

Artículo 228 n.- *El certificado de participación deberá contener:*
I.- *Nombre, nacionalidad y domicilio del titular del certificado;*
II.- *La mención de ser certificados de participación y la expresión de si es ordinario o inmobiliario;*
III.- La designación de la sociedad emisora y la ***firma autógrafa del funcionario*** *de la misma, autorizado para suscribir la emisión correspondiente;*
IV.- *La fecha de expedición del título;*
V.- *El importe de la emisión, con especificación de número y del valor nominal de los certificados que se emitan;*
VI.- *En su caso, el mínimo de rendimiento garantizado;*

VII.- *El término señalado para el pago de productos o rendimientos y del capital y los plazos, condiciones y forma en que los certificados han de ser amortizados;*
VIII.- *El lugar y modo de pago;*
IX.- *La especificación, en su caso, de las garantías especiales que se constituyan para la emisión, con expresión de las inscripciones relativas en el Registro Público;*
X.- *El lugar y la fecha del acta de emisión, con especificación de la fecha y número de la inscripción relativa en el Registro de Comercio;*
XI.- La firma autógrafa *del representante común de los tenedores de certificados*

Artículo 231.- *Tanto el certificado de depósito como el bono de prenda, deberán contener:*
I.- La mención de ser certificado de depósito y bono de prenda, respectivamente;
II.- La designación y la firma del almacén;
III.- El lugar del depósito;
IV.- La fecha de expedición del título;
V.- El número de orden, que deberá ser igual para el certificado de depósito y para el bono o los bonos de prenda relativos, y el número progresivo de éstos, cuando se expidan varios en relación con un solo certificado;
VI.- La mención de haber sido constituido el depósito con designación individual o genérica de las mercancías o efectos respectivos;
VII.- La especificación de las mercancías o bienes depositados, con mención de su naturaleza, calidad y cantidad y de las demás circunstancias que sirvan para su identificación;
VIII.- El plazo señalado para el depósito;
IX.- El nombre del depositante;
X.- La mención de estar o no sujetos los bienes o mercancías materia del depósito al pago de derechos, impuestos o responsabilidades fiscales, y cuando para la constitución del depósito sea requisito previo el formar la liquidación de tales derechos, nota de esa liquidación;
XI.- La mención de estar o no asegurados los bienes o mercancías depositados y del importe del seguro, en su caso;
XII.- La mención de los adeudos o de las tarifas en favor del Almacén o, en su caso, la mención de no existir tales adeudos.

Artículo 232.- *El bono de prenda deberá contener, además:*
I.- El Nombre del tomador del bono;
II.- El importe del crédito que el bono representa;
III.- El Tipo de interés pactado;
IV.- La fecha del vencimiento, que no podrá ser posterior a la fecha en que concluya el depósito;
V.- La firma del tenedor del certificado que negocie el bono por primera vez;
VI.- La mención, suscrita por el Almacén o por la institución de crédito que intervengan en la primera negociación del bono, de haberse hecho la anotación respectiva en el certificado de depósito.

(Énfasis añadido)

En conclusión, además de los requisitos de la firma relativa a operaciones y documentos bancarios se deberá considerar algunas normas de la LGTOC respecto a la firma, concretamente lo que establecen los artículos precedentes que hace referencia a la firma en los títulos de crédito y en diversos actos relacionados con los mismos, ya sea como obligaciones directas, en

vía de regreso, por aval, por endoso, o por aluna otra situación en que se exija la firma en estos documentos.

Las disposiciones relativas a los títulos de crédito establecen que deberán estar firmados o suscritos por: el emisor, librador, aceptante, girador, endosante, avalista, etc., lo que implica que la firma es un requisito indispensable para que el título de crédito tenga validez y ejercitar la acción derivada del título.

Alfredo A. Reyes Kraft, considera que la *"ley actual no prevé el reconocimiento de firma por parte de autoridades o fedatarios en los títulos de crédito, para darles el carácter de ejecutivos, lo cual es un adelanto y facilita su circulación. Salvo en los casos de los bonos bancarios, situación que a mi juicio ya no se justifica en nuestros días"* [187].

Ahora bien, por definición, cuando se habla de firma, el uso bancario ha entendido que ésta debe ser autógrafa y en este sentido casi se orienta la doctrina en general, a considerar autógrafa a la firma que, como dicen los usos mercantiles, es de puño y letra de quien la estampa.

Entonces, todo título de crédito requiere de la firma autógrafa, misma que no puede ser sustituida por la impresión digital o por la firma a ruego, que sólo podrá ser estampada por los medios mecánicos.[188]

3.1.1.4. Firma en Títulos de Crédito emitidos en Serie.

Los títulos emitidos en serie son emitidos de manera masiva y plantean la existencia de un crédito colectivo, cuya firma del emisor es un requisito, para el representante común de los tenedores y para quienes garanticen los títulos. Ejemplo de este tipo de documentos son:

i. Las acciones de sociedades mercantiles,
ii. Las obligaciones de sociedades mercantiles,
iii. Bonos bancarios,
iv. Obligaciones subordinadas,
v. Certificados de depósito y los bonos de prenda,
vi. Certificados de participación,
vii. Certificados de depósitos diversos, expedidos por Nacional Financiera,
viii. Conocimiento de embarque,
ix. Certificados de aportación patrimonial de las Sociedades Nacionales de Crédito.
x. Certificados de la Tesorería de la Federación (CETES)

Dichos títulos se caracterizan por exigir la firma del administrador(es) de la sociedad autorizada para ese efecto en el acta constitutiva (la firma social) en el acta de emisión como en el título.

[187] Reyes Krafft, Alfredo Alejandro. La Firma Electrónica y Las Entidades de Certificación, 2003, 1ª ed., Porrúa, México, p. 95.
[188] Cft. Reyes Krafft, Alfredo Alejandro; Op. Cit., p. 96.

Resulta indudable que tratándose de bonos bancarios y obligaciones subordinadas que la firma de la emisora deba ser autógrafa respecto del o de los administradores que lleven la firma social o las personas que señaladas para este fin en los estatutos. De ahí que se elija a personas cuya función principal sea dedicarse a firmar en sustitución de los administradores cuya principal ocupación es otra.

En cuanto a los certificados de participación, las fracciones III y XI del artículo 228-n de la LGTOC disponen claramente que estos deben contener la firma autógrafa del funcionario de la sociedad emisora, autorizado para suscribir la emisión correspondiente así como del representante común de los tenedores de certificados

> ***Artículo 228 n.-*** *El certificado de participación deberá contener:*
> ***I.-*** *Nombre, nacionalidad y domicilio del titular del certificado;*
> ***II.-*** *La mención de ser "certificados de participación" y la expresión de si es ordinario o inmobiliario;*
> ***III.-*** *La designación de la sociedad emisora y* ***la firma autógrafa del funcionario*** *de la misma, autorizado para suscribir la emisión correspondiente;*
> ***IV.-*** *La fecha de expedición del título;*
> ***V.-*** *El importe de la emisión, con especificación de número y del valor nominal de los certificados que se emitan;*
> ***VI.-*** *En su caso, el mínimo de rendimiento garantizado;*
> ***VII.-*** *El término señalado para el pago de productos o rendimientos y del capital y los plazos, condiciones y forma en que los certificados han de ser amortizados;*
> ***VIII.-*** *El lugar y modo de pago;*
> ***IX.-*** *La especificación, en su caso, de las garantías especiales que se constituyan para la emisión, con expresión de las inscripciones relativas en el Registro Público;*
> ***X.-*** *El lugar y la fecha del acta de emisión, con especificación de la fecha y número de la inscripción relativa en el Registro de Comercio;*
> ***XI.- La firma autógrafa*** *del representante común de los tenedores de certificados.*

3.1.1.5. Firma en materia de Finanzas

Tanto el abrogado artículo 86 bis de la Ley Federal de Instituciones de Fianzas (LFIF) como el vigente artículo 214 de la Ley de Instituciones de Seguros y de Fianzas (LISF) publicada en el DOF el 4 de abril de 2013, por el que también se reforman y adicionan diversas disposiciones de la Ley sobre el Contrato de Seguro (LCS), disponen casi en el mismo tenor que la celebración de las operaciones y la prestación de servicios de las instituciones de fianzas y seguros (estos últimos agregados en la reforma) , se podrán pactar mediante el uso de equipos, medios electrónicos, ópticos o de cualquier otra tecnología, sistemas automatizados de procesamiento de datos y redes de telecomunicaciones, ya sean privados o públicos, estableciendo en los contratos respectivos las bases para determinar lo siguiente:

> *I. Las operaciones y servicios cuya prestación se pacte;*

II. Los medios de identificación del usuario, así como las responsabilidades correspondientes a su uso, tanto para las Instituciones como para los usuarios;
III. Los medios por los que se hagan constar la creación, transmisión, modificaciones o extinción de derechos y obligaciones inherentes a las operaciones y servicios de que se trate, incluyendo los métodos de autenticación tales como contraseñas o claves de acceso, y
IV. Los mecanismos de confirmación de la realización de las operaciones celebradas a través de cualquier medio electrónico. [189]

Además, se señaló que el uso de los medios de identificación en sustitución de la firma autógrafa producirá los mismos efectos que las leyes otorgan a los documentos correspondientes y, en consecuencia, tendrán el mismo valor probatorio. De lo anterior se hace evidente la vigencia de la FEA en materia de seguros y fianzas.

Asimismo, se estableció que las disposiciones de carácter general emitidas por la Comisión Nacional de Seguros y Fianzas (CNSF) regulará la instalación y el uso de los equipos y medios electrónicos señalados.

De ahí que la famosa publicación de la *Circular Única de Seguros y Fianzas (CUSF)* emitida por la CNSF en el DOF el 19 de diciembre de 2014, establezca una serie de disposiciones para el uso de los medios de identificación electrónica, donde de manera destacada sobresalen los capítulos *4.10. Del uso de Medios Electrónicos para la contratación de operaciones de seguros y de fianzas ; 4.11. De la comercialización de productos de seguros de adhesión a través de Medios Electrónicos ; y 4.12. Del registro de firmas de representantes de las Instituciones para suscribir fianzas así como los capítulos relativos a los Mecanismos de Entrega de Información consistentes en el: 39.1. De los aspectos generales (del cual se desprende el Anexo 39.1.4. Lineamientos para el uso de los medios de identificación electrónica de la CUSF*[190]*); 39.2. De la información estructurada; Capítulo; 39.3. De la información no estructurada ; 39.4. Del Sistema de Citas y Registro de Personas y del Sistema de Registro de Documentos ; 39.5. Del Sistema de Notificación de Oficios de Requerimiento ; y 39.6.De otra información .*

Ello significa que es admisible la FEA tanto para la comercialización de productos de seguros, la contratación de fianzas así como para la entrega de información a la supervisora CNSF.

Por otra parte, es un tema relevante que desde la abrogada LFIF [191] hasta hoy, es un requisito anual que las instituciones hicieran saber por medio de publicación en el DOF el nombre de las personas que firmarían una póliza de fianzas, que no es más que la persona encargada de firma de las fianzas (el caso de los seguros reviste un regulación *a doc* en la LCS, por lo que el registro de firmas de representantes de las Instituciones para suscribir fianzas continua siendo un requisito para una institución nacional de fianzas; por ello, los artículos 18, 59, 62, 64 y 290 de la LISF precisan que las instituciones realizarán su objeto social por medio de sus funcionarios

[189] Artículo 214 de la Ley de Instituciones de Seguros y de Fianzas
[190] Ver Anexo 39.1.4. "Lineamientos para el uso de los medios de identificación electrónica" de la Circular Única de Seguros y Fianzas publicada por la Secretaría de Hacienda y Crédito Público (SHCP), disponible en http://www.cnsf.gob.mx/Normativa/CUSF/ANEXOS%20T%C3%8DTULO%2039/ANEXO%2039.1.4.pdf
[191] Abrogada a partir del 4 de abril de 2015 por Decreto DOF 04-04-2013.

que se designen para obligar con su firma a una institución nacional de seguros. De tal forma que tratándose de fianzas, el documento que consigne la obligación del solicitante, fiado, contrafiador u obligado solidario, con la Institución, acompañado de una copia simple de la póliza y de la certificación de las personas facultadas por el consejo de administración de la Institución de que se trate, de que ésta pagó al beneficiario, llevan aparejada ejecución para el cobro de la cantidad correspondiente y sus accesorios.

De las disposicione anteriores se deduce con facilidad que la firma en tales títulos, es un requisito que exigen las leyes para el emisor, para el representante común de los tenedores, y en su caso, para aquellos que garanticen los títulos en los supuestos en que la ley permite esta situación; y que deberá estamparse la firma de los administradores de la sociedad autorizados[192] o los mandatarios a título especial, en el acta de emisión y en los títulos seriales,.

Respecto a los bonos bancarios y obligaciones subordinadas, claramente la ley exige la firma de la emisora deberá ser autógrafa respecto de el (o los) administradores que lleven la firma social, en el resto de los demás supuestos serán quienes sean señalados en los estatutos de la emisora y en realidad.

3.1.1.6. Firma en Pólizas de Seguros.

La LCS reformada el 4 de abril de 2013, establece un procedimiento que no es similar a la de las afianzadoras, pues el uso mercantil es que el contratante acepte la pólizas de seguro sin firma, mientras que el agente autorizado por la aseguradora solo se encarga de revisar el número de póliza, el nombre del contratante y su vigencia; por lo que no ha existido inconvenientes tales como la falsificación. De tal forma que los numerales 20 y 165 son vigentes pero no positivos, en esta manera proceder:

> ***Artículo 20.-*** *La empresa aseguradora estará obligada a entregar al contratante del seguro, una póliza en la que consten los derechos y obligaciones de las partes. La póliza deberá contener:*
> *I.- Los nombres, domicilios de los contratantes y firma de la empresa aseguradora;*
> *II.- La designación de la cosa o de la persona asegurada;*
> *III.- La naturaleza de los riesgos garantizados;*
> *IV.- El momento a partir del cual se garantiza el riesgo y la duración de esta garantía;*
> *V.- El monto de la garantía;*
> *VI.- La cuota o prima del seguro;*
> *VII.- En su caso, la mención específica de que se trata de un seguro obligatorio a los que hace referencia el artículo 150 Bis de esta Ley, y*
> *VIII.- Las demás cláusulas que deban figurar en la póliza, de acuerdo con las disposiciones legales, así como las convenidas lícitamente por los contratantes.*

[192] Generalmente, la responsabilidad de llevar la firma es de uno o varios administradores, motivo por el cual se le suele llamar: firma social.

Artículo 165.- *La póliza del Contrato de Seguro de personas no podrá ser al portador. La nominativa se trasmitirá mediante declaración de ambas partes, notificada a la empresa aseguradora. La póliza a la orden se trasmitirá por medio de endoso que contenga, invariablemente, la fecha, el nombre y el domicilio del endosatario y la firma del endosante. No se admitirá prueba alguna de otra especie en esta forma de trasmisión.*

En suma, normalmente es un uso mercantil que para suscribir las pólizas de seguros se emple la firma autógrafa y, a veces, su refrendo por los agentes autorizados. El aceptar así las pólizas no ha mostrado casos de falsificación, razón por la cual no se ha creído necesario fijar un procedimiento similar al de las afianzadoras.

Finalmente, hasta hoy no se advierte que las instituciones de seguros están lejos de utilizar la FEA.

3.1.1.5. Firma en Pólizas de Fianzas.

Las pólizas de las fianzas son suscritas generalmente por autorizados por la Asamblea General o del Consejo de Administración. En su suscripción se continua aplicando el principio relativo a los catálogos de firmas, firmas A y firmas B, y se establece un límite en cuanto al monto, de acuerdo con las facultades que en cada caso señalen los órganos administradores.

Actualmente, la Ley de Instituciones de Seguros y de Fianzas regula y establee que las firmas en las pólizas de fianzas y el facsímil de las mismas, se publicarán en el Diario Oficial de la Federación[193]. De tal forma que la Comisión Nacional de Seguros y Fianzas (CNSF) anualmente requiere a cada institución los datos relativos a la denominación de la sociedad, nombres y apellidos de las personas que firmarán, su nombramiento y si son firmas A o B, y las variaciones que en las firmas se aprueben.

Tal solicitud anual lo hace la CNSF para hacer del conocimiento del Gobierno Federal, Estatales, Municipal y del público en general, las firmas autorizadas, el facsímil de cada compañía, para difundirlos mediante una circular y una publicación en el DOF.

3.1.2. Instituciones o figuras relacionadas con la Firma.

Además de los tipos de firmas referidos, existen una variedad de distintivos o formalidades dentro de la jerga mercantil que se denominan “instituciones relacionadas con la firma”, que se traducen en una serie de exigencias que facilitan en la práctica mercantil el otorgamiento de validez a ciertos documentos:

a) Conocimiento de firma
b) Catálogo de firmas
c) Firma facsimilar.

[193] Anteriormente los artículos 13, 82, 84 y 96 regulaban esta situación en la abrogada Ley Federal de Instituciones de Fianzas.

a) Conocimiento de firma.

El conocimiento de firma es el *acto por medio del cual una persona estampa su firma autógrafa para hacer constar que conoce como legítima de su otorgante, otra, que regularmente le antecede*[194]. Se trata de un uso mercantil y bancario que no se encuentra normado en una disposición legal; no obstante, se considera un uso que produce derechos.

Su mayor empleo es en cheques, en atención a que los cuentahabientes de las instituciones bancarias tienen inscrita su firma como prueba de identificación, por lo tanto, al identificar la otra firma del tenedor, se reconoce también a éste.

El conocimiento de firma es una institución que se utiliza frecuentemente en cheques en atención a que las instituciones de crédito registran las firmas de sus cuenta-habientes para identificarlos, por tanto, al identificar la diversa firma del tenedor de un título de crédito, esta aquél a su vez reconociéndolo.

Este uso fue reconocido por la SCJN en la tesis de rubro y texto siguientes:

> ***CHEQUES, FIRMA DE CONOCIMIENTO COMO MEDIO DE IDENTIFICACION PARA EL PAGO DE LOS.*** *La Ley General de Títulos y Operaciones de Crédito, no exige que el último tenedor del cheque, quien se ha identificado como tal mediante el conocimiento de firma, lo presente personalmente al banco librado y solamente él deba recibir el dinero, ni en la práctica se acostumbra exigir la identificación del presentante al momento de entregar el dinero, sino que este se da contra la ficha de cobro, recibida a cambio del documento que se paga, después de que se ha verificado la identidad del último tenedor, por lo que la persona de este es la que se identifica y no la del presentante*[195]*.*

El conocimiento de firma no tiene efectos cambiarios, pues solo sustituye a otro medio de identificación del tenedor o beneficiarios del documento.

Ahora bien, en el caso de una apertura de cuenta de cheques, un conocimiento de firma tiene como finalidad evitar en lo posible fraudes y malos manejos con los documentos de los cheques, esto es, el soporte físico del papel del cheque que el banco otorga a su cuenta-habiente (ver Apéndice II: Ejemplo de Conocimiento de firma bancaria).

b) Catálogo de firmas.

Un catálogo de firmas es un inventario de hojas sustituibles que contienen firmas autógrafas o impresas, de los funcionarios y empleados autorizados por la institución de crédito para suscripción de títulos de crédito en su nombre así como de documentos que comprometan u obliguen a esta como: expedición de giros nacionales o internacionales, autorizaciones bancarias, órdenes de pago, traspasos de fondos considerables, certificación de fondos de un

[194] BALTIERRA Guerrero, Alfredo. "La firma autógrafa en el derecho bancario", Revista de la Facultad de Derecho de México, UNAM, Núm. 121-122-123, Enero - Junio, 1982, p. 17 a 48.

[195] Véase Semanario Judicial de la Federación, Registro: 818455, tesis aislada de la Tercera Sala, Sexta Época, CVI, Cuarta Parte , página: 13, Rubro: "CHEQUES, FIRMA DE CONOCIMIENTO COMO MEDIO DE IDENTIFICACION PARA EL PAGO DE LOS."

cheque o de su insuficiencia de fondos y muchos otros más. Debe decirse que en la legislación una vez más no se menciona nada al respecto de la validez de un catálogo de firmas, pero también se trata de un uso bancario.

Generalmente se requiere que el catalogo cuente con los documentos autenticados con dos firmas, la firma "A" y la firma "B", sin que sea permitido dos firmas "B", o dos firmas "A". Ello se complementó con la actualización constante que las instituciones de crédito envían al resto de sus sucursales dentro del país.

c) Firma facsimilar.

De acuerdo con la frase "donde la ley no distingue, no se debe distinguir", cuando se habla de "firma", no se habla de firma autógrafa sino puede incluir firma facsimilar, huella digital o firma a ruego.

Una firma facsímil es una reproducción de la firma manual que se puede guardar electrónicamente o por grabado, impresión o estampación. Aunque las firmas facsimilares pueden ser arriesgadas, son legales. El uso de la firma facsímil facilita los asuntos de los empleados públicos o funcionarios que procedan. Una firma facsímil de un funcionario autorizado tiene el mismo peso que su firma manual; no obstante, puede no ser aceptable en todos los documentos del gobierno o del sector privado, dependiendo de la materia, por ejemplo en el área fiscal, muchos de los requerimientos y multas que emite el SAT contienen firma facsimilar, lo cual acarrea una serie de recursos de revocación ya que dicha firma es ilegal porque se requiere nombre y firma autógrafa del funcionario público que expidió la multa[196].

Debido a la eficiencia y rapidez que se requiere en las operaciones mercantiles, se llega a reemplazar la firma autógrafa por la firma facsímil. Dicha firma ha adquirido arraigo como la estricta y fiel imitación de la firma autógrafa, empleándose para estampar en serie tal firma. En las situaciones en que se utiliza son[197]:

[196] Véase Gaceta del Semanario Judicial de la Federación, Registro: 206419, jurisprudencia: 2a./J. 2/92 de la Segunda Sala, Octava Época, página: 15, Rubro: "FIRMA FACSIMILAR. DOCUMENTOS PARA LA NOTIFICACION DE CREDITOS FISCALES" .

[197] Cfr. BALTIERRA Guerrero, Alfredo. "La firma autógrafa en el derecho bancario", Revista de la Facultad de Derecho de México, UNAM, Núm. 121-122-123, Enero - Junio, 1982, p. 43.

I. Para signar la correspondencia de las organizaciones que constantemente se comunican con clientes;
II. Para expedición de muchos libramientos de cheques, previo convenio entre el librador y el librado.
III. Para la firma de letras de cambio, previo convenio entre girador y el beneficiario (o tomador).
IV. Para la firma de acciones y certificados provisionales de sociedades mercantiles, previo depósito del original en el Registro Público de Comercio de la localidad en que se registró la sociedad, tal como lo establece el artículo 125, fracción VIII, de la LGSM.

3.1.3. Diferencias entre Firma Autógrafa y Firma Electrónica.

El origen en latín de la palabra firma es *firmāre*, que se traduce en afirmar, dar firmeza y seguridad a algo, mientras que el término autógrafa[198] proviene del *autográphus* y significa grabar o escribir pos autógrafa se define como lo que está escrito de mano de su mismo autor.

Las funciones de las firmas autógrafas o manuscritas son las siguientes:

a) Identificar a una persona.
b) Proporcionar certidumbre en cuanto a la participación de dicha persona en el acto de la firma.
c) Vincular a una persona con el contenido de un documento firmado.
d) Usarla como medio de prueba.

En un contrato firmado, por ejemplo, la firma sirve para evidenciar que, el firmante, al firmar ha tenido la intención de considerarse vinculado al contenido del contrato; de una firma en un documento podía desprenderse que al firmar el autor había manifestado que estaba consciente de que del acto de la firma podrían derivarse consecuencias jurídicas[199]. Entonces, el reto de la firma electrónica en sentido amplio frente a la firma autógrafa fue identificar los criterios jurídicos que permiten que las firmas electrónicas que ya se encontraban en el mercado *cumplan las mismas funciones que las firmas manuscritas.* Lo cual se comparó con los medios electrónicos, el original de un MD no puede distinguirse de una copia, pues no lleva una firma manuscrita y no figura en papel.

El objetivo de las “firmas electrónicas” es ofrecer medios técnicos para que algunas o todas las funciones identificadas como características de las firmas manuscritas puedan cumplirse en un entorno electrónico.

[198] Véanse ambas voces en el Diccionario de la lengua española (DRAE) 22.ª edición, 2012.
[199] La firma en un documento también podía ser una manifestación de la voluntad de una persona para respaldar su autoría en un texto u obra; manifestar la voluntad de una persona de vincularse al contenido de un documento escrito por otra persona; asimismo, evidenciar que una persona había estado en un lugar determinado en un momento determinado.

De acuerdo con el principio de equivalencia funcional, el artículo 89 del CCo prevé que la firma electrónica consiste en los datos en forma electrónica consignados en un MD, adjuntados o lógicamente asociados al mismos por cualquier tecnología, que son utilizados para identificar al firmante en relación con el mensaje e indicar que el firmante aprueba la información contenida en el mensaje, produciendo los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio.

Mientras tanto, el artículo 93 del Código de referencia dispone que cuando la ley exija la firma de las partes en un acto jurídico, este requisito se tendrá por cumplido tratándose de MD, siempre que éste sea atribuible a estas personas.

Es pertinente señalar que los órganos jurisdiccionales en materia federal a través de la tesis *"DOCUMENTOS PRIVADOS, EFECTOS DEL RECONOCIMIENTO DE LA FIRMA EN LOS"*[200], apoyan el razonamiento consistente en que un documentos firmado por una persona implica que ésta también reconoce el contenido del mismo.

Finalmente, Alfredo A. Reyes Krafft elaboró el siguiente cuadro que refleja la distinción entre la firma autógrafa y la firma electrónica[201]:

	FIRMA AUTÓGRAFA	FIRMA ELECTRÓNICA
ELEMENTOS FORMALES		
La firma como signo personal.	**X**	
El animus signandi, voluntad de asumir el contenido de un documento.	**X**	
ELEMENTOS FUNCIONALES		
Función Identificadora, relación jurídica entre el acto firmado y la persona que lo ha firmado.	**X**	
Función de Autenticación. El autor del acto expresa su consentimiento y hace propio el mensaje	**X**	**X**
INTEGRIDAD		**X**
ACCESIBILIDAD		**X**

3.1.4. Firma Digital como sinónimo de Firma Electrónica Avanzada.

En el punto "*1.4.1.3. Firma Electrónica y Firma Digital"* se explicó que por FEA y firma digital se entiende lo mismo. Mientras que la firma electrónica y la firma digital son nociones diferentes; ya que la firma digital o FEA se diferencia de la firma electrónica en que la información generada o comunicada debe ser en forma integra, atribuible a las personas obligadas y accesible para su ulterior consulta.

[200] Véase Semanario Judicial de la Federación, Tomo XII, Agosto de 1993, Material Civil, Octava Época, Página: 422
[201] Reyes Krafft, Alfredo Alejandro. La Firma Electrónica y Las Entidades de Certificación, 2003, 1ª ed., Porrúa, México, p. 107.

Firma Electrónica (género)		**Firma Electrónica Avanzada o Firma Digital** (especies)
		Otras Firmas Electrónicas: NIP, Biométricos, contraseñas, etc.

3.1.5. Firma Electrónica Avanzada como garantía de seguridad jurídica.

Entre las cuestiones que hay que resolver en el comercio electrónico están las de seguridad e integridad de las comunicaciones, así como la privacidad y protección de los datos personales y bancarios de los consumidores y usuarios, cuando éstos circulan en Internet. En razón de la evolución de la Sociedad de la Información y el Conocimiento (SIC) se exige la generalización de la confianza de las personas en las comunicaciones.

Ya en el estudio de la FEA, el artículo 89 del CCo precisa que las actividades de comercio electrónico se someterán en su interpretación y aplicación a cuatro principios, los cuales son aplicables tanto al MD como dicha firma, a saber:

a) Neutralidad tecnológica[202],
b) Autonomía de la voluntad[203],
c) Compatibilidad internacional,
d) Equivalencia funcional[204]

Aquí se puede observar que la *"compatibilidad internacional"* es una variante de los principios generales del derecho de comercio electrónico que señala la doctrina y que tampoco se menciona la "buena fe"[205]

Por lo que sólo nos referimos al principio de compatibilidad internacional. Dicho principio se recoge en el numeral 114 del CCo, al respecto reconoce la validez y efectos jurídicos a las firmas electrónicas creadas o utilizadas fuera de la República Mexicana, siempre que la firma presente un grado de fiabilidad equivalente al de una firma creada o utilizada en la República Mexicana.

Aunque estos principios ya fueron abordados en el capítulo I, un ejemplo de la equivalencia funcional, es cuando los MD pueden tener los mismos efectos y consecuencias jurídicas que la información y documentos consignados en papel.

3.2. Enfoque tecno-legislativos de la firma electrónica

Los diferentes enfoques o aproximaciones que adoptaron los textos legales en diferentes países y Estados se clasifican de acuerdo a tres criterios. Tradicionalmente, las leyes que regulan la

[202] Supra1.2.3.
[203] Supra 1.2.5.
[204] Supra 1.2.1.
[205] Supra punto 1.2.

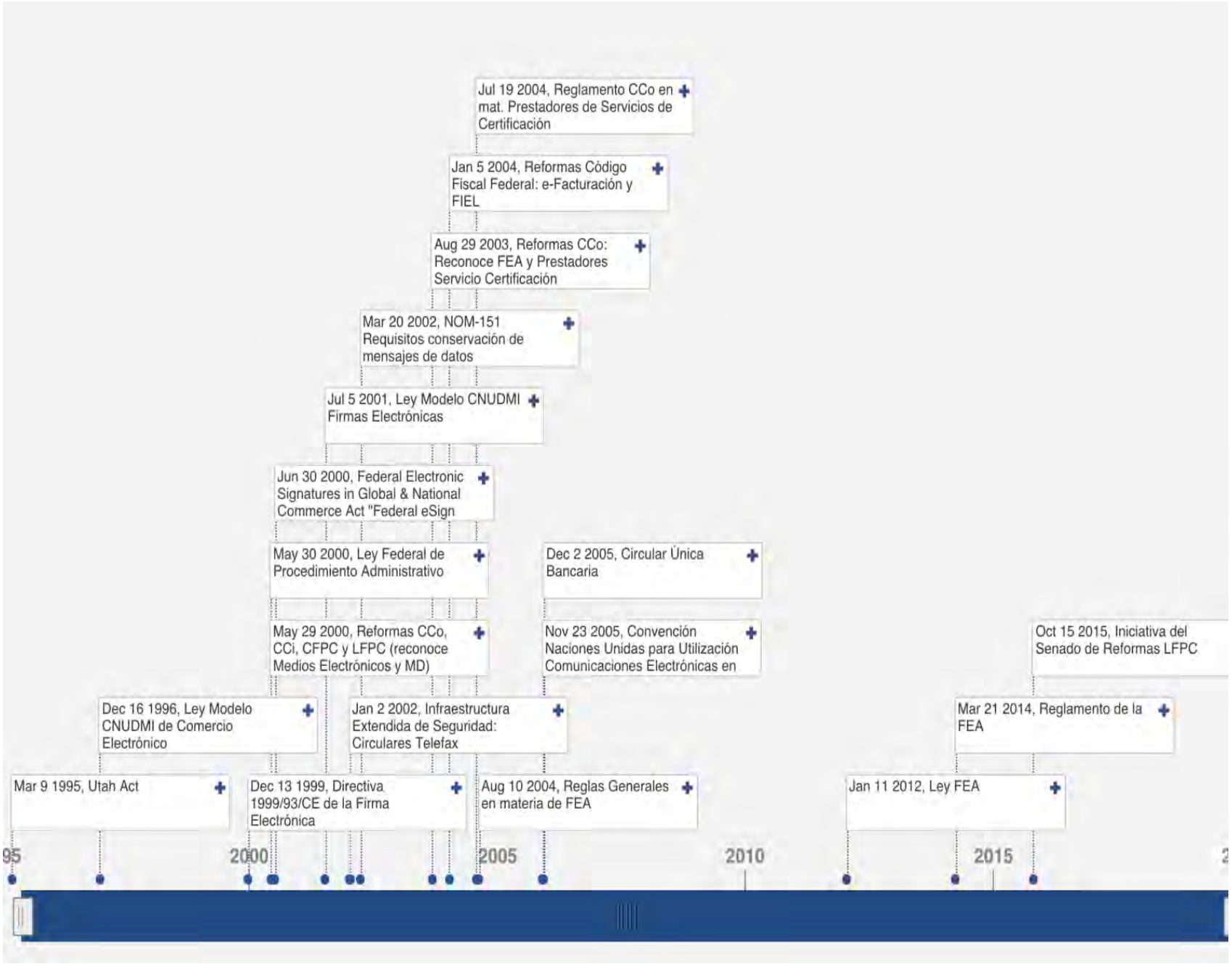
firma electrónica han sido agrupadas de acuerdo a la apertura en el reconocimiento de las diferentes tecnologías[206]

a) Enfoque obligatorio o de tecnología específica
b) Enfoque minimalista o habilitador.
c) Enfoque híbrido o de doble nivel.

a) Enfoque obligatorio o de tecnología específica. Esta postura es conocida por reconocer de manera forzosa un solo tipo de firma electrónica o digital. Entonces, solo firmas basadas en la infraestructura de llave pública son consideradas con los mismos efectos que la firma autógrafa. En este caso se encuentra *Utah Digital Signature Act*[207], La Ley de Firma Digital de Alemania y la Ley de FEA en México.
b) Enfoque minimalista o habilitador. Esta aproximación reconoce y garantiza valor legal a todo tipo de firmas digitales o electrónicas. Se trata de una regulación bastante flexible y el concepto de firma electrónica es definido de manera bastante amplia y con solo algunos requerimientos mínimos son impuestos para su reconocimiento en atención a que considera que todas las firmas tienen la capacidad de tener el mismo valor que la firma autógrafa. Este tipo de legislación es común en *The Uniform Electronic Transactions Act (UETA)*[208] y Electronic Signature in Global and National Commerce Act (E-Sign)[209][210]. Es de resaltarse que los países cuyo régimen legal es el *common law* generalmente siguen esta línea minimalista, mientras que los que se basan en un régimen de *civil law* siguen la postura obligatoria.
c) Enfoque híbrido o doble nivel. Esta aproximación mezcla las dos posturas anteriores, por un lado impone requerimientos estrictos para el reconocimiento de firmas electrónicas para alcanzar la equivalencia con la firma autógrafa, y por otro, reconoce la validez de otros tipos de firmas electrónicas. Ejemplos de este tipo de legislación son la Directiva 1999/93/CE de Firma Electrónica y la LMFE 2001.

Finalmente, con el objeto de concatenar los sucesos históricos relacionados con la FEA, se exhibe la siguiente línea del tiempo[211]:

[206] Cfr. Schellekens, Maurice H. M.: Electronic signatures: Authentication technology from a legal perspective, The Hague: Asser Press, 2004 (Information technology & law series ; 5) pp. 56-57. Similares enfoques se establecen en: CNUDMI, Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónicas, Naciones Unidas, Viena, Marzo 2009, p. 38.
[207] Véase Utah Digital Signature Act, Utah Code Ann. 46-3-101 to 602 (2004). La Ley Utha fue elaborada tomando en consideración la Guía de Firma Digital de la American Bar Association, para más información véase: Digital Signature Guidelines, Washington, American Bar Association (ABA), 1996.
[208] Uniform Electronic Transaction Act (UETA). National Conference of Commissioners for Uniform State Law (NCCUSL), 1999, accesible en http://www.ncsl.org/research/telecommunications-and-information-technology/uniform-electronic-transactions-acts.aspx -
[209] Electronic Signature in Global and National Commerce Act (E-Sign), enacted by President Clinton in 2000, accesible en https://www.fdic.gov/regulations/compliance/manual/pdf/X-3.1.pdf
[210] Internet Law & Policy Forum (ILPF), An Analysis of International Electronic and Digital Signature Implementation Initiatives, September 2000, pp. 6-7, visible en: http://www.ilpf.org/groups/index.htm#jurisdiction.
[211] La elaboración nuestra.


Jul 19 2004, Reglamento CCo en mat. Prestadores de Servicios de Certificación
Jan 5 2004, Reformas Código Fiscal Federal: e-Facturación y FIEL
Aug 29 2003, Reformas CCo: Reconoce FEA y Prestadores Servicio Certificación
Mar 20 2002, NOM-151 Requisitos conservación de mensajes de datos
Jul 5 2001, Ley Modelo CNUDMI Firmas Electrónicas
Jun 30 2000, Federal Electronic Signatures in Global & National Commerce Act "Federal eSign
May 30 2000, Ley Federal de Procedimiento Administrativo
Dec 2 2005, Circular Única Bancaria
May 29 2000, Reformas CCo, CCi, CFPC y LFPC (reconoce Medios Electrónicos y MD)
Nov 23 2005, Convención Naciones Unidas para Utilización Comunicaciones Electrónicas en
Oct 15 2015, Iniciativa del Senado de Reformas LFPC
Dec 16 1996, Ley Modelo CNUDMI de Comercio Electrónico
Jan 2 2002, Infraestructura Extendida de Seguridad: Circulares Telefax
Mar 21 2014, Reglamento de la FEA
Mar 9 1995, Utah Act
Dec 13 1999, Directiva 1999/93/CE de la Firma Electrónica
Aug 10 2004, Reglas Generales en materia de FEA
Jan 11 2012, Ley FEA
95
2000
2005
2010
2015

3.3. La Criptografía como método para la creación de la Firma Electrónica Avanzada.

Las Firmas Digitales (o Firmas Electrónicas Avanzadas) se crean y verifican utilizando *criptografía,* rama de las matemáticas aplicadas que se ocupa de trasformar mensajes en formas aparentemente ininteligibles y se devuelven luego a su forma original. La criptografía es la ciencia de cifrar y descifrar información mediante técnicas especiales y normalmente es usada para posibilitar un intercambio de mensajes que sólo pueden ser leídos por personas a las que van dirigidos y que poseen los medios para descifrarlos.

Ahora bien, la criptografía es la especie, y cuando se quiere realizar un examen de ella, se debe acudir a su género: la *criptología*, la cual comprende las técnicas de cifrado, entre las que se incluye el *criptoanálisis*, que estudia métodos empleados para descifrar textos con objeto de recuperar la información original en ausencia de las claves.

Sobre todo en la segunda guerra mundial, la criptografía fue empleada por la milicia, los políticos y/o diplomáticos. Aunque ya desde el imperio romano, con Julio César se empleaba el sistema criptográfico para comunicarse con las cabezas militares que se encontraban en el campo de batalla. Es muy conocido el algoritmo de César, el cual consistía en reemplazar una letra del abecedario por otra, como ejemplo: a por f; b por g; c por x; y así sucesivamente[212]. Sin embargo, con el desarrollo del comercio electrónico el uso de la criptografía ha dado un gran giro hacia la difusión de técnicas criptográficas para fines no militares.

Si la función de la criptografía es el empleo de algoritmos y métodos matemáticos para cifrar y descifrar mensajes; se puede concluir que es una técnica que proporciona seguridad a la transmisión y almacenamiento de datos a través de redes de telecomunicaciones, de ahí que su intención sea garantizar el secreto en la comunicación entre el emisor y destinatario de una contratación electrónica mercantil y, en segundo lugar, asegurar que la información que se envía sea auténtica en un doble aspecto: que el remitente sea realmente quien afirma ser y que el contenido del MD enviado, no haya sido alterado en su tránsito.

3.3.1. Criptografía Simétrica

La criptografía simétrica (conocida también como de clave secreta o clave única) es una técnica en la que tanto el emisor como el receptor del mensaje operan con el mismo código de encriptación y desencriptación de los mensajes o información, siendo necesario que las partes en comunicación acuerden previamente una clave secreta, con la desventaja de tener que encontrar el modo seguro de cambiar de clave.

La criptografía simétrica sólo emplea una clave para cifrar y descifrar los datos, como consecuencia dicho tipo de criptografía ofrece la autenticidad entre las partes ya que solamente la otra parte con la que se comparte la clave secreta puede haber cifrado el mensaje y también ofrece integridad, ya que si el mensaje ha sido alterado será ininteligible al descifrarlo; en

[212] Martínez Nadal, Apol·lònia : Comercio electrónico, firma digital y autoridades de certificación, 2001, 3ª ed., Madrid, Civitas, p. 42.

cuanto a la confidencialidad[213] de la información, únicamente las partes implicadas podrán descifrar el mensaje; por último, no garantiza el no rechazo de origen ya que no hace uso de una firma digital.

De lo anterior se desprende que para que la comunicación sea segura, es necesaria que la clave sea mantenida en secreto entre las partes involucradas. Entonces, se torna relevante la gestión de la distribución y utilización de la clave secreta para evitar que la misma sea modificada en su tránsito.

La criptografía simétrica tiene desventajas en relación a la distribución de las claves, tales como que no ofrece todos los servicios de seguridad exigida legalmente, a pesar de que ofrece la autenticación e integridad entre las dos partes que comparten la clave secreta, no lo hace frente a terceros (una tercera parte no podrá determinar con certeza el emisor del mensaje, ni su contenido o la persona que lo ha modificado, porque una de las partes que comparte la clave secreta común podría haberla usado para falsificar el nombre de la otra parte, o podría haber alterado el contenido del mensaje)[214].

Así, el intercambio de la misma clave para cifrar y descifrar los mensajes hace que una tercera persona no pueda determinar cuál de los dos (emisor y receptor) es el autor del mensaje. Considerando las desventajas exhibidas, los sistemas de cifrado simétricos no son idóneos y calificados para ser empleados en Internet, donde los usuarios no puede percatarse quienes uno y otro.

El antecedente de **criptoanálisis simétrico** más conocido es el realizado por la Máquina Enigma, que contenía un código secreto que Alemania utilizaba para sus comunicaciones militares cuando estaba en curso la invasión de Polonia por parte de Alemania en 1939 y Hitler era el enemigo de casi toda Europa. Dicha máquina realizaba cifrado electromecánico y generaba abecedarios según la posición de unos rodillos que podrían tener distintas órdenes y posiciones. El algoritmo que usaba dependía de una clave que está formada por: los rotores o rodillos que usaba, su orden y la posición de cada anillo, siendo esto lo más básico.

[213] Además de la confidencialidad simple, se puede llegar a otro nivel de confidencialidad es una característica de la FEA siempre y cuando se cifre también el MD que se signe. Lo anterior se realiza por medio de la clave pública del destinatario, a fin de que el MD sea descifrado por éste a través de su clave privada; ello implica que para obtener la confidencialidad y la signación de un documentos se utilizan dos pares de claves, tanto las del emisor como las del destinatario.

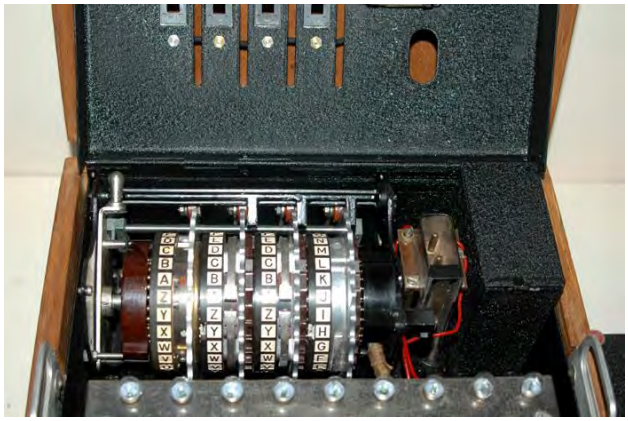
[214] Martínez Nadal, Apol·lònia : Comercio electrónico, firma digital y autoridades de certificación, 2001, 3ª ed., Madrid, Civitas, p. 43.

Maquina Enigma original[215]

La máquina Enigma era empleada en las comunicaciones alemanas durante la guerra y tenía un funcionamiento complejo. Se basaba en cinco rotores que variaban cada vez que se pulsaba una tecla, de manera que cada letra del alfabeto ofrecía un número altísimo de posibilidades. El Ejército alemán complicaba más las cosas cambiando la posición de los rotores una vez al mes; razón por la cual se consideraba indescifrable.

Una desventaja de la Máquina Enigma es que si se desea tener un contenido totalmente confidencial con 10 personas se debe apuntar o aprender las diez claves para cada persona.

La máquina Enigma contaba también con un libro de claves que contenía la clave del día y hacia un poco más difícil encontrar la clave, pero no era una clave lo suficientemente segura, sobre todo cuando los ingleses consiguieron de los polacos el algoritmo; no obstante, en 1939 el descifrado del código Enigma lo realizó el matemático Alan Turing, trabajador para el *Government Code and Cypher School* o Servicio de Inteligencia británico, quien se reunió con el Servicio de Inteligencia polaco, país que también estaba intentando desentrañar el código Enigma.



Máquina Enigma por dentro[216]

Rotores[217]

A partir de la información recibida, Turing empieza a mejorar el enfoque del método polaco. En tres meses desde que recibiera las informaciones del Servicio polaco, Turing fue capaz de descifrar el código alemán, pero ante la situación que se vivía se hacía necesario automatizar el proceso. Para ello, diseñó junto con Gordon Welchman, su propia máquina para contrarrestar la Máquina Enigma, llamada *Bomba*, la cual realizaba análisis matemáticos para determinar las posiciones más factibles de los rotores y salieron a la venta en 1940. Las máquinas *Bomba* jugaron un papel determinante descifrando los mensajes de la fuerza aérea alemana y con ellas, en 1943 ya habían descifraban un total de 84’000 mensajes de Enigma al mes.

Por otra parte, en cuanto a la parte técnica, los algoritmos simétricos son aquellos en los que la clave de descifrado puede ser deducida de la clave de cifrado, y viceversa. A manera de guisa, existen los siguientes algoritmos de cifrado simétrico:

[215] Fuente de la imagen accesible en http://www.watchtime.com/reviews/code-name-ultra-deciphering-the-bremont-codebreaker, consultada el 3 de enero de 2015.
[216] Fuente de la imagen accesible en: http://www.minelinks.com/war/enigma1.html, consultada el 3 de enero de 2015.
[217] Fuente de la imagen: accesible en: http://www.minelinks.com/war/enigma1.html, consultada el 3 de enero de 2015.

- AES
- DES
- IDEA
- 3DES
- Blowfish

La rapidez y seguridad del cifrado simétrico es evidente; no obstante, su debilidad consiste en que únicamente se emplea una clave para las operaciones de cifrado y descifrado, la cual debe conocerse por quienes se comunican, esto se traduce en que puede darse que la clave secreta al ser intercambiada o comunicada, hace pasible de intercepción, con lo que un posible atacante (en la imagen sería Eve) que lograra apoderarse de la clave, podría además de leer los mensajes que intercambian **Bob** y **Alice**[218], **(Ana** en la imagen que se muestra en el ejemplo a continuación) alterar el contenido del mismo, ya que conoce la clave, y solo le resta conocer que algoritmo se utilizó[219].

Probablemente sería más fácil saber la clave interceptándola que probándola una por una por fuerza bruta, teniendo en cuenta que la seguridad de un mensaje cifrado debe recaer sobre la clave y nunca sobre el algoritmo; por lo que sería una tarea eterna reventar la clave, como comenté en un ejemplo de ataque por fuerza bruta.

Como primer acercamiento a la criptografía asimétrica y simétrica se ilustra a través de la siguiente imágen:

G

Diferencia entre Criptografía Asimétrica y Simétrica[220]

3.3.2. Criptografía Asimétrica

La criptografía asimétrica o criptografía de clave pública (asymmetric key cryptography or public key cryptography) se originó en 1976, cuando *Whitfield Diffie y Martin Hellman* publicaron un

218 Alice y Bob son personajes ficticios usados en explicaciones criptográficas, teoría de juegos y físicas, especialmente las provenientes del inglés. Los nombres son usados por conveniencia, dado que explicaciones del tipo "La persona A quiere mandar un mensaje a la persona B" rápidamente comienzan a ser difíciles de seguir. Los nombres, políticamente correctos al usar ambos sexos, cortan la carga ambigua al usar en la explicación los adjetivos, artículos, etc. adecuados a cada sexo. Los nombres han sido elegidos de tal manera que concuerden con las primeras letras del alfabeto (persona A es Alice, persona B es Bob).

219 Rocha Vargas, Marcelo Emilio, Castello, Ricardo J. y Bollo, Daniel E., Criptografía y Firma Electrónica/Digital en el Aula, Universidad Nacional de Catamarca – Secretaría de Ciencia y Tecnología, Ed. Científica Universitaria, 7 p. accesible en: http://www.editorial.unca.edu.ar/Publicacione%20on%20line/CD%20INTERACTIVOS/DUTI/PDF/EJE2/ROCHA%20VARGAS.pdf , consultado el 12 de enero de 2015.

220 Fuente de la imagen, Criptografía Moderna, blog accesible en http://criptografiamoderna.blogspot.mx/, consultado el 2 de enero de 2015.

artículo denominando *New Directions in Cryptography*[221] en el que afirman la posibilidad de implementar *criptosistemas*[222] de clave pública usando funciones relacionadas con difíciles problemas matemáticos, el artículo fue relevante porque se centra en la autenticidad y privacidad de las comunicaciones electrónicas, con respecto a la privacidad lo resuelve con el criptosistema de llave pública y con ello mejora el problema de la confidencialidad del MD.

En cuanto a la autenticidad, señala que el criptosistema de llave pública hace posible verificar si una firma es creada por el tenedor de la clave privada. . Para 1977 Merkley y Hellman propusieron el que fue el primer sistema de cifrado de clave pública basado en el problema de la suma de subconjuntos (o *subset-sum* problema).[223] En ese mismo año Ron **R**ivest, Adi **S**hamir y Len **A**dleman propusieron un criptosistema de clave pública sustentado en el que pasó a llamarse el problema **RSA**, basado en la factorización de enteros.

Ron Rivest profetizó que factorizar un número de 125 dígitos llevaría 40.000 billones de años, pero el desafío RSA-129 fue resuelto en abril de 1994 por un equipo dirigido por D. Atkins, M. Graff, A. Lenstray P. Leyland usando 600 computadoras conectados a través de Internet. En 1985, Taher Elgamal publicó un artículo titulado *A Public key Cryptosystem and A Signature Scheme based on discrete Logarithms*, en el que propone un sistema de cifrado de clave pública basado en el problema del logaritmo discreto.

Posteriormente, Neal Koblitz y Víctor Miller proponen un nuevo enfoque del criptosistema denominado el *Criptosistema de Curvas Elípticas* (en adelante CCE)[224], en la que una curva elíptica es una curva en el plano tal que cada línea que la corta en dos puntos, la corta además exactamente en un tercer punto. El criptosistema basado en curvas elípticas más ampliamente respaldado es el llamado *Integrated Encryption Scheme* (IES)[225].

Las implementaciones de CCE son muy seguras y no se les conoce ningún ataque subexponencial que haya tenido éxito, requieren claves mucho más cortas para el mismo nivel

---

[221] Véase DIFFIE, Whitfield y HELLMAN, Martin E. "New Directions in Cryptography," IEEE Trans. on Info. Theory, Vol. IT-22, Nov. 1976, pp. 644-654 (Invited Paper).

[222] Un criptosistema o cifra es un método secreto de escritura, mediante el cual un texto en claro se transforma en un texto cifrado o criptograma. El proceso de transformar un texto en claro en texto cifrado se denomina cifrado, y el proceso inverso, es decir la transformación del texto cifrado en texto en claro, se denomina descifrado. Ambos procesos son controlados por una o más claves criptográficas.

[223] Dicho problema es este: dado un conjunto de enteros ¿existe algún subconjunto cuya suma sea exactamente cero? Por ejemplo, dado el conjunto { −7, −3, −2, 5, 8}, la respuesta es SI, porque el subconjunto { −3, −2, 5} suma cero.

[224] En el área de comunicación se debe de contar con las mismas o reglas mínimas de comunicación. Estas reglas están contenidas en los estándares los cuales se imponen a quienes quieran poder interconectarse, Existen varios estándares de Criptosistema de Curvas Elípticas (CCE) entre los más conocidos están:

a) Estándar P1363 de la IEEE de criptografía de clave pública: Specifications For Public-Key Cryptography: http://grouper.ieee.org/groups/1363/
b) Grupo de evaluación criptográfica Europeo NESSIE: New European Schemes for Signature, Integrity and Encryption: http://www.cryptonessie.org/
c) Grupo de evaluación criptográfica Japonés CRYPTREC: Cryptography Research and Evaluation Committee: ttp://www.ipa.go.jp/security/enc/CRYPTREC/index-e.html
d) Estándar SECG: The Standards for Efficient Cryptography Group (SECG): http://www.secg.org/
e) Estándar NIST: The NIST Computer Security Division: http://csrc.nist.gov

[225] IES ha sido aprobado como estándar por distintas entidades: ANS X9F1, CRYPTREC, IEEE P1363, NESSIE, NSA Suite B.

de seguridad que otros criptosistemas, son más rápidos que los anteriores, requieren menos memoria que los anteriores, son ideales para dispositivos portátiles como PDAs, smartcards, móviles, etc.[226].

Una vez expuestos los antecedentes de este tipo de criptografía asimétrica es indispensable señalar que la criptografía de clave pública emplea un par de claves asociadas: una clave privada, conocida sólo por el titular, que debe mantenerla en secreto (e incluso puede ocurrir que ni siquiera el titular conozca la clave privada, que probablemente se mantendrá en una tarjeta inteligente, y se podrá acceder a ella mediante un número de identificación personal, o, en la situación ideal, mediante un dispositivo de identificación biométrica, por ejemplo, con ella y puede ser accesible para cualquiera (e incluso puede serlo, a través, de directorios públicos de fácil acceso).

Si bien las dos claves están matemáticamente relacionadas entre sí, el diseño y ejecución en forma segura de criptosistema asimétrico hace virtualmente imposible que las personas que conocen la clave pública puedan derivar de ella la clave privada, pues la posibilidad de hacerlo depende de la longitud de la clave y de la evolución de la técnica.[227]

En este misma línea Miguel Ángel Velásquez Saenz fácilmente ejemplifica cómo funciona la criptografía asimétrica: [228]

> *(…) el destinatario me envía previamente un candado, abierto. Es "su" candado, yo no puedo abrirlo si se cierra, pues la llave solamente la tiene él. La llave permanecerá segura en su poder. Recibo el candado, escribo mi mensaje, lo meto en la caja y cierro la caja con el candado que recibí. A partir de ese momento, ni yo mismo, que escribí el mensaje, puedo ya verlo. Está protegido por el candado. Envío la caja y el destinatario la abre con su llave. Así funciona la llave pública y privada. La llave pública es el candado y su pareja es la llave de metal (llave privada) que lo abre. Por supuesto, esta pareja debe ser fabricada una para la otra.*

A continuación se explica el cifrádo asimétrico de acuerdo con la imagen inmediata posterior: Alice (**Ana** en la figuara) desea enviar un mensaje a **Bob**, y que el mismo permanezca confidencial, para ello utiliza la clave pública de **Bob** para encriptar el mensaje y poder transmitirlo por un canal inseguro, Eve captura el mensaje pero **no** puede descifrarlo, ya que el único que posee la clave capaz de desencriptar el mensaje es Bob, que tiene la clave privada asociada a la clave pública utilizada por **Ana** para cifrar el mensaje.

Con motivo del tiempo de cómputo, es no es posible conocer una clave a partir de la otra.
Para explicarlo, Alice (Ana en la imagen) y Bob cuentan sus pares de claves respectivas:

---

[226] Algunos ejemplos de protocolos que usan CCE son EC Digital Signature Algorithm (ECDSA) e Intercambio de llaves EC Diffie-Hellman (ECDH).

[227] Martínez Nadal, Apol·lònia : Comercio electrónico, firma digital y autoridades de certificación, 2001, 3ª ed., Madrid, Civitas, p. 45 y 46

[228]Velasquez Saenz, Miguel angel. Criptografía Moderna, 2013, Colombia, blog accesible en http://criptografiamoderna.blogspot.mx, consultado el 2 de enero de 2015.

1) Cuando el remitente usa la clave pública del destinatario para cifrar el mensaje, una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje, ya que es el único que la conoce. Por tanto se logra la confidencialidad del envío del mensaje, nadie salvo el destinatario puede descifrarlo.
2) Cuando el propietario del par de claves usa su clave privada para cifrar el mensaje, cualquiera puede descifrarlo utilizando su clave pública. En este caso se consigue por tanto la identificación y autentificación del remitente, ya que se sabe que sólo pudo haber sido él quien empleó su clave privada (salvo que alguien se la hubiese podido robar). Esta idea es el fundamento de la firma electrónica.

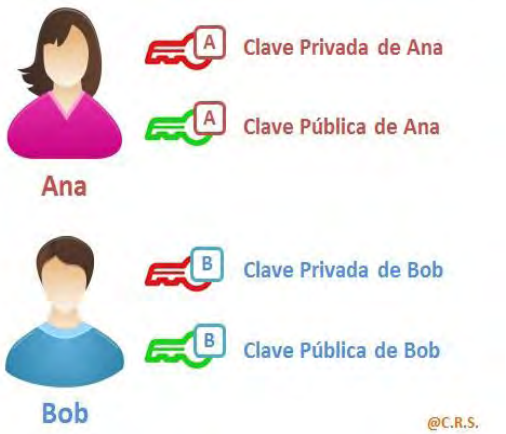


Figura de Claves Públicas y Privadas de Ana y Bob[229]

El procedimiento de cifrado de clave pública se representa en la siguiente imagen y texto:

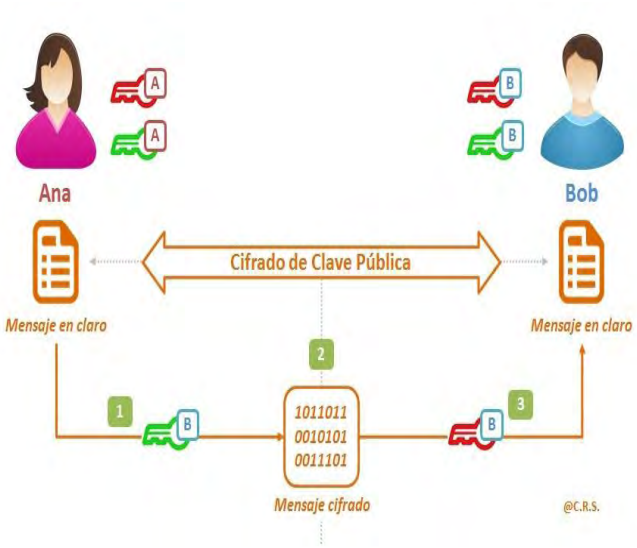


Figura del procedimietno de cifrado de clave pública[230]

1) Ana escribe un mensaje a Bob y dese que él únicamente pueda leerlo; por ello, lo cifra con la clave pública de Bob, accesible a todos los usuarios.
2) Se produce el envío del mensaje cifrado no siendo necesario el envío de la clave.
3) Sólo Bob puede descifrar el mensaje enviado por Ana ya que sólo él conoce la clave privada correspondiente.
4) El mecanismo elimina la necesidad del envío de la clave, siendo por lo tanto un sistema más seguro pero con el inconveniente de la lentitud del proceso; razón por la cual , el procedimiento generalmente, se acostumbre realizar el cifrado del MD empleando un algoritmo de clave pública junto a uno de clave simétrica.

En los algoritmos de clave asimétrica se utilizan claves de cifrado y descifrado diferentes, y tienen la característica de que no puede calcularse o derivarse una clave de la otra, y que

[229] La imagen es de Secur-IT @C.R.S., Cripotrafía, accesible en: https://securitcrs.wordpress.com/criptografia/criptografia-asimetrica-clave-privada-y-clave-publica/, consultado el 12 de enero de 2015.
[230] La imagen es de Secur-IT @C.R.S., Cripotrafía, accesible en: https://securitcrs.wordpress.com/criptografia/criptografia-asimetrica-clave-privada-y-clave-publica/, consultado el 12 de enero de 2015.

conforman un par fuertemente vinculado.

Esta característica, hace posible que la clave de cifrado se difunda, es decir se haga pública, de allí que estos algoritmos también se conozcan como de clave pública y se elimina la necesidad de intercambiar claves secretas, que como hemos visto, era necesario cuando se utilizan mecanismos de clave simétrica.

Entonces, cuando alguien desea enviar un mensaje en forma *confidencial,* lo cifra con la clave pública del destinatario teniendo la seguridad que sólo este último será capaz de descifrarlo ya que solo él conoce la clave privada asociada con la clave pública que se utilizó para cifrar el mensaje. [231]

Los MD cifrados asimétricamente únicamente pudieron ser creados por quien posee la clave privada asociada a la clave pública, por ende se habla de un atributo de este sistema: la *autenticación,* ya que cualquiera que posea la clave pública podrá verificar la identidad del emisor. Por otro lada y en razón de que únicamente el emisor del MD tiene la clave privada, no puede negar haber emitido el mensaje, de tal manera que se habla del atributo de *no repudio*.

Entonces para lograr los atributos de *confidencialidad, autenticidad y no repudio,* el emisor debe cifrar el mensaje con su clave privada y con la clave pública del destinatario. De esta forma, se sabe que sólo el verdadero destinatario puede leerlo, y éste sabe que sólo el emisor pudo haberlo generado.

Los tipos de criptografía asimétrica más comúnmente usados son:

- RSA
- ElGamal
- DSA (Digital Signature Algorithms)

En suma, a partir de las criptografías simétrica y asimétrica se pueden establecer las siguientes diferencias.

DIFERENCIAS ENTRE CRIPTOGRAFÍA SIMÉTRICA Y ASIMÉTRICA		
Atributo	**Clave simétrica**	**Clave asimétrica**
Años en uso	Rápida	Menos de 50
Velocidad	Rápida	Lenta
Uso principal	Cifrado de grandes volúmenes de datos	Intercambio de claves Firma digital o FEA
Claves	Compartidas entre emisor y receptor	Privada: solo conocida por una persona Pública: conocida por todos.

[231] Rocha Vargas, Marcelo Emilio, Castello, Ricardo J. y Bollo, Daniel E., Criptografía y Firma Electrónica/Digital en el Aula, Universidad Nacional de Catamarca – Secretaría de Ciencia y Tecnología, Ed. Científica Universitaria, p.8, accesible en: http://www.editorial.unca.edu.ar/Publicacione%20on%20line/CD%20INTERACTIVOS/DUTI/PDF/EJE2/ROCHA%20VARGAS.pdf , consultado el 12 de enero de 2015.

Intercambio de claves	Difícil de intercambiar por un canal inseguro	• La clave pública se comparte por cualquier cana. • La clave privada nunca se comparte.
Longitud de claves *(De acuerdo al año 2012)*	56 bist (vulnerable) 256 bits (seguro)	1024 bits mínimo
Algoritmos *(De acuerdo al año 2012)*	DES, 3DES, Blowfish, IDEA, AES	Diffie-Hellman, RSA, DSA, ElGamal
Servicios de seguridad	• Confidencialidad • Integridad • Autenticación	• Confidencialidad • Integridad • Autenticación • No repudio.

3.3.3. Criptografía Híbrida.

Frente a ambos tipos de criptografías quede claro que un usuario de tales cifrados se enfrenta a la necesidad de optimizar tiempos así como recursos, y para ello, se requiere, por un lado, el empleo de la criptografía asimétrica para que el remitente envíe la clave al destinatario, y por otro, remita el mensaje cifrado simétricamente para ser posteriormente descifrable con la clave enviada asimétricamente.

Si tomamos en consideración que el problema de ambos sistemas criptográficos es que el simétrico es inseguro y el asimétrico es lento, se entiende el por qué del surgimeitno de la *Criptografía Híbrida* como la unión de las ventajas de las dos anteriores.

La forma de enviar un MD en la criptografía híbrida se detalla a continuación:[232]

a) Se genera una clave pública y otra privada por parte del destinatario.
b) Se cifra un archivo de forma síncrona.
c) El destinatario envía al emisor su clave pública.
d) Se cifra la clave usada para encriptar el archivo con la clave pública del destinatario.
e) Se envía el archivo cifrado síncronamente y la clave del archivo cifrada asíncronamente que solo puede ver el destinatario.

[232] Rodeiro, Ángel. "Tipos de criptografía: simétrica, asimétrica e hibrida", en Seguridad y Alta Disponibilidad: Novedades a nivel seguridad informática, accesible en: http://www.genbetadev.com/seguridad-informatica/tipos-de-criptografia-simetrica-asimetrica-e-hibrida, consultado el 3 de enero de 2015.

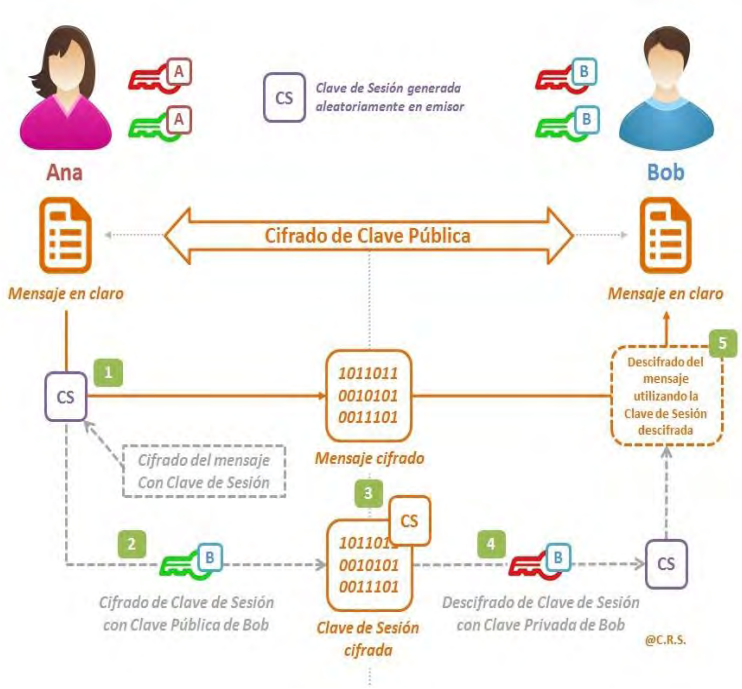


Figura del procedimiento de la Criptografía Híbrida[233]

1. Ana escribe un mensaje a Bob. Lo cifra con el sistema de criptografía de clave simétrica. La clave que utiliza se llama Clave de Sesión y se genera aleatoriamente.
2. Para enviar la Clave de Sesión de forma segura, esta se cifra con la clave pública de Bob, utilizando por lo tanto criptografía de clave asimétrica.
3. Envío de la Clave de Sesión y del mensaje, ambos cifrados, a Bob.
4. Bob recibe el mensaje cifrado con la clave de sesión y esta misma cifrada con su clave pública. Para realizar el proceso inverso (descifrado), en primer lugar Bob utiliza su clave privada para descifrar la Clave de Sesión.
5. Una vez ha obtenida la Clave de Sesión, utiliza esta para poder descifrar el mensaje. Con este sistema conseguimos:

a) Confidencialidad: sólo podrá leer el mensaje el destinatario del mismo.
b) Integridad: el mensaje no podrá ser modificado.

En suma, a través del uso de este sistema, se obtiene la certeza de la confidencialidad; sin embargo, aún sigue pendiente el problema de autenticación y de no repudio, que es resulto por el mecanismo de la FEA o firma digital.

3.3.4. Firma Electrónica Avanzada y la función hash.

Se ha dicho ya en varias ocasiones que una desventaja de la criptografía de clave asimétrica es la merma en la velocidad cuando se realiza el cifrado a comparación con lo criptografía de clave simétrica porque crecen con el tamaño del mensaje a cifrar y tienen un costo muy elevado[234]; por ello, se pensó que la FEA de un MD debe realizarse utilizando una función de control o hash; lo anterior implica que la FEA de un MD no se hacía mediante el cifrado del mismo usando la clave privada del emisor, sino mediante el cifrado del resumen del texto generado a través de un algoritmo de resumen de texto o empleado una "función hash".

La recomendación UIT-T.X.810[235], define el hash y la función unidireccional como:

> ***Hash:*** *característica de un ítem de datos, por ejemplo un valor de comprobación criptográfico o*

[233] La imagen es de Secur-IT @C.R.S., Cripotrafía, accesible en: https://securitcrs.wordpress.com/criptografia/criptografia-asimetrica-clave-privada-y-clave-publica/, consultado el 12 de enero de 2015.
[234] Fernández Gómez, Eva. Comercio electrónico. Madrid: McGraw-Hill/Interamericana de España, S.A.U, 2006, p.116; y Rico Carrillo, M. Comercio electrónico. Internet y Derecho, 2. ª ed. Venezuela: LEGIS, 2005, p.203.
[235] Recomendación de la Unión Internacional de Telecomunicaciones UIT-T.X.810 (1995 s), pág. 3.

el resultado de la ejecución de una función de cálculo unidireccional sobre los datos, que es suficientemente peculiar del ítem de datos y que no es factible, mediante cálculo, hallar otro ítem de datos que posea las mismas características;
***Función unidireccional**: función matemática cuyo cálculo es fácil, pero que, cuando se conoce un resultado no es factible, mediante cálculo, hallar cualquiera de los valores que pueden haber sido suministrados para obtenerlo .*

En síntesis, el algoritmo hash es una función matemática que se aplica sobre un conjunto de datos o documentos de cualquier tamaño y, como resultado, se obtiene otro de tamaño reducido a 246, en ocasiones denominado *resumen o digest* de los datos originales, de longitud fija (entre 128 o 160 bits) e independiente de la longitud del MD original.

El resumen o *hash* del MD se caracteriza por su irreversibilidad (esto es, a partir del resumen no puede obtenerse el mensaje completo inicial), y por ser único del mensaje (es decir, es computacionalmente imposible obtener un segundo mensaje que produzca el mismo resumen o *hash*), de forma que cualquier cambio en el mensaje produciría un hash diferente. Posteriormente, el hash de menor extensión es cifrado con la clave privada de criptografía asimétrica del firmante (que proporciona integridad, autenticidad y no repudio), para que por último, ambos mensajes, el MD original, completo y en claro, y la firma digital (el hash o resumen cifrado), sean remitidos conjuntamente al destinatario.[236]

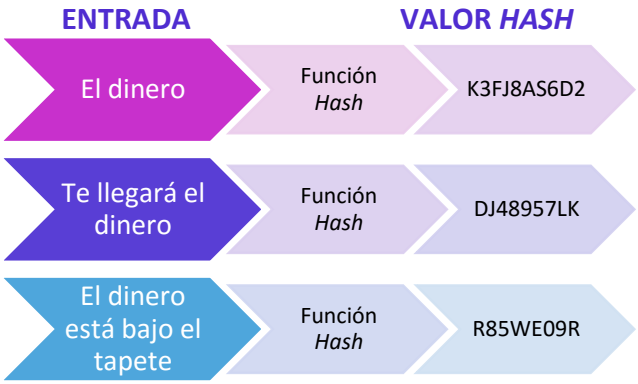


Figura: Funcionamiento del Hash[237]

Aunado a lo anterior, si se requiere confidencialidad, la criptografía asimétrica puede proporcionar también seguridad, cifrando el mensaje conjunto de la clave pública del destinatario, el cual podrá descifrarlo (solo él puede hacerlo) aplicando su propia clave privada. Sin embargo, aunque ello es posible, es también costoso. Por ello, para efectos de confidencialidad se recurre a la criptografía simétrica por ser menos costosa (aunque la criptografía asimétirca sigue siendo necesario para el intercambio de la clave secreta compartida).

[236] Martínez Nadal, Apol·lònia : Comercio electrónico, firma digital y autoridades de certificación, 2001, 3ª ed., Madrid, Civitas, P. 51-52.
[237] La ilustración es nuestra.

Es importante detallar que el objetivo del hash es simplificar la firma digital del mensaje cuando éste es muy largo, donde al hacer uso de la función *hash* el mensaje no se encripta sino que comprime los textos para que el destinatario pueda comprobar la integridad del MD con mayor rapidez. Al aplicar la firma digital se encripta sólo la función hash y no todo el documento, lo que permite que a la hora de descifrar el mensaje el proceso dure menos tiempo[238].

Matemáticamente hablando, una función de hash H(M) también llamada función resumen, es una funciónque opera sobre un mensaje M de longitud arbitraria, y produce una salida hde longitud fija[239].

$$h = H(M)$$

Una buena función de hash, en general reúne una serie de propiedades, a modo de ejemplo citaremos algunas:

- Las funciones de hash, son irreversibles*,* es decir que dado un hash no existe forma de poder recuperar algo del texto claro original, es decir la función de hash no es reversible.
- Dado un mensaje M, es muy difícil encontrar otro mensaje M', tal que H(M) = H(M')
- No es factible encontrar o descubrir texto claro, que verifique un valor de hash específico. Es decir dado h, es difícil encontrar un M tal que H(M) = h
- Un cambio en un bit del texto claro, debería traducirse en un cambio de al menos el 50% en el hash resultante.

Hemos dicho que el firmante genera, mediante una función matemática, una "huella digital" del mensaje, la cual se cifra con la clave privada del firmante. El resultado es lo que se denomina firma digital, quese enviará adjunta al mensaje original. De esta manera el firmante adjuntará al documento unamarca que es única para dicho documento y que sólo él es capaz de producir.

Para realizar la verificación del mensaje, en primer término el receptor generará la huella digitaldel mensaje recibido, luego descifrará la firma digital del mensaje utilizando la clave pública delfirmante y obtendrá de esa forma la huella digital del mensaje original; si ambas huellasdigitales coinciden, significa que no hubo alteración y que el firmante es quien dice serlo.

[238] En la jerga de los conocedores de sistemas de seguridad informática los algoritmos hash son RSA con digestión SHA-2-256, los tamaños de claves son de al menos 2048 bits para usuarios y de 4096 bits para las ACR y ACI.

[239] Rocha Vargas, Marcelo Emilio, Castello, Ricardo J. y Bollo, Daniel E., Criptografía y Firma Electrónica/Digital en el Aula, Universidad Nacional de Catamarca – Secretaría de Ciencia y Tecnología
Ed. Científica Universitaria, p.10 y 11, accesible en: http://www.editorial.unca.edu.ar/Publicacione%20on%20line/CD%20INTERACTIVOS/DUTI/PDF/EJE2/ROCHA%20VARGAS.pdf , consultado el 12 de enero de 2015.

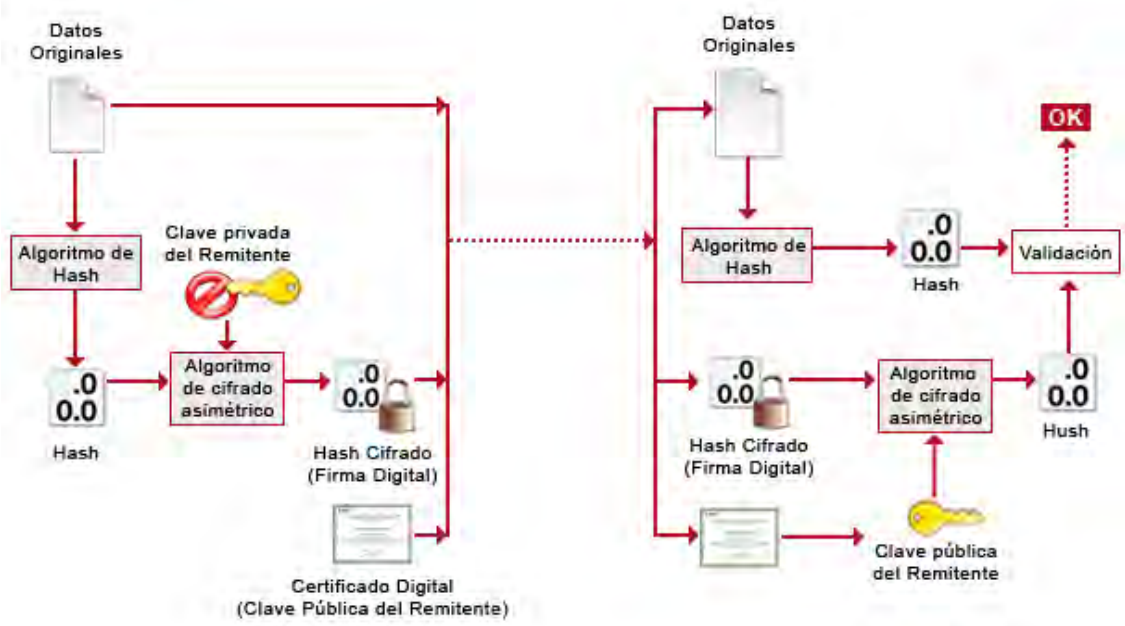


Figura: Funcionamiento del Algoritmo Hash[240]

La función *hash* permite garantizar la integridad de un MD, por lo que al combinar la función hash y el mecanismo de cifrado asimétrico, se crea el entorno para poder firmar digitalmente un MD. Las funciones hash más comúnes son:

- MD5
- *Secure Hash Algorithm 2* (SHA-2) que ya a superado al SHA1.
- MD4

3.3.5. Generación y verificación de la Firma Electrónica Avanzada.

El legado de la criptografía asimétrica es que proporciona un método para la creación de FEA´s, pues tales firmas hacen posible que el destinatario de un mensaje verifique la autenticidad del origen del MD y corroborar verificar que el MD no hubiese sido modificado posteriormente a su creación. De este modo, la FEA ofrece el soporte técnico para la autenticación e integridad de los MD así como el no repudio de origen, ya que el emisor de un MD firmado digitalmente no podrá impugnar que él no es el emisor.

[240] Imagen recabada de: https://www.incibe.es/extfrontinteco/img/dnie/contenido_esquema1.jpg, accesible el 2 de febrero de 2015.

La respuesta ante la lentitud e incremento del tamaño del MD obtenido después de un cifrado asimétrico, es el empleo de la *función o algoritmo hash*. Al ejecutar dicha *función* sobre un MD se consigue como producto una serie de datos menor al MD original, de tamaño fijo e independiente de aquél y con el atributo de estar asociado unívocamente al MD original, ya que no es posible que existan dos mensajes que tengan el mismo resumen hash.

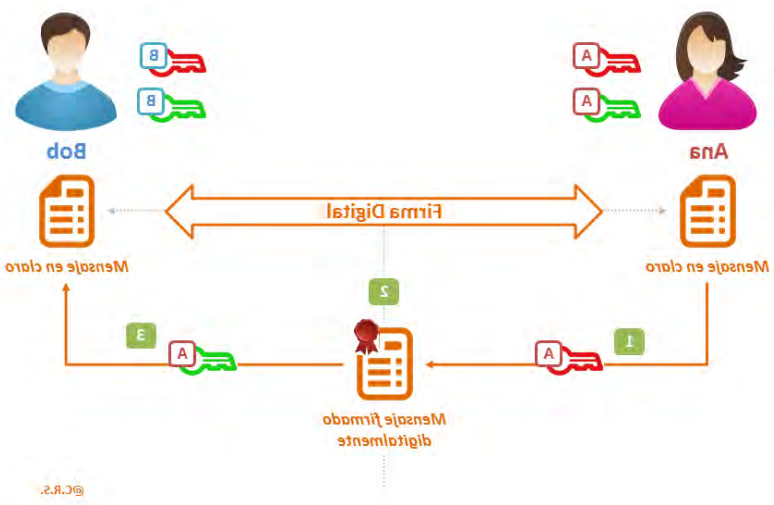


Figura del Procedimiento de la FEA[241]

Es indudable la seguridad que se genera cuando un MD es descifrado empleando la clave pública pues únicamente pudo cifrarse por la clave privada; por ende, la FEA es un cifrado del MD que se está firmando pero utilizando la clave privada en lugar de la pública.

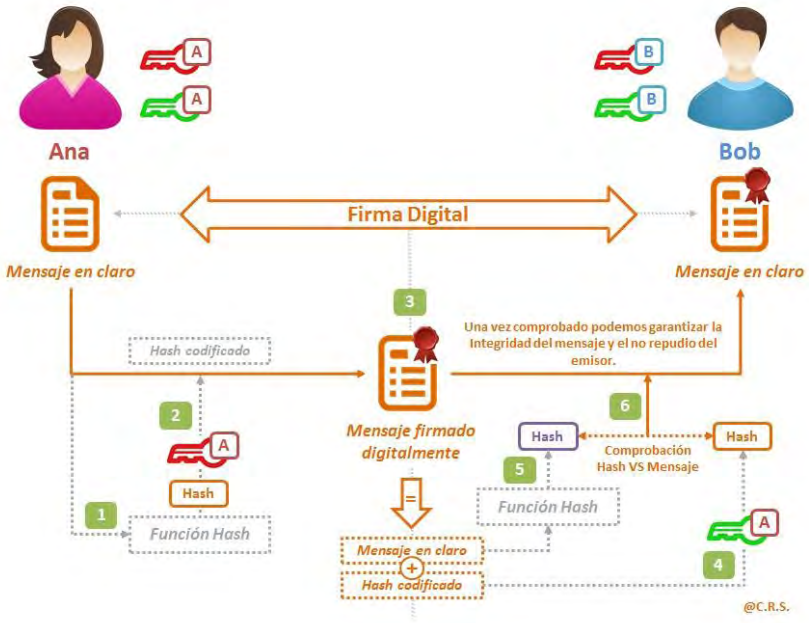


Figura del procedimiento de creación y verificación de la FEA a través del *hash*[242]

[241] La imagen es de Secur-IT @C.R.S., Cripotrafía, accesible en: https://securitcrs.wordpress.com/criptografia/criptografia-asimetrica-clave-privada-y-clave-publica/, consultado el 12 de enero de 2015.

[242] La imagen es de Secur-IT @C.R.S., Cripotrafía, accesible en: https://securitcrs.wordpress.com/criptografia/criptografia-asimetrica-clave-privada-y-clave-publica/, consultado el 12 de enero de 2015.

En términos breves, si Alice desea enviar información segura a Bob, Alice realiza un cálculo matemático en su documento, conocido como una función *hash,* que crea una cadena única de código llamado un "resumen o compendio del mensaje" (o *message digest*). Debido a que el compendio del mensaje se basa en el contenido específico de un documento original de Alice, cualquier cambio en el documento otorgaría un resumen de mensaje diferente. Alice luego encripta este resumen del mensaje usando su clave privada, adjunta esta firma digital al final del documento, y envía el documento a Bob.

Cuando Bon recibe el mensaje de Alice, puede ejecutar de forma independiente la misma función hash en el mensaje original para determinar cuál debe ser el contenido del compendio del mensaje original. A continuación descifra la firma digital de Alice, utilizando la clave pública de Clare. Si Bob que el compendio del mensaje en la firma digital descifrada de Clare coincide con el resumen del mensaje que calculó Bob a partir de su mensaje, entonces Bob conoce que la información no ha sido alterada y que el mensaje sólo pudo ser enviado a través de clave privada de Alice. Si, por otro lado, los resúmenes no coinciden, entonces no hay autenticidad del MD[243].

Cómo se advierte del ejemplo anterior, en este procedimiento de uso de la firma digital concurren dos procesos progresivos que consisten en: la generación de la firma del mensaje por el emisor del mismo; y la verificación de la firma digital por el receptor del mensaje.

En cuanto al primero, esto es, la generación de la FEA se inicia con la obtención de un mensaje en claro escrito por el emisor en el que éste aplica a ese mensaje una función hash o resumen, mediante la cual obtiene un resumen del mensaje. Al finalizar esa aplicación, el emisor cifra digitalmente ese mensaje comprimido utilizando su clave privada, es decir, lo firma.

A continuación, el emisor envía el hash firmado junto con el mensaje en claro al receptor quien deberá proceder a la verificación de la firma. Este último recibe el mensaje con los siguientes elementos:

a) El mensaje inicial (también denominado *Mensaje en Claro*)
b) La firma del mensaje, que a su vez se compone de dos elementos: el hash cifrado y la clave privada del emisor.

En cuanto al segundo, esto es, la verificación de la FEA. Se tiene que atender a la forma en cómo se puede verificar la FEA. Son varias las alternativas, primero se debe tener la clave pública del emisor, para que después el destinatario utilice la clave pública del emisor para descifrar el *hash* firmado con la clave privada del mismo y así obtiene el hash. Acto seguido, el receptor aplicar al MD, que aparece en claro o no cifrado, la misma función hash que utilizó el emisor con anterioridad obteniendo igualmente un mensaje-resumen. Si el MD ha sido cifrado para garantizar la confidencialidad del mismo, previamente el receptor deberá descifrarlo utilizando

[243] C. Bradford Biddle, Misplaced Priorities: The Utah Digital Signature Act and Liability Allocation in a Public Key Infrastructure, 33 SAN DIEGO L. REV. 1143, 1149 (1996).

para ello su propia clave privada[244]

De este modo, el receptor compara el hash recibido y descifrado y el hash obtenido por él mismo. Si ambos coinciden totalmente evidencia que el mensaje no ha sufrido modificación durante su transmisión[245], es decir, es íntegro o auténtico. El hash descifrado por el receptor con la clave pública del emisor ha sido necesariamente cifrado con la clave privada del emisor y, por tanto, proviene del emisor.

En el caso de que los hash no concuerden significa que el mensaje ha sido modificado por un tercero durante el proceso de transmisión y si el hash descifrado por el destinatario es ininteligible quiere decir que no ha sido cifrado con la clave privada del emisor. Por lo que el mensaje no es auténtico o no ha sido firmado por el emisor sino por alguien extraño a ello.

En este contexto fue como el legislador mexicano se convenció de los beneficios de la criptografía asimétrica para la implemetación de la FEA, la cual ya había sido reconocida internacionalmente como la única que concede un alto nivel de certeza en cuanto a identificación, privacidad, atribución, seguridad e integridad de los MD firmados; que no es más que la garant{ía de confidencialidad, la autenticidad, la integridad y el no repudio de la transmisión de los MD en las comunicaciones electrónicas.

3.4. Autoridades de Certificación y Prestadores de Servicios de Certificación de la FEA

Ahora bien, todo cifrado asimétrico como mecanismo de cración de una FEA requiere de la existencia de un PSC como un tercero, jurídica y económicamente diferenciado del emisor y destinatario del MD, que proporcione un software a través de una plataforma para generar un par de claves[246]. En materia federal, la Ley de FEA reconoce directamente a esta tecnología como altamente segura, disponible y en el mercado.

Una apropiada marcha del sistema requiere que el mismo garantice la autenticación de las partes. Si no hay autenticación no se podría garantizar o confirmar la identificación del ente emisor del MD o documento electrónico, para lograr el elemento de autenticación se hace uso de un tercero de confianza, que no es más que el PSC que asegura o avala que un sujeto es el correcto titular de la clave pública. Dicho prestador de servicios llevara un registro de todos los titulares de las claves que el haya registrado.

El empleo de los certificados se fundan en el esquema de Infraestructura de Clave Pública (ICP)[247], el cual fue adoptado por México. La infraestructura integra la figura del PSC, quien

[244] Baker y Hurst. The limits of trust: Cryptography, Governments and Electronic Commerce, 1998, The Hague, Kluwer Law International, pp. 2-5.
[245] Martínez Nadal, Apol·lònia: Comercio electrónico, firma digital y autoridades de certificación, 2001, 3ª ed., Madrid, Civitas, p. 48-49.
[246] Illescas Ortíz, Rafael: Derecho de la contratación electrónica, 2009, 2ª ed., Madrid, Civitas Thomson Reuters, p.86 y 87.
[247] La Infraestructura de Clave Pública es un conjunto de políticas, procesos, servidores, software y centros de servicios utilizados con el propósito de administrar certificados y pares de claves públicas y privadas. Véase National Institute of

resuelve el problema de atribución que surge de la falta de vinculación intrínseca de las claves pública y privada con las personas físicas o morales; es decir, sin el PSC las claves son simplemente un par de números.

Dicha cuestión fácilmente se solucionó mediante la participación de este tercero o PSC que también es conocido con los nombres de Autoridad de Certificación (AC), Entidad Certificadora, Prestador o Proveedor de Servicios de Certificación. Independiente del nombre, se insiste en que dicho tercero tendrá la función de verificar la vinculación entre una persona y un par de claves por medio de la expedición de certificados que permitan a la parte que confía verificar que *alguien* resulta confiable.

Ahora, un esquema de la ICP consiste en:

a) El papel del creador de la clave (y firmante);
b) La función de quien "confía" en la validez de una firma, y
c) El rol de certificación.

La función de creación de la FEA y la de confianza son comunes a todos los modelos de ICP. En los modelos más populares de ICP, las tres funciones las desempeñan personas distintas (el ejemplo es la ICP desarrollada por la Secretaría de Economía); sin embargo, un segundo supuesto puede consistir en que dos de esas funciones las desempeñe la misma persona, cuando la persona que emite los certificados puede ser también la persona que confía en dichos certificados (el ejemplo es el modelo de ICP que sigue la Secretaría de Hacienda y Crédito Público).

Entonces, mientras que la función del PSC es similar en todas las ICP en las que se presenta, la naturaleza jurídica y el marco jurídico creado a su alrededor para que las partes puedan confiar en él, puede variar de ICP a ICP. Ello quedó evidenciado con el hecho de que cuando existe un ambiente donde las partes se conocen y están vinculadas por contratos, el PSC no necesariamente debe ser algún tercero ajeno al grupo de personas que firma y que confían en la firma electrónica.

Por el contrario, en un ambiente donde las partes no se conocen o no están vinculadas por contratos o normatividad común (como podría ser una transacción entre una Universidad y una autoridad gubernamental) ambas partes deberán contar un tercero que pueda garantizar que el MD que una de las partes recibe está vinculado al firmante. En estos casos, el PSC se fundamente en una ley que garantiza su probidad y su capacidad tecnológica.

La ICP fue adoptada por México por considerar que concede la mayor certidumbre de la transmisión electrónica, por la participación imprescindible de un tercero de confianza. Así, a nivel federal, Ley de Firma Electrónica Avanzada (LFEA) del 11 de enero de 2012, define tanto

Standards and Technology, 2001. U.S. Government Publication. Disponible en: http://csrc.nist.gov/publications/ nistpubs/800-32/sp800-32.pdf, consulta 3 septiembre de 2014.

las figuras de PSC como el de AC.

> **Prestador de Servicios de Certificación:** *las instituciones públicas conforme a las leyes que les son aplicables, así como los notarios y corredores públicos y las personas morales de carácter privado que de acuerdo a lo establecido en el Código de Comercio sean reconocidas con tal carácter para prestar servicios relacionados con la firma electrónica avanzada y, en su caso, expedir certificados digitales;*
> **Autoridad Certificadora:** *las dependencias y entidades de la Administración Pública Federal y los* ***prestadores de servicios de certificación*** *que conforme a las disposiciones jurídicas, tengan reconocida esta calidad y cuenten con la infraestructura tecnológica para la emisión, administración y registro de certificados digitales, así como para proporcionar servicios relacionados con los mismos;*
>
> ***(Énfasis añadido)***

Cabe señalar que una característica de las ICP es que se basan en distintos niveles jerárquicos de autoridad, en la Ley Modelo de Firmas Electrónicas se distinguen[248]:

a) Entidad principal: única que certificará la tecnología y las prácticas a todas las partes autorizadas a emitir certificados o pares de claves criptográficas en relación con el empleo de dichos pares de claves y lleva un registro de las entidades de certificación subordinadas (o autoridad raíz).
b) Diversas entidades de certificación: situadas bajo la autoridad principal que certifican que la clave pública de un usuario corresponde a la clave privada del mismo.
c) Diversas entidades locales de registro: que reciben de los usuarios peticiones de pares claves criptográficas o de certificados relativos al empleo de esos pares de claves y que exijan pruebas de identidad a los posibles usuarios y las verifiquen.

Alfredo A. Reyes Krafft enuncia las funciones de la Agencia Registradora, Agencia Certificadora y del Agente Certificado, en la materia financiera, listado que ilustra no solo las responsabilidades en esta área sino en general para cualquier materia: [249]

Agencia Registradora	Agencia Certificadora	Agente Certificador
• Contar con reglas y procedimientos de operación • Mantener registro de certificados digitales (público) • Permitir consultas en línea al registro • Difundir disposiciones de Banxico (sitio web).	• Reglas y procedimientos sobre prácticas de certificación (de identidad) adoptadas. • Emitir y, en su caso, revocar certificados digitales (requisitos Banxico). • Proporcionar un certificado digital y los medios para la creación y verificación de	• Identificar a titulares solicitantes (comparecencia personal) con idetificación oficial fiable. • Obtener declaración con firma autógrafa del titular (atribución, responsabilidad y conformidad con límites de responsabilidad de AC) • Conservación de

[248] La Ley Modelo de Firmas Electrónicas no recomendó una estructura nacional particular de ICP; sino que reconoció que la organización de una ICP podía comprender diversas cuestiones técnicas y de orden público elegidas por cada Estado.
[249] El cuadro es una reproducción íntegra del eleaborado por Alfredo Reyes Krafft, Op. Cit., p. 207.

• Reportes a Banxico de actividades. • Responder por negligencia en proceso de registro o revocación. • Respaldo electrónico de su base de datos.	firma electrónica. • Registrar ante AR los certificados digitales que emita. • Conservar solicitudes por 10 años. • Difundir disposiciones de Banxico (sitio web) • Reportes a Banxico de actividades • Responder por negligencia en proceso de emisión o revocación de certificados. • Informar a titulares de revocación de certificados, en su caso.	documentación física por cuando menos 10 años. • Responder por daños y perjuicios en caso de negligencia en el proceso de identificación del titular. • Contar con respaldo de información y documentación.

En México se eligió este esquema de ICP, esto es, la estructura y cuadro de funcionamiento de las AC de ICP, que considera una estructura en dos niveles jerárquicos: el nivel uno, que suele ser ocupado por una autoridad pública, y el nivel dos, que es la autoridad subordinada, generalmente privada, subordinada a aquel, pero que de manera progresiva puede irse desglosando en más entidades.

Por otra parte y siguiendo con el ejemplo de María y Luis, cuando se hace del conocimiento la clave pública de un usuario para efectos de negociación, es necesario que la otra parte este segura de que ciertamente se trata de la clave pública de la parte que indica ser la titular. En este sentido pueden suscitarse el siguiente caso:

Que Ana se haga pasar por María ante Luis, y le envíe la clave pública de Ana para negociar. Pero también, puede darse el caso que Ana robe la clave privada de María y firme un contrato electrónico de manera auténtica con Luis, pero siendo un poseedor ilegítimo.

Además de las AC o PSC como figuras más completas para resolver la cuestión de la distribución de claves públicas de manera fiable, existen otras vías para hacerlo[250]:

a) Registro de claves públicas, este sistema facilita el acceso a las claves públicas por parte de terceros, pero no resuelve la situación de la distribución fiable de las mismas, pues no existe garantía de la identidad del titular.

b) *Web of trust,* es un programa que utiliza *Pretty good privacy (PGP)* o Privacidad bastante buena que se basa en un sistema de encriptación, elaborado por Phil Zimmermann[251], cuyo

[250] Martínez Nadal, Apol·lònia: Comercio electrónico, firma digital y autoridades de certificación, 2001, 3ª ed., Madrid, Civitas, pp. 66-68.

[251] Accesible en http://www.pgpi.org/., consulta del 3 de diciembre de 2014.

objeto es proteger la información distribuida a través de Internet mediante el uso de criptografía de clave pública, privada y la gestión de claves así como facilitar la autenticación de documentos electrónicos o MD. El programa está disponible de manera gratuita por el autor a fin de que el receptor del MD una vez que reciba la clave pública del emisor junto con el mensaje, pueda transformarlo y descifrarlo; el receptor valorará si la clave pública empleada está vinculada con el individuo identificado como emisor; para ello, el receptor corroborará con otro individuo de confianza, que sería una tercera parte que puede afirmar o negar conocer la clave pública del emisor. Se considera que el beneficio de este sistema es la independencia de una autoridad central.

3.5. Certificados Digitales y Certificados de Seguridad

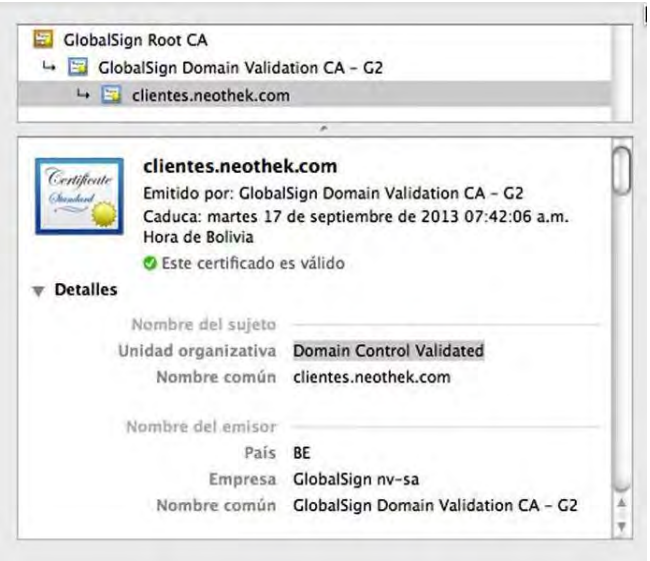
Un certificado digital es un documento electrónico que prueba que una clave pública específica corresponde a una persona física o moral en particular, el cual está signado electrónicamente por la agencia que certificó la identidad del individuo.

Normalmente, los elementos de los certificados digitales son:

a) La versión: Identifica el formato del certificado
b) El número de serie: Identifica este certificado
c) El Id de Algoritmo de firma: Algoritmo usado para firmar el certificado
d) El nombre del emisor: Nombre de la autoridad certificadora
e) El período de validez: Fecha de inicio y fecha final
f) El asunto: materia o tema del documento electrónico.
g) La llave pública: Identifica el dueño del certificado
h) La firma del Emisor: Valor de llave pública y algoritmo

Ahora bien, por lo que hace a los certificados digitales de la FEA, la LFEA de 2012, los define como el MD o registro que confirme el vínculo entre un firmante y la clave privada.

Todo certificado debe ser firmado digitalmente por la autoridad de certificación o PSC, donde la firma de la autoridad y su certificado puede a su vez cotejarse utilizando la clave pública de este frente a otra autoridad certificadora, que puede tener un rango superior o una subordinación en el esquema de AC. Una vez firmado por este, lo debe hacer público en un directorio o medio accesible a otros medios de comunicación. Al terminar la etapa de validez del certificado o habiéndose dado la revocación o suspensión del mismo, evidentemente ya no debería de confiarse en él.



Ejemplo de los requisitos de información de un certificado digital

La SE, publicó en el DOF el 19 de julio de 2004 el Reglamento del CCo en Materia de Prestadores de Servicios de Certificación (RCCPSC) en el que se establecen los requisitos para que los prestadores citados expidan los certificados de FEA.

Ahora bien, del artículo 100 al 113 el CCo incluyó un capítulo III denominado *De los Prestadores de Servicios de Certificación* el cual será analizado en los puntos 4.4. y 4.5. del capítulo IV de este trabajo. Por ahora, basta aducir que en material mercantil, el numeral 100 del CCo establece que podrán ser PSC, previa acreditación ante la SE:

> *I. Los notarios públicos y corredores públicos;*
> *II. Las personas morales de carácter privado, y*
> *III. Las instituciones públicas, conforme a las leyes que les son aplicables.*
> *La facultad de expedir Certificados no conlleva fe pública por sí misma, así los notarios y corredores públicos podrán llevar a cabo certificaciones que impliquen o no la fe pública, en documentos en papel, archivos electrónicos, o en cualquier otro medio o sustancia en el que pueda incluirse información.*

En cuanto al *"tipo de certificado"* el mercado ofrece tres tipos:

a) Certificado de Servidor (que asegura la existencia y denominación de una entidad en Internet);
b) Certificado de Representación (que asegura la existencia y denominación del representante signatario del certificado); y
c) Certificado Personal (que asegura la existencia y denominación del signatario del certificado).

Los tres tipos de certificado deben ser tomados en cuenta para vincularlo con el "*el tipo de*

acreditación", pues si se requiere acreditación *sin fe pública* de la identidad y/o personalidad del solicitante cambiará significativamente a si se desea obtener con *fe pública* de Notario o Corredor Público quien le cobrará a la AR por separado los servicios del Fedatario Público. Recordemos que ambos fedatarios son requeridos como una formalidad cuando se trata de instrumentos públicos en los términos de los artículos 1237 y 1391 fracción II del CCo.

1. Tipo de certificado.

a) **Certificado de Servidor**: El certificado tendrá como única finalidad asegurar la existencia y denominación de una entidad en Internet. Estos certificados serán utilizados a través de aplicaciones en servidores con protocolo SSL (Secure Sockets Layer). **PSC World** emite certificados SSL que soportan encriptación de hasta 128 bits utilizando tecnología Microsoft Server-Gated Cryptography (Codificación Controlada por el Servidor, ***SGC*** por sus siglas en inglés).

b) **Certificado de Representación**: El certificado tendrá como única finalidad asegurar la existencia y denominación del signatario del certificado. Estos certificados serán emitidos a personas físicas con actividad empresarial o personas morales para garantizar frente a terceros su identidad, autenticidad e integridad de sus mensajes, así como que el representante legal de una empresa manifieste que su representada se encuentra capacitada legalmente para la celebración del acto y acreditar que la personalidad que ostenta y las facultades con que cuenta no le han sido limitadas, modificadas o revocadas. **PSC World** emite este tipo de certificado con una longitud en su llave de 1024 bits.

c) **Certificado Personal**: El certificado tendrá como única finalidad asegurar la existencia y denominación del signatario del certificado. Estos certificados serán emitidos a personas físicas para garantizar frente a terceros su identidad, autenticidad e integridad de sus mensajes. **PSC World** emite este tipo de certificado con una longitud en su llave de 1024 bits.

2. Tipo de acreditación

a) **Sin Fe Pública** de acreditación de la identidad y/o personalidad del Solicitante: Son acreditados ante un Agente Certificador de PSC World

LISTA DE PRECIOS DE CERTIFICADOS SIN FE PÚBLICA		
Tipo de Certificado	Valor en Diciembre de 2013[252]	Valor en Diciembre de 2015[253]
Certificado de Representación-1024 bits	$2,000 M.N.	$4,990 M.N.
Certificado Personal-1024 bits	$1,000 M.N.	$4,990 M.N.

b) **Con Fe Pública** de acreditación de la identidad y/o personalidad del Solicitante: Son acreditados por un Fedatario Público (Notario o Corredor Público), autorizado como Agente Certificador de PSC World.

Los certificados emitidos por PSC World con Fe Pública de acreditación de la identidad y/o personalidad del Solicitante, se registran con Ratificación de Firma, por lo tanto son

[252] Los precios son de acuerdo a la fecha en que fueron recolectados, 3 de noviembre de 2014 en la página web de la empresa.
[253] http://www.pscworld.com/precios.html

instrumentos públicos en los términos de los artículos 1237 y 1391 fracción II del CCo.

El costo es determinado por el valor de la ***Lista de Precios de los Certificados Sin Fe Pública*** más los servicios del Fedatario Público[254].

LISTA DE PRECIOS DE CERTIFICADOS CON FE PÚBLICA						
	Valor en Diciembre de 2013[255]			Valor en Diciembre de 2015[256]		
TIPO DE CERTIFICADO	Valor sin Fe Pública	Servicios Fedatario	Importe Total	Valor Sin Fe Pública	Servicios Fedatario	Importe Total
Certificado de Representación-1024 bits	$2,000 M.N.	$2,500 M.N.	$4,500 M.N.	$4,990 M.N.	$6,250 M.N.	$11,240 M.N.
Certificado Personal-1024 bits	$1,000 M.N.	$1,700 M.N.	$2,700 M.N.	$4,990 M.N.	$6,250 M.N.	$11,240 M.N.

Asimismo, con respecto a las *"condiciones comerciales"* se toma en cuenta el precio de manera anual con beneficios consistentes en un descuento en el precio de renovación así como también si el solicitante requiere la acreditación de la identidad y/o de la personalidad, caso en el que deberá realizarse en el lugar designado por él, motivo por el cual dicho servicio tendrá un costo adicional y se sumará al costo final.

Certificados de Seguridad.
Si una empresa desea vender en línea, esto es, comercializar en línea bienes o servicios y recibes pagos de forma directa o a través de terceros, debe adquirir un certificado digital de seguridad para proteger la información que le proporcionan sus clientes potenciales. El certificado permite encriptar la información y proteger la transmisión de datos entre el usuario y el servidor web además permite conocer la identidad de ambos, es decir, un certificado digital es un archivo electrónico que identifica de modo único a individuos y servidores web.

Lo anterior significa que además de los certificados digitales de la FEA se comercializan otros certificados de seguridad, los cuales se diferencian en que estos certifican a los servicios web, esto es, aseguran la existencia y seguridad de una página web y de correos electrónicos.

a) **Certificado de Sitio Web**: El certificado tendrá como única finalidad asegurar la existencia y denominación de una entidad en Internet. Estos certificados serán utilizados a través de aplicaciones en servidores con protocolo SSL (Secure Sockets Layer). Normalmente, una AC emite certificados SSL que pueden ofrecer soporte desde encriptación de hasta 128 bits utilizando tecnología Server-Gated Cryptography (SGC) o Codificación Controlada por el

[254] Si el solicitante requiere que la acreditación de la identidad y/o personalidad se realice en un lugar por él designado, dicho servicio tendrá un costo adicional y podrá ser rechazada la petición por el Agente Certificador.
[255] Información de la empresa PSC World, visible en http://www.pscworld.com/precios.html Los precios son de acuerdo a la fecha en que fueron recolectados, 3 de noviembre de 2014.
[256] Información de la empresa PSC World, visible en http://www.pscworld.com/precios.html Los precios son de acuerdo a la fecha en que fueron recolectados, 31 de enero de 2016.

Servidor.

b) **Certificado de Correo Confiable**: El certificado tendrá como única finalidad asegurar la existencia y denominación de la cuenta de correo electrónico. Estos certificados serán emitidos a personas físicas para garantizar ante terceros su identidad, autenticidad e integridad de los mensajes mediante aplicaciones de correo electrónico seguro S/MIME, así como para cifrar y firmar mensajes de correo electrónico. Generalmente una AC emite este tipo de certificado con una longitud en su llave de 1024 bits.

El certificado de seguridad debe instalarse en los siguientes casos[257]:

- Los sitios donde el usuario pueda comprar y pagar en línea deberán contar con una medida de seguridad *Secure Socket Layer* (SSL)[258] para encriptar datos personales y financieros en la página donde soliciten esta información.
- Las compañías que reciban pagos de un tercero deberán contar con un SSL que encripte el envío de datos personales y financieros desde la página donde los soliciten.
- Los sitios que reciben el pago a través de un depósito o transferencia bancaria y envíen el bien a la dirección del comprador deberán contar con un SSL para encriptar sólo el envío de datos personales.

No es necesario contar con un SSL cuando el usuario proporcione datos personales sólo para recibir información o para ser contactado por el proveedor, toda vez que no hay una operación comercial.

Los certificados que comúnmente se utilizan para encriptar la información son de 128 y 256 bits, aunque los hay de mayor nivel de encriptación.

Al administrador se le solicita un *Certificate Signing Request* (CSR) o petición de firma que se genera en el servidor, donde está montada la página web. El CSR es toda la información de la empresa junto con el dominio para emitir el certificado.

- Para la entrega confidencial del certificado de la autoridad certificadora, el cliente deberá generar una cuenta con un password que lo identifique como tal.
- Al final de este proceso se le envía al cliente el certificado junto con el manual para la instalación en el servidor. Si es necesario recibe asesoría vía telefónica.

[257] Carlos Enrique García Soto. Certificados de seguridad, en Boletín electrónico Brújula de compra de Profeco (www.profeco.gob.mx), 02 de marzo 2009, consultado el 21 de diciembre de 2015.

[258] SSL en español significa capa de conexión segura. Es un protocolo criptográfico empleado para realizar conexiones seguras entre un cliente (como lo es un navegador de Internet) y un servidor (como lo son las computadoras que despachan páginas web). Este protocolo ha sido sucedido por TLS, que son las siglas en inglés de Transport Layer Security (en español seguridad de la capa de transporte). Versiones de TLS tienen un equivalente en SSL, por ejemplo TLS 1.2 corresponde a SSL 3.3; de ahí que aún sea común que se refiera al protocolo TLS como SSL y que en un contexto informal se utilicen estos términos de forma intercambiable.
Por supuesto, las versiones de estos protocolos de seguridad han evolucionado respondiendo a vulnerabilidades que hackers han ido encontrando.

Si el proveedor de un bien o servicio muestra el certificado de seguridad en un lugar visible de su sitio, da confianza al consumidor toda vez que éste puede revisar que lo emitió una empresa especializada. Así, tiene la tranquilidad de que sus datos personales y financieros no están en riesgo al comprar en línea.

En 2009, la PROFECO recabó los siguientes precios, los cuales dependen de los años de vigencia solicitados:

Proveedor	Certificado	Certificado de 1 año precio con IVA ($)	Certificado de 2 años precio con IVA ($)
Advantage Security Systems	Thawte SSL123	2,448.59	4,256.28
	VeriSign Secure site Pro con EV	24,633.82	44,288.28
Digital Server	GeoTrust QuickSSL	2,512.75	5,025.50
	GeoTrust QuickSSL Premium	3,293.03	6,586.05
PSC World	Geotrust	2,958.03	4,765.72
Raxa Host México	RapidSSL	1,091.35	No disponible en el sitio
	VeriSign Secure site	6,313.50	No disponible en el sitio
Smart Advanced Solutions	GeoTrust QuickSSL	4,091.94	6,162.56
	GeoTrust QuickSSL Premium	4,913.62	7,805.91
Spice	Thawte SSL123	2,448.59	4,256.28
	Thawte SSL	4,091.94	7,378.64
SuEspacio.Net	RapidSSL Wildcard	2,530.00	No disponible en el sitio
	Positivessl Wildcard	2,564.50	No disponible en el sitio

3.6. Certificación de la autoridad de certificación.

A través de este análisis se ha advertido que siempre puede existir incertidumbre en conocer de manera indubitable la clave pública de la autoridad de certificación, y dado que no existe una única autoridad de certificación para todos, debe admitirse que habrá muchas AC en el mundo y que no todos los usuarios tendrán la correcta clave pública en sus manos. Entonces, para producir un certificado de confianza, la autoridad de certificación debe contar con un certificado válido y garantizado de sí mismo. Lo anterior arroja la siguiente interrogante: ¿quién certifica a la autoridad de certificación? la respuesta es que dicha certificación la obtendrá a través de otra autoridad de certificación, pero hay dos posibles formas de llegar a ella.

a) Por certificación de una autoridad de certificación
b) Por la Autocertificación.

En cuanto a la primera, la *certificación de una autoridad de certificación,* la certeza de que un usuario tiene la clave pública de la autoridad de certificación se obtiene al buscar si esta se encuentra certificada por otra autoridad, la cual puede estar en un nivel subordinado o superordinada a la misma. Ello propicia que aparezca un modelo de cadena de certificados (*certification path o certificate chain*), en el que están basados todos los sistemas de distribución de claves públicas a través de certificados al por mayor que crean certificados en forma de árbol.

Regresando al ejemplo de la autoridad de certificación llamada la "Luna", supongamos que esta recurre a certificarse ante otra llamada el "Sol", pero nótese que el problema de certificación se traslada de una a otra autoridad, porque ahora quien fue la autoridad que certificó al " Sol".

Respecto a la segunda, la *autocertificación* es una forma que han *de facto* impulsado algunas AC que por iniciativa propia colocan su clave pública de autoridad certificadora en el sitio web de la empresa, pero enfrenta el problema de que cualquiera que sepa modificar un sitio web o controlar el tránsito de datos en la red puede cambiar la clave pública y con ello alterar la validez de los certificados expedidos por esa autoridad. Aquí, la confianza y credibilidad se obtiene de la experiencia y reputación de la empresa de certificación así como de sus prácticas de certificación. Dicha situación ya había sido planteada por *American Bar Association*[259] al establecer que aquellos que buscaran un bajo nivel de responsabilidad para proteger transacciones de menor costo o riesgo podría elegir un certificado de bajo grado de seguridad de una autoridad de certificación y, en caso contrario, buscar una reconocida en el medio.

La generalidad de los países que cuentan con una ley de firma digital que otorga un alto valor probatorio a la FEA o fiable, aceptan que la jerarquía de las AC debe darse por lo menos en tres niveles jerárquicos, donde el primer nivel lo ocupa la autoridad certificadora raíz.

El caso de Alemania es particularmente interesante porque en las disposiciones de la *Ley de Firma Digital*[260]*,* se permite conceder licencias y emitir certificados de clave pública para los certificadores y mantiene el acceso a todos los certificados de clave pública emitidos junto con sus teléfonos y direcciones de certificados, suspensiones y revocaciones, a través de telecomunicaciones accesibles.

La presencia de una autoridad certificadora internacional sería ideal, pero a su falta, se considera que el reconocimiento de certificados extranjeros a través de certificaciones cruzadas sería lo mejor, para ello, las autoridades certificadoras sustancialmente equivalentes reconocen el servicio proporcionado por otras, con el objeto de que el tenedor respectivo de la clave pueda usar su firma digital en el comercio internacional.

Finalmente, las AC utilizan un determinado tipo de tecnología, lo que genera diversidad en la forma técnica en que operan los certificados, no son interoperables, quizás este problema se puede resolver fácilmente en países que forman parte de la Unión Europea en el que la tecnología sí es interoperable pero lamentablemente México no es el caso, dado que el problema de interoperabilidad es abordado someramente en las *Reglas generales a las que deberán sujetarse los prestadores de servicios de certificación*, expedida el 10 de agosto de 2004, conforme a nuestra Ley de FEA. Su análisis será abordado en el capítulo V de este trabajo.

[259] ABA, Digital Signature Guidelines, Washington, American Bar Association, 1996.
[260] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG) del 16.05.2001, accesible en http://www.gesetze-im-internet.de/bundesrecht/sigg_2001/gesamt.pdf, o indirectamente en http://www.ictparliament.org/legislationlibrary/Digital%20Signatures.html, consulta 22 de noviembre de 2014.

3.7. Necesidad de determinación del tiempo en el sistema de certificados.

Un certificado no prueba el instante de creación o envió del MD, y dada la importancia del factor temporal, es necesario conocer la fecha en que se firmó digitalmente porque a partir de ahí se verificará si la signatura fue hecha dentro del periodo de vigencia o expiración del certificado.

Pueden suscitarse casos en que el certificado de una autoridad de certificación llamada "El sol" haya expedido un certificado a otra autoridad de certificación llamada "La Luna" por una vigencia de 2003 a 2008, y "La Luna" expide a un usuario otro certificado con vigencia 2007 a 2011, lo cual no provocará de inicio su revocación anticipada, porque lo importante es que la firma del certificado del usuario se realizase durante la vigencia del certificado relativo a "La Luna".

Caso distinto se suscita cuando se da la revocación de un certificado por el robo o extravío de la clave privada del titular, pues evidentemente resulta necesario la terminación por adelantado. Mientras la revocación hace que el certificado deje de ser operativo.

La vigencia de los certificados en materia comercial es de 2 años, mientras que en materia fiscal ha sido modificada con el tiempo, pues su vigencia se determinaba de acuerdo a la fecha de expedición del certificado.

El SAT cambió la periodicidad de los certificados con fundamento en el Decreto del 1° de julio de 2010 y la reforma al CFF del 12 de diciembre de 2011 y el resultado fue la siguiente periodicidad:

- 24 meses para certificados emitidos antes del 1 de abril de 2010 para personas físicas (PF) y personas morales (PM).
- 27 meses para certificados emitidos a partir del 1 de abril de 2010 (PF y PM).
- 48 Meses para certificados emitidos a partir del 1 de julio de 2010 (PF y PM).
- 27 meses para certificados emitidos a partir del 12 de octubre de 2010 (PM).
- 48 Meses para certificados emitidos a partir del 1 de enero de 2012 (PM).
- El certificado de la FIEL para personas físicas y morales tienen una vigencia de 4 años.

3.8. Sello temporal digital

Para garantizar que las firmas fueron creadas en un momento en que las claves y el certificado eran válidos o bien que el MD ha sido enviado en un momento específico, se requiere introducir un signo o rastro temporal a través de sellos temporales digitales (en inglés *digital seal o digital time stamp*) que garanticen que será imposible sellar un documento con otra fecha y hora. Esto contribuye a que si una datación o momento puede ser importante para el valor probatorio de unos MD firmados, se fijará un sello temporal infalsificable[261].

[261] Véase Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP), Network Working Group, Request for Comments: 3161, 2001.

El material que debe ser sellado digitalmente son los MD relevantes, los certificados, las listas de certificados revocados, cada versión de las declaraciones de prácticas de certificación y todo contenido que se considera en dichas declaraciones.

Un *digital seal* crea una marca que señala la hora y fecha tomando en consideración el meridiano de *Greenwich* (GMT) y *Universal Time Conventions* (UTC).


Time Stamp Certificate

DigiStamp

Printed by: Rick Borgers

Certified File

File name: Drawings.gif

Comment: describe phase 1 of the invention

Fingerprint: 4c26adfd26fdd1662564440e38da71ee5b620f6d

Date and Time

August 11, 2001 4:11:09 PM GMT

DigiStamp's digital signature of Fingerprint, Data and Time

Ejemplo Sello temporal digita (e-TimeStamps)l[262]

Los servicios de sellado temporal pueden ser suministrados por una autoridad de certificación pero también se puede considerar la opción de que lo haga una entidad de confianza distinta, pues lo realmente importante en el valor probatorio de un sello temporal es que éste haya sido formado por un sistema seguro y confiable. Dentro de estos sistemas seguros de suministro de sellos digitales existen varios:

a) Sistema de envío y sellado por un tercero de confianza.
b) Sistema de envío de un hash del mensaje que anexa hora/fecha y luego es sellado por un tercero de confianza.
c) Sistema de vinculación de documentos para impedir alteraciones de sello temporal.

a) El *sistema de envío y sellado por un tercero de confianza* es un sello temporal que se fija por un tercero, pero es tan elemental que genera los siguientes inconvenientes: el MD puede ser interceptado por alguien antes de cumplir el fin de ser estampado; y, el MD o documento electrónico que se remite puede ser tan pesado que puede tardar mucho tiempo y hacer que el proveedor de estampado tenga que invertir recursos para grandes almacenamientos.
b) El *sistema de envío de un hash del mensaje que anexa hora y fecha y luego es sellado por un tercero de confianza* requiere que se remita al proveedor el hash del mensaje en vez del MD completo, y sobre ese fija el sellado. El inconveniente es que el proveedor de servicio de sellado digital puede en contubernio con el autor del mensaje sellado, cambiarle la fecha real del sellado temporal.
c) El *sistema de vinculación de documentos para impedir adulteraciones de sello temporal* es un procedimiento avanzado y difícil[263] que hace imposible que el proveedor de sellado lo

[262] DigiStamp, Inc. (empresa en Dallas, TX, USA, disponible en su página web: https://www.digistamp.com/technical/how-a-digital-time-stamp-works/example-of-a-certificate/, fecha de consulta 1 de enero de 2015.
[263] Procedimiento propuesto en: BAYER, Dave HABER Stuart, STORNETTA, W. Scott. Improving the Efficiency and Reliability of Digital Time-Stamping, en CAPOCELLI, Renato, DE SANTIS, Alfredo y VACCARO, Ugo, Sequences II: Methods in Communication, Security, and Computer Science, 1993, Springer, New York, pp. 329-334

haga de forma inadecuada porque el sello va ligado a una secuencia de bits del mensaje anterior sellado por la misma autoridad y a una secuencia de bits del mensaje posterior.

3.9. Declaración de Prácticas de Certificación y Políticas de Certificación.

Toda Agencia Certificadora tiene la obligación de difundir sus Declaraciones de Prácticas de Certificación (DPC), que consisten en una descripción detallada de las normas o prácticas que la empresa declara convenir en la prestación de sus servicios de certificación cuando emite y gestiona certificados digitales en su rol de Agencia Certificadora; además se incluyen las normas a seguir por la Agencia Registradora (AR) y los Agentes de Certificación acreditadas por la empresa.

Lo anterior es así porque cuando la empresa emite un certificado digital, también establece cierto nivel de seguridad a todos los agentes que depositarán su confianza en la validez de dicho certificado, como instrumento que da garantías sobre la identidad del titular del mismo. En ese sentido, establece que se han tomado las medidas y procedimientos adecuados para constituir la correspondencia entre dicho certificado y una cierta entidad en particular. Asimismo, dichas declaraciones son un mecanismo para evaluar la calidad y grado de confianza que se puede depositar en un certificado digital, y esto solo se puede saber a través de la revisión de las prácticas usadas por la Agencia Certificadora para emitir dicho certificado.

Respecto a este tema, se torna relevante conocer de qué versión de trata para determinar el tiempo en que le fueron aplicables al certificado, pues puede darse el caso de existencia de distintas versiones de las declaraciones de prácticas de certificación de una misma autoridad, estas declaraciones determinan el tipo de norma aplicable que utilizó esta autoridad de certificación.

Una Declaración de Prácticas de Certificación (DCP) es la descripción detallada de normas (prácticas) que las Autoridades Certificadoras (AC) convienen en la prestación del servicio de certificación al emitir y gestionar certificados digitales en su rol de Autoridad. Las AC de un organismo son la autoridad encargada de administrar y procesar el sistema y plataforma de otorgamiento de certificados, generalmente lo son las Direcciones Generales encargadas de administrar un servicio en el que se requiere una FEA, también suelen ser AC las Direcciones Generales de TIC's.

Dichas declaraciones son aplicables también a la Agencia Registradora (AR) y los Agentes de Certificación (AgC), llamados igualmente terceros de confianza, acreditados por las propias organizaciones. Un ejemplo de Declaración de las Prácticas de Certificación de la SE se muestra en el Apéndice III-A: Declaración de Prácticas de Certificación de la AC-DGNM[264] y AC-SIGER[265].

[264] Autoridad Certificadora de la Dirección General de Normatividad Mercantil (DGNM) de la Secretaría de Economía.
[265] Autoridad Certificadora de Sistema Integral de Gestión Registral de la Secretaría de Economía.

Entre las reglas utilizadas por la AC para interpretar los nombres distintivos (DN) de los titulares o suscriptores de Certificados de FEA cumplen con los estándares internacionales ISO/IEC 9594-8 y el RFC 3280. Así, se eligen diversos tipos de estándares, que son seleccionados tomando en consideración el organismo que lo propone y el ámbito de competencia que tiene, por ejemplo la mayoría de las empresas prestadoras de servicios de certificación consideran los estándares de *International Telecommunication Union* o Unión Internacional de Telecomunicaciones (ITU/UIT), específicamente la Recomendación denominada *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marcos para certificados de claves públicas y atributos*[266] que es fácilmente localizable bajo el nombre de *Recomendación UIT-T X.509 | Norma Internacional ISO/CEI 9594-8.*

A través de tal recomendación se define un marco para certificados de clave pública y para certificados de atributo. El marco de certificado de clave pública es la especificación básica para los certificados de clave pública, para los diferentes componentes que constituyen una infraestructura de clave pública (PKI) para los procedimientos de validación y para la revocación de certificados de clave pública, etc. El marco de certificado de atributo es la especificación básica para los certificados de atributo y los diferentes componentes que constituyen una infraestructura de gestión de privilegios (PMI). Estos marcos pueden ser utilizados por organismos de normalización para perfilar su aplicación a PKI y PMI.

Por otra parte, las Políticas de Certificación son un conjunto de reglas que indican la aplicabilidad de un certificado a una comunidad y clase de aplicaciones con requerimientos comunes de seguridad.

En el documento que las contiene, se describen las Políticas de Certificados para la Autoridad Certificadora Raíz de una organización. La Política de Certificados se aplica a la solicitud, validación, aceptación, emisión o revocación de los certificados digitales dentro de una Infraestructura de Clave Pública (PKI por sus siglas en inglés).

La organización, a través de algún área certificará las claves públicas de las Autoridades Certificadoras que hayan sido acreditadas previamente por dicha área. Un ejemplo de las Políticas de Certificación de la SE muestra en el Apéndice III-B.

[266] Recomendación de ITU-T, accesible en http://www.itu.int/itu-t/recommendations/rec.aspx?rec=11735&lang=es, consultado el 30 julio 2015.

CAPÍTULO IV. CONFIGURACIÓN E INCORPORACIÓN NACIONAL DE LAS SOLUCIONES TÉCNICO-JURÍCAS DEL COMERCIO ELECTRÓNICO A LOS SECTORES PRIVADO Y PÚBLICO.

4.1. Actual regulación constitucional de los medios electrónicos.

La regulación de los medios electrónicos en la CPEUM hasta antes de las reformas constitucionales de 20 de julio de 2007 y 11 de junio de 2013, según Ernesto Villanueva[267], carecía de precisión a nivel constitucional; mientras que Miguel Carbonell señalaba que está era bastante escueta[268]. De igual forma, todavía en 2006 se hablaba de la necesidad de constitucionalización del *derecho de acceso a las tecnologías de la información y comunicación*[269]

De ahí que la precisión constitucional deseada llegó a través de las reformas al artículo 6 constitucional de fechas 20 de julio de 2007 y 11 de junio de 2013, cuyo efecto fue no sólo reconocer el derecho al acceso a la información, sino que a la par, introducir a los medios electrónicos y la garantía de acceso a las Tecnologías de la Información y Comunicación (TIC) por parte del Estado así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e Internet.

Con esta inclusión, de los medios electrónicos le son extensivos los principios de los derechos humanos[270] establecidos en el párrafo segundo tercero del artículo 1º de la CPEUM: relativos a la libertad de expresión y acceso a la información (artículo 6 de la CPEUM); el universalidad, interdependencia, indivisibilidad, progresividad y un interpretación *pro persona*.

Pero ¿cuáles son estos derechos a los medios electrónicos? y ¿dónde quedan regulados? El derecho humano a la imprenta, sensu lato se encuentra en el artículo 7 de la CPEUM; el derecho de la propiedad y otorgamiento de concesiones así como el espacio aéreo para la trasmisión de medios electrónicos de comunicación por ondas radioeléctricas y por señales satelitales en el artículo 27 y 28 constitucionales; y, el derecho humano de legalidad y seguridad jurídica, cuyo texto reza que nadie puede ser molestado en sus papeles, sino en virtud de mandamiento escrito de la autoridad competente, que funde motive la causa legal del procedimiento, en el artículo 16 de la CPEUM, donde de acuerdo a los principios los Derechos Humanos, la

[267] VILLANUEVA, Ernesto. Régimen Jurídico de las Libertades de Expresión e Información en México, Instituto de Investigaciones Jurídicas-UNAM, México, 1998, p.59 y ss.

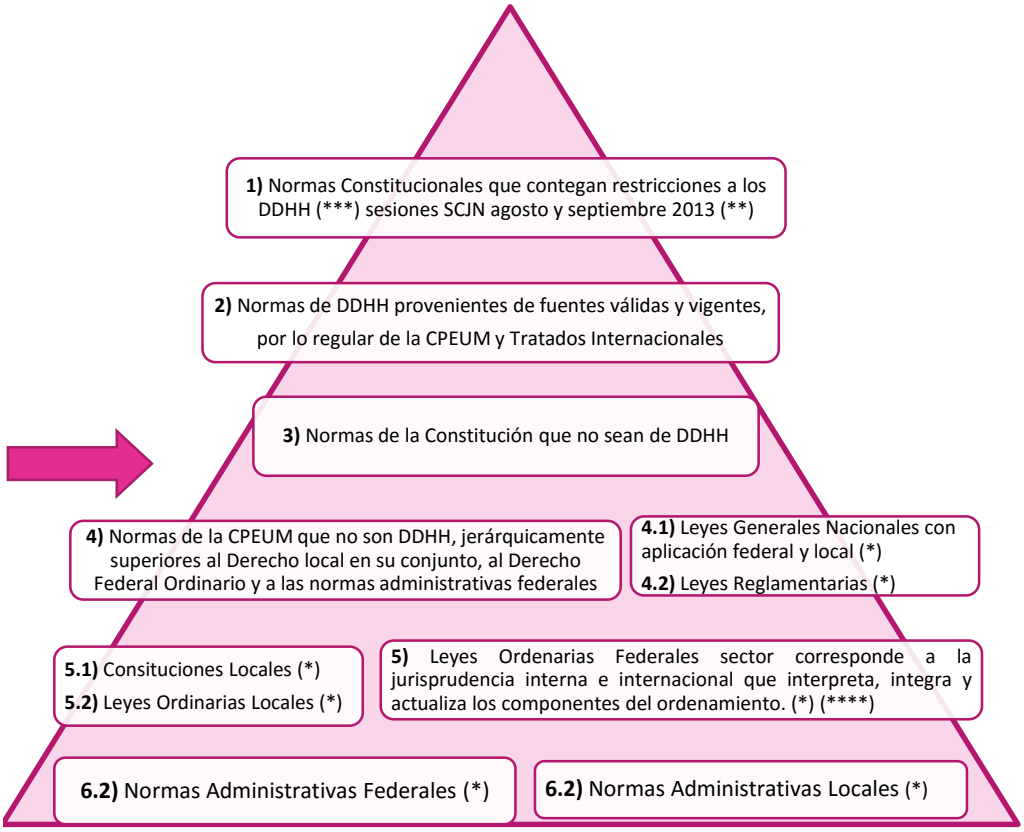
[268] CARBONELL, Miguel. "Notas sobre la Regulación Constitucional de los Medios Electrónicos de Comunicación", en Boletín Mexicano de Derecho Comparado, número 104, Mayo - Agosto 2002, Nueva Serie Año XXXV, conferencia impartida en la ciudad de Morelia, Michoacán, dentro del Seminario Nacional de Responsabilidad, Autorregulación y Legislación en Radio y Televisión, el 17 de julio de 2001; accesible en http://biblio.juridicas.unam.mx/revista/DerechoComparado/numero/104/abs/abs1.htm, fecha de consulta 1 mayo de 2015.

[269] Véase LÓPEZ-AYLLÓN, Sergio (coord.). Democracia, Transparencia y Constitución: Propuestas para un debate necesario, 1ª ed., 2006, México, Ed. UNAM-IFAI, p. 235.

[270] Antes de la reformas de fecha 6 y 10 de junio de 2011 eran garantías individuales.

hermenéutica de la palabra papeles abarca un espectro más amplio que los documentos impresos de una personas, incluye la información contenida a través de medios electrónicos[271].

Por otra parte, la jerarquía los Tratados Internacionales en materia comercial a partir de la reforma de Derechos Humanos 10 de junio de 2011 a sufrido modificaciones en una posición vertical, el cuadro a continuación lo explica.



(*) Si contienen normas de DDHH se sitúan en la Pre-cúspide
(**) Contradicción de tesis 293/2011 del 3 de septiembre de 2013: entre (A) 1er Tribunal Colegiado en Materias Administrativa y de Trabajo del XI Circuito y (B) el 7o Tribunal Colegiado en Materia Civil del I Circuito.
(A) Rubro: Derechos humanos contenidos en la CPEUM y en los tratados internacionales. Constituyen el parámetro de control de regularidad constitucional, pero cuando en la constitución haya una restricción expresa al ejercicio de aquéllos, se debe estar a lo que establece el texto constitucional.
(B) Rubro: Jurisprudencia emitida por la Corte Interamericana de Derechos Humanos. Es vinculante para los jueces mexicanos siempre que sea más favorable a la persona.
(***) Derechos Humanos (DDHH)
(****) Entre el Derecho Federal Ordinario y el Derecho Local no hay relación de jerarquía, sino de ámbito de competencia.

Jerarquía de Normas en el Orden Jurídico Mexicano a partir de la reforma en Derechos Humanos del 10/junio/2011[272]

Se hace presente la antigua discusión entre el Derecho Internacional y el Derecho Interno, en específico la relativa a la jerarquía los Tratados Internacionales en materia comercial se definió más a partir de la citada reforma en Derechos Humanos del 10 de junio de 2011**,** en razón de

[271] Cfr. BECERRA, Ricardo, "Internet llega a la Constitución (el derecho de acceso a la información y los sistemas electrónicos)", en Salazar Ugarte, Pedro (coord.), El derecho de acceso a la información en la Constitución mexicana: razones, significados y consecuencias, México, UNAM / IFAI, 2008, pp. 71-88.
[272] Adaptación del cuadro inédito denominado "Jerarquía de Normas en el Orden Jurídico Mexicano" del Jorge U. Carmona Tinoco.

que los Tratados Internacionales a que se refiere el artículo 89, fracción X, y 76, fracción I en relación con el artículo 133 de la CPEUM, deja claro que se ubican en la jerarquía establecida en el numeral ***4****) Normas de la CPEUM que no son DDHH, jerárquicamente superiores al Derecho local en su conjunto, al Derecho Federal Ordinario y a las normas administrativas federales;* ello en razón de que los Tratados Internacionales en materia comercial conservan su mismo estatus de conformidad con la tesis aislada, 9a. Época; Pleno; Semanario Judicial de la Federación y su Gaceta; Tomo XXV, abril de 2007; p. 6:

> ***TRATADOS INTERNACIONALES. SON PARTE INTEGRANTE DE LA LEY SUPREMA DE LA UNIÓN Y SE UBICAN JERÁRQUICAMENTE POR ENCIMA DE LAS LEYES GENERALES, FEDERALES Y LOCALES. INTERPRETACIÓN DEL ARTÍCULO 133 CONSTITUCIONAL.*** *La interpretación sistemática del artículo 133 de la Constitución Política de los Estados Unidos Mexicanos permite identificar la existencia de un orden jurídico superior, de carácter nacional, integrado por la Constitución Federal, los tratados internacionales y las leyes generales. Asimismo, a partir de dicha interpretación, armonizada con los principios de derecho internacional dispersos en el texto constitucional, así como con las normas y premisas fundamentales de esa rama del derecho, se concluye que los tratados internacionales se ubican jerárquicamente abajo de la Constitución Federal y por encima de las leyes generales, federales y locales, en la medida en que el Estado Mexicano al suscribirlos, de conformidad con lo dispuesto en la Convención de Viena Sobre el Derecho de los Tratados entre los Estados y Organizaciones Internacionales o entre Organizaciones Internacionales y, además, atendiendo al principio fundamental de derecho internacional consuetudinario "pacta sunt servanda", contrae libremente obligaciones frente a la comunidad internacional que no pueden ser desconocidas invocando normas de derecho interno y cuyo incumplimiento supone, por lo demás, una responsabilidad de carácter internacional.*

4.2. Incorporación de la Contratación Electrónica Segura en el Derecho Nacional: Reforma del 29 de mayo de 2000 a diversos ordenamientos legales.

4.2.1. Reforma del 29 de mayo de 2000 al Código de Comercio, Código Civil Federal y Código Federal de Procedimientos Civiles.

A través de las reformas al CCiF del 29 de mayo de 2000 se consideró a los medios electrónicos en las contracciones, se modificó el artículo 1º para corregir el Código Civil para el Distrito Federal en Materia Común y para toda la República en Materia Federal en el CCiF, que dio como resultado la tan criticada convivencia de un CCiF y un Código Civil para el Distrito Federal.

En este apartado nos referiremos al CCiF y a los artículos 1803, 1805, 1811 y 1834 bis, los cuales estipulan y conceden a los medios electrónicos la validez para expresar la voluntad:

> ***Artículo 1803.-*** *El consentimiento puede ser expreso o tácito, para ello se estará a lo siguiente:*
> *I.- Será expreso cuando la voluntad se manifiesta verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos, y*
> *II.- El tácito resultará de hechos o de actos que lo presupongan o que autoricen a presumirlo, excepto en los casos en que por ley o por convenio la voluntad deba manifestarse expresamente.*
>
> ***Artículo 1805.-*** *Cuando la oferta se haga a una persona presente, sin fijación de plazo para*

aceptarla, el autor de la oferta queda desligado si la aceptación no se hace inmediatamente. La misma regla se aplicará a la oferta hecha por teléfono o a través de cualquier otro medio electrónico, óptico o de cualquier otra tecnología que permita la expresión de la oferta y la aceptación de ésta en forma inmediata.

Artículo 1811.- *La propuesta y aceptación hechas por telégrafo producen efectos si los contratantes con anterioridad habían estipulado por escrito esta manera de contratar, y si los originales de los respectivos telegramas contienen las firmas de los contratantes y los signos convencionales establecidos entre ellos.*
Tratándose de la propuesta y aceptación hechas a través de medios electrónicos, ópticos o de cualquier otra tecnología no se requerirá de estipulación previa entre los contratantes para que produzca efectos.

Artículo 1834 Bis.- *Los supuestos previstos por el artículo anterior[273] se tendrán por cumplidos mediante la utilización de medios electrónicos, ópticos o de cualquier otra tecnología, siempre que la información generada o comunicada en forma íntegra, a través de dichos medios sea atribuible a las personas obligadas y accesible para su ulterior consulta.*
En los casos en que la ley establezca como requisito que un acto jurídico deba otorgarse en instrumento ante fedatario público, éste y las partes obligadas podrán generar, enviar, recibir, archivar o comunicar la información que contenga los términos exactos en que las partes han decidido obligarse, mediante la utilización de medios electrónicos, ópticos o de cualquier otra tecnología, en cuyo caso el fedatario público, deberá hacer constar en el propio instrumento los elementos a través de los cuales se atribuye dicha información a las partes y conservar bajo su resguardo una versión íntegra de la misma para su ulterior consulta, otorgando dicho instrumento de conformidad con la legislación aplicable que lo rige.

De las anteriores modificaciones y adiciones se advierte que:

a) El consentimiento puede ser expreso o tácito, siendo expreso cuando la voluntad se manifiesta por medios electrónicos.
b) Se consideran contratos entre presentes los celebrados a través de medios electrónicos, siempre y en cuando la aceptación se de forma inmediata, como en el caso del uso del teléfono.
c) Si no se está en el supuesto anterior, serán considerados contratos entre ausentes.
d) El segundo párrafo que se adicionó al artículo 1811 estipula la validez de los medios electrónicos dentro de cualquier acto jurídico, sin requerir que los contratantes lo declaren expresamente.
e) Se autoriza el uso de medios electrónicos cuando se requiera la forma escrita ante fedatario público, siempre que se pueda atribuir a la persona su obligación y que el documento pueda ser utilizado en posteriores ocasiones y el fedatario conserve una versión íntegra de la operación para consulta.

En cuanto a las modificaciones al CPCF del 29 de mayo de 2000, se añadió el artículo 210-A,

[273] "Artículo 1834.- Cuando se exija la forma escrita para el contrato, los documentos relativos deben ser firmados por todas las personas a las cuales se imponga esa obligación. Si alguna de ellas no puede o no sabe firmar, lo hará otra a su ruego y en el documento se imprimirá la huella digital del interesado que no firmó."

para otorgar validez probatoria a la información que conste en cualquier medio electrónico.

> ***Artículo 210-A.-*** *Se reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología.*
> *Para valorar la fuerza probatoria de la información a que se refiere el párrafo anterior, se estimará primordialmente la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas obligadas el contenido de la información relativa y ser accesible para su ulterior consulta.*
> *Cuando la ley requiera que un documento sea conservado y presentado en su forma original, ese requisito quedará satisfecho si se acredita que la información generada, comunicada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología, se ha mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y ésta pueda ser accesible para su ulterior consulta*.

De lo anterior se colige, que el requisito para la validez probatoria es una evaluación de la misma conforme con la fiabilidad del medio por el que haya sido generado y que se acredite que no ha sido modificada ni alterada y que pueda ser accesible para otras consultas[274].

Respecto a las reformas al CCo, la recepción del Derecho del Comercio Electrónico y la FEA de las Leyes Modelos contemplan las siguientes transformaciones progresivas no solo en el CCo, sino también en diversos reglamentos, reglas y normas oficiales mexicanas:

a) Reformas al CCo en materia de firma electrónica publicadas el 29 de agosto del 2003 en el D.O.F.
b) Reformas al CCo en materia de firma electrónica publicadas el 29 de mayo del 2000 en el D.O.F.
c) Reglamento del CCo en Materia de Prestadores de Servicios de Certificación (Publicado el 19 de julio del 2004 en el D.O.F.)
d) Reglas Generales a las que deberán sujetarse los PSC (Publicadas el 10 de agosto del 2004 en el D.O.F.)
e) Acuerdo que modifica las Reglas Generales a las que deberán sujetarse los prestadores de servicios de certificación (Publicado el 5 de marzo del 2007 en el D.O.F.)
f) NOM-151-SCFI-2002, Prácticas comerciales-Requisitos que deben observarse para la conservación de MD publicada el 4 de junio del 2002 en el D.O.F.

En este contexto, el título segundo denominado: “Del Comercio Electrónico” fue incluido en el CCo con la siguiente clasificación:

Título Segundo: Del Comercio Electrónico		
a)	Artículos 89 al 95	Capítulo I :De los Mensajes de Datos
b)	Artículos 96 al 99	Capítulo II: De las Firmas
c)	Artículos 100 al 113	Capítulo III: De los Prestadores de Servicios de Certificación

[274] Acosta Romero, Miguel y Lara Luna, Julieta Arelí. Nuevo derecho mercantil, 1. ed., 2000, México, Porrúa, p. 521.

d)	Artículo 114	Capítulo IV: Reconocimiento de Certificados y Firmas Electrónicas Extranjeras

El CCo gozó de más modificaciones que el resto de los dos códigos señalados (CFPC y CCiF). En él se reformaron los artículos relativos al RPCSE a fin de que las inscripciones se puedan elaborar de manera automatizada durante todo el procedimiento de creación de una empresa; se modifica el artículo 80 para agregar a los medios electrónicos ópticos o de cualquier otra tecnología, señalando que los contratos y convenios mercantiles se perfeccionarán a la hora de la aceptación de la propuesta, siguiendo la teoría de la expedición.

Asimismo, se adiciona un nuevo Título II denominado "Del Comercio Electrónico" que va de los artículos 89 al 94, cuyos datos de relevancia son: la inclusión del concepto de MD y la precisión del momento del envío y recepción de éste; la estimación de que el documento se reputa recibido cuando se haya entregado el acuse de recibo respectivo, esto es, cuando el emisor ha recibido el MD; la adopción de las reglas señaladas en el CCiF respecto a la forma escrita en los contratos mercantiles ante fedatario público; y la presunción de que un MD se ha expedido desde el domicilio del emisor y ha sido recibido en el domicilio del destinatario. Finalmente, la reforma puntualizó el valor probatorio de los MD en procesos mercantiles en el CCo en los artículos 1205 y 1298-A:

> ***Artículo 1205.-*** *Son admisibles como medios de prueba todos aquellos elementos que puedan producir convicción en el ánimo del juzgador acerca de los hechos controvertidos o dudosos y en consecuencia serán tomadas como pruebas las declaraciones de las partes, terceros, peritos, documentos públicos o privados, inspección judicial, fotografías, facsímiles, cintas cinematográficas, de videos, de sonido, mensajes de datos, reconstrucciones de hechos y en general cualquier otra similar u objeto que sirva para averiguar la verdad.*
> ***Artículo 1298-A.-*** *Se reconoce como prueba los mensajes de datos. Para valorar la fuerza probatoria de dichos mensajes, se estimará primordialmente la fiabilidad del método en que haya sido generada, archivada, comunicada o conservada.*

Las anteriores modificaciones y adiciones, son una consecuencia de la confianza con que se adoptó de la Ley Modelo de Comercio Electrónico en el CCiF, CFPC y CCo en el año 2000[275]; incluso, en la Exposición de Motivos de la Reforma multicitada, el legislador reconoció que a pesar de que en aquel tiempo muchas de las actividades gubernamentales y privadas ya se podían llevar a cabo por medios electrónicos (desde la constitución de una sociedad hasta el pago de impuestos), aún no existía un ordenamiento legal que regulara satisfactoriamente las transacciones electrónicas y que otorgara certeza jurídica a quienes las realizaban. Se esperaba, entonces, que las reformas referidas ayudaran a brindar certeza jurídica en materia de transacciones por medios electrónicos y que esta seguridad incidiera en forma positiva en la

[275] Adicionalmente la LFPC fue reformada también el 29 de mayo de 2000. Teniendo como finalidad incorporar las disposiciones mínimas que aseguren los derechos básicos del consumidor en las operaciones realizadas a través del uso de medios electrónicos, con base en los lineamientos emitidos por la OCDE (Exposición de Motivos del 22 de marzo de 2000). Se estableció la obligación, entre otras, del proveedor de: i) guardar confidencialidad respecto de la información proporcionada por el consumidor, y ii) utilizar elementos técnicos que brinden seguridad y confidencialidad a la información proporcionada por el consumidor e informarle a éste, previo a la transacción, las características generales de dichos elementos.

competitividad de la economía mexicana[276].

Esa confianza del legislador mexicano en las TIC así como en el reconocimiento del principio de equivalencia funcional, se hace patente en la Exposición de Motivos de la multicitada reforma al CCo.

> *No debería haber razón para negar validez jurídica a los contratos celebrados por medio de mensaje electrónicos ya que cumplen con la finalidad o razón de ser de los requisitos establecidos por la ley y los contratos tradicionales; incluso, superan en muchos aspectos a sus contrapartes en papel. Por eso mismo deberían tener validez probatoria.*

En suma, como resultado de tres reformas a los CCiF, CCo y CFPC, se incorporaron los siguientes cambios:

- **a)** Se contempló la validez y fuerza obligatoria a la propuesta y aceptación de un contrato cuando éstas se hicieran a través de medios electrónicos (artículo 1811 del CCiF).
- **b)** Se incorporó el principio de equivalencia funcional con respecto a firma y documento al establecerse que cuando en una transacción se exija la forma escrita y la firma, los requisitos se tendrán por cumplidos, con relación a un MD, siempre y cuando:
  i) fuera posible atribuirlos a la persona que contrae la obligación, y,
  ii) la información relativa sea accesible para su ulterior consulta (artículo 1834 bis del CCiF).
- **c)** Se reconoció como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o de cualquier otra tecnología (artículo 210-A del CFPC)[277].
- **d)** Se decretaron los criterios que un juez deberá valorar para determinar la fuerza probatoria de la información que conste en medios electrónicos. Para la valoración de la fuerza probatoria de un MD, el juez estimará: i) la fiabilidad del método utilizado para generar, comunicar, recibir o archivar la información, y ii) si es posible atribuir a las personas obligadas el contenido de la información relativa y si la información que conste en medios electrónicos es accesible para su ulterior consulta (artículo 210-A del CFPC).

[276] Desde esta primera reforma existe, en la Exposición de Motivos, una referencia expresa al aumento de competitividad que el legislador espera mediante el impulso de la adopción de medios electrónicos en las organizaciones. Algunos códigos de procedimientos civiles estatales (Campeche, Colima, Guanajuato, Jalisco, México, Michoacán y Nuevo León) también reconocen como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o de cualquier otra tecnología; en otros códigos estatales se reconocen como medios de prueba todos aquellos elementos aportados por los descubrimientos de la ciencia y tecnología (Aguascalientes, Guerrero, Morelos, Oaxaca). La Ley sobre el Uso de Medios Electrónicos y Firma Electrónica Avanzada para el Estado de Hidalgo establece que la firma electrónica simple no puede ser excluida como prueba en juicio, por el solo hecho de presentarse en forma electrónica, asimismo establece que la firma electrónica avanzada, siempre que éste basada en un certificado en los términos de la ley y que haya sido producida por un dispositivo seguro de creación de firma, será admisible como medio de prueba.

[277] Algunos códigos de procedimientos civiles estatales (Campeche, Colima, Guanajuato, Jalisco, México, Michoacán y Nuevo León) también reconocen como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o de cualquier otra tecnología; en otros códigos estatales se reconocen como medios de prueba todos aquellos elementos aportados por los descubrimientos de la ciencia y tecnología (Aguascalientes, Guerrero, Morelos, Oaxaca). La **Ley sobre el Uso de Medios Electrónicos y Firma Electrónica Avanzada para el Estado de Hidalgo** establece que la firma electrónica simple no puede ser excluida como prueba en juicio, por el solo hecho de presentarse en forma electrónica, asimismo establece que la firma electrónica avanzada, siempre que éste basada en un certificado en los términos de la ley y que haya sido producida por un dispositivo seguro de creación de firma, será admisible como medio de prueba.

e) Se fijó la equivalencia funcional entre un documento "original" y la información contenida en medios electrónicos. Al valorar si un MD puede ser considerado legalmente como un "documento original" (es decir, como un documento que fue conservado en original y que debe ser presentando en original) el juez deberá valorar si la información se mantuvo integra e inalterada a partir del momento en que se generó tal información por primera vez en su forma definitiva y si dicha información puede ser accesible para su ulterior consulta (artículo 210-A del CFPC).

f) Se dispuso que los comerciantes están obligados a conservar por un plazo mínimo de 10 años los originales de los MD en que se consignaran contratos, convenios o compromisos que den nacimiento a derechos y obligaciones (artículo 49 del CCo).

g) Se decretaron las reglas para determinar cuándo queda perfeccionado un convenio o contrato celebrado por medios electrónicos (artículo 80 del CCo).

h) Se incluyó un título denominado "Del Comercio Electrónico" (artículos 89 y siguientes del CCo). Dicho título establece reglas básicas sobre envío y recepción de MD; muchas de sus disposiciones fueron posteriormente adicionadas y reformadas por la inclusión de las reformas de 2003, mismas que derivaron de la incorporación de la Ley Modelo de Firmas Electrónicas.

i) Se incorporó el principio de equivalencia funcional entre documento y firma, con relación a MD, siempre y cuando la información se mantenga integra y sea accesible para su ulterior consulta (artículo 93 del CCo).

Posteriormente, el 29 de agosto de 2003 el legislador incorporó una nueva reforma que impactó a la legislación mercantil, incorporó la Ley Modelo de Firmas Electrónicas en nuestros CCo mediante una reforma sustancial al capítulo en materia de Comercio Electrónico[278]. La reforma clarificó el concepto de la firma electrónica e introdujo el concepto de la FEA, asimismo facultó a la SE para constituirse como Autoridad Raíz Certificadora (ARC), en materia de comercio. En consecuencia, esta segunda reforma, además de aclarar conceptos importantes, puso los cimientos para la edificación del sistema de ICP, que actualmente administra la SE. Este sistema ha permitido el surgimiento de los PSC como entidades facilitadoras del comercio, así como en la faceta gobierno-ciudadano.

La evolución legislativa con esta reforma de 2003 se explica con los siguientes hechos:

a) Inclusión de la seguridad en la contratación por medio de dos figuras: la autenticidad del autor y la autenticación del contenido.

b) Admisión en el CCo de las principales definiciones de la Ley Modelo de Firmas Electrónicas, como son: MD, firmante, PSC, parte que confía, entre otros (artículo 89).

c) Integración al CCo de la definición de FEA o Fiable (artículo 89): ·"aquella firma electrónica que es capaz de cumplir los requisitos del artículo 97 del Código"; éste último artículo recoge los criterios de "fiabilidad" que fueron desarrollados por el Grupo de Expertos con respecto a la operación de las firmas electrónicas en un esquema de ICP,

[278] Decreto por el que se reforman y adicionan diversas disposiciones del CCo en Materia de Firma Electrónica, publicado en el Diario Oficial de la Federación del 29 de agosto de 2003.

cuando un tercero participa como PSC.

d) Inclusión de la figura del PSC, como un tercero investido por la legislación mercantil para validar, por su probidad y tecnología, el proceso de emisión, identificación y atribución de firmas electrónicas; dentro del esquema de ICP, administrado por la SE, solamente pueden ser PSC: los notarios públicos y corredores públicos[279], las personas morales de carácter privado y las instituciones públicas. En consecuencia, una firma avalada por un certificado expedido por alguna de estas entidades es el idóneo para firmar un contrato mercantil[280].

e) Que los certificados otorgados por la SE a los fedatarios públicos y corredores públicos obligan a estos últimos a reconocer desde el día de su otorgamiento como propia y auténtica la información que en lo sucesivo envíe por medios electrónicos, que sea distinguida a través de la firma electrónica que se produzca a partir de la utilización de los datos de creación de firma y del certificado que se ha generado por medio de la SE con número de serie xxxx y la vigencia del xxx al xxx. Además, ambos fedatarios deben manifestar que conocen el alcance de los artículos 11 y 12 del Reglamento del Registro Público de Comercio, y que el certificado y sus datos de creación de firma los utilizará para los efectos que marcan los artículos 30 Bis y 30 Bis 1 del CCo[281].

f) Ampliación de los criterios de equivalencia funcional que permiten determinar bajo qué criterios un MD y una firma electrónica pueden cumplir la función que en el comercio prestan los documentos por escrito, los firmados y aquellos que la ley requiere que sean presentados en original (artículos 93 y 93 bis del CCo); se incorporan reglas también que deberán cumplirse para que dichos acuerdos puedan hacerse constar en escritura pública (artículo 93 del CCo).

---

[279] La facultad de expedir certificados no conlleva fe pública; los notarios y corredores públicos podrán realizar certificaciones que impliquen o no la fe pública.

[280] La legislación aplicable a los PSC es la siguiente: el Reglamento del CCo en Materia de Prestadores de Servicios de Certificación, publicado el 19 de julio de 2004 en el Diario Oficial de la Federación; la NOM 151; las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación, publicadas en el Diario Oficial de la Federación del 10 de agosto de 2004, y el Acuerdo que modifica las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación, publicadas en el Diario Oficial de la Federación del 5 de marzo de 2007.

[281] Los numerales 11 y 12 del Reglamento del Registro Público de Comercio, publicado en el DOF el 24 DE OCTUBRE DE 2003 establece:

Artículo 11.- La firma electrónica que se utilizará en el procesamiento de los actos registrales conforme a lo previsto en los artículos 21 bis fracción II inciso c) y 30 bis del Código de Comercio, será Avanzada o Fiable; por tanto el uso de los medios de identificación electrónica que certifique la Secretaría, acreditará que los datos de creación de la firma, corresponden exclusivamente al Firmante y que estaban, en el momento de la firma, bajo el control exclusivo de él. La persona autorizada para firmar electrónicamente será el responsable único y final de mantener la confidencialidad de las claves de acceso y contraseñas autorizadas por la Secretaría, por tanto la información registral así firmada le será atribuible. La certificación de los medios de identificación para firmar electrónicamente la información del Registro lo hará la Secretaría, conforme a los lineamientos que al efecto emita mediante publicación en el Diario Oficial de la Federación.

Artículo 12.- La autorización del notario o corredor público para acceder por medios electrónicos a través del SIGER a la base de datos del Registro en la entidad federativa de que se trate, será cancelada por la Secretaría cuando lo haga con fines distintos a los autorizados o si ha revelado la clave privada para el uso de su firma electrónica, independientemente de las demás responsabilidades en que pudieran incurrir. El notario o corredor público al que le haya sido cancelada su autorización, en términos de lo previsto por el párrafo anterior, quedará impedido para solicitar nueva autorización por el término de dos años, contados a partir de la fecha de publicación correspondiente de la cancelación respectiva, y la Secretaría lo pondrá en conocimiento del gobierno de la entidad federativa de que se trate para que aplique las sanciones correspondientes tratándose de notarios públicos, y hará lo procedente en el caso de corredores públicos. Lo anterior se entenderá sin perjuicio de que el infractor pueda efectuar la solicitud de inscripción de actos otorgados ante su fe a través del procedimiento físico, en términos de lo previsto por este Reglamento.

g) Adición del marco de obligaciones y responsabilidades de cada una de las partes que intervienen en una operación y que resulta muy importante para brindarle solidez jurídica a una ICP: las obligaciones del firmante (artículo 99 del CCo); las obligaciones del destinatario (o intermediario) y aquellas de la parte que confía (artículo 107 del CCo), asimismo las obligaciones del PSC (artículos 103 y 104 del CCo, entre otros).

h) Reconocimiento de los efectos y validez de certificados electrónicos emitidos fuera de México, siempre y cuando dichos certificados pudieran demostrar una fiabilidad equivalente a los certificados expedidos en México.

Finalmente, cabe señalar La configuración legal de las soluciones técnicas y normativas de los MD y firmas electrónicas en varios países[282] fue a través de una ley especial para regular los MD y las firmas electrónicas, mientras que como se evidenció aquí, en México se incluyó dicha regulación en un CCo, y después de varios años se advirtió la necesidad de legislar una LFEA y su reglamento.

4.2.1.1. Obligación de los comerciantes.

El numeral 47 del CCo establece que los comerciantes están obligados a conservar debidamente archivadas las cartas, telegramas y otros documentos en relación con su negocio o giro.

La expresión más evidente de estas obligaciones se encuentra en el incorporado artículo 49 del CCo que precisa que los comerciantes están obligados a conservar por un plazo mínimo de diez años los originales de *aquellas cartas, telegramas, mensajes de datos o cualesquiera otros documentos* en que se *consignen contratos, convenios o compromisos que den nacimiento a derechos y obligaciones.* Para efectos de la conservación o presentación de originales, en el caso de MD, se requerirá que la información se haya mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y sea accesible para su ulterior consulta.

Dicha motivación se enlaza con el contenido del artículo 93 bis que señala que sin perjuicio de lo dispuesto en el artículo 49 de este Código, cuando la ley requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho respecto a un MD:

I. Si existe garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como MD o en alguna otra forma, y
II. De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona a la que se deba presentar.

Para efectos de este artículo, se considerará que el contenido de un MD es íntegro, si éste ha permanecido completo e inalterado independientemente de los cambios que hubiere podido

[282] Entre estos países se encuentran Venezuela, España y Chile.

sufrir el medio que lo contiene, resultado del proceso de comunicación, archivo o presentación. El grado de confiabilidad requerido será determinado conforme a los fines para los que se generó la información y de todas las circunstancias relevantes del caso.

Es de importancia mencionar que el artículo 10 de la Ley Modelo de la CNUDMI de Comercio Electrónico de 1996 configuró un numeral 10 que más tarde fue recogida por nuestra legislación:

> ***Artículo 10.*** *Conservación de los mensajes de datos*
> *1) Cuando la ley requiera que ciertos documentos, registros o informaciones sean conservados, ese requisito quedará satisfecho mediante la conservación de los mensajes de datos, siempre que se cumplan las condiciones siguientes:*
> *a) Que la información que contengan sea accesible para su ulterior consulta; y*
> *b) Que el mensaje de datos sea conservado con el formato en que se haya generado, enviado o recibido o con algún formato que sea demostrable que reproduce con exactitud la información generada, enviada o recibida; y*
> *c) Que se conserve, de haber alguno, todo dato que permita determinar el origen y el destino del mensaje, y la fecha y la hora en que fue enviado o recibido.*
> *2) La obligación de conservar ciertos documentos, registros o informaciones conforme a lo dispuesto en el párrafo 1) no será aplicable a aquellos datos que tengan por única finalidad facilitar el envío o recepción del mensaje.*
> *3) Toda persona podrá recurrir a los servicios de un tercero para observar el requisito mencionado en el párrafo 1), siempre que se cumplan las condiciones enunciadas en los incisos a), b) y c) del párrafo 1).*

Por último, se debe también atender a la Norma Oficial Mexicana NOM-151-SCFI-2002: *"Prácticas comerciales: Requisitos que deben observarse para la conservación de mensajes de datos"* cuyo fundamento es el artículo 49 del CCo, normatividad que por su importancia se aborda más adelante en un apartado en específico.

4.2.1.2. Valor probatorio de la información transmitida por medios electrónicos.

Dentro de la reforma del Código de Comercio del 29 de mayo de 2000 se consideró admitir como prueba los MD así como la fiabilidad de los medios electrónicos como pruebas; cuyo efecto primordial fue el establecimiento de las presunciones respecto a la identificación y autenticidad de los MD además del examen de fiabilidad.

Para ello fue necesario reformar una vez más el citado Código y con fecha 29 de agosto de 2003 se adicionó un método fiable para la transmisión de los MD que provinieran efectivamente de un emisor o destinatario, así como para asegurar la integridad del MD, siendo este método el relacionado con la FEA o fiable. Lo que se traduce en la incorporación de las figuras técnico-jurídicas de integridad, confidencialidad, autenticidad y no repudio, que no es más que la seguridad en los medios electrónicos.
En este sentido, la seguridad en el comercio electrónico se ha convertido en una de las mayores preocupaciones para los usuarios y proveedores de bienes o servicios a la hora de realizar el comercio en línea. Existe sobre todo el temor de los usuarios a proporcionar sus datos (nombre,

dirección y número de tarjeta de crédito) a través de Internet para efectuar el pago, ya que pueden ser interceptados por terceros no autorizados y suplantar así su identidad con el fin de utilizarla ilícitamente en su beneficio, lo que representaría un grave riesgo[283]. Igualmente, se presenta desconfianza por parte de los usuarios en que el pedido cursado y pagado sea realmente entregado, donde las causas pueden ser múltiples, desde ser un mensaje sea alterado de forma accidental o maliciosa durante la transmisión del MD, que el emisor niegue haberlo transmitido, que el destinatario niegue haberlo recibido; o que la información transmitida sea leída por un tercero no autorizado.

El CCo vigente, señala que los documentos privados exhibidos como pruebas en juicio y que no son objetados por las partes, surtirán sus efectos como si hubieran sido reconocidos expresamente. Con tal intención el numeral 1298-A de la normatividad reconoce como prueba a los MD, cuyo valor probatorio se tasará de acuerdo a la fiabilidad del método con el que el MD haya sido creado, archivado, comunicado o conservado.

Ahora bien, en materia probatoria, existen varias presunciones respecto al origen de un MD, que permiten en el ámbito de la tecnología saber si procede del emisor (artículos 90 y 90 bis). Provendrá del emisor si:

a) Ha sido enviado por el propio emisor (artículo 90),
b) Se envió usando medios de identificación, tales como claves o contraseñas del emisor, o persona facultada para actuar en su nombre (artículo 90),
c) Fue remitido por un sistema de información programado por el emisor (artículo 90),
d) El destinatario aplicó en forma adecuada el procedimiento acordado previamente con el emisor (artículo 90 bis) y
e) El MD que reciba el destinatario resulta de actos de un intermediario que le haya dado acceso a algún método utilizado por el emisor para identificar un MD como propio (artículo 90 bis).

Las dos presunciones legales a que se refiere el artículo 90 bis del CCo no serán aplicables cuando el destinatario tuvo conocimiento y o debió tenerlo, en el supuesto de haber actuado con la debida diligencia o aplicado algún método contenido, respecto a que el MD no provenía del emisor.

Se presume que se actuó con la debida diligencia, si el método que empleó el destinatario cumple con los requisitos establecidos en el propio Código para la evaluación de la fiabilidad de las firmas electrónicas. No está de más señalar que los artículos 90 y 90 bis contienen presunciones *iuris tantum,* esto es, admiten prueba en contrario, que en el caso implica quien niega una presunción legal que tiene la contraparte está obligado a probar, de conformidad con el artículo 1196 del multicitado Código.

[283] Ribas Alejandro, Javier. Riesgo legales en Internet. Especial referencia a la protección de datos personales, en Mateu de Ros, Rafael. y Cendoya Ménendez de Vigo, Juan Manuel (coord.). Derecho de internet. Contratación electrónica y firma digital. Navarra: Aranzadi, S.A., 2000, p.147.

Es propicio ejemplificar la forma en que se emplean las presunciones legales de los artículos 90 y 90 bis del CCo de acuerdo al siguiente caso hipotético:

Juan ofrece en venta un libro a Sara a través de la emisión de un MD enviado a su correo electrónico programado por Juan (sistema de información).

- **Primera presunción:** Se presume que la oferta proviene de Juan, pues se utilizó un sistema de información programado por Juan. Por ende, si Juan quisiere desconocer la autoría de su oferta, en términos del artículo 1196 del CCo, tendría la carga de la prueba para desvirtuar que el sistema de información no fue programado por él.
- **Segunda presunción:** Se presume que la oferta fue enviada por Juan, y por ende, Sandra podrá aceptar o rechazar la misma, siempre que Sandra hubiere aplicado en forma adecuada el procedimiento acordado con Juan para verificar si el MD provenía de Juan. Por tanto, esta presunción no existirá si Sandra no actuó con la debida diligencia para determinar que el MD no provenía de Juan.
- **Tercera presunción:** Se presume que Sandra actuó con la debida diligencia para determinar que la oferta provenía de Juan, cuando el método que utilizó cumple con la fiabilidad de la firmas electrónicas de conformidad con el artículo 97 del Código. En el caso de que Sandra considere que la firma electrónica no es fiable, no existirá la presunción de que el MD y por ende, la oferta se hubieren enviado. En caso de que Juan aduzca que la oferta fue rechazada porque Sandra no la contestó inmediatamente (conforme a lo dispuesto en el artículo 80 del Código), Sandra podrá argumentar que la oferta nunca fue enviada, y por tanto, la carga de la prueba la tendrá Juan (para probar que el MD fue enviado en términos del artículo 90 bis del Código).

En resumen, los artículos que exponen estas presunciones son los que van del 1194 al 1205 del CCo:

> ***"Artículo 1194.-*** *El que afirma está obligado a probar. En consecuencia, el actor debe probar su acción y el reo sus excepciones.*
> ***Artículo 1195.-*** *El que niega no está obligado a probar, sino en el caso en que su negación envuelva afirmación expresa de un hecho.*
> ***Artículo 1196.-*** *También está obligado a probar el que niega, cuando al hacerlo desconoce la presunción legal que tiene a su favor el colitigante.*
> ***Artículo 1197.-*** *Solo los hechos están sujetos a prueba: el derecho lo estará únicamente cuando se funde en leyes extranjeras: el que las invoca debe probar la existencia de ellos y que son aplicables al caso.*
> ***Artículo 1198.-*** *Las pruebas deben ofrecerse expresando claramente el hecho o hechos que se trata de demostrar con las mismas, así como las razones por los que el oferente considera que demostrarán sus afirmaciones; si a juicio del tribunal las pruebas ofrecidas no cumplen con las condiciones apuntadas, serán desechadas, observándose lo dispuesto en el artículo 1203 de este ordenamiento. En ningún caso se admitirán pruebas contrarias a la moral o al derecho.*
> ***Artículo 1199.-*** *El juez recibirá el pleito a prueba en el caso de que los litigantes lo hayan solicitado, o de que él la estime necesaria.*

Artículo 1200.- *Cualquiera cuestión que se suscite con ocasión de lo dispuesto en los dos artículos anteriores, el juez la resolverá de plano.*
Artículo 1201*.- Las diligencias de prueba deberán practicarse dentro del término probatorio; el juez deberá fundar la resolución que permita su desahogo fuera de dicho término, las cuales deberán mandarse concluir en los juicios ordinarios dentro de un plazo de veinte días, y en los juicios especiales y ejecutivos dentro de diez días, bajo responsabilidad del juez, salvo casos de fuerza mayor.*
Artículo 1202.- *No obstan a lo dispuesto en el artículo anterior las reglas que se establecen para la recepción de pruebas en incidentes, o las documentales de las que la parte que las exhibe manifieste bajo protesta de decir verdad, que antes no supo de ellas, o habiéndolas solicitado y hasta requerido por el juez, no las pudo obtener, o las supervenientes.*
Artículo 1203.- *Al día siguiente en que termine el período del ofrecimiento de pruebas, el juez dictará resolución en la que determinará las pruebas que se admitan sobre cada hecho, pudiendo limitar el número de testigos prudencialmente. En ningún caso se admitirán pruebas contra del derecho o la moral; que se hayan ofrecido extemporáneamente, sobre hechos no controvertidos o ajenos a la litis; sobre hechos imposibles o notoriamente inverosímiles, o bien que no reúnan los requisitos establecidos en el artículo 1198 de este Código. Contra el auto que admita alguna prueba que contravenga las prohibiciones señaladas anteriormente o que no reúna los requisitos del artículo 1198, procede la apelación en efecto devolutivo de tramitación conjunta con la sentencia definitiva, cuando sea apelable la sentencia en lo principal. En el mismo efecto devolutivo y de tramitación conjunta con dicha sentencia, será apelable la determinación en que se deseche cualquier prueba que ofrezcan las partes o terceros llamados a juicio, a los que siempre se les considerará como partes en el mismo.*
Artículo 1204.- *La citación se hará, lo más tarde, el día anterior a aquel en que deba recibirse la prueba.*
Artículo 1205.- *Son admisibles como medios de prueba todos aquellos elementos que puedan producir convicción en el ánimo del juzgador acerca de los hechos controvertidos o dudosos y en consecuencia serán tomadas como pruebas las declaraciones de las partes, terceros, peritos, documentos públicos o privados, inspección judicial, fotografías, facsímiles, cintas cinematográficas, de videos, de sonido, mensajes de datos, reconstrucciones de hechos y en general cualquier otra similar u objeto que sirva para averiguar la verdad."*

Por otra parte y con la finalidad de dotar de niveles de seguridad a las transacciones electrónicas y a operaciones comerciales tales como la conclusión de contratos o el pago con tarjeta (de crédito o débito) realizadas en Internet, es necesario el cumplimiento de un conjunto de elementos básicos de seguridad que se resumen en la palabra **A**H**ÍNCO:** la **A**utenticación, **I**ntegridad, el **N**o repudio del origen así como destino y **C**onfidencialidad[284].

a) Autenticación: Permite a las partes intervinientes en la transacción protegerse de que son realmente quienes dicen ser sin que exista la posible equivocación de identidades ni la suplantación por parte de un tercero. De este modo, todos conocen ciertamente la identidad del otro evitando fraudes. El consumidor requiere estar seguro de que está negociando con quien dice ser para no proporcionar sus datos bancarios a alguien que pudiera utilizarlos de manera fraudulenta.

[284] Martínez Nadal, Apol·lònia. Comercio electrónico, firma digital y autoridades de certificación, 2001, 3ª ed., Madrid, Civitas, p. 33.

b) Integridad: Se trata de garantizar que la información intercambiada no sea modificada o alterada ilícitamente durante su envío a través de redes telemáticas. Para lograrlo, se utilizan protocolos de seguridad (SSL, SET y 3D Secure) capaces de detectar cualquier cambio que se haya producido en la información transmitida.

c) Confidencialidad[285]: Enviar MD secretos a través de canales inseguros como Internet, utilizando la clave pública del destinatario, de conocimiento público, el remitente puede estar seguro de que sólo el destinatario, el tenedor de la clave privada, podrá descifrar el mensaje. El protocolo SET y SSL garantizan la confidencialidad emplea la criptografía para cifrar (encriptar) los datos que se van a enviar.

d) El no rechazo o no repudio: Es aquel servicio que garantiza a las partes intervinientes en una transacción o comunicación que la otra parte ha participado evidentemente en la comunicación, impidiendo el repudio de una transacción (cuando un cliente niega haber realizado la compra o haber enviado un mensaje) y proporcionando a compradores y vendedores la misma confianza que existe en las compras convencionales usando las actuales redes de autorización de créditos de las compañías de tarjetas de pago. Esto significa que las partes que intervienen en el contrato no podrán rechazar las obligaciones contractuales salvo que prueben que concurre un vicio del consentimiento.

El no repudio puede dividirse a su vez en dos clases:

- **No repudio de origen,** que implica que el emisor del mensaje no niegue haber enviado el mensaje.
- **No repudio de destino**, por el que el receptor no puede negar la recepción del mensaje. Es imprescindible tener la certeza de que el MD ha sido efectivamente enviado y recibido por las partes intervinientes y, al mismo tiempo, tener posibilidad de demostrarlo. Si no existe dicha posibilidad cualquiera de las partes podría negar su participación en la transacción y desvincularse de las obligaciones que les corresponden y podrían poner a la otra parte que no la niega en una situación difícil, debiendo tener la prueba de su existencia.

Como forma para evitar el repudio del mensaje aparece la figura de los terceros de confianza que certifiquen la emisión y recepción en la que aparece fecha y hora.

Pero la modalidad de pago también cuenta con otros elementos que son necesarios para emplear el sistema de pago, a saber:

i) Intimidad: el banco emisor de la tarjeta de crédito puede acceder a la información sobre los pedidos del titular y puede elaborar perfiles de hábitos de compra de sus clientes.

[285] No siempre la criptografía asimétrica tiene las dos funciones; por ejemplo con el algoritmo RSA sí, pero no el Digital Signature Standard (DSS) se permite el intercambio de claves públicas y privadas ni la encriptación, por ello, sólo permite realizar firmas digitales de manera rápida pero no ofrece la confidencialidad.

ii) Verificación inmediata: proporciona al comerciante una verificación inmediata, antes de completarse la compra, de la disponibilidad de crédito y de la identidad del cliente. De esta forma, el comerciante puede cumplimentar los pedidos sin riesgo de que posteriormente se invalide la transacción.

Finalmente, cabe traer a colación el primer estudio expuesto en una sentencia en materia administrativa con motivo del uso de medios electrónicos en materia fiscal, del rubro siguiente[286]:

CONTRIBUCIONES. LA COPIA SIMPLE DEL COMPROBANTE DE PAGO POR MEDIOS ELECTRÓNICOS OBTENIDA MEDIANTE IMPRESORA, FAX O CUALQUIER OTRO MEDIO ANÁLOGO ES APTA PARA ACREDITAR EL ACTO DE APLICACIÓN DEL ARTÍCULO TERCERO TRANSITORIO DE LA LEY DEL IMPUESTO SOBRE LA RENTA VIGENTE EN EL AÑO DOS MIL TRES. Del artículo 31, segundo párrafo, del Código Fiscal de la Federación y de la regla 2.9.17. de la Resolución Miscelánea Fiscal vigente en febrero del año dos mil tres se desprende que cuando los contribuyentes realicen el cumplimiento de sus deberes fiscales por medios electrónicos, no es obligatorio que presenten la declaración correspondiente en las formas aprobadas por la Secretaría de Hacienda y Crédito Público, en virtud de que los contribuyentes podrán presentar la declaración en las citadas formas para obtener el sello o impresión de la máquina registradora, lo que significa que se está en presencia de una facultad o derecho del gobernado que puede o no ejercer y no de un deber; en igual forma, es una facultad de éste obtener copia certificada de las declaraciones presentadas por medios electrónicos. Ahora bien, el pago de contribuciones por medios electrónicos constituye un instrumento para facilitar el cumplimiento de las obligaciones fiscales de los gobernados y la pronta y eficaz recaudación, cuya forma de operar implica que los causantes tengan una clave de acceso al sistema tributario cuando realicen pagos por transferencia electrónica, en tanto que la institución financiera proporcionará el sello digital. El concepto del "equivalente funcional" entre los documentos consignados en papel y aquellos consignados por vía electrónica tiene por objeto establecer una serie de características numéricas y criptográficas que identifican a la persona y aprobar la información que aparece en el mensaje, de ahí que la reproducción de la información mediante impresora, fax o cualquier otro medio análogo, que naturalmente se reduce a copia simple, no significa, en modo alguno, que carezcan de valor probatorio para demostrar el acto de aplicación del artículo tercero transitorio de la Ley del Impuesto sobre la Renta, vigente en el año dos mil tres, reclamado, por el simple hecho de que consten en copia simple, antes bien, son confiables partiendo de la base de los fines del artículo 31 del ordenamiento citado, que sirvió de fundamento para generar la información electrónica, en virtud de que la seguridad de la operación se encuentra en la clave digital que es original, adminiculada con los demás datos como son el registro federal de contribuyentes, la fecha de pago, el número de cuenta, el número de operación, el periodo, el impuesto y la cantidad que se paga y, en todo caso, el fisco federal, de no estar de acuerdo con su contenido, está en posibilidad de impugnarlo, y si no lo hizo, tal omisión se traduce en su aceptación tácita para todos los efectos legales, porque la presentación de una declaración escrita para obtener el sello oficial en original o la impresión en ella de la máquina registradora, después de haber realizado el pago o cumplimiento de obligaciones fiscales por medios electrónicos, es una facultad o derecho del gobernado que puede o no ejercer a su juicio, porque no se trata de un deber, una obligación. Por tanto, la fuerza probatoria deriva de la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas obligadas el contenido de la información relativa y ser exigida para su ulterior consulta, de conformidad con lo dispuesto por el artículo 210-A del Código Federal de Procedimientos Civiles, aplicado supletoriamente en términos del artículo 2o. de la Ley de Amparo, y no de la aplicación dogmática de una regla general de que las copias

[286] Véase Semanario Judicial de la Federación, Tomo XIX, Enero de 2004, Material Administrativa, Novena Época, página: 1492.

simples carecen, por sí mismas, de valor, por el hecho de que el sello digital se encuentra en una copia simple obtenida de impresora, fax, entre otros, ya que los avances tecnológicos, a nivel mundial, trajeron como resultado que el legislador introdujera los medios electrónicos para crear, modificar, extinguir o cumplir obligaciones, según se advierte de los artículos 31 del código tributario, 89 a 114 del Código de Comercio, 188 y 210-A del Código Federal de Procedimientos Civiles, entre otros ordenamientos, que establecen excepciones a la regla general citada. Por consiguiente, si al realizar el pago provisional del impuesto sustitutivo del crédito al salario que le corresponde, el acuse referido es el único documento que obtuvo el particular al realizar su pago de esa forma, es claro que si las autoridades hacendarias no lo objetaron, por razones de lealtad procesal, de probidad y buena fe frente al Juez, quien debe evitar que se trastoquen dichos valores, debe considerarse apto y suficiente para demostrar el pago de referencia y, por ende, el acto concreto de aplicación de la norma tildada de inconstitucional y su interés jurídico para cuestionarla; con mayor razón si la quejosa, en el escrito de demanda, manifestó bajo protesta de decir verdad que la copia simple en la que consta la firma electrónica, es real, sin perjuicio de las responsabilidades que le pudieran resultar, en el supuesto de que llegara a faltar a la verdad, sobre todo si se toma en cuenta que la autoridad fiscal se abstuvo de cuestionar la veracidad de la firma electrónica, no obstante que cuenta con la base de datos que contiene los sellos digitales y las firmas electrónicas.

Del examen de su discurso legal se advierte que el primer acto de aplicación de las normas fiscales reclamadas se acredita con la exhibición de la constancia de recepción de la declaración y pago respectivo que fueron ofrecidos por medios electrónicos.

Llama especialmente la atención el hecho de que el tribunal colegiado expositor de la tesis utiliza el principio de equivalencia funcional de la información consignada en medios electrónicos en concordancia con los numerales 89 a 114 del CCo así como 188 y 210 del CFPC, exhibiendo que dicho principio tiene como propósito identificar a la persona y aprobar la información que aparece en el mensaje; por tanto, la reproducción mediante impresora del comprobante de pago por ese medio, aun cuando sea por su naturaleza copia simple, no significa que no tenga valor probatorio para probar el acto de aplicación; de tal forma que el órgano jurisdiccional aplicó de manera supletoria el argumento de que el método utilizado por el contribuyente era fiable alejándose de otras posturas jurisprudenciales[287] de antaño relativas a que quien exhibió impresiones que provienen de páginas de Internet, para que tuvieran pleno valor demostrativo debieron corroborarse con otros elementos de convicción.

Este razonamiento del principio de equivalencia funcional no hace sino reafirmar el inicio del reconocimiento del fundamento de que los medios electrónicos crean, modifican y extinguen obligaciones.

4.2.1.3. Valor probatorio de la FEA.

El CCo desde su artículo 1049 refiere que son juicios mercantiles los que tienen por objeto ventilar y decidir las controversias que se deriven de los actos comerciales, y que cuando para una de las partes que intervienen en un acto, tenga naturaleza comercial y, para la otra, tenga

[287] Véase Semanario Judicial de la Federación y su Gaceta, Tomo XV, Febrero de 2002, Material Civil, Novena Época, Página: 806

naturaleza civil, la controversia se regirá conforme a las leyes mercantiles. Por tanto, si un comerciante pacta con alguien más y existe necesidad de llevar el reclamo a los tribunales, el procedimiento se debe regir por las normas del CCo, esto es, el procedimiento mercantil es preferente a todos los que libremente convengan las partes, pudiendo ser un procedimiento convencional ante tribunales o un procedimiento arbitral, y en este último caso, siempre que el mismo se hubiere formalizado en escritura pública, póliza ante corredor o ante el juez que conozca de la demanda en cualquier estado del juicio, y se respeten las formalidades esenciales del procedimiento.

Ahora bien, conforme al artículo 1054 del CCo, en caso de no existir convenio entre las partes sobre el procedimiento ante tribunales, y salvo que las leyes mercantiles establezcan un procedimiento especial o una supletoriedad expresa, los juicios mercantiles se regirán por las disposiciones del libro respectivo del CCo y, en su defecto, se aplicará supletoriamente el CFPC y, en caso de que no regule suficientemente la institución cuya supletoriedad se requiera, la ley de procedimiento local respectiva.

Así entonces, el artículo 1055 indica que los juicios mercantiles, son ordinarios, orales, ejecutivos o especiales regulados por cualquier ley comercial. Todos los juicios mercantiles, con excepción de los orales cuyas reglas son especiales, se sujetarán a los requisitos que el CFPC señala: formalidades en los ocursos, traducción de documentos redactados en idioma extranjero, actuaciones judiciales con letra, etc.

Derivado de lo anterior y para efectos de este trabajo, se reflexionará respecto al valor probatorio que debería otorgar un juez cuando alguna de las partes alegue no haber emitido su voluntad y/o desconozca el uso del medio electrónico y/o de FEA.

En este sentido, en caso de una negativa de una parte, existe la presunción legal de que al utilizar los medios electrónicos y la FEA, existe voluntad de obligarse en los términos pactados, pero el tema de carga probatoria en caso de negativa de una parte, daría lugar a que la presunción legal de negación de su voluntad, debiera acreditarse a través de testigos expertos, es decir, a través del ofrecimiento de peritos en ingeniería en sistemas, ingeniería en cómputo, informática o alguna profesión similar.

En tal supuesto hay demostrar que científicamente el proceso de certificación para obtener la FEA o su utilización resultan tan falibles que requieren su validación y, por ende, llevaría a desacreditar las características de la FEA: el **A**H**ÍNCO: A**utenticidad; **I**ntegridad; **N**o repudio y **C**onfidencialidad obtenida.

Al respecto, el artículo 1205 refiere que son admisibles como medios de prueba **todos aquellos elementos que puedan producir convicción en el ánimo del juzgador acerca de los hechos controvertidos o dudosos** y, en consecuencia, serán tomadas como pruebas las declaraciones de las partes, terceros, **peritos, documentos públicos o privados,** inspección judicial, fotografías, facsímiles, cintas cinematográficas, videos, sonido, MD, reconstrucciones de hechos

y en general cualquier otra similar u objeto que sirva para averiguar la verdad (énfasis añadido).

En relación con el numeral anterior, artículo 1237 del CCo indica que son instrumentos públicos los que están reputados como tales en las leyes comunes y, además, las pólizas de contratos mercantiles celebrados con intervención de corredor y autorizados por éste, conforme a lo dispuesto en el mismo ordenamiento y, conforme al artículo-1238, por exclusión de lo anterior, que el documento privado es cualquiera otro no comprendido en lo dispuesto en el artículo 1237.

Ahora bien, en los artículos 1252 y 1254 del CCo, se regula la prueba pericial y algunas de las particularidades que las partes u oferentes deben cumplir para que sea admitida su prueba así como los derechos que la contraparte pronuncie en relación a la pertinencia de la prueba ofrecida, o bien, para el derecho de nombrar un perito, el cual tendrá la oportunidad de emitir su dictamen en la materia solicitada.

Así tenemos que dentro de los requisitos para que sea aceptada la probanza, el código precisa que los peritos deben tener título en la ciencia, arte, técnica, oficio o industria a que pertenezca la cuestión sobre la que ha de oírse su parecer, en cuyo caso, si la ciencia, arte, técnica, oficio o industria requieren título para su ejercicio, o requiriéndolo, no hubiere peritos en el lugar, caso en el cual podrán ser nombrada cualesquier persona entendida a satisfacción del juez, aun cuando no tengan título. Lo anterior, no es óbice para que el juez deseche de oficio las periciales ofrecidas para este conocimiento así como las que se encuentren ya acreditadas en autos o se refieran a simples operaciones aritméticas o similares.

Las partes podrán proponer la prueba pericial, dentro del término de ofrecimiento de pruebas, pero considerando lo siguiente:

I. Señalar **con toda precisión:**

a) La ciencia, arte, técnica, oficio o industria sobre la cual deba practicarse la prueba;
b) Los puntos sobre los que versará y las cuestiones que se deben resolver en la pericial;
c). La cédula profesional, calidad técnica, artística o industrial del perito que se proponga, nombre, apellidos y domicilio de éste, **con la correspondiente relación de tal prueba con los hechos controvertidos.**

La consecuencia de no cumplir con cualquiera de los requisitos anteriores, es que el juez desechará de plano la prueba en cuestión.

A pesar de que el CCo, continúa en el artículo 1253 señalando reglas para el caso de admisión de la prueba, consideramos que primero debemos estar al supuesto contenido en el artículo 1254 que refiere que el juez, **antes de admitir la prueba pericial**, dará vista a la contraria por el término de tres días, para que manifieste sobre la **pertinencia de tal prueba y** para que **proponga la ampliación de otros puntos y cuestiones además de los formulados por el**

oferente, para que los peritos dictaminen y designe perito de su parte, debiendo nombrarlo en la misma ciencia, arte, técnica, oficio o industria, en que la haya ofrecido la contraparte, así como su cédula profesional, o en su caso los documentos que justifiquen su capacidad científica, artística, técnica, etc. requisito sin el cual no se le tendrá por designado, y habrá que estarse a las consecuencias legales de tener presunta o procesalmente consentido el de la contraria con las variantes que veremos a continuación.

En caso de que la contraparte del oferente cumpliere con lo anterior, tendríamos que estar a tres supuestos:

1.- Un solo testigo hace prueba plena cuando ambas partes convengan expresamente en pasar por su dicho, siempre que éste no esté en oposición con otras pruebas que obren en autos. En cualquier otro caso, su valor quedará a la prudente apreciación del tribunal. (artículo 216 del CFPC).

2.- Las razones esgrimidas sobre la impertinencia de la probanza, son consideradas correctas por el juzgador y decide **no admitir la prueba; y**

3.- El oferente formula razones de impertinencia pero además cumple con ampliar (o no) el interrogatorio, designa perito y acompaña el documento que valida su experiencia, y en todo caso, el juzgado puede considerar improcedentes las razones planteadas tales como la no pertinencia de la prueba. Si cumple con requisitos de ofrecimiento de perito, lo tendrá por señalado y, en consecuencia, el juez la admitirá, quedando obligadas las partes a:

- Que sus peritos, dentro del plazo de tres días, presenten escrito en el que acepten el cargo conferido y protesten su fiel y legal desempeño, debiendo anexar el original o copia certificada de su cédula profesional o documentos que acrediten su calidad de perito en el arte, técnica, oficio o industria para el que se les designa; **manifestando, bajo protesta de decir verdad, que conocen los puntos cuestionados y pormenores relativos a la pericial, así como que tienen la capacidad suficiente para emitir dictamen sobre el particular**, quedando obligados a rendir su dictamen dentro de los **diez días siguientes a la fecha en que hayan presentado los escritos de aceptación y protesta del cargo de peritos**, salvo que existiera en autos causa bastante por la que tuviera que modificarse la fecha de inicio del plazo originalmente concedido.
- La consecuencia de no exhibir los documentos justificativos de su calidad, es que no se tenga por presentado al perito aceptando el cargo, con la correspondiente sanción para las partes, sin que sea necesaria la ratificación de dichos dictámenes ante la presencia judicial;

Ahora bien, cuando se trate de juicios ejecutivos, especiales o cualquier otro tipo de controversia de trámite singular, donde por lo regular son asuntos cuya celeridad es notoria y los términos procesales en ocasiones se acortan, las partes quedan obligadas a cumplir dentro de los tres días siguientes al proveído en que se les tengan por designados tales peritos, conforme a lo ordenado en el párrafo anterior, quedando los peritos obligados a rendir su

dictamen **dentro de los cinco días siguientes a la fecha en que hayan aceptado y protestado el cargo** con la misma salvedad que la que se establece en la párrafo inmediato anterior.

Si los dictámenes rendidos por los peritos de las partes resultan substancialmente contradictorios, se designará al perito tercero en discordia tomando en cuenta lo ordenado por el artículo 1255 de este código.

Siendo importante señalar que la falta de presentación del escrito del perito designado por la oferente de la prueba, donde acepte y proteste el cargo, dará lugar a que **se tenga por desierta dicha pericial.**

Ahora bien, qué sucede si es la contraparte no designó perito, o el perito por ella designado no presenta su escrito de aceptación y protesta del cargo en la forma y plazo exigido, ello trae como consecuencia que el juez tenga a ésta parte conforme con el dictamen pericial que rinda el perito del contrario.

Y para el supuesto de que el perito designado por alguna de las partes, que haya aceptado y protestado el cargo conferido, no presente su dictamen pericial en el término concedido, la legislación procesal mercantil señala que se entenderá que dicha parte **acepta aquél que se rinda por el perito de la contraria, y la pericial se desahogará con ese dictamen.**

Si ambos peritos de las partes, no rindieran su dictamen dentro del término concedido, **el juez designará en rebeldía de ambas, un perito único** rendirá su dictamen dentro del plazo señalado en las fracciones III y IV del artículo 1253 del CCo.

La legislación también prevé que el juez sancionará a los peritos omisos con multa hasta de $3,373.59 y corresponderá a la SE actualizar cada año por inflación este monto expresado en pesos y publicarlo en el DOF, a más tardar el 30 de diciembre de cada año.

Por lo visto, la misma legislación procesal contempla casos, presunciones y sanciones generadas por omisión en el cumplimiento de requisitos o tiempos para actos procesales en el ofrecimiento y aceptación para éste tipo de probanzas, y también regula la posibilidad de que expresamente las partes, en cualquier momento, puedan convenir en la designación de un sólo perito para que rinda su dictamen al cual se sujetarán, y en un debido derecho de defensa, también se contempla que en cualquier momento las partes pueden manifestar su conformidad con el dictamen del perito de la contraria y hacer observaciones al mismo, **que serán consideradas en la valoración que realice el juez en su sentencia**.

Ahora bien, continuando con el valor probatorio que el juzgado debiera dar a cada probanza, debemos considerar que de acuerdo al artículo 197 del CFPC, de aplicación supletoria a la materia mercantil, el tribunal goza de la más amplia libertad para hacer el análisis de las pruebas rendidas; para determinar su valor unas enfrente a otras, y fijar el resultado de la valuación contradictoria; a menos que la ley fije las reglas para hacer esta valuación, observando, sin embargo, respecto de cada especie de prueba, lo dispuesto en este capítulo.

Aunando a lo anterior, que el CCo en relación al valor de las pruebas regula desde el artículo 1287 como se va a calificar la prueba confesional hecha ante autoridad judicial (pero debemos considerar que pudiera referirse a lo señalado en la demanda o contestación de demanda), refiriendo que hará prueba plena cuando concurren en ella las circunstancias siguientes:

I. Que sea hecha por persona capaz de obligarse;
II. Que sea hecha con pleno conocimiento y sin coacción ni violencia;
III. Que sea de hecho propio y concerniente al negocio;
IV. Que se haya hecho conforme a las prescripciones del cap. XIII.

Por su parte, el artículo 1289 del CCo, en lo referente a la confesión a través de la prueba de posiciones desahogada durante la etapa procesal correspondiente, para que se consideren plenamente probados los hechos sobre los que versen las posiciones que judicialmente han sido dadas por absueltas en sentido afirmativo, se requiere:

I. Que el interesado sea capaz de obligarse;
II. Que los hechos sean suyos y concernientes al pleito;
III. Que la declaración sea legal.

De igual manera el código impone en el artículo 1292 CCo de forma tazada o fija la regla de que los instrumentos públicos hacen prueba plena, aunque se presenten sin citación la contraparte, salvo su derecho de redargüirlos de falsos y para pedir su cotejo con los protocolos y archivos. En caso de inconformidad con el protocolo o archivo, los instrumentos no tendrán valor probatorio en el punto en que existiere la inconformidad, y por tanto consideramos que estaríamos a las reglas de valoración para la prueba pericial.

Conforme al artículo 1296 la procedencia de los documentos privados **no objetados por la parte contraria se tendrán por admitidos y surtirán sus efectos como si hubieren sido reconocidos expresamente**.

El documento que un litigante presenta, prueba plenamente en su contra, en todas sus partes, aunque el colitigante no lo reconozca, y conforme al añadido artículo 1298-A se reconoce como prueba los MD, pero para valorar la fuerza probatoria de dichos mensajes, se estimará primordialmente la **fiabilidad del método en que haya sido generada, archivada, comunicada o conservada.**

Conforme al artículo 1301 del mismo CCo, la fe de los demás **juicios periciales**, incluso el cotejo de letras, **será calificada por el juez según las circunstancias**, pero tratándose de pruebas técnicas pero precisas deberá el juez estimarlas con un valor adecuado para demostrar el consentimiento del compromiso comercial en atención a la fiabilidad del método de generación, archivo, comunicación y conservación por tratarse de la FEA.

Así las cosas, encontramos diversos criterios jurisprudenciales que consideramos importantes para efecto de redondear la idea anterior, cuyo rubro y texto se trascriben:

> ***DOCUMENTOS Y CORREOS ELECTRÓNICOS. SU VALORACIÓN EN MATERIA MERCANTIL[288].***
> *La doctrina explica que en la época contemporánea cuando se habla de prueba documental no se puede pensar sólo en papel u otro soporte que refleje escritos perceptibles a simple vista, sin ayuda de medios técnicos; se debe incluir también a los documentos multimedia, es decir, los soportes que permiten ver estos documentos en una computadora, un teléfono móvil, una cámara fotográfica, etcétera. En varios sistemas jurídicos se han equiparado totalmente los documentos multimedia o informáticos, a efectos de valoración. Esa equivalencia es, básicamente, con los privados, y su admisión y valoración se sujeta a requisitos, sobre todo técnicos,* ***como la firma electrónica****, debido a los problemas de fiabilidad de tales documentos, incluyendo los correos electrónicos, ya que es posible falsificarlos e interceptarlos, lo cual exige cautela en su ponderación, pero sin desestimarlos sólo por esa factibilidad. Para evitar una pericial en informática que demuestre la fiabilidad del documento electrónico, pero complique su ágil recepción procesal, el juzgador puede consultar los datos técnicos reveladores de alguna modificación señalados en el documento, aunque de no existir éstos, atenderá a la posibilidad de alteración y acudirá a la experticia, pues el documento electrónico puede quedar en la memoria RAM o en el disco duro, y podrán expedirse copias, por lo que para comprobar el original deberán exhibirse documentos asistidos de peritos para su lectura. Así es, dado que la impresión de un documento electrónico sólo es una copia de su original. Mayor confiabilidad merece el documento que tiene firma electrónica, aunque entre esa clase de firmas existe una gradación de la más sencilla a la que posee mayores garantías técnicas, e igual escala sigue su fiabilidad, ergo, su valor probatorio.* ***Así, la firma electrónica avanzada prevalece frente a la firma electrónica simple, ya que los requisitos de producción de la primera la dotan de más seguridad que la segunda, y derivan de la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional sobre las Firmas Electrónicas. Esta propuesta de normatividad, al igual que la diversa Ley Modelo sobre Comercio Electrónico, fue adoptada en el Código de Comercio, el cual sigue el criterio de equivalencia funcional que busca equiparar los documentos electrónicos a los tradicionales elaborados en soporte de papel, mediante la satisfacción de requisitos que giran en torno a la fiabilidad y trascienden a la fuerza probatoria de los mensajes de datos. Por ende, conforme a la interpretación de los artículos 89 a 94, 97 y 1298-A del Código de Comercio, en caso de que los documentos electrónicos reúnan los requisitos de fiabilidad legalmente previstos, incluyendo la existencia de una firma electrónica avanzada, podrá aplicarse el criterio de equivalente funcional con los documentos que tienen soporte de papel, de manera que su valor probatorio será equivalente al de estos últimos.*** *En caso de carecer de esa firma y haberse objetado su autenticidad, no podrá concedérseles dicho valor similar, aunque su estimación como prueba irá en aumento si en el contenido de los documentos electrónicos se encuentran elementos técnicos bastantes, a juicio del juzgador, para estimar altamente probable su autenticidad e inalterabilidad, o bien se complementan con otras probanzas, como la pericial en informática que evidencie tal fiabilidad. Por el contrario, decrecerá su valor probatorio a la calidad indiciaria si se trata de una impresión en papel del documento electrónico, que como copia del original recibirá el tratamiento procesal de esa clase de documentos simples, y se valorará en conjunto con las restantes pruebas aportadas al juicio para, en función de las circunstancias específicas, determinar su alcance demostrativo.*
>
> **(Énfasis añadido)**

> ***PRUEBA PERICIAL EN MATERIA MERCANTIL. SI EL PERITO DE ALGUNA DE LAS PARTES OMITE RENDIR SU DICTAMEN EN EL PLAZO FIJADO, A DICHA PARTE SE LE TENDRÁ POR CONFORME CON EL EMITIDO***

[288] Décima Época, Tribunales Colegiados de Circuito, Semanario Judicial de la Federación y su Gaceta, Libro XIV, Noviembre de 2012, Tomo 3 , tesis aislada en matria civil: I.4o.C.19 C (10a.), página: 1856.

DE SU CONTRAPARTE, PERO NO SIGNIFICA QUE SE LE OTORGUE PLENO VALOR PROBATORIO[289]. *El Código de Comercio en su libro quinto denominado "De los juicios mercantiles", título primero intitulado "Disposiciones generales", capítulos XV y XX, de rubros: "De la prueba pericial" y "El valor de las pruebas", integrados por los artículos 1252 a 1258 y 1287 a 1306, respectivamente, regula lo referente a la finalidad, ofrecimiento y desahogo de la prueba pericial, y de su contenido se advierte que el propósito de la intervención de los peritos en una controversia es que proporcionen elementos reales y objetivos que permitan al juzgador encontrar la verdad respecto del problema planteado, a fin de que su resolución resulte apegada a los principios de equidad, lógica y justicia que deben regir a las sentencias. Además, para el desahogo de dicha probanza los artículos 1252 y 1253, fracción VI, del citado código disponen que cada parte nombrará un perito, si uno de ellos no rinde su dictamen en el plazo fijado, el legislador previó una sanción procesal consistente en que se tendrá a la parte del perito que no lo rindió, por conforme con el dictamen emitido por el perito de su contraparte; sin embargo, esa ordenanza en sí misma, no tiene el alcance de que se le otorgue pleno valor probatorio al dictamen existente, ya que esa tarea valorativa corresponde al juzgador en términos del artículo 1301. Consecuentemente, si bien es cierto que el Código de Comercio establece como consecuencia por la indolencia de una de las partes en ofrecer y desahogar su prueba pericial, el que se le tenga por conforme con el peritaje de su contraria, también lo es que ese hecho no da lugar a otorgar pleno valor probatorio a la que obra en autos.*

PRUEBA PERICIAL. PARA CONCEDERLE VALOR PROBATORIO NO NECESARIAMENTE DEBE DESAHOGARSE EN FORMA COLEGIADA (CÓDIGO DE COMERCIO POSTERIOR A LAS REFORMAS DEL VEINTICUATRO DE MAYO DE MIL NOVECIENTOS NOVENTA Y SEIS)[290].

Con anterioridad a las reformas del veinticuatro de mayo de mil novecientos noventa y seis, en cuanto hace a la prueba pericial, el Código de Comercio, en su libro quinto, denominado "De los juicios mercantiles", título primero, capítulo décimo quinto, disponía que el juicio de peritos tendría lugar en los negocios relativos a alguna ciencia o arte, y en los casos en que expresamente lo previnieran las leyes; que si los que debían nombrar un perito no pudieren ponerse de acuerdo, el Juez designaría uno de entre los que propusieran los interesados y el que fuere designado practicaría la diligencia; que los peritos debían tener título en la ciencia o arte a que perteneciera el punto sobre el que había de oírse su juicio, si la profesión o el arte no estuvieren legalmente reglamentados, o aun estándolo, no hubiere peritos en el lugar, podría ser nombrado cualesquiera persona entendida, aun cuando no tuviera título; que el Juez podía asistir a la diligencia que practicaran los peritos, pedirles todas las aclaraciones que estimaran conducentes y exigirles la práctica de nuevas diligencias; que cuando la ley fijara bases a los peritos para formar su juicio se sujetarían a ellas, pudiendo, sin embargo, exponer y fundar las consideraciones que en su concepto debían modificarlo; y que cuando el juicio pericial tuviere por objeto el avalúo de alguna cosa, las partes podían asistir a la diligencia respectiva, a cuyo efecto el Juez señalaría día y hora, si lo pidiere alguna de ellas. De lo anterior se advierte que el Código de Comercio no establecía la posibilidad de que el juicio se sustanciara únicamente con los dictámenes de las partes, cuando éstos resultaban contradictorios; sin embargo, con posterioridad a las reformas de mil novecientos noventa y seis, el legislador estableció la posibilidad de que se emitiera sentencia aun cuando no se hubiera desahogado en forma colegiada la prueba pericial, pues en el artículo 1255, estableció que sólo cuando los dictámenes rendidos en juicio resulten sustancialmente contradictorios de tal modo que el Juez considere que no es posible encontrar conclusiones que le aporten elementos de convicción, podrá designar un perito tercero en discordia. Esto es, la designación de un perito tercero en discordia es una facultad potestativa que le otorga la ley al juzgador, pues de la redacción del numeral antes citado no se desprende obligación para que el juzgador nombre un perito en caso de que los dictámenes rendidos por las partes resulten contradictorios. Así, la circunstancia de que en un procedimiento exclusivamente se hayan desahogado los dictámenes rendidos por los peritos de las

[289] Novena Época, Tribunales Colegiados de Circuito, Semanario Judicial de la Federación y su Gaceta, Tomo XXXI, Marzo de 2010, tesis aislada en materia civil: IV.1o.C.102 C, página: 3032.

[290] Novena Época,Tribunales Colegiados de Circuito, Semanario Judicial de la Federación y su Gaceta,Tomo XXV, Enero de 2007, Tesis aislada en materia civil: I.4o.C.103 C, página: 2308.

partes, sin que se haya desahogado una pericial a cargo de un perito tercero en discordia, no implica que la prueba carezca de valor probatorio porque no fue desahogada en forma colegiada, no obstante que los dictámenes de los peritos de las partes resulten contradictorios, pues la ausencia del dictamen del perito tercero en discordia no determina la ineficacia de este medio de convicción, ya que el Juez debe analizar los medios que le fueron aportados por las partes en su conjunto, atendiendo a las reglas de la lógica y la experiencia y si no tiene a su disposición sino sólo dos dictámenes, puede valorarlos y determinar, en su caso, cuál de ellos le causa mayor convicción y vincularlo con lo actuado durante el juicio, de acuerdo con los principios de la lógica y de la experiencia. Por tanto, el juzgador debe analizar si los dictámenes rendidos en el juicio por los especialistas en la materia reúnen los requisitos de la lógica, técnica, ciencia y equidad que para el caso puedan exigirse; de ahí que la legislación mercantil le permite al juzgador evaluar en forma discrecional la prueba pericial, atendiendo a la sana crítica, según lo establece el artículo 1301 del Código de Comercio que dispone que "La fe de los demás juicios periciales, incluso el cotejo de letras, será calificada por el Juez según las circunstancias.

PERICIAL EN MATERIA MERCANTIL. PARA QUE ESA PRUEBA PUEDA VALORARSE, NO ES NECESARIA LA INTERVENCIÓN DE UN PERITO TERCERO EN DISCORDIA[291].
De una sana interpretación del artículo 1255 del Código de Comercio se desprende que cuando los dictámenes rendidos en un proceso de orden mercantil resulten sustancialmente contradictorios, de tal manera que el Juez instructor considere que no es posible encontrar conclusiones que le aporten elementos de convicción, éste podrá designar un perito tercero en discordia quien lo allegará de nuevos elementos para conocer la verdad de los hechos controvertidos, pero si la autoridad jurisdiccional no hace uso de esa facultad que de manera exclusiva le otorga el Código de Comercio, debe entenderse que aun siendo discrepantes los dictámenes periciales presentados por los peritos nombrados por cada una de las partes en el juicio, sí son susceptibles de ser valorados y generar convicción suficiente al juzgador para conocer la verdad, lo que significa que, necesariamente, éste deberá orientar su criterio de acuerdo con aquel que cumpla con la mayor precisión científica en cuanto a su elaboración, sin dejar de atender las circunstancias especiales del caso, pues solamente así estará en aptitud de otorgarle valor probatorio pleno a uno de ellos, sin que sea necesario, en este supuesto, la opinión de un perito tercero en discordia, en razón de que cuando la norma incluye el término "podrá", en este caso debe ser interpretado en sentido potestativo, no de carácter obligatorio para el titular del órgano jurisdiccional; luego, de no haber estimado necesario ejercitar esa facultad, el juzgador debe valorar los dictámenes existentes, por más contradictorios que resulten.

FIRMA ELECTRÓNICA AVANZADA. LA PRESUNCIÓN PREVISTA EN EL ARTÍCULO 19-A, PÁRRAFO ÚLTIMO, DEL CÓDIGO FISCAL DE LA FEDERACIÓN, NO TRANSGREDE EL PRINCIPIO DE PRESUNCIÓN DE INOCENCIA, EN SUS VERTIENTES DE REGLA PROBATORIA Y ESTÁNDAR DE PRUEBA[292]. *El precepto y párrafo citados prevén que se presumirá, sin que se admita prueba en contrario, que los documentos digitales que contengan firma electrónica avanzada de las personas morales fueron presentados por el administrador único, el presidente del consejo de administración o la persona o personas, cualquiera que sea el nombre con el que se les designe, que tengan conferida la dirección general, la gerencia general o la administración de la persona moral de que se trate, en el momento en que se presentaron los documentos digitales. Dicha presunción no impacta en la materia penal, por lo que la autoridad ministerial debe probar la existencia de la conducta ilícita relacionada con la presentación de documentos digitales por los representantes de una persona moral, ante lo cual el sujeto activo estará en posibilidad de demostrar que la conducta no le es imputable, debiéndosele admitir todas las pruebas tendentes a demostrarlo y, por ende, no se releva al juzgador de su deber de analizar todas las pruebas aportadas al proceso, tanto las que permitan acreditar la tipicidad de la conducta, como las que la desvirtúen. De ahí que el principio de presunción de inocencia, en su vertiente de regla*

[291] Novena Época, Tribunales Colegiados de Circuito, Semanario Judicial de la Federación y su Gaceta, Tomo XVII, Marzo de 2003, tesis aislada en material civil: I.3o.C.282 C, página: 1755.
[292] Décima Época, Primera Sala, Gaceta del Semanario Judicial de la Federación, Libro 14, Enero de 2015, Tomo I, tesis aislada en materia constitucional: 1a. IX/2015 (10a.), página: 762.

probatoria, que establece los requisitos que debe cumplir la actividad probatoria y las características que deben reunir los medios de prueba aportados por el Ministerio Público para poder considerar que existe prueba de cargo válida y destruir así el estatus de inocente que tiene todo procesado, no es vulnerado. Además, el hecho de que el inculpado deba allegar al proceso los elementos de prueba respecto de su inocencia, no implica que se esté relevando al órgano acusador de la carga de adminicular y comprobar los elementos de culpa, ya que la presunción de inocencia sólo se agota en la medida en que existan pruebas suficientes que acrediten la responsabilidad del inculpado y que éstas no hayan sido desvirtuadas por la defensa. Por las mismas razones, el numeral analizado tampoco viola el principio de presunción de inocencia, en su vertiente de estándar de prueba o regla de juicio, que ordena a los jueces la absolución de los inculpados cuando durante el proceso no se aportaron pruebas de cargo suficientes para acreditar la existencia del delito y su responsabilidad.

TRANSFERENCIAS ELECTRÓNICAS. NO CONSTITUYEN DOCUMENTOS PRIVADOS, SINO ELEMENTOS DE PRUEBA DERIVADOS DE LOS DESCUBRIMIENTOS DE LA CIENCIA, CUYA VALORACIÓN QUEDA AL PRUDENTE ARBITRIO DEL JUZGADOR[293].

Conforme a lo dispuesto en el artículo 1205 del Código de Comercio y 210-A del Código Federal de Procedimientos Civiles, de aplicación supletoria al ordenamiento legal citado en primer término, por disposición de su numeral 1063, se advierte que en materia mercantil la ley reconoce como medios de prueba todos aquellos elementos que puedan producir convicción en el ánimo del juzgador acerca de los hechos controvertidos, tales como las declaraciones de las partes, periciales y documentos, entre otros, así como la información generada o comunicada en medios electrónicos, ópticos o en cualquier otra tecnología. Ahora bien, las transferencias de dinero realizadas vía electrónica, constituyen una información aportada como descubrimiento de la ciencia que reflejan imágenes en una pantalla electrónica, cuya expresión está supeditada a que se plasme en un objeto o cosa material para su exteriorización y manejo fuera del aparato que lo emite y reproduce, como lo es un documento, en el que la impresión escrita de una imagen proviene de la tecnología, es decir, derivada precisamente de la orden dada a un aparato electrónico, el cual finalmente editará la información que le es suministrada. Por tal motivo, a ese instrumento de información electrónico no le es atribuible el carácter de documento privado al carecer de la característica esencial de que pueda imputársele a persona alguna su elaboración o materialización ante la falta de firma autógrafa para efectos de su reconocimiento, en términos de los artículos 1238, 1241, 1242 y 1245 de la citada codificación mercantil. Precisado lo anterior, queda al prudente arbitrio del juzgador la valoración de la información recabada de medios electrónicos, de conformidad con el segundo párrafo del invocado artículo 210-A, pues para ello se atenderá a la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas obligadas el contenido de la información relativa y ser accesible su ulterior consulta. En ese sentido, si las transferencias obtenidas vía electrónica fueron exhibidas como prueba por la parte demandada, y éstas no fueron reconocidas por su contraria o por la institución bancaria ante la cual se realizó, ni contienen sello o firma digital, entendida ésta como una cadena de caracteres generada con motivo de la transacción electrónica, que permita autenticar el contenido de ese documento digital, resulta inconcuso que tales constancias solamente tienen el valor de indicio, y no constituyen un medio probatorio eficaz para demostrar que, efectivamente, se haya realizado el pago, ante la falta de desahogo de diversos medios probatorios que robustezcan tal circunstancia, como pueden ser la prueba pericial en informática y/o confesional, entre otras.

4.2.2. Reforma del 29 de mayo de 2000 a la Ley Federal de Protección al Consumidor.

[293] Novena Época, Tribunales Colegiados de Circuito,Semanario Judicial de la Federación y su Gaceta, Tomo XXXIII, Marzo de 2011, tesis aislada en material civil: XVII.2o.C.T.23 C, página: 2467.

Es indiscutible que la multicitada reforma de los tres Códigos (CCo, CCiF y CFPC) impacta la actividad de los consumidores al realizar compraventas, quienes debían ser protegidos ante los abusos en los medios electrónicos, de ahí la reforma que ahora nos ocupa de la LFPC. Dicha reforma emuló la Recomendación del Consejo de la OCDE relativa a los Lineamientos para la Protección al Consumidor en el contexto del Comercio Electrónico de 1999[294] e integró los resultados del foro de esa Organización denominado *Gateways to the Global Market: Consumers and Electronic Commerce*[295], ambos documentos básicamente aportaron los siguientes señalamientos:

a) Suministrar información clara y accesible que permita decidir conscientemente al consumidor.
b) Atender a las técnicas de comercialización o *marketing* que se presenta en los medios electrónicos frente a niños, ancianos y enfermos.
c) Respetar si los consumidores no desean recibir avisos comerciales a través de medios electrónicos,
d) Vigilar que los ofrecimientos se hagan de forma clara, equitativa y sin engaños, fraudes, prácticas desleales u otra práctica que origine daño o menoscabo al consumidor.

Dichas nociones fueron plasmadas en la LFPC el 29 de mayo de 2000 y se agregaron otras que previeron lo siguiente:

a) Extensión de la protección de los consumidores a contrataciones electrónicas y la promoción de la elaboración de códigos de ética para proveedores en donde se atienda y cuiden este tipo de contrataciones (artículo 1º).
b) Incorporación de capítulo III-bis denominado "De los derechos de los consumidores en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología", adicionado con un único numeral, el 76 bis, que establece las pautas para realizar las contrataciones electrónicas:

> ***Artículo 76 Bis.-*** *Las disposiciones del presente Capítulo aplican a las relaciones entre proveedores y consumidores en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología. En la celebración de dichas transacciones se cumplirá con lo siguiente:*
> *I. El proveedor utilizará la información proporcionada por el consumidor en forma confidencial, por lo que no podrá difundirla o transmitirla a otros proveedores ajenos a la transacción, salvo autorización expresa del propio consumidor o por requerimiento de autoridad competente;*
> *II. El proveedor utilizará alguno de los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por el consumidor e informará a éste, previamente a la celebración de la transacción, de las características generales de dichos elementos;*

[294] Recomendation of the OECD Council Concerning Guidelines for Consumer Protection in the context of Electronic Commerce (Recomendación del Consejo del la OCDE relativa a los Lineamientos para la Protección al Consumidor en el contexto del Comercio Electrónico), 9 de diciembre de 1999, traducción al español de la Secretaría de Comercio y Fomento Industrial y la Procuraduría Federal del Consumidor, 10 pp.
[295] OECD. Gateways to the Global Market: Consumers and Electronic Commerce, Reporte del Foro: Caminos al Mercado Global: los consumidores y el comercio electrónico, Marzo de 1997,l Comité de Política del Consumidor, Paris, p.136.

III. El proveedor deberá proporcionar al consumidor, antes de celebrar la transacción, su domicilio físico, números telefónicos y demás medios a los que pueda acudir el propio consumidor para presentarle sus reclamaciones o solicitarle aclaraciones;
IV. El proveedor evitará las prácticas comerciales engañosas respecto de las características de los productos, por lo que deberá cumplir con las disposiciones relativas a la información y publicidad de los bienes y servicios que ofrezca, señaladas en esta Ley y demás disposiciones que se deriven de ella;
V. El consumidor tendrá derecho a conocer toda la información sobre los términos, condiciones, costos, cargos adicionales, en su caso, formas de pago de los bienes y servicios ofrecidos por el proveedor;
VI. El proveedor respetará la decisión del consumidor en cuanto a la cantidad y calidad de los productos que desea recibir, así como la de no recibir avisos comerciales, y
VII. El proveedor deberá abstenerse de utilizar estrategias de venta o publicitarias que no proporcionen al consumidor información clara y suficiente sobre los servicios ofrecidos, en especial tratándose de prácticas de mercadotecnia dirigidas a la población vulnerable, como los niños, ancianos y enfermos, incorporando mecanismos que adviertan cuando la información no sea apta para esa población.

a) La confidencialidad de los datos otorgados por el consumidor al proveedor, asegurando la no transmisión de los datos a otro proveedor, salvo autorización, también haciendo uso de los elementos técnicos que brinden la debida seguridad y confidencialidad.
b) El proveedor deberá otorgar al consumidor sus teléfonos y domicilio fiscal para el caso de alguna reclamación.
c) Con una fracción muy débil debido a la palabra 'evitará' se intenta que los proveedores no utilicen medios engañosos para ofertar el producto, por lo que deben otorgar datos veraces de la información y características del mismo. Este deber provoca que el consumidor tenga el derecho a conocer toda la información sobre condiciones, términos, costo, cargas, forma de pago, etc., sobre el producto ofertado, se debe tomar en consideración:[296]

Desde el 29 de mayo de 2000 hasta hoy la LFPC ha sufrido 19 reformas, las cuales han intentado adaptarse e integrar a nuevas formas de comercio que ofrecen nuevos y substanciales beneficios a los consumidores, incluyendo el acceso a diversos bienes y servicios. En el capítulo V de este trabajo, precisamos el por qué dichos intentos han sido insuficientes e ineficaces.

4.2.2.1. Normas y principios básicos de protección al consumidor

Son principios básicos en las relaciones de consumo[297]: a) la protección de la vida, salud y seguridad del consumidor contra los riesgos provocados por productos, prácticas en el abastecimiento de productos y servicios considerados peligrosos o nocivos; b) la educación y divulgación sobre el consumo adecuado de los productos y servicios, que garanticen la libertad para escoger y la equidad en las contrataciones; c) la información adecuada y clara sobre los

[296] Acosta Romero, Miguel y Lara Luna, Julieta Arelí. Nuevo derecho mercantil, 1. ed., 2000, México, Porrúa, p. 524.
[297] La taxonomía para presentar la información respecto a los temas relevantes en material de protección al consumidor fue tomada de la clasificación que hace Pina Vara en Derecho Mercantil Mexicano, 2005, 30ª ed., Porrúa, México, p. 210 a 221.

diferentes productos y servicios, con especificación correcta de cantidad, características, composición, calidad y precio, así como sobre los riesgos que representen; d) la efectiva prevención y reparación de daños patrimoniales y morales, individuales o colectivos; e) el acceso a los órganos administrativos con vistas a la prevención de daños patrimoniales y morales, individuales o colectivos, garantizando la protección jurídica, económica, administrativa y técnica a los consumidores; f) el otorgamiento de información y de facilidades a los consumidores para la defensa de sus derechos; g) la protección contra la publicidad engañosa y abusiva, métodos comerciales coercitivos y desleales, así como contra prácticas y cláusulas abusivas o impuestas en el abastecimiento de productos y servicios; h) la real y efectiva protección al consumidor en las transacciones efectuadas a través del uso de medios convencionales, electrónicos, ópticos o de cualquier otra tecnología y la adecuada utilización de los datos aportados; e, i) el respeto a los derechos y obligaciones derivados de las relaciones de consumo y las medidas que garanticen su efectividad y cumplimiento (artículo 1o de la LFPC).

4.2.2.2. Sujetos: Obligaciones y Derechos del consumidor y proveedor.

Son sujetos de la ley, los proveedores y los consumidores así como las entidades de las administraciones públicas federal, estatal, municipal y del gobierno del Distrito Federal, cuando tengan el carácter de proveedores o consumidores.

La ley define al *consumidor* como la *persona física o moral que adquiere, realiza o disfruta como destinatario final bienes, productos o servicios*. No se consideran consumidores a las personas morales que adquieran bienes o servicios para integrarlos en procesos de producción o de servicios a terceros, a menos que estén acreditadas como microempresas o microindustrias en términos de la Ley para el Desarrollo de la Competitividad de la Micro, Pequeña y Mediana Empresa y de la Ley Federal para el Fomento de la Microindustria y la Actividad Artesanal, respectivamente y conforme a los requisitos que se establezcan el Reglamento de la ley.

Mientras que por *proveedor* se entiende que es la *persona física o moral en términos del CCiF, que habitual o periódicamente ofrece, distribuye, vende, arrienda o concede el uso o disfrute de bienes, productos y servicios* (artículos 2 y 6 LPFC).

Se excluye de los *proveedores* a los servicios que se presten en virtud de una relación o contrato de trabajo, los servicios profesionales que no sean de carácter mercantil y los servicios que presten las sociedades de información crediticia; así como también a los servicios regulados por las leyes financieras que presten las instituciones y organizaciones cuya supervisión o vigilancia esté a cargo de la Comisión Nacional Bancaria y de Valores; de Seguros y Fianzas; del Sistema de Ahorro para el Retiro o de cualquier órgano de regulación, de supervisión o de protección y defensa dependiente de la Secretaría de Hacienda y Crédito Público (SHCP)[298].

Son obligaciones de los proveedores:

[298] Véase artículo 5 LPFC.

a) Informar y respetar los precios, tarifas, garantías, cantidades, calidades, medidas, intereses, cargos, términos, plazos, fechas, modalidades, reservaciones y demás condiciones conforme a las cuales se hubiera ofrecido, obligado o convenido con el consumidor la entrega del bien o prestación del servicio, y bajo ninguna circunstancia serán negados estos bienes o servicios a persona alguna;
b) Exhibir de forma notoria y visible el monto total a pagar por los bienes, productos o servicios que ofrezca al consumidor, donde dicho monto deberá incluir impuestos, comisiones, intereses, seguros y cualquier otro costo, cargo, gasto o erogación adicional que se requiera cubrir con motivo de la adquisición o contratación respectiva, sea ésta al contado o a crédito;
c) Respetar el precio máximo y las tarifas establecidas conforme a la obligación anterior;
d) Entregar al consumidor factura, recibo o comprobante, en el que consten los datos específicos de la compraventa, servicio prestado u operación realizada;
e) Permitir al personal acreditado de la Procuraduría el acceso al lugar o lugares objeto de la verificación;
f) Proporcionar a la Procuraduría, en un término no mayor de quince días, la información o documentación necesaria que les sea requerida para el cumplimiento de sus atribuciones, así como para sustanciar los procedimientos a que se refiere esta ley;
g) Que la información o publicidad relativa a bienes, productos o servicios que se difundan por cualquier medio o forma, sean veraces, comprobables y exentos de textos, diálogos, sonidos, imágenes, marcas, denominaciones de origen y otras descripciones que induzcan o puedan inducir a error o confusión por engañosas o abusivas;
h) Cumplir con su ofrecimiento;
i) No negar o condicionar al consumidor los bienes, productos o servicios por razones de género, nacionalidad, étnicas, preferencia sexual, religiosas o cualquiera otra particularidad;
j) No establecer preferencias o discriminación alguna respecto a los solicitantes del servicio;
k) Dar las facilidades o contar con los dispositivos indispensables para que las personas con discapacidad puedan utilizar los bienes o servicios que ofrecen; y,
l) Otorgar garantía del bien o servicio que se ofrezca que no podrá ser inferior a sesenta días contados a partir de la entrega del bien o la prestación total del servicio (artículo 7, 7 bis, 8, 12, 13, 32, 42, 50, 58, 77 y 84 LPFC).

Queda prohibido a los proveedores:

a) Llevar a cabo acciones que atenten contra los derechos del consumidor y por los de sus colaboradores, subordinados y toda clase de vigilantes, guardias o personal auxiliar que les presten sus servicios, independientemente de la responsabilidad personal en que incurra el infractor;
b) Atentar contra la libertad o seguridad o integridad personales de los consumidores bajo pretexto de registro o averiguación. En el caso de que alguien sea sorprendido en la comisión flagrante de un delito, los proveedores, sus agentes o empleados se limitarán, bajo su responsabilidad, a poner sin demora al presunto infractor a disposición de la autoridad competente;
c) Aplicar métodos o prácticas comerciales coercitivas y desleales, ni cláusulas o condiciones abusivas o impuestas en el abastecimiento de productos o servicios;

d) Prestar servicios adicionales a los originalmente contratados que no hubieren sido solicitados o aceptados expresamente, por escrito o por vía electrónica, por el consumidor; e) Negar al consumidor la venta, adquisición, renta o suministro de bienes o servicios que se tengan en existencia. Tampoco podrá condicionarse la venta, adquisición o renta de otro producto o prestación de un servicio. Se presume la existencia de productos o servicios cuando éstos se anuncien como disponibles;
f) Elaborar convenios, códigos de conducta o cualquier otra forma de colusión entre proveedores, publicistas o cualquier grupo de personas para restringir la información que se pueda proporcionar a los consumidores;
g) Negar o condicionar bienes, productos o servicios al consumidor por razones de género, nacionalidad, étnicas, preferencia sexual, religiosas o cualquiera otra particularidad;
h) Establecer preferencias o discriminación alguna respecto a los solicitantes del servicio, tales como selección de clientela, condicionamiento del consumo, reserva del derecho de admisión, exclusión a personas con discapacidad y otras prácticas similares, salvo por causas que afecten la seguridad o tranquilidad del establecimiento, de sus clientes o de las personas discapacitadas, o se funden en disposiciones expresas de otros ordenamientos legales; e
i) Aplicar o cobrar tarifas superiores a las autorizadas o registradas para la clientela en general, ni ofrecer o aplicar descuentos en forma parcial o discriminatoria. Tampoco podrán aplicar o cobrar cuotas extraordinarias o compensatorias a las personas con discapacidad por sus implementos médicos, ortopédicos, tecnológicos, educativos o deportivos necesarios para su uso personal, incluyéndose el perro guía en el caso de invidentes (artículo 9,10, 43, 45, 58 LFPC).

Son derechos del consumidor además de los señalados en el párrafo previo al anterior:

a) Recuperar, en el momento de su devolución, la suma íntegra que haya erogado por depósito o envase o empaque del producto;
b) Cuando el cobro se le haga mediante cargo directo a una cuenta de crédito, débito o similar del consumidor, el cargo no podrá efectuarse sino hasta la entrega del bien, o la prestación del servicio, excepto cuando exista consentimiento expreso del consumidor para que éstas se realicen posteriormente;
c) Que le sea indicado en la publicidad el nombre, domicilio, teléfono y, en su defecto, la dirección electrónica del proveedor; de la empresa que, en su caso, envíe la publicidad a nombre del proveedor, y de la Procuraduría;
d) Exigir directamente a proveedores específicos y a empresas que no utilicen información sobre consumidores con fines mercadotécnicos o publicitarios, a no ser molestado en su domicilio, lugar de trabajo, dirección electrónica o por cualquier otro medio, para ofrecerle bienes, productos o servicios, y que no le envíen publicidad;
e) Exigir a proveedores y a empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios, que la información relativa a él mismo no sea cedida o transmitida a terceros, salvo que dicha cesión o transmisión sea determinada por una autoridad judicial;
f) Que se le cumpla lo ofrecido ante la falta de veracidad en los informes, instrucciones, datos y condiciones prometidas o sugeridas o a la reposición de los gastos necesarios que pruebe haber

efectuado el adquirente y, en su caso, al pago de la bonificación o compensación del veinte por ciento del precio pagado;
g) Cuando el autor la promoción u oferta no cumple su ofrecimiento, el consumidor podrá optar por exigir el cumplimiento, aceptar otro bien o servicio equivalente o la rescisión del contrato y, en todo caso, tendrá derecho al pago de la diferencia económica entre el precio al que se ofrezca el bien o servicio objeto de la promoción u oferta y su precio normal, sin perjuicio de la bonificación o compensación del veinte por ciento del precio pagado;
h) A elegir entre la reposición del producto o a la devolución de la cantidad pagada, contra la entrega del producto adquirido, y en todo caso, a una bonificación, en los siguientes casos:

h.1) Cuando el contenido neto de un producto o la cantidad entregada sea menor a la indicada en el envase, recipiente, empaque o cuando se utilicen instrumentos de medición que no cumplan con las disposiciones aplicables, considerados los límites de tolerancia permitidos por la normatividad,

h.2) Si el bien no corresponde a la calidad, marca, o especificaciones y demás elementos sustanciales bajo los cuales se haya ofrecido o no cumple con las normas oficiales mexicanas;

h.3) Si el bien reparado no queda en estado adecuado para su uso o destino, dentro del plazo de garantía (artículo 11, 15, 17, 37, 50 y 92 LFPC).

Además, el artículo 14 de la LFPC establece el plazo de prescripción de un año, salvo otros términos previstos por esta ley. En caso de afectaciones a los derechos de las niñas, niños y adolescentes, el término de prescripción será de diez años.

Finalmente, las disposiciones enfocadas al tema de protección al consumidor en el comercio electrónico, son las que la LFPC denomina: *transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología,* en ellas tanto proveedores y consumidores deberán cumplir con lo siguiente:

I. El proveedor utilizará la información proporcionada por el consumidor en forma confidencial, por lo que no podrá difundirla o transmitirla a otros proveedores ajenos a la transacción, salvo autorización expresa del propio consumidor o por requerimiento de autoridad competente;
II. El proveedor utilizará alguno de los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por el consumidor e informará a éste, previamente a la celebración de la transacción, de las características generales de dichos elementos;
III. El proveedor deberá proporcionar al consumidor, antes de celebrar la transacción, su domicilio físico, números telefónicos y demás medios a los que pueda acudir el propio consumidor para presentarle sus reclamaciones o solicitarle aclaraciones;
IV. El proveedor evitará las prácticas comerciales engañosas respecto de las características de los productos, por lo que deberá cumplir con las disposiciones relativas a la información y publicidad de los bienes y servicios que ofrezca, señaladas en esta Ley y demás disposiciones que se deriven de ella;
V. El consumidor tendrá derecho a conocer toda la información sobre los términos, condiciones, costos, cargos adicionales, en su caso, formas de pago de los bienes y servicios ofrecidos por el proveedor;

VI. El proveedor respetará la decisión del consumidor en cuanto a la cantidad y calidad de los productos que desea recibir, así como la de no recibir avisos comerciales, y,
VII. El proveedor deberá abstenerse de utilizar estrategias de venta o publicitarias que no proporcionen al consumidor información clara y suficiente sobre los servicios ofrecidos, y cuidará las prácticas de mercadotecnia dirigidas a población vulnerable, como niños, ancianos y enfermos, incorporando mecanismos que adviertan cuando la información no sea apta para esa población. Las infracciones este tipo de transacciones serán sancionadas con multa por el equivalente de una y hasta dos mil quinientas veces el salario mínimo general vigente para el Distrito Federal (artículos 76 y 128 LFPC)[299].

4.2.2.3. Garantías.

Todo bien o servicio que se ofrezca con garantía deberá sujetarse a lo dispuesto por LA LFPC y a lo pactado entre proveedores y consumidor, la cual no podrá ser inferior a sesenta días contados a partir de la entrega del bien o la prestación total del servicio. Las garantías ofrecidas no pueden ser inferiores a las que determinen las disposiciones aplicables ni prescribir condiciones o limitaciones que reduzcan los derechos que legalmente corresponden al consumidor. El cumplimiento de las garantías es exigible, indistintamente, al productor y al importador del bien o servicio, así como al distribuidor, salvo en los casos en que alguno de ellos o algún tercero asuma por escrito la obligación. El cumplimiento de las garantías deberá realizarse en el domicilio en que haya sido adquirido o contratado el bien o servicio, o en el lugar o lugares que exprese la propia póliza. El proveedor deberá cubrir al consumidor los gastos necesarios erogados para lograr el cumplimiento de la garantía en domicilio diverso al antes señalado (artículos 77 y 79 LFPC).

El consumidor puede optar por pedir la restitución del bien o servicio, la rescisión del contrato o la reducción del precio, y en cualquier caso, la bonificación o compensación, cuando la cosa u objeto del contrato tenga defectos o vicios ocultos que la hagan impropia para los usos a que habitualmente se destine, que disminuyan su calidad o la posibilidad de su uso, o no ofrezca la seguridad que dada su naturaleza normalmente se espere de ella y de su uso razonable. Cuando el consumidor opte por la rescisión, el proveedor tiene la obligación de reintegrarle el precio pagado y, en su caso, los intereses a que se refiere el segundo párrafo del artículo 91 de esta ley, sin perjuicio de la indemnización que en su caso corresponda por daños y perjuicios (artículo 82 de la LFPC).

Los productores deberán asegurar y responder del suministro oportuno de partes y refacciones, así como del servicio de reparación, durante el término de vigencia de la garantía y, posteriormente, durante el tiempo en que los productos sigan fabricándose, armándose o distribuyéndose. Mediante normas oficiales mexicanas la SE podrá disponer que determinados productos deban ser respaldados con una garantía de mayor vigencia por lo que se refiere al suministro de partes y refacciones, tomando en cuenta la durabilidad del producto.

[299] Decreto del 29 de mayo de 2000 por el que se reforman y adicionan los siguientes instrumentos jurídicos nacionales: CCiF, Código Federal de Procedimientos Civiles, CCo y la LFPC, SECOFI, p. 6.

Finalmente, el tiempo que duren las reparaciones efectuadas al amparo de la garantía no es computable dentro del plazo de la misma. Cuando el bien haya sido reparado se iniciará la garantía respecto de las piezas repuestas y continuará con relación al resto. En el caso de reposición del bien deberá renovarse el plazo de la garantía (artículo 80 y 83 de la LFPC).

4.2.2.4. Precios

El artículo 34 de la Ley Orgánica de la APF faculta a la SE a establecer la política de precios, y con el auxilio y participación de las autoridades locales, vigilar su estricto cumplimiento, particularmente en lo que se refiere a artículos de consumo y uso popular, y establecer las tarifas para la prestación de aquellos servicios de interés público que considere necesarios, con la exclusión de los precios y tarifas de los bienes y servicios de la APF; y definir el uso preferente que deba darse a determinadas mercancías.

La Procuraduría tiene la facultad de vigilar y verificar el cumplimiento de las disposiciones en materia de precios y tarifas establecidos o registrados por la autoridad competente y coordinarse con otras autoridades legalmente facultadas para inspeccionar precios para lograr la eficaz protección de los intereses del consumidor y, a la vez evitar duplicación de funciones (artículo 24, frac. XII de la LFPC)

Los pagos hechos en exceso del precio máximo determinado o, en su caso, estipulado, son recuperables por el consumidor. Si el proveedor no devuelve la cantidad cobrada en exceso dentro del término de 5 días hábiles siguientes a la reclamación además de la sanción que corresponda, estará obligado a pagar el máximo de los intereses a que se refiere este artículo. La acción para solicitar esta devolución prescribe en un año a partir de la fecha en que tuvo lugar el pago. Los intereses se calcularán con base en el costo porcentual promedio de captación que determine el Banco de México, o cualquiera otra tasa que la sustituya oficialmente como indicador del costo de los recursos financieros (artículo 91 de la LFPC).

4.2.2.5. Publicidad e información

Tratándose de servicios, los proveedores que ofrezcan diversos planes y modalidades de comercialización, deberán informar al consumidor sobre las características, condiciones y costo total de cada uno de ellos. En el caso de que únicamente adopten un plan específico de comercialización de servicios, tales como paquetes o sistemas todo incluido, deberán informar a los consumidores con oportunidad y en su publicidad, lo que incluyen tales planes y que no disponen de otros.

Tratándose de contratos de tracto sucesivo, el proveedor podrá realizar una investigación de crédito para asegurarse que el consumidor está en condiciones de cumplirlo; igualmente, no se considerará que se viole esta disposición cuando haya un mayor número de solicitantes que el de bienes o servicios disponibles (artículo 43 de la LFPC)

La información o publicidad relativa a bienes, productos o servicios que se difundan por cualquier medio o forma, deberán ser veraces, comprobables y exentos de textos, diálogos, sonidos, imágenes, marcas, denominaciones de origen y otras descripciones que induzcan o puedan inducir a error o confusión por engañosas o abusivas. Se entiende por información o publicidad engañosa o abusiva aquella que refiere características o información relacionadas con algún bien, producto o servicio que pudiendo o no ser verdaderas, inducen a error o confusión al consumidor por la forma inexacta, falsa, exagerada, parcial, artificiosa o tendenciosa en que se presenta.

La información o publicidad que compare productos o servicios, sean de una misma marca o de distinta, no podrá ser engañosa o abusiva en términos de lo dispuesto en el párrafo anterior. Mientras que la información de productos importados expresará su lugar de origen y, en su caso, los lugares donde puedan repararse, así como las instrucciones para su uso y las garantías correspondientes.

Además, los datos que ostenten los productos o sus etiquetas, envases y empaques y la publicidad respectiva, tanto de manufactura nacional como de procedencia extranjera, se expresarán en idioma español y su precio en moneda nacional en términos comprensibles y legibles conforme al sistema general de unidades de medida, sin perjuicio de que, además, se expresen en otro idioma u otro sistema de medida (artículo 32, 33 y 34 de la LFPC).

Cuando se trate de productos o servicios que de conformidad con las disposiciones aplicables, se consideren potencialmente peligrosos para el consumidor o lesivos para el medio ambiente o cuando sea previsible su peligrosidad, el proveedor deberá incluir un instructivo que advierta sobre sus características nocivas y explique con claridad el uso o destino recomendado y los posibles efectos de su uso, aplicación o destino fuera de los lineamientos recomendados. El proveedor responderá de los daños y perjuicios que cause al consumidor la violación de esta disposición, sin perjuicio de la bonificación del veinte por ciento del precio pagado (artículo 41 de la LFPC)

Cuando se expendan al público productos con alguna deficiencia, usados o reconstruidos, deberá advertirse de manera precisa y clara tales circunstancias al consumidor y hacerse constar en los propios bienes, envolturas, notas de remisión o facturas correspondientes. (artículo 39 de la LFPC)

La Procuraduría podrá:

a) Ordenar al proveedor que suspenda la información o publicidad que viole las disposiciones de esta ley y, en su caso, al medio que la difunda;
b) Ordenar que se corrija la información o publicidad que viole las disposiciones de esta ley en la forma en que se estime suficiente; y,
c) Imponer las sanciones que correspondan, en términos de esta ley (artículo 35 de la LFPC).

4.2.2.6. Sistemas de ventas y prácticas comerciales

La SE determinará la política de protección al consumidor y está facultada para expedir normas oficiales mexicanas y normas mexicanas respecto de los requisitos que deberán cumplir los sistemas y prácticas de comercialización de bienes, entre las que están: las promociones, ofertas y ventas a domicilio (artículo 19, de la LFPC).

Para los efectos de la ley, se consideran promociones las prácticas comerciales consistentes en el ofrecimiento al público de bienes o servicios que cuenten:

a) Con el incentivo de proporcionar adicionalmente otro bien o servicio iguales o diversos, en forma gratuita, a precio reducido o a un solo precio;
b) Con un contenido adicional en la presentación usual de un producto, en forma gratuita o a precio reducido;
c) Con figuras o leyendas impresas en las tapas, etiquetas, o envases de los productos o incluidas dentro de aquéllos, distintas a las que obligatoriamente deben usarse; y
d) Con el incentivo de participar en sorteos, concursos y otros eventos similares.

Por "oferta", "barata", "descuento", "remate" o cualquier otra expresión similar se entiende el ofrecimiento al público de productos o servicios de la misma calidad a precios rebajados o inferiores a los normales del establecimiento (artículo 46 de la LFPC).

En las promociones y ofertas se observarán las siguientes reglas:

I. En los anuncios respectivos deberán indicarse las condiciones, así como el plazo de duración o el volumen de los bienes o servicios ofrecidos; dicho volumen deberá acreditarse a solicitud de la autoridad. Si no se fija plazo ni volumen, se presume que son indefinidos hasta que se haga del conocimiento público la revocación de la promoción o de la oferta, de modo suficiente y por los mismos medios de difusión, y
II. Todo consumidor que reúna los requisitos respectivos tendrá derecho a la adquisición, durante el plazo previamente determinado o en tanto exista disponibilidad, de los bienes o servicios de que se trate (artículo 48 de la LFPC).

No se necesitará autorización ni aviso para llevar a cabo promociones, excepto cuando así lo dispongan las normas oficiales mexicanas, en los casos en que se lesionen o se puedan lesionar los intereses de los consumidores. No podrán imponerse restricciones a la actividad comercial en adición a las señaladas en esta ley, ni favorecer específicamente las promociones u ofertas de proveedores determinados (artículo 47 de la LFPC).

Cuando el autor de la promoción u oferta no cumple su ofrecimiento, el consumidor podrá optar por exigir el cumplimiento, aceptar otro bien o servicio equivalente o la rescisión del contrato y, en todo caso, tendrá derecho al pago de la diferencia económica entre el precio al que se ofrezca el bien o servicio objeto de la promoción u oferta y su precio normal, sin perjuicio de la bonificación o compensación del 20 veinte por ciento del precio (artículo 50 de la LFPC).

4.2.2.7. Ventas a domicilio, mediatas o indirectas

Por venta a domicilio, mediata o indirecta, se entiende la que se proponga o lleve a cabo fuera del local o establecimiento del proveedor, incluidos el arrendamiento de bienes muebles y la prestación de servicios. Lo dispuesto no es aplicable a la compraventa de bienes perecederos recibidos por el consumidor y pagados de contado. (artículo 51 de la LFPC). En este respecto debe considerarse que una venta a domicilio mediata o indirecta no es una venta en línea o vía electrónica o a distancia, pues la Ley regula específicamente este caso, el cual se verá adelante.

Los proveedores que realicen venta a domicilio, mediata o indirecta por medios en los cuales sea imposible la entrega del documento al celebrarse la transacción, tales como teléfono, televisión, servicios de correo o mensajería u otros en que no exista trato directo con el comprador, deberán: a) Cerciorarse de que la entrega del bien o servicio efectivamente se hace en el domicilio del consumidor o que el consumidor está plenamente identificado; b) Permitir al consumidor hacer reclamaciones y devoluciones por medios similares a los utilizados para la venta; c) Cubrir los costos de transporte y envío de mercancía en caso de haber devoluciones o reparaciones amparadas por la garantía, salvo pacto en contrario; d) Informar previamente al consumidor el precio, fecha aproximada de entrega, costos de seguro y flete y, en su caso, la marca del bien o servicio (artículo 53 de la LFPC).

Las ventas a domicilio, mediatas o indirectas deberán constar por escrito y contener:

a) Nombre y dirección del proveedor e identificación de la operación y de los bienes y servicios de que se trate; y,
b) Garantías y requisitos señalados por esta ley. El proveedor está obligado a entregar al consumidor una copia del documento respectivo. El contrato se perfeccionará a los cinco días hábiles contados a partir de la entrega del bien o de la firma del contrato, lo último que suceda.

Durante ese lapso, el consumidor tendrá la facultad de revocar su consentimiento sin responsabilidad alguna. La revocación deberá hacerse mediante aviso o entrega del bien en forma personal, por correo registrado, o por otro medio fehaciente. La revocación hecha conforme a este artículo deja sin efecto la operación, debiendo el proveedor reintegrar al consumidor el precio pagado. En este caso, los costos de flete y seguro correrán a cargo del consumidor. Tratándose de servicios, lo anterior no será aplicable si la fecha de prestación del servicio se encuentra a diez días hábiles o menos de la fecha de la orden de compra (artículos 52 y 56 de la LFPC).

En este apartado, se hace notar que las disposiciones relativas a las ventas a domicilio, mediatas o indirectas, que regula el artículo 51 de la LFPC, no son reglas aplicables a las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología.

4.2.2.8. Servicios

El proveedor de bienes, productos o servicios no podrá negarlos o condicionarlos al consumidor por razones de género, nacionalidad, étnicas, preferencia sexual, religiosas o cualquiera otra particularidad, ni podrán establecer preferencias o discriminación alguna respecto a los solicitantes del servicio, tales como selección de clientela, condicionamiento del consumo, reserva del derecho de admisión, exclusión a personas con discapacidad y otras prácticas similares, salvo por causas que afecten la seguridad o tranquilidad del establecimiento, de sus clientes o de las personas discapacitadas, o se funden en disposiciones expresas de otros ordenamientos legales.

Dichos proveedores en ningún caso podrán aplicar o cobrar tarifas superiores a las autorizadas o registradas para la clientela en general, ni ofrecer o aplicar descuentos en forma parcial o discriminatoria. Tampoco podrán aplicar o cobrar cuotas extraordinarias o compensatorias a las personas con discapacidad por sus implementos médicos, ortopédicos, tecnológicos, educativos o deportivos necesarios para su uso personal, incluyéndose el perro guía en el caso de invidentes.

Los proveedores están obligados a dar las facilidades o contar con los dispositivos indispensables para que las personas con discapacidad puedan utilizar los bienes o servicios que ofrecen. (artículo 58 de la LFPC)

Los prestadores de servicios están obligados a:

a) Exhibir a la vista del público la tarifa de los principales servicios ofrecidos, con caracteres claramente legibles. Las tarifas de los demás, en todo caso, deberán estar disponibles al público;
b) Antes de la prestación de un servicio, el proveedor deberá presentar presupuesto por escrito;
c) En caso de reparaciones, el presupuesto deberá describir las características del servicio, el costo de refacciones y mano de obra, así como su vigencia, independientemente de que se estipulen mecanismos de variación de rubros específicos por estar sus cotizaciones fuera del control del proveedor; y
d) Expedir factura o comprobante de los trabajos efectuados, en los que deberán especificarse las partes, refacciones y materiales empleados; el precio de ellos y de la mano de obra; la garantía que en su caso se haya otorgado (artículo 57, 59 y 62 de la LFPC).

Las personas dedicadas a la reparación de toda clase de productos deberán emplear partes y refacciones nuevas y apropiadas para el producto de que se trate, salvo que el solicitante del servicio autorice expresamente que se utilicen otras. Cuando las refacciones o partes estén sujetas a normas de cumplimiento obligatorio, el uso de refacciones o partes que no cumplan con los requisitos da al consumidor el derecho a exigir los gastos necesarios que pruebe haber efectuado y, en su caso, a la bonificación del veinte por ciento del precio pagado. Los prestadores de servicios de mantenimiento o reparación deberán bonificar al consumidor en términos del artículo 92 TER si por deficiencia del servicio el bien se pierde o sufre tal deterioro que resulte total o parcialmente inapropiado para el uso a que esté destinado (artículo 60 y 61 de la LFPC).

La ley regula tres tipos especiales de servicios:

a) Los sistemas de comercialización consistentes en la integración de grupos de consumidores que aportan periódicamente sumas de dinero para ser administradas por un tercero, únicamente podrán operar para efectos de adquisición de bienes determinados o determinables, sean muebles nuevos o inmuebles destinados a la habitación o a su uso como locales comerciales, en los términos que señale el reglamento respectivo, y sólo podrán ponerse en práctica previa autorización de la Secretaría, pero su plazo de operación no podrá ser mayor a cinco años para bienes muebles y de quince años para bienes inmuebles;
b) El servicio de tiempo compartido sólo podrá iniciarse cuando el contrato respectivo esté registrado en la Procuraduría y;
c) Las casas de empeño que son los proveedores personas físicas o sociedades mercantiles no reguladas por leyes y autoridades financieras que en forma habitual o profesional realicen u oferten al público contrataciones u operaciones de mutuo con interés y garantía prendaria, tales personas no podrán prestar servicios ni realizar operaciones de las reservadas y reguladas por las leyes vigentes a las instituciones del sistema financiero nacional (artículos 63, 64 y 65 de la LFPC).

4.2.2.9. Operaciones de crédito

En toda operación a crédito al consumidor, se deberá:

a) Informar al consumidor previamente sobre el precio de contado del bien o servicio de que se trate, el monto y detalle de cualquier cargo si lo hubiera, el número de pagos a realizar, su periodicidad, el derecho que tiene a liquidar anticipadamente el crédito con la consiguiente reducción de intereses, en cuyo caso no se le podrán hacer más cargos que los de renegociación del crédito, si la hubiere. Los intereses, incluidos los moratorios, se calcularán conforme a una tasa de interés fija o variable;
b) De existir descuentos, bonificaciones o cualquier otro motivo por el cual sean diferentes los pagos a crédito y de contado, dicha diferencia deberá señalarse al consumidor;
c) De utilizarse una tasa fija, también se informará al consumidor el monto de los intereses a pagar en cada período;
d) De utilizarse una tasa variable, se informará al consumidor sobre la regla de ajuste de la tasa, la cual no podrá depender de decisiones unilaterales del proveedor sino de las variaciones que registre una tasa de interés representativa del costo del crédito al consumidor, la cual deberá ser fácilmente verificable por el consumidor;
e) Informar al consumidor el monto total a pagar por el bien, producto o servicio de que se trate, que incluya, en su caso, número y monto de pagos individuales, los intereses, comisiones y cargos correspondientes, incluidos los fijados por pagos anticipados o por cancelación; proporcionándole debidamente desglosados los conceptos correspondientes;
f) Respetarse el precio que se haya pactado originalmente en operaciones a plazo o con reserva de dominio, salvo lo dispuesto en otras leyes o convenio en contrario; y

g) En caso de haberse efectuado la operación, el proveedor deberá enviar al consumidor al menos un estado de cuenta bimestral, por el medio que éste elija, que contenga la información relativa a cargos, pagos, intereses y comisiones, entre otros rubros. (artículos 66 de la LFPC).

Para el cálculo y aplicación de intereses la ley incluye tres prevenciones:

a) En los contratos de compraventa a plazo o de prestación de servicios con pago diferido, se calcularán los intereses sobre el precio de contado menos el enganche que se hubiera pagado;
b) Únicamente se podrán capitalizar intereses cuando exista acuerdo previo de las partes, en cuyo caso el proveedor deberá proporcionar al consumidor estado de cuenta mensual (es improcedente el cobro que contravenga esto); y
c) Los intereses se causarán exclusivamente sobre los saldos insolutos del crédito concedido y su pago no podrá ser exigido por adelantado, sino únicamente por períodos vencidos (Artículos 67, 68 y 69 de la LFPC).

En los casos de compraventa a plazos de bienes muebles o inmuebles, si se rescinde el contrato, el vendedor y comprador deben restituirse mutuamente las prestaciones que se hubieren hecho; el vendedor que hubiera entregado la cosa tendrá derecho a exigir por el uso de ella el pago de un alquiler o renta y, en su caso, una compensación por el demérito que haya sufrido el bien; mientras que el comprador que haya pagado parte del precio tiene derecho a recibir los intereses computados conforme a la tasa que, en su caso, se haya aplicado a su pago (artículo 70 de la LFPC).

En los casos de operaciones en que el precio deba cubrirse en exhibiciones periódicas, cuando se haya pagado más de la tercera parte del precio o del número total de los pagos convenidos y el proveedor exija la rescisión o cumplimiento del contrato por mora, el consumidor tendrá derecho a optar por la rescisión en los términos del artículo anterior o por el pago del adeudo vencido más las prestaciones que legalmente procedan. Los pagos que realice el consumidor, aún en forma extemporánea y que sean aceptados por el proveedor, liberan a aquél de las obligaciones inherentes a dichos pagos (artículo 71 de la LFPC).

4.2.2.10. Operaciones con inmuebles

Los actos relacionados con inmuebles sólo estarán sujetos de protección al consumidor, cuando los proveedores sean fraccionadores, constructores, promotores y demás personas que intervengan en la asesoría y venta al público de viviendas destinadas a casa habitación o cuando otorguen al consumidor el derecho de usar inmuebles mediante el sistema de tiempo compartido, en los términos de los artículos 64 y 65 de la presente ley.

El proveedor deberá poner a disposición del consumidor al menos lo siguiente:

I. En caso de preventa, el proveedor deberá exhibir el proyecto ejecutivo de construcción completa, así como la maqueta respectiva y, en su caso, el inmueble muestra;

II. Los documentos que acrediten la propiedad del inmueble. Asimismo, deberá informar sobre la existencia de gravámenes que afecten la propiedad del mismo, los cuales deberán quedar cancelados al momento de la firma de la escritura correspondiente;
III. La personalidad del vendedor y la autorización del proveedor para promover la venta;
IV. Información sobre las condiciones en que se encuentre el pago de contribuciones y servicios públicos;
V. Para el caso de inmuebles nuevos o preventas, las autorizaciones, licencias o permisos expedidos por las autoridades correspondientes para la construcción, relativas a las especificaciones técnicas, seguridad, uso de suelo, la clase de materiales utilizados en la construcción; servicios básicos con que cuenta, así como todos aquellos con los que debe contar de conformidad con la legislación aplicable. En el caso de inmuebles usados que no cuenten con dicha documentación, se deberá indicar expresamente en el contrato la carencia de éstos;
VI. Los planos estructurales, arquitectónicos y de instalaciones o, en su defecto, un dictamen de las condiciones estructurales del inmueble. En su caso, señalar expresamente las causas por las que no cuenta con ellos así como el plazo en el que tendrá dicha documentación;
VII. Información sobre las características del inmueble, como son la extensión del terreno, superficie construida, tipo de estructura, instalaciones, acabados, accesorios, lugar o lugares de estacionamiento, áreas de uso común con otros inmuebles, porcentaje de indiviso en su caso, servicios con que cuenta y estado físico general del inmueble;
VIII. Información sobre los beneficios que en forma adicional ofrezca el proveedor en caso de concretar la operación, tales como acabados especiales, encortinados, azulejos y cocina integral, entre otros;
IX. Las opciones de pago que puede elegir el consumidor, especificando el monto total a pagar en cada una de las opciones;
X. En caso de operaciones a crédito, el señalamiento del tipo de crédito de que se trata, así como una proyección del monto a pagar que incluya, en su caso, la tasa de interés que se va a utilizar, comisiones y cargos. En el caso de la tasa variable, deberá precisarse la tasa de interés de referencia y la fórmula para el cálculo de dicha tasa. De ser el caso, los mecanismos para la modificación o renegociación de las opciones de pago, las condiciones bajo las cuales se realizaría y las implicaciones económicas, tanto para el proveedor como para el consumidor;
XI. Las condiciones bajo las cuales se llevará a cabo el proceso de escrituración, así como las erogaciones distintas del precio de la venta que deba realizar el consumidor, tales como gastos de escrituración, impuestos, avalúo, administración, apertura de crédito y gastos de investigación. De ser el caso, los costos por los accesorios o complementos;
XII. Las condiciones bajo las cuales el consumidor puede cancelar la operación, y
XIII. Se deberá indicar al consumidor sobre la existencia y constitución de garantía hipotecaria, fiduciaria o de cualquier otro tipo, así como su instrumentación.

Todo bien inmueble cuya transacción esté regulada por esta Ley, deberá ofrecerse al consumidor con la garantía correspondiente, la cual no podrá ser inferior a cinco años para cuestiones estructurales y tres años para impermeabilización; para los demás elementos la garantía mínima será de un año. Todos los plazos serán contados a partir de la entrega real del bien. En el tiempo en que dure la garantía el proveedor tendrá la obligación de realizar, sin

costo alguno para el consumidor, cualquier acto tendiente a la reparación de los defectos o fallas presentados por el bien objeto del contrato.

El tiempo que duren las reparaciones efectuadas al inmueble al amparo de la garantía no es computable dentro del plazo de la misma; una vez que el inmueble haya sido reparado se iniciará la garantía respecto de las reparaciones realizadas, así como con relación a las piezas o bienes que hubieren sido repuestos y continuará respecto al resto del inmueble.

Habiendo hecho valer cualquiera de estas garantías y si persisten los defectos o fallas imputables al proveedor, éste se verá obligado de nueva cuenta a realizar todas las reparaciones necesarias para corregirlas de inmediato, así como a otorgarle, en el caso de defectos o fallas leves, una bonificación del cinco por ciento sobre el valor de la reparación; en caso de defectos o fallas graves, el proveedor deberá realizar una bonificación del veinte por ciento de la cantidad señalada en el contrato como precio del bien. Se entiende por defectos o fallas graves, aquellos que afecten la estructura o las instalaciones del inmueble y comprometan el uso pleno o la seguridad del inmueble, o bien, impidan que el consumidor lo use, goce y disfrute conforme a la naturaleza o destino del mismo. Se entenderá por defectos o fallas leves, todos aquellos que no sean graves. En caso de que los defectos o fallas graves sean determinados por el proveedor como de imposible reparación, éste podrá optar desde el momento en que se le exija el cumplimiento de la garantía, por sustituir el inmueble, en cuyo caso se estará a lo dispuesto por la fracción I siguiente, sin que haya lugar a la bonificación. En caso de que en cumplimiento de la garantía decida repararlas y no lo haga, quedará sujeto a la bonificación y a lo dispuesto en el párrafo siguiente.

Para el supuesto de que, aún después del ejercicio de la garantía y bonificación antes señaladas, el proveedor no haya corregido los defectos o fallas graves, el consumidor podrá optar por cualquiera de las dos acciones que se señalan a continuación:

I. Solicitar la sustitución del bien inmueble, en cuyo caso el proveedor asumirá todos los gastos relacionados con la misma, o
II. Solicitar la rescisión del contrato, en cuyo caso el proveedor tendrá la obligación de reintegrarle el monto pagado, así como los intereses que correspondan, conforme lo previsto en el segundo párrafo del artículo 91 de esta ley (artículos 73 bis a quintus).

Los proveedores deberán efectuar la entrega física o real del bien materia de la transacción en el plazo pactado con el consumidor y de acuerdo con las especificaciones previamente establecidas u ofrecidas.

La Procuraduría podrá promover ante la autoridad judicial, cuando vea amenazado el interés jurídico de los consumidores, el aseguramiento de los bienes a que se refiere este capítulo, en aquellas operaciones que considere de difícil o imposible cumplimiento, mientras subsista la causa de la acción (artículos 74 y 76 LFPC).

4.2.2.11. Órganos.

La PROFECO es un organismo descentralizado de servicio social con personalidad jurídica y patrimonio propio. Tiene funciones de autoridad administrativa y está encargada de promover y proteger los derechos e intereses del consumidor y procurar la equidad y seguridad jurídica en las relaciones entre proveedores y consumidores. Su funcionamiento se regirá por lo dispuesto en esta ley, los reglamentos de ésta y su estatuto (artículo 20 LFPC).

La Procuraduría tiene las siguientes atribuciones**:**

I. Promover y proteger los derechos del consumidor, así como aplicar las medidas necesarias para propiciar la equidad y seguridad jurídica en las relaciones entre proveedores y consumidores;
II. Procurar y representar los intereses de los consumidores, mediante el ejercicio de las acciones, recursos, trámites o gestiones que procedan;
III. Representar individualmente o en grupo a los consumidores ante autoridades jurisdiccionales y administrativas, y ante los proveedores;
IV. Recopilar, elaborar, procesar y divulgar información objetiva para facilitar al consumidor un mejor conocimiento de los bienes y servicios que se ofrecen en el mercado. En el caso de servicios educativos proporcionados por particulares, deberá informar a las y los consumidores, los nombres de los educadores que obtengan resultados suficientes, una vez que apliquen las evaluaciones, así como la aptitud del personal administrativo que labora en el plantel;
V. Formular y realizar programas de educación para el consumo, así como de difusión y orientación respecto de las materias a que se refiere esta ley;
VI. Orientar a la industria y al comercio respecto de las necesidades y problemas de los consumidores;
VII. Realizar y apoyar análisis, estudios e investigaciones en materia de protección al consumidor;
VIII. Promover y realizar directamente, en su caso, programas educativos y de capacitación en las materias a que se refiere esta ley y prestar asesoría a consumidores y proveedores;
IX. Promover nuevos o mejores sistemas y mecanismos que faciliten a los consumidores el acceso a bienes y servicios en mejores condiciones de mercado;
IX bis.- Promover en coordinación con la Secretaría la formulación, difusión y uso de códigos de ética, por parte de proveedores, que incorporen los principios previstos por esta Ley respecto de las transacciones que celebren con consumidores a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología;
IX Ter. Promover la coordinación entre las autoridades federales, estatales y municipales que corresponda, a fin de asegurar la protección efectiva al consumidor en contra de la información o publicidad engañosa o abusiva;
X. Actuar como perito y consultor en materia de calidad de bienes y servicios y elaborar estudios relativos;
XI. Celebrar convenios con proveedores y consumidores y sus organizaciones para el logro de los objetivos de esta ley;

XII. Celebrar convenios y acuerdos de colaboración con autoridades federales, estatales, municipales, del gobierno del Distrito Federal y entidades paraestatales en beneficio de los consumidores; así como acuerdos interinstitucionales con otros países, de conformidad con las leyes respectivas;
XIII. Vigilar y verificar el cumplimiento de las disposiciones en materia de precios y tarifas establecidos o registrados por la autoridad competente y coordinarse con otras autoridades legalmente facultadas para inspeccionar precios para lograr la eficaz protección de los intereses del consumidor y, a la vez evitar duplicación de funciones;
XIV. Vigilar y verificar el cumplimiento de las disposiciones contenidas en esta ley y, en el ámbito de su competencia, las de la Ley Federal sobre Metrología y Normalización, así como de las normas oficiales mexicanas y demás disposiciones aplicables, y en su caso determinar los criterios para la verificación de su cumplimiento;
XIV bis. Verificar que las pesas, medidas y los instrumentos de medición que se utilicen en transacciones comerciales, industriales o de servicios sean adecuados y, en su caso, realizar el ajuste de los instrumentos de medición en términos de lo dispuesto en la Ley Federal sobre Metrología y Normalización;
XV. Registrar los contratos de adhesión que lo requieran, cuando cumplan la normatividad aplicable, y organizar y llevar el Registro Público de contratos de adhesión;
XVI. Procurar la solución de las diferencias entre consumidores y proveedores y, en su caso, emitir dictámenes en donde se cuantifiquen las obligaciones contractuales del proveedor, conforme a los procedimientos establecidos en esta ley;
XVII. Denunciar ante el Ministerio Público los hechos que puedan ser constitutivos de delitos y que sean de su conocimiento y, ante las autoridades competentes, los actos que constituyan violaciones administrativas que afecten la integridad e intereses de las y los consumidores;
XVIII. Promover y apoyar la constitución de organizaciones de consumidores, proporcionándoles capacitación y asesoría, así como procurar mecanismos para su autogestión;
XIX. Aplicar las sanciones y demás medidas establecidas en esta ley, en la Ley Federal sobre Metrología y Normalización y demás ordenamientos aplicables;
XX. Requerir a los proveedores o a las autoridades competentes a que tomen medidas adecuadas para combatir, detener, modificar o evitar todo género de prácticas que lesionen los intereses de los consumidores, y cuando lo considere pertinente publicar dicho requerimiento;
XX Bis. En el caso de que en ejercicio de sus atribuciones identifique aumentos de precios, restricciones en la cantidad ofrecida o divisiones de mercados de bienes o servicios derivados de posibles prácticas monopólicas en términos de lo dispuesto por la Ley Federal de Competencia Económica, la Procuraduría, en representación de los consumidores, podrá presentar ante la COFECO la denuncia que corresponda;
XXI. Ordenar se informe a los consumidores sobre las acciones u omisiones de los proveedores que afecten sus intereses o derechos, así como la forma en que los proveedores los retribuirán o compensarán;
XXII.- Coadyuvar con las autoridades competentes para salvaguardar los derechos de la infancia, adultos mayores, personas con discapacidad e indígenas, y
XXIII.- Las demás que le confieran la ley y otros ordenamientos (Artículo 24 LFPC).

La Procuraduría, para el desempeño de las funciones que le atribuye la ley, podrá aplicar las siguientes medidas de apremio:

I. Apercibimiento;
II. Multa de $214.40 a $21,440.56;
III. En caso de que persista la infracción podrán imponerse nuevas multas por cada día que transcurra sin que se obedezca el mandato respectivo, hasta por $8,576.23, y
IV. El auxilio de la fuerza pública (artículo 25 LFPC).

Para la elaboración de sus planes y programas de trabajo, la Procuraduría llevará a cabo consultas con representantes de los sectores público, social y privado; con instituciones nacionales de educación superior, así como con organizaciones de consumidores.

Asimismo, asesorará a la SE en cuestiones relacionadas con las políticas de protección al consumidor y opinará sobre los proyectos de normas oficiales mexicanas y sobre cualquiera otra medida regulatoria que pueda afectar los derechos de los consumidores (artículos 31 de la LFPC).

4.2.3. Iniciativa a la Ley Federal de Protección al Consumidor de 2015

El 15 de octubre de 2015 diversos Senadores de la República mexicana del PRI, PAN, PRD y PT sometieron a consideración de las Comisiones Unidas de Comercio y Fomento Industrial y de Estudios Legislativos la *Iniciativa con Proyecto de Decreto por el que se reforman y adicionan diversas disposiciones de la Ley Federal de Protección al Consumidor*[300], la cual pretende proteger los derechos al consumidor, mejorar la información de mercados y garantizar el derecho a la realización de operaciones comerciales claras y seguras.

El 8 de mayo de 2014 se publicó en el DOF el Acuerdo por el que se aprueba el Programa Nacional de Protección de los Derechos del Consumidor 2013-2018 por medio del cual la PROFECO se coordina con las entidades y dependencias de la APF a fin de proteger y promover los derechos de los consumidores a través del fortalecimiento de estar relaciones gubernamentales.

Por otro lado, esta reforma considera estudios globales que revelan que compradores mexicanos demandan flexibilidad en el comercio electrónico[301], debido a la gran preferencia de estas compras en tienda, tendencias de tiempos de entrega y uso de la telefonía. Entre otros hallazgos del comercio electrónico se incluyen que:

[300] Ver iniciativas del Comisión de Comercio y Fomento Industrial del Senado de la República mexicana, accesible en http://www.senado.gob.mx/sgsp/gaceta/63/1/2015-10-15-1/assets/documentos/Iniciativa_PRI_PROFECO.pdf, fecha de consulta 8 de diciembre de 2015.
[301] ComScore. Estudio Global Revela que Compradores Mexicanos Demandan Flexibilidad, accesible en: https://www.comscore.com/esl/Prensa-y-Eventos/Comunicados-de-prensa/2015/3/ESTUDIO-GLOBAL-REVELA-QUE-COMPRADORES-MEXICANOS-DEMANDAN-FLEXIBILIDAD, del 3 de Marzo de 2015, fecha de consulta: 2 de mayo de 2015.

a) Los consumidores en línea quieren alternativas para destinos de entrega y más opciones de pago.
b) La telefonía es un catalizador para la compra omnicanal y los minoristas deben reconocer sus limitantes.
c) El envío gratuito sigue siendo importante, principalmente para el retorno de la compra.

Por ende, las líneas de acción a seguir por la Iniciativa se destinan a:

a) Modernizar el sistema de atención y procuración de justicia respecto a los derechos del consumidor.
b) Desarrollar el *Sistema Nacional de Protección al Consumidor*, que integre y coordine las acciones de los gobiernos, poderes y sociedad civil, para que el ciudadano cuente con los elementos necesarios y haga valer sus derechos en cualquier circunstancia.
c) Fortalecer la *Red Inteligente de Atención al Consumidor* como medio para que el Estado responda eficientemente a las demandas de la población.
d) Establecer el *Acuerdo Nacional para la Protección de los Derechos de los Consumidores*, buscando una mayor participación y compromiso de los actores económicos en torno a las relaciones comerciales.

La importancia de esta iniciativa de reforma y adiciones radica en que tres de cada cuatro internautas mexicanos realizan compras en línea cuyo valor en 2014 superó los 162 mil millones de pesos[302], de acuerdo con la Asociación Mexicana de Internet (AMIPCI) y entre los retos del comercio electrónico en México están considerar:

a) La falta de información del historial sobre la confiabilidad de los proveedores,
b) La dificultad en los procesos de compra,
c) La insuficiente diversidad en los métodos de pago,
d) El bajo nivel de confianza del consumidor en la transacción y
e) Falta de protección de los datos personales de los consumidores, de conformidad con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), publicada en el DOF el 5 de julio de 2010.

Cabe señalar que el proyecto de referencia en lo relativo al comercio electrónico con acierto refiere la necesidad de cumplir con las recomendaciones de las Directrices de la OCDE para la Protección de los Consumidores de Prácticas Comerciales Transfronterizas Fraudulentas y Engañosas, a fin de que se facilite el comercio electrónico, permitan a los consumidores disfrutar de un nivel de protección igual al comercio no electrónico, proporcionen a los ciberconsumidores la posibilidad de identificar al proveedor, nombre legal, domicilio, dirección de correo electrónico, número telefónico, información explícita sobre el bien o servicio; amplia y clara información de costos, palcos de entrega, términos, condiciones de pago, restricciones, información de existencias así como garantías disponibles.

[302] Destinan internautas 5 mil pesos a compras en línea, en Con$umo Cuidado, 24 de julio de 2015, sitio web de información periodística accesible en: http://consumocuidado.com.mx/destinan-internautas-5-mil-pesos-en-promedio-a-comprar-en-linea/el, consultado el 2 de diciembre de 2015.

Los temas que abarca la Iniciativa son:

a) En materia de transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología, adiciona artículos en donde establece no sólo los derechos de los consumidores, sino también los mecanismos eficientes y reglas claras que faciliten a los consumidores un mejor conocimiento de los proveedores que ofrecen bienes y servicios mediante el comercio electrónico.
b) Plantea que la duración de la garantía no podrá ser inferior a noventa días contados a partir de la entrega del bien o la prestación del servicio. Aumenta de treinta a noventa días el término del derecho del consumidor, en el supuesto de que cuando el producto haya sido reparado o sometido a mantenimiento y el mismo presente deficiencias imputables al autor de la reparación o del mantenimiento dentro de los noventa días naturales posteriores a la entrega del producto al consumidor, éste tendrá derecho a que sea reparado o mantenido de nuevo sin costo alguno. En el caso de aparatos eléctricos, electrónicos, electrodomésticos y telefónicos, se propone que la garantía no puede ser menor de un año, contados a partir de la entrega del bien.
c) Propone establecer requisitos que deberán cumplir los proveedores de servicios de tiempos compartidos para obtener el registro para operar como tal, y así estar registrados en el *Registro de Tiempos Compartidos*.
d) Establece que cuando los proveedores tomen conocimiento de que alguno de sus bienes, productos o servicios pueda implicar riesgos para la vida, la salud, la seguridad o la economía de los consumidores, estarán obligados a informar de inmediato a la Procuraduría Federal del Consumidor, en un plazo no mayor a 24 horas, contados a partir de conocer el riesgo sobre el producto involucrado. Propone aumentar los días de clausura, a efecto de que las resoluciones de la Procuraduría cuenten con mayor fuerza y se desaliente la reincidencia de las conductas infractoras.
e) Pretende incluir a los OCA, al Servicio de Administración Tributaria, a la Comisión Nacional Bancaria y de Valores, dentro del listado de autoridades obligadas a proporcionar los datos necesarios para identificar y localizar al proveedor. Se establecen las reglas de las solicitudes de información relacionadas con el sistema financiero y las de materia fiscal, así como los fines que serán para identificar y localizar al proveedor dentro de los procedimientos que sustancia la Procuraduría, debiéndose guardar la más estricta confidencialidad. Señala que la Comisión Nacional de Seguridad de la Secretaría de Gobernación estará obligada a proporcionar a la PROFECO los antecedentes penales de los socios, accionistas, administradores o representantes de las casas de empeño, a fin de salvaguardar la integridad y derechos de los consumidores a través de la prevención en la comisión de delitos.
f) Se propone adicionar un *Capítulo XVI: Del pago de multas y el procedimiento administrativo de ejecución,* con objeto de que la PROFECO, se allegue de mayores recursos e ingresen directamente a su patrimonio.
g) La iniciativa plantea diversas adecuaciones derivadas de la reforma financiera y de telecomunicaciones.

Al realizar una matriz DAFO o FODA[303] analizando sus características internas (Debilidades y Fortalezas) y su situación externa (Amenazas y Oportunidades) del proyecto de esta Iniciativa, el resultado muestra los siguientes resultados:

Matriz FODA para el análisis del Proyecto de Iniciativa de la LFPC

ÚTIL	DAÑINO
FORTALEZAS	**DEBILIDADES**
• Aplicación de sanciones por reincidencia en 1 año a fin de no esperar desde la impugnación del comerciante de las resoluciones de la PROFECO. • Robustecimiento de las facultades de la PROFECO para aplicar mayores sanciones, clausuras definitivas y arrestos administrativos hasta por 72 horas para los sectores donde se registran mayores quejas[304]. • Establecimiento de la responsabilidad solidaria entre los diversos agentes económicos para la prestación de un bien y/o servicio. • Los proveedores estarán obligados a registrar los servicios que ofrecen, formatos de los contratos de adhesión y costos; en caso contrario, se sancionará conforme a lo dispuesto en el artículo 128 bis de la LFPC. • Ampliación del plazo de 5 a 30 días hábiles para cancelar un contrato antes de perfeccionarlo, a fin de dar tiempo al consumidor de una mejor reflexión sobre su compra y que tenga oportunidad de revocar su consentimiento durante ese lapso, sin responsabilidad alguna. • PROFECO, en casos graves, podrá sancionar con clausura total o parcial, la cual podrá ser de hasta 120 días y con multa.	• Las facultades de la PROFECO para la aplicación de sanciones, permite que el monto de las multas ingrese a su patrimonio, genera un conflicto de interés de la Profeco "al convertirse en beneficiaria de las multas aplicadas" e incluso para aplicar el procedimiento administrativo de ejecución. • Las transacciones efectuadas a través de los medios electrónicos, ópticos o de cualquier otra tecnología no excluyen el incumplimiento de las demás disposiciones de esta ley, por lo que se deberá de analizar con mucho detenimiento.
OPORTUNIDADES	**AMENAZAS**
• La ampliación de garantías en transacciones comerciales para que no sea inferior a 90 días a partir de la entrega del bien o la prestación total del servicio. En aparatos eléctricos, electrónicos, electrodomésticos y telefónicos, la garantía no podrá ser menor a un año. • Se establece el derecho a reponer el bien por uno nuevo, porque actualmente solo se obliga a componerlo. • Las contrataciones colectivas de espacios vacacionales, la iniciativa propone crear el registro público de tiempos compartidos, a fin de contrarrestar los fraudes registrados al ofrecer inmuebles en zonas donde no existen desarrollos hoteleros o inmobiliarios, o con el incumplimiento de los contratos por parte de los proveedores o empresas.	• Las visitas de verificación al comerciante por requerimiento de información pueden ser impugnadas de inconstitucionales. • Estas visitar fomentarían la promoción del juicios de amparo por la vulneración de las garantías de seguridad jurídica establecidas en el artículo 16 constitucional y como contrargumento el derecho humano del consumidor titulado y reconocido por el Estado.

Nuestra propuesta consiste en que las medidas de apremio señaladas en el artículo 25 del Proyecto de iniciativa sean consideradas en jerarquía para su aplicación: en primer lugar el apercibimiento como medida correctiva y el resto de las medidas podrían aplicarse en un orden gradual de menor a mayor gravedad.

4.3. Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación.

El Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación (RCCMPSC) publicadas en el DOF el 19 de julio de 2004, tiene por objeto establecer las normas

[303] Proviene de las siglas en inglés SWOT (Strengths, Weaknesses, Opportunities y Threats).
[304] Ejemplos como la Comisión Federal de Electricidad (CFE), o casos de rebeldía que se presentan en sectores como gasolineras y distribuidores de gas LP, que impiden el acceso a verificadores de la Procuraduría Federal del Consumidor.

reglamentarias a las que deben sujetarse los PSC en materia de firma electrónica y expedición de Certificados para actos de comercio.

La SE elaborará una relación de los Prestadores de Servicio de Certificación acreditados o suspendidos y de las personas físicas o morales que actúen en su nombre de conformidad con lo previsto en el artículo 104, fracción I del CCo. La relación deberá contener también a las personas físicas que formen parte del personal de los sujetos antes señalados. Además la SE deberá mantener actualizada y disponible dicha relación para todos los usuarios, lo que podrá hacer a través del dominio que determine para tal efecto.

Los interesados en obtener la acreditación como PSC, de conformidad con el artículo 5º del RCCMPSC, deberán:

A. Presentar la solicitud de acreditación en los formatos que determine la SE;

B. Adjuntar a la solicitud, según corresponda, lo siguiente:

a) En caso de los notarios o corredores públicos, copia certificada de la patente, título de habilitación o documento que en términos de la legislación de la materia les acredite estar en ejercicio de la fe pública;
b) En caso de las personas morales, copia certificada de su acta constitutiva, póliza u otro instrumento público, que acredite su constitución de acuerdo con las leyes mexicanas y que su objeto social sea el establecido en el artículo 101 del CCo, y
c) Las instituciones públicas, copia certificada del instrumento jurídico de su creación o, en su caso, copia certificada jurídica aplicable;

C. Comprobar que se cuenta al menos con los siguientes elementos:

a) Humanos.- Un profesionista jurídico, un profesionista informático y cinco auxiliares de apoyo informático;
b) Materiales.- Espacio físico apropiado para la actividad, controles de seguridad, accesos y perímetros de seguridad física, medidas de protección, así como con las políticas necesarias para garantizar la seguridad del área;
c) Económicos.- Capital que comprenderá al menos el equivalente a una cuarta parte de la inversión requerida para cumplir con los elementos humanos, tecnológicos y materiales, y un seguro de responsabilidad civil cuyo monto será determinado por la SE con base en el análisis de las operaciones comerciales y mercantiles en que sean utilizados los Certificados y no será menor al equivalente a treinta veces el salario mínimo general diario vigente en el Distrito Federal correspondiente a un año, y
d) Tecnológicos.- Consistentes en:

I) Análisis y evaluación de riesgos y amenazas,
II) Infraestructura informática,
III) Equipo de cómputo y software,

IV) Política de Seguridad de la Información,
V) Plan de continuidad del Negocio y Recuperación ante Desastres,
VI) Plan de Seguridad de Sistemas,
VII) Estructura de Certificados,
VIII) Estructura de la Lista de Certificados Revocados,
IX) Sitio electrónico,
X) Procedimientos que informen de las características de los procesos de creación y verificación de FEA,
XI) Política de Certificados,
XII) Declaración de Prácticas de Certificación,
XIII) Modelos de las autoridades certificadora y registradora,
XIV) Plan de administración de claves.

Los elementos descritos en la presente fracción "**C.**" anterior, deberán ajustarse a las especificaciones que determine la SE en las RGSPSC, a efecto de que las prácticas y políticas que se apliquen garanticen la continuidad del servicio, la seguridad de la información y su confidencialidad;

D. Contar con procedimientos claros y definidos de conformidad con las RGSPSC que emita la SE;

E. Adjuntar a la solicitud una carta suscrita por cada persona física que pretenda operar o tener acceso a los sistemas que utilizará en caso de ser acreditado, donde dicha persona manifieste bajo protesta de decir verdad y advertido de las penas en que incurren los que declaran falsamente ante una autoridad distinta a la judicial, de que no fue condenado por delito contra el patrimonio de las personas y mucho menos inhabilitado para el ejercicio de la profesión, o para desempeñar un puesto en el servicio público, en el sistema financiero o para ejercer el comercio;

F. Contar con una póliza de fianza por el monto y condiciones que se determinan en el presente Reglamento y en las RGSPSC que al efecto expida la SE;

G. Acompañar a su solicitud, escrito de conformidad para ser sujeto de auditoría por parte de la SE en todo momento, para que ésta verifique el cumplimiento de los requisitos para obtener y mantener la acreditación como PSC. Cuando el interesado pretenda que sus datos de creación de firma electrónica permanezcan en resguardo fuera del territorio nacional, deberá solicitarlo a la SE. En este caso, el interesado manifestará por escrito su conformidad de asumir los costos que impliquen a la SE el traslado de su personal para efectuar sus auditorías,

H. Registrar ante la SE su Certificado, en los términos que establece el RGSPSC.

Por otra parte, los notarios o corredores públicos podrán solicitar la acreditación a través de personas morales, conforme a lo que establezca la legislación que les rige. En ningún caso se les eximirá de la responsabilidad individual, ni aun cuando para obtener la acreditación compartan la infraestructura que les permita prestar los servicios de certificación.

La SE desahogará el trámite para obtener la acreditación como PSC en los términos de lo dispuesto por la Ley Federal de Procedimiento Administrativo y establecerá en las RGSPSC las condiciones a que se sujetará la fianza que otorgarán los interesados que obtengan su acreditación, previo al inicio de operaciones como PSC. Una vez que reciba la fianza verificará que contenga lo señalado en el CCo, en este Reglamento y en las RGSPSC que al efecto expida y, hecho lo anterior, procederá a expedir el certificado respectivo al interesado y lo registrará a efecto de que éste pueda iniciar operaciones.

La SE como autoridad certificadora y registradora, deberá comprobar la identidad del PSC o su representante, para que éste pueda generar sus datos de creación de firma electrónica, sujetándose a lo dispuesto por los artículos 104, fracción IV y 105 del CCo.

El PSC o su representante no podrán revelar los Datos de Creación de Firma Electrónica que correspondan a su propio Certificado y en todo caso serán responsables de su mala utilización. Dicho Certificado tendrá una vigencia de diez años.

En lo que respecta a los certificados, el PSC deberá proporcionar a la SE su dirección electrónica, la que deberá incluir en cada Certificado que expida para verificar en forma inmediata su validez, suspensión o revocación. Esta dirección se utilizará por la SE para agregarla a un dominio propio de consulta en línea, a través del cual la Parte que Confía[305] podrá cerciorarse del estado que guarda cualquier Certificado emitido por un Prestador de Servicios de Certificación.

Los PSC deberán enviar en línea, mediante el procedimiento que establezcan las **RGSPSC** que expida la SE, una copia de cada certificado que generen. Los certificados enviados se resguardarán por la SE bajo el más estricto mecanismo de seguridad física y lógica.

Para los efectos del artículo 108, fracción III del CCo, los datos de acreditación ante la SE, que contendrán los certificados que expidan los PSC, incluirán al menos (artículo 17):

I. El nombre, denominación o razón social y domicilio del PSC;
II. La dirección electrónica donde podrá verificarse la lista de certificados revocados a PSC, y
III. Los demás que, en atención al avance tecnológico, se establezcan en las **RGSPSC** que expida la SE.

El PSC deberá notificar a la SE cualquier cambio que pretenda efectuar respecto de los datos a que se refiere el presente artículo.

Asimismo, la SE determinará en las **RGSPSC** que expida, la utilización de un sello de tiempo para asegurar la fecha y hora de la emisión, suspensión y revocación del certificado.

[305] La parte que confía es alguién que deposita en el certificado la garantía de integridad, autenticidad y no repudio. Esta figura no la define la Ley Modelo CNUDMI sobre Firmas Electrónicas pero si la menciona en el artículo 11 de dicha Ley.

Mientras que la emisión, registró y conservación de los Certificados por parte de los PSC se efectuará en territorio nacional. La SE, a través de las **RGSPSC** preverá los mecanismos que garanticen que los certificados emitidos por los PSC, en ningún caso, contengan elementos que puedan generar confusión en la Parte que Confía.

En cuanto a las auditorias, para efecto del artículo 102, inciso A), fracción VI del CCo, las auditorías que efectúe la SE al prestador de Servicios de Certificación, se desahogarán en los términos previstos por la Ley Federal de Procedimiento Administrativo para las visitas de verificación, las cuales se practicarán de oficio o a petición del titular del certificado, firmante o de la Parte que Confía.

En materia de sanciones a los PSC o su personal, la SE suspenderá de manera temporal de uno hasta dos meses; de tres hasta cuatro meses; y de cinco hasta seis meses en el ejercicio de sus funciones al PSC incurra en faltas leves; pero suspenderá de manera definitiva a quienes reincidan en faltas leves, no compruebe la identidad de los solicitantes y cualesquiera circunstancias pertinentes para la emisión de un Certificado; proporcione documentación o información falsa para obtener la acreditación como PSC; altere, modifique o destruya los certificados que emita; registre, conserve o expida certificados fuera del territorio nacional; revele los datos de creación de Firma Electrónica que correspondan a su propio certificado; entre las conductas más relevantes.

Cuando la SE suspenda a un PSC en sus funciones, deberá revocar su correspondiente Certificado, ya sea de manera temporal o definitiva, y lo agregará al listado de certificados revocados en el dominio que establezca para tal efecto y publicará un extracto de la resolución en el DOF, a efecto de que cualquier usuario verifique en todo momento si un PSC puede o no ejercer su función. En el caso de suspensión definitiva la SE deberá además revocar la acreditación.

La SE tomará las medidas necesarias que garanticen, en beneficio de los usuarios, la continuidad del servicio materia del presente Reglamento en los términos de las **RGSPSC** que emita la SE.

Los argumentos en contra de la expedición de un *Reglamento del CCo en Materia de PSC* se dirige en el sentido de que los PSC no deberían enfrentarse a barreras de entrada para establecer su negocio, por lo que todo requerimiento que sea excesivo en la ley es un obstáculo para el mercado de PSC.

Muchos países generalmente tienen solo uno o dos PSC, mientras que en algunos países donde se han expedido un buen número de certificados cualificados el motivo tiene que ver con la forma en que son expedidos y/o por la promoción del propio gobierno del Estado[306].

[306] Cfr. Dumortier, J., Kelm, S., Nilsson, H., Skouma, G., Van Eecke, P., "The Legal and Market Aspects of Electronic Signatures", Datenschutz und Datensichering, 2004, n° 3, p. 141.

Por otra parte, cabe mencionar que en materia de derecho comparado es loable el trabajo realizado por la Unión Europea para estimular PSC con alto nivel de calidad a través de la creación de un *Clúster de prestadores de servicios de certificación de firmas electrónicas* a nivel regional con el objeto de establecer un número limitado de proveedores pero con niveles altos calidad en los esquemas de acreditación, a través de una acreditación voluntaria.[307]

4.4. Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación y el Acuerdo que modifica dichas Reglas.

Ahora corresponde hacer una descripción y análisis del contenido de las *Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación* (RGSPSC) publicadas en el DOF el 10 de agosto de 2004 así como de su *Acuerdo que Modifica las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación* (AMRGSPSC) publicadas el 05 de marzo de 2007, que no hace sino profundizar en cada una de las formalidades y obligaciones de los elementos de las RGSPSC.

El artículo 102 incisos A) fracciones II y III del CCo y 5º, fracción III, del RCCMPSC señalan que la SE tendrá por satisfechos los elementos humanos, materiales, económicos, tecnológicos y procedimientos a que se refieren dichas disposiciones, elementos:

Corresponde nuevamente citar los elementos que deberán reunir los PSC de conformidad con el Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación (RCCMPSC), pero que en las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación detallan a profundidad.

1) Elementos humanos:
   a) Profesional Jurídico
   b) Profesional Informático
   c) Personal Auxiliar del Profesional Informático

2) Elementos materiales y sus procedimientos

3) Elementos económicos

4) Elementos tecnológicos y sus procedimientos:

   a) Análisis y Evaluación de Riesgos y Amenazas.
   b) Política de Seguridad de la información.
   c) Plan de Continuidad del Negocio y Recuperación ante Desastres.
   d) Plan de Seguridad de Sistemas.
   e) Estructura de Certificados.
   f) Estructura de la Lista de Certificados Revocados (LCR).
   g) Sitio electrónico de alta disponibilidad.
   h) Procedimientos de creación, verificación y revocación de FEA
   i) Política de Certificados

[307] Cfr. DUMORTIER, J., KELM, S., NILSSON, H., SKOUMA, G., VAN EECKE, P., "The Legal and Market Aspects of Electronic Signatures", Datenschutz und Datensichering, 2004, n° 3, p. 144.

j) Declaración de Prácticas de Certificación.
k) Modelo Operacional de la Autoridad Certificadora
l) Modelo Operacional de la Autoridad Registradora.
m) Plan de Administración de Claves.

5) Proporcionar a la SE la documentación con la que acredite el cumplimiento de los requisitos previstos en el Código, el RCCMPSC y las RGSPSC.

1) Elementos humanos

Los profesionales jurídico e informático, serán responsables de aprobar el plan de continuidad del negocio que señalan las presentes Reglas Generales. El grado académico, los cursos con los que deben contar los profesionales jurídico, informático, así como el personal auxiliar del profesional informático y los requisitos que deben cumplir serán al menos los siguientes:

a) Profesional jurídico deberá:

I. Ser licenciado en derecho o abogado con título y cédula profesional registrados en la Secretaría de Educación Pública;

II. Demostrar al menos dos años de experiencia en materia notarial o de correduría pública, o en materia mercantil y servicios, procedimientos o actividades relacionadas con la acreditación de la personalidad;

III. Acreditar al menos un año de experiencia comprobable en actividades relacionadas con cualquier área del derecho informático o comercio electrónico;

IV. Cumplir con el requisito establecido en el artículo 102 inciso A) fracción IV del CCo y el artículo 5 fracción V del RGSPSC;

V. Comprobar que conoce la operación como usuarios de los sistemas informáticos que habrá de utilizar el Solicitante de Acreditación y el PSC, y

VI. Solicitud de examen para encargado de identificación correspondiente, misma que aplicará la Secretaría dentro de los cuarenta y cinco días siguientes a la presentación de la solicitud del Solicitante de Acreditación, previa notificación de fecha, hora y lugar en el que se aplicará el mismo.

Los requisitos de los apartados del “II.” al “V.” podrán acreditarse con declaración ante fedatario público, en la cual el profesionista jurídico manifieste bajo protesta de decir verdad y advertido de las penas en que incurren los que declaran falsamente ante una autoridad distinta a la judicial, que cumple con cada uno de los requisitos y que incluya los datos de las empresas o instituciones y fechas en las que adquirió la experiencia, sus cargos y las actividades y funciones desempeñadas.

b) Profesional informático deberá:

I. Ser licenciado o ingeniero en área Informática o afín, con título y cédula profesional registrados en la Secretaría de Educación Pública;

II. Comprobar al menos dos años de experiencia en el campo de seguridad informática con declaración ante fedatario público en la cual el profesionista informático manifieste bajo

protesta de decir verdad y advertido de las penas en que incurren los que declaran falsamente ante una autoridad distinta a la judicial, que cumple con la misma y que incluya los datos de las empresas o instituciones y fechas en las que adquirió la experiencia, sus cargos y las actividades y funciones desempeñadas. Además, deberá contar con diploma en seguridad informática o, en su caso, tener alguna certificación en esta área como: *GIAC Gold Standard Certificates* (GGSC), *GIAC Security Leadership Certificate* (GSLC), *CISSP Certification y SSCP Certification* o equivalentes, y

III. Cumplir con el requisito establecido en el artículo 102 inciso A) fracción IV del CCo y el artículo 5 fracción V del RGSPSC.

c) Personal Auxiliar del Profesional Informático se conformará por:

a. Un oficial de Seguridad ;
b. Un administrador de sistemas ;
c. Un operador de sistemas;
d. Un administrador de bases de datos, y
e. Un administrador de redes.

2) Elementos materiales y sus procedimientos:

a) En atención al dinamismo del avance tecnológico y la necesidad de preservar la seguridad física y lógica en la prestación del servicio de certificación, los elementos materiales que deberán estar en disposición del solicitante de acreditación y del prestador de servicios de acreditación y los procedimientos aplicables en este ámbito, deberán contener como mínimo las características siguientes:

b) Las áreas y los servicios en los cuales se maneja información confidencial requerirán procedimientos de controles de acceso, deberán estar supervisados continuamente, a efecto de reducir al mínimo los riesgos.

c) Las implantaciones de los controles deberán evitar riesgo, daño o pérdida, de los activos, alteración o sustracción de información.

d) Los accesos físicos a las áreas de generación de certificados, gestión de revocación de certificados y área de residencia de servidores, deberán estar protegidas con puertas y muros sólidos y firmes, chapas seguras, controles de acceso, sistemas de extinción de incendios y alarmas de seguridad, y se encontrarán limitados sólo al personal autorizado mediante controles de autenticación de por lo menos dos factores para asegurar que no habrán accesos no autorizados. Los servicios compartidos por otra entidad distinta al PSC o por personal de éste no dedicado al servicio de certificación, deberán estar fuera del perímetro de seguridad.

e) El acceso de visitas a las áreas con información confidencial deberá ser autorizado por el Oficial de Seguridad. El visitante deberá portar una credencial en todo momento para identificarse. Se deberá registrar toda actividad que realice el visitante con la fecha y hora de ingreso y salida.

f) Un documento que se denominará “Política de Seguridad Física”, a que se sujetará la prestación del servicio, el cual será presentado por el Solicitante de Acreditación con su

solicitud y que el PSC deberá mantener actualizado. El documento denominado “Política de Seguridad Física” deberá contemplar y desarrollar por lo menos los siguientes aspectos:

I. Control de acceso físico;
II. Protección y recuperación ante desastres;
III. Protecciones contra robo, forzamiento y entrada no autorizada a los espacios físicos;
IV. Medidas de protección en caso de incendio, contra fallas de servicios eléctricos o de telecomunicaciones, y
V. Un procedimiento de actualización para autorización de acceso al personal a las áreas restringidas.

Las áreas seguras deben ser oficinas cerradas dentro del perímetro de seguridad física, contener mobiliario con gabinetes y chapas seguras. Para la selección y el diseño de áreas seguras se debe tomar en cuenta la posibilidad de daños por fuego, sismo, inundación, explosiones, desórdenes civiles, y otras formas de desastres naturales y causados por el hombre. Todos los servicios claves deberán situarse alejados de las áreas de acceso y atención al público.

Los dispositivos como fax y fotocopiadoras deberán ubicarse dentro de las áreas seguras que así lo requieran, siempre bajo control para no comprometer la seguridad ni la confidencialidad de la información. Mientras que todo el material de desecho deberá ser destruido sin posibilidad de recuperación antes de desecharlo.

Las puertas y ventanas deberán estar siempre cerradas y aseguradas, instalando protecciones internas o externas en las mismas. Deberá contarse con sistemas de detección de intrusión física en puertas y ventanas del perímetro de seguridad. Aquellas salas desocupadas que estén dentro del perímetro de seguridad, deberán tener activado el sistema de detección de intrusos todo el tiempo.

La gestión de los servicios de procesamiento de información deberá estar físicamente separada del resto de los servicios.

Finalmente, deberán establecerse procedimientos y prácticas de seguridad para el personal dentro del perímetro de seguridad, que contemplen por lo menos lo siguiente:

a) El personal deberá conocer y entender los procedimientos y prácticas de seguridad dentro del perímetro de seguridad;
b) Las áreas vacías deberán cerrarse y revisarse periódicamente llevando una bitácora de tal revisión;
c) El personal de soporte que no es parte del personal del Solicitante de Acreditación o del PSC, deberá acceder a las áreas restringidas sólo en caso necesario y si es autorizado por el Profesional Informático o el Oficial de Seguridad, además de ser acompañado por personal que sí lo esté;
d) No se deberá permitir dentro del perímetro de seguridad equipo de grabación, audio o video, con excepción del propio equipo de seguridad; y de comunicaciones.
e) Las actividades sin supervisión dentro de las áreas seguras deberán definirse para evitar problemas de seguridad, y prevenir actividades contrarias al servicio;

f) La recepción de insumos y la salida de basura deberán estar controladas y separadas del área de procesamiento de la información, para evitar accesos no autorizados;

g) Los requerimientos de seguridad para las áreas de atención a clientes se determinarán a partir del Análisis y Evaluación de Riesgos y Amenazas a que se refieren las presentes Reglas Generales;

h) El personal que acceda a las áreas externas de recepción de insumos y de desechos deberá estar controlado. Se deberá contar con los mecanismos que impidan que el personal no autorizado acceda a través de estas áreas al perímetro de seguridad;

i) Los procedimientos y prácticas para inspeccionar el material que ingrese, en busca de potenciales peligros antes de ser trasladados desde las áreas externas a las áreas de uso;

j) El equipo instalado deberá estar protegido para reducir las amenazas;

k) Contar con respaldo de sistemas no interrumpible de energía eléctrica, y con planta de energía eléctrica de emergencia para asegurar la continuidad del servicio de certificación;

l) El cableado eléctrico y de datos de los servicios de información confidencial deberá ser compatible con los estándares vigentes en la materia y protegidos contra daños e intervenciones;

m) Las líneas eléctricas no deberán interferir el funcionamiento del cableado de datos;

n) Contar con el personal o los contratos de mantenimiento requerido para garantizar la continua disponibilidad e integridad de los equipos, de acuerdo a las especificaciones y periodos recomendados por los fabricantes;

o) Evitar que equipos, información y software salgan de los perímetros de seguridad sin autorización.

p) Evitar que el equipo portátil contenga información confidencial. Si hay alguna razón que justifique equipos portátiles que contengan información confidencial o procesos críticos de la operación o información de los usuarios de los certificados, éstos nunca deberán salir del perímetro de seguridad designado;

q) Evitar que los equipos sean reutilizados o queden en desuso conteniendo información confidencial;

r) Los discos duros, disquetes y demás medios de almacenamiento de información magnético u óptico que ya no se utilicen deberán ser destruidos antes de salir del perímetro de seguridad;

s) Establecer un mecanismo para registrar el mal funcionamiento, fallas, mantenimientos preventivos y correctivos, de los equipos sensibles para la operación del servicio;

t) Adoptar la política de *Escritorio limpio y pantalla limpia* para evitar riesgos de acceso no autorizado, pérdidas o daños a la información durante o fuera del horario de trabajo, y

u) La Seguridad Física propuesta por el Solicitante de Acreditación y el PSC, deberá ser compatible con las normas y criterios internacionales y al menos con el estándar *ETSI TS 102 042 -sección 7.4.4 Physical and Environment security- e ISO/IEC 17799 sección 7.*

3) Elementos económicos:

Los elementos económicos con que deberá contar el Solicitante de Acreditación y el PSC comprenderán al menos:

El seguro, cuyo monto aplicable para cada año será el determinado por la Secretaría con base en un análisis de las operaciones comerciales y mercantiles en que sean utilizados los Certificados, y no será menor al equivalente a treinta veces el salario mínimo general diario vigente en el Distrito Federal correspondiente a un año. En caso de que un PSC sea acreditado para otro u otros servicios de firma electrónica adicionales, de los mencionados en el apartado 2.bis., la cobertura del seguro deberá incluir la totalidad de los servicios.

4) Elementos tecnológicos y sus procedimientos.

Los elementos tecnológicos y sus procedimientos garantizarán la continuidad del servicio, por lo que deberán ser compatibles con las normas y criterios internacionales, en atención a lo siguiente:

a) Análisis y Evaluación de Riesgos y Amenazas.
El Solicitante de Acreditación o el PSC deberán elaborar un documento denominado *Análisis y Evaluación de Riesgos y Amenazas*, en el que desarrolle los apartados y aspectos que a continuación se indican:

- Realizar un estudio que identifique los riesgos e impactos que existen sobre las personas y los equipos, así como recomendaciones de medidas para reducirlos;
- Implementación de medidas de seguridad para la disminución de los riesgos detectados o riesgos mínimos;
- Proceso de evaluación continua para adecuar la valoración de riesgos a condiciones cambiantes del entorno, y
- Determinar un proceso equivalente o adoptar el descrito en los documentos siguientes: *Risk Management Guide for Information Technology Systems, Special Publication 800-30. Recommendations of the National Institute of Standards and Technology, October 2001, Handbook 3, Risk Management,* Version 1., Australian Communications Electronic Security Instruction 33 (ACSI 33), o aquellos que les sustituyan.

La Infraestructura informática deberá incluir al menos lo siguiente:

- Una Autoridad Certificadora;
- Una Autoridad Registradora;
- Depósitos para: Datos de Creación de Firma Electrónica del PSC y su respaldo, certificados y *Listas de Certificados Revocados* (LCR) basadas en un servicio de *Protocolo de Acceso de Directorio de Peso ligero* (LDAP) o equivalente y un *Protocolo de Estatus de Certificados en Línea* (OCSP);
- Los procesos de administración de la Infraestructura;
- Un manual de Política de Certificados (PC);
- Una Declaración de Prácticas de Certificación (DPC), y
- Los manuales de operación de las Autoridades Certificadora y Registradora.

El equipo de cómputo y software deberá incluir:

a. Por lo menos un servidor de misión crítica para la Autoridad Certificadora y la Autoridad Registradora, contemplando otro servidor de las mismas características para redundancia por seguridad.
b. Un servidor de misión crítica, contemplando redundancia por seguridad, para LDAP, LCR y OCSP.
c. Una computadora para almacenar el sistema de administración de la Infraestructura que se opera.
d. Un Sistema de Sello o Estampado de Tiempo, para insertar fecha y hora de emisión de los certificados, con las especificaciones y en los términos del apartado 7 de las presentes Reglas.
e. Un dispositivo de alta seguridad que sea compatible con el estándar *FIPS-140 nivel 3*, contemplando redundancia por seguridad, para almacenar los Datos de Creación de Firma Electrónica del PSC.
f. Un enlace mínimo de 512 Kilo Bytes, contemplando redundancia con un enlace de al menos 256 Kilo Bytes a Internet.
g. Un ruteador, contemplando redundancia por seguridad.
h. Un muro de fuego (firewall), contemplando redundancia por seguridad.
i. Un sistema de monitoreo de red.
j. Un sistema confiable de antivirus.
k. Herramientas confiables de detección de vulnerabilidades.
l. Sistemas confiables de detección y protección de intrusión.
m. Las computadoras personales e impresoras necesarias para la prestación del servicio.

b) Política de seguridad de la información.
La Política de Seguridad deberá constar por escrito y cumplir con los siguientes requisitos:

- Ser congruente con el objeto del PSC;
- Los objetivos de seguridad determinados deberán ser, claros, generales y no técnicos y resultado del *Análisis y Evaluación de Riesgos y Amenazas*;
- Estar basada en las recomendaciones del estándar ISO 17799 sección tres;
- Contar con los manuales de Política General y los necesarios para establecer políticas específicas;
- Con base en el *Análisis y Evaluación de Riesgos y Amenazas* deberán identificarse los objetivos de seguridad relevantes y las amenazas potenciales relacionadas a los servicios suministrados, así como las medidas a tomar para evitar y limitar los efectos de tales riesgos y amenazas;
- Describir las reglas, directivas y procedimientos que indiquen cómo son provistos los servicios y las medidas de seguridad asociadas;
- Señalar el periodo de revisión y evaluación de la Política de Seguridad;
- Ser consistente con la DPC y con la PC a que se refieren las presentes Reglas Generales, y
- Incluir un proceso similar al descrito en: *Internet Security Policy: A Technical Guide, by the National Institute of Standards and Technologies* (NIST).

c) Plan de Continuidad del Negocio y Recuperación ante Desastres.

El Solicitante de Acreditación y el PSC deberán elaborar y presentar un *Plan de Continuidad del Negocio y Recuperación ante Desastres,* que describa cómo actuará en caso de interrupciones del servicio. El Plan deberá ser mantenido y probado periódicamente, y describir los procedimientos de emergencia a seguir en al menos los siguientes casos:

- Afectación al funcionamiento de software en el que se basarán los servicios del PSC;
- Incidente de seguridad que afecte la operación del sistema en el que se basan los servicios del PSC;
- Robo de los datos de creación de Firma Electrónica del PSC;
- Falla de los mecanismos de auditoría;
- Falla en el hardware donde se ejecuta el producto en el que se basarán los servicios del PSC, y
- Mecanismos para preservar evidencia del mal uso de los sistemas.
- En el *Análisis y Evaluación de Riesgos y Amenazas* se considerará el impacto que sufrirá el negocio, en caso de interrupciones no planificadas.
- El Plan de Continuidad del Negocio y Recuperación ante Desastres deberá ser compatible con las normas y criterios internacionales, al menos con los lineamientos descritos en el estándar *ISO 17799 sección 11 o el estándar ETSI TS 102 042 sección 7.4.8,* o los que les sustituyan.

Además deberá ser coherente con los niveles de riesgo determinados en el *Análisis y Evaluación de Riesgos y Amenazas* y seguirá un proceso similar al descrito en: *NIST ITL Bulletin June 2002, Contingency Planning Guide for Information Systems; NIST Special Publication 800-34, Contingency Planning Guide for Information Systems, June 2002; y NIST Special Publication 800-30 Risk Management Guide*, u otros textos posteriores equivalentes.

d) Plan de Seguridad de Sistemas.

Los solicitantes de acreditación o los PSC deberán contar con un *Plan de Seguridad de Sistemas* coherente con la *Política de Seguridad de la Información*, que describa los requerimientos de seguridad de los sistemas y de los controles a implantar y cumplir; así como delinear las responsabilidades y acceso de las personas a los sistemas.

El *Plan de Seguridad de Sistema* incorporará:

- La Política de Seguridad de la Información, seguridad organizacional, control y clasificación de activos, administración de operaciones y comunicaciones, control de accesos, desarrollo y mantenimiento de sistemas, seguridad del personal, seguridad ambiental y física que sean compatibles con los señalados por la norma ISO 17799;
- Los mecanismos y procedimientos de seguridad propuestos que se aplicarán en todo momento;
- La forma en que se garantizará el logro de los objetivos de la PC y de la DPC. En caso de claves criptográficas, la manera en que se efectuará su administración, y
- Las medidas de protección del depósito público de certificados y de información privada obtenida durante el registro.

- Implantación del Plan de Seguridad de Sistemas.

El Solicitante de Acreditación y el PSC, verificarán que operaciones, procedimientos y mecanismos permitan alcanzar sus objetivos y lograr el riesgo mínimo determinado en el *Análisis y Evaluación de Riesgos y Amenazas*, así como los controles de los aspectos mencionados en el *Plan de Seguridad de Sistemas*. La capacidad de administrar las instalaciones debe ser acorde con dicho Plan.

La Implantación del Plan debe garantizar el logro de los objetivos de la PC y DPC, el cual debe de ser compatible por lo menos con el estándar ISO 17799, o las que le sustituyan.

e) Estructura de Certificados.

- La estructura de datos del certificado debe ser compatible con el estándar ISO/IEC 9594-8; además de contener los datos que aparecen en el artículo 108 del CCo, para ser considerados como válidos.
- Los algoritmos utilizados para la FEA deben ser compatibles con los estándares de la industria *RFC 3280. Internet X509 Public Key Infraestructure Certificate and Certificate Revocation List (CRL) Profile (Obsoletes 2459), R. Housley, W. Polk, W. Ford, D. Solo*, April 2002, o los que les sustituyan que provean un nivel adecuado de seguridad tanto para la firma del PSC como del usuario.
- En el caso de las claves utilizadas para la generación de una FEA, su tamaño deberá proveer el nivel de seguridad de 1024 bits para los usuarios y de 2048 bits para los PSC. Deberán utilizar funciones hash conforme a estándares de la industria, actuales y que provean el adecuado nivel de seguridad para este tipo de firmas tanto del PSC como del usuario.
- Contendrán referencia o información suficiente para identificar o localizar uno o más sitios de consulta donde se publiquen las notificaciones de revocación de los certificados y al menos los que indican estas Reglas Generales.

f) Estructura de la Lista de Certificados Revocados (LCR).

La estructura e información de la Lista de Certificados Revocados deberá ser compatible con la última versión del estándar *ISO/IEC 9594-8* o la que le sustituya, e incluir por lo menos la siguiente información:

- Número de serie de los certificados revocados por el emisor con fecha y hora de revocación;
- La identificación del algoritmo de firma utilizado;
- El nombre del emisor;
- La fecha y hora en que fue emitida la Lista de Certificados Revocados;
- La fecha en que emitirá la próxima Lista de Certificados Revocados que no podrá exceder de veinticuatro horas, con independencia de mantener el *Protocolo de Estatus de Certificados en Línea* (OCSP), y

- La Lista de Certificados Revocados deberá ser firmada por el PSC que la haya emitido, con sus datos de creación de firma.

g) Sitio electrónico de alta disponibilidad

El solicitante de acreditación y el PSC deberán señalar un sitio electrónico de alta disponibilidad con mecanismos redundantes o alternativos de conexión y de acceso público a través de Internet que permitirá a los usuarios consultar los certificados emitidos de forma remota, continua y segura compatible con el estándar ISO/IEC 9594-8 o el que le sustituya, a efecto de garantizar la integridad y disponibilidad de la información ahí contenida. En dicho sitio se incluirá la PC y DPC.

h) Procedimientos de creación, verificación y revocación de FEA

El solicitante de acreditación y el PSC definirán procedimientos que informen de las características de los procesos de creación y verificación de Firma Electrónica Avanzada, así como aquellos que aplicarán para dejar sin efecto definitivo los certificados.

i) Política de Certificados

El solicitante de acreditación y el PSC deberá establecer una PC conforme a la cual se establecerá la confianza del usuario en el servicio, que:

- Asegure su concordancia con la DPC y los procedimientos operacionales;
- Permita la interoperabilidad con los PSC ya acreditados y con la SE;
- Indique a quién se le puede otorgar un certificado y cómo se aplicará el proceso de registro, y que se deberá verificar en forma fehaciente la identidad del usuario. Cuando se trate de un certificado que habrá de ser utilizado para generar FEA deberá describir la forma en que se precisarán los propósitos, objetivos y alcances del Certificado y sus limitaciones. Asimismo, se deberán describir las obligaciones que contrae el PSC y el usuario en la emisión y utilización del certificado;
- Dé a conocer las medidas de privacidad y de protección de datos que se aplicarán en materia de Firma Electrónica Avanzada. La Política de Certificados será pública;
- Deberá establecer bajo qué circunstancias se puede revocar un certificado y quiénes pueden solicitarlo, y
- Tendrá que ser compatible por lo menos con el estándar *ETSI TS 102 042* o el que le sustituya.

j) Declaración de Prácticas de Certificación.

En la DPC, que deberá elaborar y mantener actualizado el solicitante de acreditación y el PSC, determinarán:

- Los procedimientos de operación para otorgar certificados y el alcance de aplicación de los mismos;

- Las responsabilidades y obligaciones del PSC y de la persona a identificar. Particularmente desarrollará aquellas inherentes a la emisión, revocación y expiración de certificados;
- La vigencia de los certificados. Y una vez otorgada la acreditación por la Secretaría, la fecha de inicio de operaciones;
- Detalladamente el método de verificación de identidad del usuario que se utilizará para la emisión de los certificados;
- Procedimientos de protección de confidencialidad de la información de los solicitantes;
- Un procedimiento para registrar la fecha y hora de todas las operaciones relacionadas con la emisión de un certificado y conservarlas de manera confiable;
- Los procedimientos que se seguirán en los casos de suspensión temporal o definitiva del PSC y la forma en que la administración de los certificados emitidos pasarán a la Secretaría o a otro PSC, en el caso, de suspensión definitiva;
- Las medidas de seguridad adoptadas para proteger sus datos de creación de firma electrónica;
- Los controles que se utilizarán para asegurar que el propio usuario genere sus datos de creación de firma electrónica, autenticación de usuarios, emisión de certificados, revocación de certificados, auditoría y almacenamiento de información relevante, y
- La DPC deberá ser compatible por lo menos con el estándar ETSI TS 102 042 y el RFC 3647 o el que le sustituya.

k) Modelo Operacional de la Autoridad Certificadora

I. El solicitante de acreditación y el PSC deberán definir su *Modelo Operacional de la Autoridad Certificadora* conforme al cual operará y prestará sus servicios al fungir como autoridad certificadora a efecto de lograr confiabilidad e interoperabilidad, que desarrollará los apartados siguientes:

- Cuáles son los servicios prestados;
- Cómo se interrelacionan los diferentes servicios;
- En qué lugares se operará;
- Qué tipos de certificados se entregarán;
- Si se generarán certificados con diferentes niveles de seguridad;
- Cuáles son las políticas y procedimientos de cada tipo de certificado, y
- Cómo se protegerán los activos.

II. El *Modelo Operacional de la Autoridad Certificadora* deberá contener un resumen que incluya:

- Contenido del documento;
- La historia del posible PSC, y
- Relaciones comerciales con proveedores de insumos o servicios para sus operaciones.

III. El *Modelo Operacional de la Autoridad Certificadora* deberá comprender los siguientes aspectos:

- Interfaces con las Autoridades Registradoras;
- Implementación de elementos de seguridad;
- Procesos de administración;
- Sistema de directorios para los certificados;
- Procesos de auditoría y respaldo, y Bases de Datos a utilizar.

IV. El *Modelo Operacional de la Autoridad Certificadora* deberá considerar la PC, DPC, la *Política de Seguridad de la Información* y el *Plan de Seguridad de Sistemas* por lo que se refiere a la generación de claves.

V. El *Modelo Operacional de la Autoridad Certificadora* deberá incluir los requerimientos de seguridad física del personal, de las instalaciones y del módulo criptográfico.

Vl. *Modelo Operacional de la Autoridad Registradora.*

i. El solicitante de acreditación y el PSC deberán definir su Modelo Operacional de la Autoridad Registradora conforme al cual operará y prestará sus servicios con su autoridad registradora a efecto de lograr confiabilidad e interoperabilidad, que desarrollará los apartados siguientes:

- Cuáles son los servicios de registro que se prestarán;
- En qué lugares se ofrecerán dichos servicios, y
- Qué tipos de certificados generados por la Autoridad Certificadora se entregarán.

ii. El PSC deberá ofrecer los mecanismos para que el propio usuario genere en forma privada y segura sus Datos de Creación de Firma Electrónica. Deberá indicar al usuario el grado de fiabilidad de los mecanismos y dispositivos utilizados.
iii. El Modelo Operacional de la Autoridad Registradora deberá comprender los siguientes aspectos:

- Interfaces con Autoridad Certificadora;
- Implementación de dispositivos de seguridad;
- Procesos de administración;
- Procesos de auditoría y respaldo;
- Bases de Datos a utilizar;
- Privacidad de datos, y
- Descripción de la seguridad física de las instalaciones

iv. El Modelo Operacional de la Autoridad registradora deberá establecer el método para proveer de una identificación unívoca del usuario y el procedimiento de uso de los Datos de Creación de Firma Electrónica.

m) Plan de Administración de Claves.

I. El solicitante de acreditación y el PSC deberán definir su *Plan de Administración de Claves* conforme al cual generará, protegerá y administrará sus claves criptográficas, respecto de los apartados siguientes:

- Claves de la Autoridad Certificadora;
- Almacenamiento, respaldo, recuperación y uso de los Datos de Creación de Firma Electrónica de la Autoridad Certificadora del PSC;
- Distribución del certificado de la Autoridad Certificadora;
- Administración del ciclo de vida del hardware criptográfico que utilice la Autoridad Certificadora, y
- Dispositivos seguros para los usuarios.

II. Los procedimientos implantados de acuerdo al *Plan de Administración de Claves*, deberán garantizar la seguridad de las claves en todo momento, aun en caso de cambios de personal, componentes tecnológicos, y demás que señalan las presentes Reglas Generales.

III. El *Plan de Administración de* Claves deberá establecer como requerimiento mínimo el utilizar aquellas con longitud de 1024 bits para los usuarios y de 2048 bits para los Prestadores de Servicios de Certificación.

IV. El PSC, su autoridad certificadora y registradoras, utilizarán dispositivos seguros para almacenar sus datos de creación de firma electrónica, compatibles como mínimo con el estándar FIPS-140 nivel 3 en sus elementos de seguridad e implantación de los algoritmos criptográficos estándares, o el que le sustituya.

V. El *Plan de Administración de Claves* tendrá que ser compatible por lo menos con el estándar ETSI TS 102 042 sección 7.2 -Generación de la clave de la Autoridad Certificadora, Almacenamiento, Respaldo y Recuperación de la clave de la Autoridad Certificadora, Distribución de la clave pública de la Autoridad Certificadora, uso de clave de la Autoridad Certificadora, fin del ciclo de vida de la clave de la Autoridad Certificadora y Administración del ciclo de vida del Hardware criptográfico-, o el que le sustituya.

5) El solicitante de acreditación y el PSC, deberán proporcionar a la SE, la documentación con la que acredite el cumplimiento de los requisitos previstos en el Código, el Reglamento o en las presentes Reglas Generales conforme a lo siguiente:

- Tratándose de documentos públicos en copia certificada o en copia simple con el original para cotejo, o
- Tratándose de documentos privados en copia simple, y
- Una copia en disco compacto de toda la documentación presentada.

Para los efectos del artículo 102, inciso A), fracción V, del CCo, y del apartado 2.bis., de las presentes Reglas, en relación con el artículo 89 del CCo, las condiciones a las que se sujetará

la fianza que otorguen los solicitantes que obtengan su acreditación, previo al inicio del ejercicio de sus funciones como Prestadores de Servicios de Certificación, serán conforme a lo siguiente:

- Una vez resuelta la procedencia de la solicitud de acreditación, en términos de la fracción IV del artículo 7 del Reglamento, el interesado deberá presentar la fianza de compañía debidamente autorizada a favor de la Tesorería de la Federación, en el término establecido en el artículo 8 del mencionado Reglamento:
- El solicitante que haya sido acreditado como PSC para expedir Certificados, deberá otorgar una fianza por un monto mínimo equivalente a cinco mil veces el salario mínimo general diario vigente en el Distrito Federal, monto que deberá incrementarse por cada persona, física o moral adicional, que contemple para efectos del artículo 104, fracción I del CCo, para prestar el servicio de certificación en nombre y por cuenta del solicitante, hasta por un monto máximo equivalente a cien mil veces el salario mínimo general diario vigente en el Distrito Federal.
- En caso de que un PSC acreditado por la Secretaría para expedir Certificados fuera acreditado para prestar también uno o más servicios adicionales de firma electrónica de los mencionados en el numeral 2.bis., deberá ampliar la cobertura de la fianza ya otorgada, para incluir las actividades de los nuevos servicios, por el monto señalado en el numeral anterior.

Para los efectos del artículo 10 del Reglamento, la Secretaría a través de sus servidores públicos comprobarán la identidad del solicitante de acreditación o del PSC o su representante, utilizando cualquiera de los medios admitidos en derecho.

- Tratándose de la identificación del representante de un PSC que sea persona moral privada o institución pública, éste deberá acreditar su personalidad y la legal existencia de su representado a la Secretaría.
- El PSC generará sus Datos de creación de firma electrónica, en el nivel de seguridad más alto de sus instalaciones, a fin de dar certeza y seguridad a todos los elementos necesarios para la creación de los mismos y bajo la supervisión de la Secretaría, en dicha generación se podrá utilizar cualquier tecnología por lo que el procedimiento técnico variará de acuerdo a la que se utilice, lo anterior a fin de cumplir con el principio de neutralidad tecnológica.

Para los efectos de los artículos 113 del Código y 16 del Reglamento, el procedimiento para obtener la copia de cada Certificado generado por un PSC, será mediante envío en línea de cada Certificado a la Secretaría, lo cual será en tiempo real, es decir, se enviará una copia de cada certificado inmediatamente después del momento de expedición de los Certificados generados por el PSC en su autoridad certificadora.

- En el caso que el PSC por caso fortuito o de fuerza mayor debidamente comprobado a la Secretaría, no pudiese llevar a cabo el envío a que se refiere el apartado anterior, el PSC deberá hacer la réplica por cualquier medio en un término no mayor a seis horas.
- Además del envío en línea de la copia de los Certificados, el PSC remitirá dicha copia a la Secretaría en medios ópticos o electrónicos dentro de las veinticuatro horas siguientes a la generación de los Certificados, a fin de garantizar redundancia del procedimiento técnico descrito en el apartado 5 anterior de estas Reglas Generales.
- El PSC deberá cerciorarse que la Secretaría recibió la copia de cada certificado.

Para los efectos del artículo 108 fracción III del Código y 17 fracción III, del Reglamento, los datos de acreditación ante la Secretaría observarán los siguientes elementos.

- El Certificado emitido por el PSC debe contener los datos que aparecen en el artículo 108 del CCo, para ser considerado válido.
- Los certificados emitidos por el PSC deberán contener la dirección electrónica de la Secretaría, en donde se podrá consultar la Lista de los Certificados Revocados de Prestadores de Servicios de Certificación.

Para los efectos del artículo 108, fracción VI del CCo y 18 del Reglamento, así como, en caso de que sea necesario, del apartado 2.bis., de las presentes Reglas, la fecha y hora de emisión del Certificado o de la prestación del servicio de firma electrónica, se determinará conforme a lo siguiente:

- El PSC deberá llevar un registro de sellos digitales de tiempo, los cuales serán emitidos ya sea por la Secretaría, por un sistema propio o por el de otro PSC acreditado para este servicio, para asegurar y dejar constancia de la fecha y hora de la emisión de los Certificados generados por el PSC o de la prestación de los servicios de firma electrónica que lo requieran. En caso de que se solicite la acreditación para la emisión de sellos digitales de tiempo y para otro servicio adicional de los señalados en el numeral 2.bis., se podrán otorgar ambas acreditaciones por medio de un mismo trámite, siempre que para dicho servicio sea indispensable el sellado digital de tiempo.
- El sistema de sellos digitales de tiempo deberá cumplir, en todo momento, por lo menos, con el *Estándar Internacional Internet X.509 Public Key Infraestructure Time Stamp y considerar los RFC 3161 y 3628*, o los que lo suplan, previo aviso que la Secretaría haga por escrito a los PSC.

Para efectos del artículo 19 del Reglamento, la SE verificará que los PSC cumplan con la estructura de certificados referida en las presentes Reglas Generales en la Estructura de Certificados citada con anterioridad, así como con los estándares internacionales, el CCo, el Reglamento y estas Reglas Generales, con el objetivo de asegurar que los certificados emitidos por los PSC, en ningún caso, contengan elementos que puedan generar confusión en la Parte que Confía.

Para los efectos del artículo 104 fracción IV del CCo, los casos en que estará a disposición el contenido privado del Registro de Certificados de un PSC se sujetarán a lo dispuesto por la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

El PSC que en términos del artículo 104 fracción VI, quiera cesar de manera voluntaria su actividad, previo pago de derechos tiene que informar el motivo de dicho cese con cuarenta y cinco días de anticipación a la Secretaría a efecto de que la misma se cerciore que se ha cumplido con lo establecido en el artículo 16 del Reglamento y el apartado 5, 5.1 y 5.2 de las RGSPSC.

Estas Reglas estarán sujetas a cambios y a una revisión anual de la SE, debido a los constantes cambios en la industria, a los estándares, normas y criterios internacionales reconocidos para prestar el servicio de certificación.

Por otra parte y en cuanto hace al *Acuerdo que Modifica las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación* (AMRGSPSC), publicadas en el DOF el 5 marzo de 2007, tuvieron como objetivo adicionar a las RGSPSC los puntos 2.bis., 2.bis.1., 2.bis.1.1., 2.bis.1.2., 2.bis.2. y 3.3.; modificar las Reglas 2.3.1., 3., 3.2., 7., 7.1. y 7.2., y derogar las Reglas 3.1.1., 3.1.2., 7.3. y 7.4. de dichas Reglas Generales a las que deberán sujetarse los PSC, publicadas el 10 de agosto de 2004 en el Diario Oficial de la Federación (DOF), para quedar como siguen:

2.bis. *En caso de que el Solicitante de Acreditación refiera en su solicitud, además de la emisión de Certificados, la prestación de otro u otros servicios de firma electrónica, como son la conservación de mensajes de datos, el sellado digital de tiempo y la validación de Certificados, conforme lo prevé el artículo 89 del Código de Comercio, se aplicará lo siguiente:*

2.bis.1. *Deberá cumplir, para cada uno de los servicios adicionales señalados en el numeral anterior, lo siguiente:*

2.bis.1.1. *Lo establecido en los apartados 2.4.1., 2.4.3., 2.4.4., 2.4.5., 2.4.6. y 2.4.9., en relación con los servicios adicionales a la emisión de certificados para los que solicita su acreditación.*

2.bis.1.2. *El modelo operacional a que hace referencia el apartado 2.4.13., respecto del servicio de que se trate.*

2.bis.2. *En caso de que un Prestador de Servicios de Certificación ya acreditado por la Secretaría para la emisión de Certificados, solicite su acreditación para otro servicio de firma electrónica de los señalados en el apartado 2.bis., se tendrán por cumplidos los numerales 2.1, 2.2, 2.3 y 2.5.*

2.3.1. *El seguro, cuyo monto aplicable para cada año será el determinado por la Secretaría con base en un análisis de las operaciones comerciales y mercantiles en que sean utilizados los Certificados, y no será menor al equivalente a treinta veces el salario mínimo general diario vigente en el Distrito Federal correspondiente a un año. En caso de que un Prestador de Servicios de Certificación sea acreditado para otro u otros servicios de firma electrónica adicionales, de los mencionados en el apartado 2.bis., la cobertura del seguro deberá incluir la totalidad de los servicios.*

3.- *Para los efectos del artículo 102, inciso A), fracción V, del Código de Comercio, y del apartado 2.bis., de las presentes Reglas, en relación con el artículo 89 del Código de Comercio, las condiciones a las que se sujetará la fianza que otorguen los solicitantes que obtengan su acreditación, previo al inicio del ejercicio de sus funciones como Prestadores de Servicios de Certificación, serán conforme a lo siguiente:*

3.1.1. *Se deroga.*

3.1.2. *Se deroga.*

3.2*. El solicitante que haya sido acreditado como Prestador de Servicios de Certificación para expedir Certificados, deberá otorgar una fianza por un monto mínimo equivalente a cinco mil veces el salario mínimo general diario vigente en el Distrito Federal, monto que deberá incrementarse por cada persona, física o moral adicional, que contemple para efectos del artículo 104, fracción I del Código de Comercio, para prestar el servicio de certificación en nombre y por cuenta del solicitante, hasta por un monto máximo equivalente a cien mil veces el salario mínimo general diario vigente en el Distrito Federal.*

3.3. *En caso de que un Prestador de Servicios de Certificación acreditado por la Secretaría para expedir Certificados fuera acreditado para prestar también uno o más servicios adicionales de firma electrónica de los mencionados en el numeral 2.bis., deberá ampliar la cobertura de la fianza ya otorgada, para incluir las actividades de los nuevos servicios, por el monto señalado en el numeral anterior.*

7. *Para los efectos del artículo 108, fracción VI del Código de Comercio y 18 del Reglamento, así como, en caso de que sea necesario, del apartado 2.bis., de las presentes Reglas, la fecha y hora de emisión del Certificado o de la prestación del servicio de firma electrónica, se determinará conforme a lo siguiente:*
7.1. *El Prestador de Servicios de Certificación deberá llevar un registro de sellos digitales de tiempo, los cuales serán emitidos ya sea por la Secretaría, por un sistema propio o por el de otro Prestador de Servicios de Certificación acreditado para este servicio, para asegurar y dejar constancia de la fecha y hora de la emisión de los Certificados generados por el Prestador de Servicios de Certificación o de la prestación de los servicios de firma electrónica que lo requieran. En caso de que se solicite la acreditación para la emisión de sellos digitales de tiempo y para otro servicio adicional de los señalados en el numeral 2.bis., se podrán otorgar ambas acreditaciones por medio de un mismo trámite, siempre que para dicho servicio sea indispensable el sellado digital de tiempo.*
7.2. *El sistema de sellos digitales de tiempo deberá cumplir, en todo momento, por lo menos, con el estándar internacional Internet X.509 "Public Key Infraestructure Time Stamp" y considerar los RFC 3161 y 3628, o los que lo suplan, previo aviso que la Secretaría haga por escrito a los Prestadores de Servicios de Certificación.*

7.3. *Se deroga.*
7.4. *Se deroga.*

4.5. Norma Oficial Mexicana NOM-151-SCFI-2002: *Prácticas comerciales: Requisitos que deben observarse para la conservación de mensajes de datos.*

La NOM-151-SCFI-2002 tiene por objeto establecer los requisitos que deben observarse para la conservación del contenido de MD que consignen contratos, convenios o compromisos y que en consecuencia originen el surgimiento de derechos y obligaciones, y que deberán observar todos los comerciantes que conserven MD y/o digitalicen documentos en términos de lo dispuesto en los artículos 33, 38 y 49 del CCo[308].

[308] "**Artículo 33.-** El comerciante está obligado a llevar y mantener un sistema de contabilidad adecuado. Este sistema podrá llevarse mediante los instrumentos, recursos y sistemas de registro y procesamiento que mejor se acomoden a las características particulares del negocio, pero en todo caso deberá satisfacer los siguientes requisitos mínimos:
A) Permitirá identificar las operaciones individuales y sus características, así como conectar dichas operaciones individuales con los documentos comprobatorios originales de las mismas.
B) Permitirá seguir la huella desde las operaciones individuales a las acumulaciones que den como resultado las cifras finales de las cuentas y viceversa;
C) Permitirá la preparación de los estados que se incluyan en la información financiera del negocio; D) Permitirá conectar y seguir la huella entre las cifras de dichos estados, las acumulaciones de las
cuentas y las operaciones individuales;
E) Incluirá los sistemas de control y verificación internos necesarios para impedir la omisión del registro de operaciones, para asegurar la corrección del registro contable y para asegurar la corrección de las cifras resultantes."
"Artículo 38.- El comerciante deberá conservar, debidamente archivados, los comprobantes originales de sus operaciones, de tal manera que puedan relacionarse con dichas operaciones y con el registro que de ellas se haga, y deberá conservarlos por un plazo mínimo de diez años."
"Artículo 49.- Los comerciantes están obligados a conservar por un plazo mínimo de diez años los originales de aquellas cartas, telegramas, mensajes de datos o cualesquiera otros documentos en que se consignen contratos, convenios o compromisos que den nacimiento a derechos y obligaciones.
Para efectos de la conservación o presentación de originales, en el caso de mensajes de datos, se requerirá que la información se haya mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y sea accesible para su ulterior consulta. La Secretaría de Economía emitirá la Norma Oficial Mexicana que establezca los requisitos que deberán observarse para la conservación de mensajes de datos."

De acuerdo con el marco jurídico vigente, es decir el CCo y demás disposiciones aplicables a la materia, los comerciantes están obligados a mantener y llevar un sistema de contabilidad adecuado, mismo que puede llevarse a través de medios digitales y con ayuda de las tecnologías de la información y cumplimentar los requisitos mínimos establecidos en el artículo 33 del CCo.

El CCo estableció que cuando la ley exigiera forma escrita para los actos, convenios o contratos, la exigencia de la forma escrita se tendría por cumplida, tratándose de MD, siempre que la información en él contenida:

- Se mantuviera integra[309].
- Fuera accesible para su ulterior consulta.

Como se puede observar, bajo la legislación mercantil, únicamente la información contenida en un MD que cumpla dichos requisitos podrá ser equivalente a aquellos documentos para los que la ley requiere "forma escrita" o firma (artículo 93).

Luego, se autorizó a la SE para la emisión de una NOM-151 que estableciera los requisitos a observarse para conservar los MD en forma íntegra e inalterada y hacerlos accesibles para su ulterior consulta, cuyo fundamento en el artículo 49, segundo párrafo del CCo.

La NOM-151publicada el 4 de junio de 2002 y actualmente en vigor[310], establece estos requisitos, mismos que resultan esenciales para conservar y presentar información contenida en MD cuando la ley solicite que cierta información deba ser conservada y presentada, en su caso, en original[311].

El campo de aplicación de dicha norma es de observancia general para todos los comerciantes que deban conservar los mensajes en que se consignen los documentos referidos, así como para todas aquellas personas con quienes los comerciantes otorguen o pacten dichos contratos, convenios o compromisos.

En la NOM-151 se incluyen varios conceptos utilizados, entre los más relevantes están:

- *Aceptación de autoría:* A la propiedad de un algoritmo de firma digital que permite atribuir a una persona física o moral la autoría de un MD inequívocamente.
- *Autenticación:* Al proceso en virtud del cual se constata que una entidad es la que dice ser y que tal situación es demostrable ante terceros.

[309] Se considerará que el contenido de un MD es íntegro, si éste ha permanecido completo e inalterado independientemente de los cambios que hubiere podido sufrir el medio que lo contiene, resultado del proceso de comunicación, archivo o presentación (artículo 94).
[310] El 19 de diciembre de 2005 se publicó en el DOF la Resolución por la que se da a conocer la fecha de entrada en vigor de la Norma Oficial Mexicana NOM-151-SCFI-2002, Prácticas comerciales - Requisitos que deben observarse para la conservación de mensajes de datos, publicada el 4 de junio de 2002.
[311] Los comerciantes se encuentran obligados a conservar los originales de aquellos documentos (incluidos mensajes de datos) en los que se consignen contratos, convenios o compromisos que den nacimiento a derechos y obligaciones (artículo 49 del Código de Comercio).

- *Archivo parcial:* Al MD representado en formato Abstract Syntax Notation One (Notación sintáctica abstracta 1 (ASN.1).
- *Confidencialidad:* Al estado que existe cuando la información permanece controlada y es protegida de su acceso y distribución no autorizada.

El procedimiento que se debe conducir para la conservación de los MD requiere de la utilización de la tecnología PKI y de la existencia y participación de PSC. Los documentos electrónicos o MD que se deseen conservar se podrá almacenar en uno o varios archivos diferentes y/o en una o varias computadoras[312].

El método para digitalizar archivos soportados en medio físico consiste en que la migración deberá ser cotejada por un TLA, quien constatará que dicha migración se realice íntegra e inalterablemente tal y como se generó por primera vez en su forma definitiva.

Dentro de los elementos objetivos que intervienen en la conservación de mensajes de datos están la firma electrónica o digital; la constancia emitida por el PSC, equipos y software en sentido amplio.

Le corresponde a la SE la vigilancia de dicha norma de acuerdo a sus funciones, la legislación aplicable y su entrada en vigor, la cual depende de la existencia de infraestructura y publicación de aviso en el DOF.

La parte más relevante de la NOM-151 de referencia obra en el punto *7. apéndice normativo* en el que se establecen los elementos necesarios para su implantación, la descripción del algoritmo de conservación de información y la definición ASN.1[313] de los objetos usados. También describe brevemente el algoritmo y se muestran dos archivos de texto que serán usados para construir los objetos ASN.1 resultantes de aplicar la Norma a estos dos archivos.

Los objetos ASN.1 creados son mostrados a través de un vaciado hexadecimal de su contenido en formato BER. Se incluyen las claves de criptografía que se usaron en la creación de los ejemplos con el propósito de que se pueda verificar la implantación de la Norma.

Para formar un archivo parcial se crea un mensaje en formato ASN.1 que contiene:

(i) el nombre del archivo del sistema de información en el que está o estuvo almacenado el contenido del archivo,
(ii) el tipo del archivo, y
(iii) el contenido del mismo; con el objetivo de guardar la relación lógica que existe entre estos tres elementos.

[312] Cfr. Reyes Krafft, Alfredo Alejandro. La Firma Electrónica y Las Entidades de Certificación, 2003, 1ª ed., Porrúa, México, p. 57.
[313] Es una norma para representar datos independientemente de la máquina que se esté usando y sus formas de representación internas. Es un protocolo de nivel de presentación en el modelo OSI.

Ahora bien, para obtener los compendios o resúmenes digitales se calcula el compendio o resumen digital del archivo o archivos parciales resultado del proceso anterior, usando el algoritmo MD5. Luego se conforma un expediente electrónico donde se creará un mensaje ASN.1 que contiene:

- **(i)** el nombre del expediente, que debe de coincidir con el nombre con el que se identifica en el sistema de información en donde está o estuvo almacenado,
- **(ii)** un índice, que contiene el nombre y el compendio de cada archivo parcial que integra el expediente,
- **(iii)** la identificación del operador del sistema de conservación, y
- **(iv)** su firma digital de acuerdo a la definición correspondiente en la presente NOM.

Para la obtención de la constancia el sistema de conservación deberá usar el protocolo de aplicación descrito en el apéndice de la NOM para enviar el expediente al PSC, quien emitirá una constancia en formato ASN.1 y la regresará al sistema de conservación, haciendo uso del mismo protocolo.

El expediente opcionalmente podrá enviarse como un anexo de correo electrónico, siendo aplicables en este caso los protocolos Internet correspondientes.

También podrá usarse la transmisión vía Web siempre que el expediente se reciba como un archivo y siempre que se utilice un directorio protegido por nombre de usuario y contraseña. Para ello, la forma en que lo envíe deberá ser como la siguiente:

La constancia deberá regresar al cliente como un archivo de tipo *mime application/octet-stream*.[314]

El PSC podrá recibir, si así lo acuerda con sus clientes, medios físicos conteniendo los archivos correspondientes a los expedientes. Además el PSC formará una constancia en formato ASN.1 que contendrá:

- **(i)** el nombre del archivo en donde está almacenada la constancia,
- **(ii)** el expediente enviado por el sistema de conservación,
- **(iii)** fecha y hora del momento en que se crea la constancia,
- **(iv)** la identificación del PSC y
- **(v)** su firma digital de acuerdo a la definición correspondiente de la Norma

Para la verificación de la autenticidad de una constancia se realizará por medio del uso de un sistema de verificación que lleve a cabo los pasos siguientes:

- **(i)** verificar la firma digital del PSC en la constancia;

[314] Los MIME Types (Multipupose Internet Mail Extensions) son la manera estándar de mandar contenido a través de la red. Los tipos MIME especifican tipos de datos, como por ejemplo texto, imagen, audio, etc.

(ii) verificar la firma digital del operador del sistema de conservación en el expediente contenido en la constancia, y
(iii) recalcular el compendio de él o los archivos parciales y verificar que coincidan con los compendios asentados en el expediente.

Con el propósito de poder verificar los objetos ASN.1 definidos en este documento se incluyen las claves privadas que fueron usadas para generar las firmas de los documentos mencionados. Durante el proceso de generación de claves no se generó la clave pública y ya se ha perdido la información de generación de dichas claves.

El *Front End de Comunicaciones* (FEC) es la referencia de implantación para el PSC es un programa desarrollado para manejar las comunicaciones en aplicaciones con arquitectura cliente/servidor, fue diseñado pensando en aplicaciones que requieran intercambiar mensajes en tiempo real.

Se puede usar la definición de este sistema para especificar el protocolo de comunicación entre los clientes del PSC y los sistemas que se indican en la Norma. La SE deberá contar con un sistema de referencia para que el o los prestadores de servicios de certificación tengan un estándar contra el cual verificar que la implantación de la norma es correcta.

Los objetivos del FEC son:

(i) Simplificar la programación de los sistemas con arquitectura cliente/servidor, de tal manera que al desarrollar un sistema se dejen a un lado los detalles relacionados al manejo de las comunicaciones y el esfuerzo se centre en los detalles propios del sistema.
(ii) Lograr un ambiente de operación flexible que permita la interacción de programas desarrollados en distintas plataformas, sistemas operativos y lenguajes.
(iii) Optimar el uso de los recursos y permitir que los sistemas que lo usen operen en tiempo real.

El FEC se encarga de realizar algunas tareas que, en la arquitectura cliente/servidor tradicional, serían realizadas por el servidor, por ejemplo:

(i) Autenticar a los clientes que desean establecer comunicación con algún servidor.
(ii) Notificar la conexión o desconexión de un cliente al servidor adecuado.
(iii) Notificar a los clientes si un servidor está o no en servicio.
(iv) Verificar continuamente el estado de los clientes y servidores conectados.

Es por ello que su uso proporciona las siguientes ventajas:

(i) Provee de transparencia en la localización de clientes y servidores.
(ii) Simplifica la programación de servidores.
(iii) Permite la interacción de programas desarrollados en distintas plataformas.
(iv) Minimiza el uso de recursos de la red de comunicaciones.

A diferencia de los documentos que obran en papel, los documentos digitales reducen los inconvenientes de administración de archivos, resguardo por cuestiones de seguridad y privacidad y reducen los costos, lo que deviene en una eficiencia al interior de las organizaciones. El panorama es todavía mejor cuando se piensa en los documentos digitalizados que además son archivados con la FEA, lo que les otorga directamente los atributos de la firma citada, que son la **integridad, inalterabilidad y confidencialidad**.

Con la reforma al CCo del 29 de agosto del 2003, el artículo 49 dispone que los comerciantes tener por cumplida la obligación de conservar su documentación original contractual y otro tipo de documentos que asienten derechos obligaciones por el plazo mínimo de 10 años si esto se resguarda por medio de los MD siempre que haya mantenido íntegra e inalterada la información a partir del momento en que se generó por primera vez en su forma definitiva y sea accesible para su ulterior consulta. En este contexto, la Secretaría de Comercio y Fomento Industrial emitió la NOM-151.

Asimismo, el artículo 93 bis del CCo establece que sin perjuicio de lo dispuesto en el artículo 49, cuando la ley requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho respecto a un MD:

a) Si existe garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como MD o en alguna otra forma, y
b) De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona a la que se deba presentar.

Para efectos de este artículo, se considerará que el contenido de un MD es íntegro, si éste ha permanecido completo e inalterado independientemente de los cambios que hubiere podido sufrir el medio que lo contiene, resultado del proceso de comunicación, archivo o presentación.

Por otra parte, el artículo 100 de la LIC establece la posibilidad de que las instituciones de crédito opten por grabar todos aquellos documentos relacionados con sus labores con la misma validez jurídica que los originales.

> ***Artículo 100.-*** *Las instituciones de crédito podrán microfilmar o grabar en discos ópticos, o en cualquier otro medio que les autorice la Comisión Nacional Bancaria y de Valores, todos aquellos libros, registros y documentos en general, que obren en su poder, relacionados con los actos de la propia institución, que mediante disposiciones de carácter general señale la Comisión Nacional Bancaria y de Valores, de acuerdo a las bases técnicas que para la microfilmación o la grabación en discos ópticos, su manejo y conservación establezca la misma.*
> *Los negativos originales de cámara obtenidos por el sistema de microfilmación y las imágenes grabadas por el sistema de discos ópticos o cualquier otro medio autorizado por la Comisión Nacional Bancaria y de Valores, a que se refiere el párrafo anterior, así como las impresiones obtenidas de dichos sistemas o medios, debidamente certificadas por el funcionario autorizado de la institución de crédito, tendrán en juicio el mismo valor probatorio que los libros, registros y*

documentos microfilmados o grabados en discos ópticos, o conservados a través de cualquier otro medio autorizado.
Transcurrido el plazo en el que las instituciones de crédito se encuentran obligadas a conservar la contabilidad, libros y demás documentos de conformidad con el artículo 99 de esta Ley y las disposiciones que haya emitido la Comisión Nacional Bancaria y de Valores, los registros que figuren en la contabilidad de la institución harán fe, salvo prueba en contrario, en los juicios respectivos para la fijación de los saldos resultantes de las operaciones a que se refieren las fracciones I y II del artículo 46 de esta Ley.

Mientras que las *Disposiciones de Carácter General Aplicables a las Instituciones de Crédito*, publicadas en el DOF el 2 de diciembre de 2005[315] emitidas por la Comisión Nacional Bancaria y de Valores (CNBV) establecen la posibilidad de grabar actos de las instituciones de crédito, entendiendo por grabación todo acto mediante el cual un libro, registro o documento original, es *transformado a una imagen en formato digital en medio óptico o magnético, utilizando equipos y programas de cómputo diseñados para tal efecto.*

El artículo 300 de esas Disposiciones establece que las Instituciones para la microfilmación o grabación, podrán aplicar la tecnología estándar existente en el mercado, siempre que reúna los requisitos de seguridad que se establecen en los Anexos 50 y 51 de estas Disposiciones.

Asimismo, cabe resaltar los artículos 1 y 301 del Capítulo IX: Microfilmación y digitalización de documentos relacionados con las operaciones activas, pasivas y de servicios así como el *Anexo 50: Instructivo para microfilmación y destrucción de documentos* y el *Anexo 51: Instructivo para grabación y destrucción de documentos.*

De una interpretación integral de los preceptos anteriores, se desprende que otorgan la posibilidad de la grabación de los libros, registros y documentación relativos a sus operaciones activas, pasivas y de servicios, para la posterior destrucción del soporte físico, con excepción hecha de los originales de los libros, registros y documentación, relativos a sus operaciones activas, pasivas y de servicios, así como aquélla relacionada con su contabilidad, ni tampoco podrán destruir, aun cuando se hubieren microfilmado o grabado, los originales de los documentos públicos relativos a su contabilidad, la escritura constitutiva y sus modificaciones, las actas de asambleas generales de accionistas, sesiones de Consejo, y sus comités, las actas de emisión de valores, los estados financieros, la documentación de apoyo a dichos estados financieros, el dictamen del auditor externo, así como la que ampare la propiedad de bienes propios o de terceros cuyo original se encuentre bajo su custodia.

En todo caso, dicha información deberá conservarse durante los plazos que establecen las disposiciones legales en materia mercantil y fiscal aplicables. Asimismo, tampoco podrán destruirse los documentos de valor histórico que, en su caso, correspondan a la Institución o que aquélla mantenga en custodia.

[315] El 19 de mayo de 2014 se promulgó una Resolución que modifica las disposiciones de carácter general aplicables a las instituciones de crédito, pero no afecto en nada la materia que estamos tratando.

Con respecto al sector financiero varios cambios en este tema son descritos, el artículo 117 Bis de Ley de Ahorro y Crédito Popular (LACP) y los artículos 233, 234, 237, 238 y 255 a 265 de las *Disposiciones de Carácter General aplicables a las Entidades de Ahorro y Crédito Popular y Organismos de Integración* a que se refiere la LACP emitidas por la Comisión Nacional Bancaria y de Valores (CNBV)

> ***Artículo 117 Bis*** *de la LACP.- Las Sociedades Financieras Populares podrán microfilmar o grabar en discos ópticos, o en cualquier otro medio que les autorice la Comisión, todos aquellos libros, registros y documentos en general, que obren en su poder, relacionados con los actos de la propia Sociedad, que mediante disposiciones de carácter general señale la Comisión, de acuerdo a las bases técnicas que para la microfilmación o la grabación en discos ópticos, su manejo y conservación establezca la misma.*
>
> ***Artículo 233*** *de las Disposiciones citadas.- Para efectos de lo previsto en esta Sección, el proceso denominado grabación es aquél en el cual un documento original será convertido a una imagen en formato digital, utilizando equipos y programas de cómputo diseñados para tal efecto, y microfilmación aquél en el cual un documento original es reproducido en una película.*
>
> ***Artículo 234.-*** *Toda documentación que tenga carácter probatorio o pueda ser necesaria para aclaraciones con terceros, o que su contenido pueda ser atribuible a las personas obligadas, deberá conservarse durante un periodo mínimo de 12 años, ya sea en original, microfilmada o grabada.*
>
> ***Artículo 237.-*** *Los registros auxiliares, pólizas y fichas de contabilidad, comprobantes anexos a las mismas y la documentación justificativa y de apoyo contable, en general, así como los estados mensuales de contabilidad y su documentación complementaria y de apoyo que se hubiere microfilmado o grabado, deberán conservarse íntegramente cuando menos durante el ejercicio contable al que correspondan y durante los dos años siguientes, sujetándose, en su caso, a las disposiciones fiscales aplicables. Se exceptúa de lo previsto en este artículo la documentación comprobatoria de la disposición de saldos a favor de terceros, la cual podrá destruirse, previa microfilmación o grabación, a partir de tres meses después de haber sido pagados.*
>
> ***Artículo 238.-*** *La documentación de carácter puramente informativo que no esté relacionada con aquélla a la que se refieren los Artículos 236 y 237 anteriores, deberá conservarse durante un plazo mínimo de 6 meses después de que hayan cumplido su cometido. Queda a juicio de cada Entidad determinar la documentación de este tipo que deberá ser microfilmada o grabada, quedando bajo su absoluta responsabilidad resolver sobre la destrucción de la misma.*

De todos los anteriores artículos se desprende que el CCo otorga validez jurídica al archivo de MD cuando exista garantía confiable de que se ha conservado la integridad de la documentación original, a partir del momento en que se generó por primera vez en su forma definitiva.

Se hace notar que derivado del artículo 49 del CCo, la Secretaría de Comercio y Fomento Industrial emitió las bases o requisitos para la conservación de los MD, a los cuales los conglomero en la *NOM-151-SCFI-2002: Prácticas comerciales-Requisitos que deben observarse para la conservación de mensajes de datos*, que no son más que lineamientos conforme a los cuales se realiza migración de la documentación en papel a MD. Es así como en su artículo 4.3 precisa:

> ***4.3*** *Sin perjuicio de lo que dispongan otros ordenamientos jurídicos aplicables, cuando se pretenda conservar en un medio electrónico, óptico o de cualquier otra tecnología, información derivada de un acto de comercio, que se encuentre soportada en un medio físico similar o distinto a aquéllos,*

los comerciantes podrán optar por migrar dicha información a una forma digital y, observar para su conservación en forma digital, las disposiciones a que se refiere la presente Norma Oficial Mexicana. La migración de la información deberá ser cotejada por ***un tercero legalmente autorizado****, que constatará que dicha migración se realice integra e inalterablemente tal y como se generó por primera vez en su forma definitiva. El tercero legalmente deberá ser una persona física o moral que cuente con la capacidad tecnológica suficiente y que cumpla con los requisitos legales aplicables.*

En suma, este el precepto que marca el origen de la figura del TLA, de la cual, no hay otro señalamiento antes de la expedición de la NOM-151 en 2002.

Respecto al TLA surgen las siguientes apreciaciones:

a) Dado que actualmente, no ha sido otorgada a ninguna persona o institución el reconocimiento de TLC, existen posibles personas físicas y morales que pueden desempeñarse como tal: los fedatarios públicos o los corredores públicos debido a que cuentan con fe pública, previa autorización de la SE. O bien, cualquier persona que sin ser fedataria, tenga la capacidad tecnológica suficiente, la cual tampoco está definida en la NOM ni en ninguna otra disposición, por lo tanto no es posible determinar si dichos fedatarios cuentan con la tecnología necesaria;

b) Respecto a la actividad que realizará un TLA, existe la duda de si éste constatará el proceso de migración o si la constatación debe aparejarse de una fe pública. La fe pública supone exactitud, es decir, que lo narrado por el fedatario resulte fiel al hecho por él presenciado. Esto implicaría que todos y cada uno de los documentos migrados deberían ser cotejados por el fedatario, cuando esta situación no es necesaria para toda la documentación que las empresas estén en posibilidades de migrar.

c) Si el resultado de dicha constatación del proceso de migración implica que los MD tengan la calidad de documentos públicos en términos de los artículos 93, 129, 130, 202 y 203 del CFPC, que son aquellos cuya formación está encomendada a funcionarios públicos revestidos de fe pública, y que dichos documentos hacen prueba plena. Los MD ya denominados en esta etapa compendios digitales no alcanzarán bajo ninguna forma la calidad de instrumentos públicos, pues siguen perteneciendo a la categoría de documentos privados; pues erróneamente podría considerarse que con la participación de un fedatario público como TLA el documento se transformaría en documento con pleno valor probatorio, pero lo anterior no es así, dado que la migración presenciada por el fedatario solo implica que se incluirá su sello de certificación en el nuevo compendio digital que equivale al documento original que tuvo a la vista. Ello permite concluir que no es necesaria la figura de fedatario público como TLA, en razón de que la migración puede darse con o sin fe pública, y más aún, en términos económicos, lo costoso que puede salir la contratación de un notario haría que las empresas se desalentaran y por ende, no hagan uso de este recurso de migración.

Mientras la SE no regule una definición de TLA, los lineamientos conforme a los cuales deben actuar y su formas de acreditar la capacidad tecnológica, no podrá ser una figura aplicable.

Por otra parte, dentro de las atribuciones que creemos indispensables se deben incluir para la actuación de un TLA están la de auditar periódicamente a los comerciantes que tengan un proceso de digitalización, lo que les permitiría asegurar la calidad de los compendios digitales así como la validación de integridad e inalterabilidad de ellos, a partir del momento en que se generaron como MD.

Existen dos referentes internacionales en relación a los requisitos que deben observarse para la conservación de MD. El primero es el caso de Italia, a través de las *Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonche' di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo* n. 82 del 2005[316].

El segundo caso, es el de España a través de la *Orden EHA/962/2007* de 10 de abril de 2007, por la que se desarrollan determinadas disposiciones sobre facturación telemática y conservación electrónica de facturas, contenidas en el Real Decreto 1496/2003, de 28 de noviembre, por el que se aprueba la digitalización certificada de facturas recibidas y documentos sustitutivos recibidos y de otros documentos o justificantes que los obligados tributarios podrán digitalizar en forma certificada de las facturas, documentos sustitutivos y de cualesquiera otros documentos que conserven en papel que tengan el carácter de originales a fin de que pueda prescindir de los originales en papel que les sirvieron de base.

En dicha orden se establece que la digitalización certificada es el proceso tecnológico que permite, mediante la aplicación de técnicas fotoelectrónicas o de escáner, convertir la imagen contenida en un documento en papel en una imagen digital codificada conforme a alguno de los formatos estándares de uso común y con un nivel de resolución que sean admitidos por la Agencia Estatal de Administración Tributaria.

En este orden de ideas, el proceso de digitalización deberá ser realizado por el propio obligado tributario o bien por un tercero prestador de servicios de digitalización, en nombre y por cuenta de aquél, utilizando en ambos casos un software de digitalización certificado en los términos de la misma Orden. También el proceso de digitalización deberá garantizar la obtención de una imagen fiel e íntegra de cada documento digitalizado, imagen digital signada con firma electrónica con base en un certificado electrónico instalado en el sistema de digitalización e invocada por el software de digitalización certificada.

Además este certificado debe corresponder al obligado tributario cuando la digitalización certificada se realice por el mismo o al prestador de servicios de digitalización en otro caso. Luego, el resultado de la digitalización certificada se deberá organizar en torno a una base de datos documental y que por cada documento digitalizado se conserve un registro de datos con todos los campos exigibles de los libros de registros al igual que un campo en el que se contenga

[316] Decreto del Presidente del Consejo de Ministros del 13 de noviembre de 2014, publicado en la Gaceta oficial de la República Italiana, accesible en http://www.gazzettaufficiale.it/eli/id/2015/01/12/15A00107/sg, consultado el 2 de febrero de 2015.

la imagen binaria del documento digitalizado o que enlace al fichero que la contenga, en ambos casos con la firma electrónica de la imagen. Finalmente, el obligado a la conservación deberá disponer de un software de digitalización certificado.

Cabe señalar que el Artículo 7, inciso "d" de la *Orden EHA/962/2007* que venimos analizando refiere que el obligado a la conservación deberá disponer del software de digitalización certificado con determinadas funcionalidades:

> ***1.-*** *Firma de la base de datos que garantice la integridad de datos e imágenes al cierre de cada período de liquidación al que esté sometido el obligado tributario.*
> ***2.-*** *Acceso completo y sin demora injustificada a la base de datos. A estos efectos, se entiende por acceso completo aquél que posibilite una consulta en línea a los datos que permita la visualización de los documentos con todo el detalle de su contenido, la búsqueda selectiva por cualquiera de los datos que deban reflejarse en los libros registro regulados en el artículo 62 y siguientes del Real Decreto 1624/1992, de 29 de diciembre, la copia o descarga en línea en los formatos originales y la impresión a papel de aquellos documentos que sean necesarios a los efectos de la verificación o documentación de las actuaciones de control fiscal.*
> ***3.-*** *Las entidades desarrolladoras que deseen homologar software de digitalización que cumplan los requisitos del apartado 2 de este artículo deberán cumplir los siguientes trámites:*
>
> ***a)*** *Las entidades interesadas presentarán una solicitud ante el Director del Departamento de Informática Tributaria de la Agencia Estatal de Administración Tributaria que deberá contener una declaración responsable de cumplimiento de los requisitos exigidos en la presente Orden, acompañada de la documentación que acredite su cumplimiento.*
> ***b)*** *En particular, el solicitante deberá aportar, junto con la solicitud, las normas técnicas en las que se base el procedimiento de digitalización certificada que pretenda homologar, así como los protocolos o normas y procedimientos de seguridad, de control y de explotación referidos a la creación y consulta de la base de datos documental que contenga las imágenes digitalizadas de los documentos originales en papel suministrados por el obligado tributario y los mecanismos de firma electrónica utilizados.*
> ***c)*** *Adicionalmente, la documentación aportada deberá contener un informe emitido por una entidad de auditoría informática independiente con solvencia técnica acreditada en el ámbito del análisis y la evaluación de la actividad desarrollada, en el que se exprese la opinión acerca del cumplimiento, por parte de la entidad solicitante, de las condiciones establecidas en esta Orden para la admisión de su sistema de digitalización certificada cuya homologación se solicita y sobre los procedimientos utilizados.*
> ***d)*** *Cuando la solicitud presentada no contenga todos los elementos que sean necesarios para permitir la verificación de los requisitos exigidos normativamente, se podrá requerir al solicitante para que en el plazo de 10 días, contados a partir del día siguiente al de la notificación del requerimiento, subsane los defectos de que adolezca, con indicación de que si así no lo hiciera se le tendrá por desistido y se procederá al archivo de la solicitud sin más trámite. Cuando el requerimiento de subsanación haya sido atendido en plazo pero no se entiendan subsanados los defectos observados, se notificará al solicitante la denegación de acuerdo con lo previsto en la letra e siguiente.*
> ***e)*** *Para efectuar la mencionada verificación, el Departamento de Informática Tributaria podrá recabar cuanta información complementaria entienda necesaria para comprobar la exactitud de lo declarado por el solicitante, así como efectuar las comprobaciones adicionales que crea convenientes.*
> ***f)*** *Una vez verificado el cumplimiento de los requisitos establecidos en esta Orden, el Director del Departamento de Informática Tributaria acordará la homologación del software de*

digitalización presentado y su inclusión en una lista que se hará pública en la página web de la Agencia Estatal de Administración Tributaria, www.agencia tributaria.es. En la resolución se describirán las condiciones en que la solicitud se entiende concedida y la referencia identificativa de la misma. En caso contrario, en el escrito de denegación de la autorización se deberá motivar la causa que impide la autorización. El acuerdo que se dicte será recurrible en alzada ante el Director General de la Agencia Estatal de Administración Tributaria.

g) *El Director del Departamento de Informática Tributaria resolverá acerca de la solicitud de admisión en un plazo de seis meses. Si la verificación no hubiera finalizado en ese plazo, o no se hubiera dictado resolución expresa, la solicitud podrá entenderse desestimada por silencio administrativo.*

h) *Podrá efectuar la solicitud a que se refiere este artículo cualquier entidad desarrolladora establecida en España o en cualquier otro Estado miembro de la Unión Europea.*

En suma, el citado artículo 7 establece los requerimientos a seguir para digitalizar de forma certificada todas las facturas y demás documentos fiscales con valor legal en España. Mientras que la Resolución de 24 de octubre de 2007 de la Agencia Estatal de Administración Tributaria de España, ahonda en requerimientos de plan de gestión de la calidad, auditoria informática, formatos de conservación, aplicación de procesos de digitalización, protocolos y normas de seguridad, softwares etc.

Es importante precisar que aunque en la normatividad española citada no se establece alguna figura como el TLA, sí hace referencia a un software de digitalización que será auditado y presentado ante la Agencia Estatal de Administración Tributaria de España para que pueda funcionar a efectos de dar validez jurídica a las imágenes provenientes de un proceso de digitalización certificada.

Retomando el ámbito de competencia mexicano, la autoridad encargada de emitir los lineamientos en esta temática es la Secretaria de Economía, a través de su Dirección General de Normatividad Mercantil, conforme el Acuerdo Delegatorio publicado en el DOF el 10 de noviembre de 2006, dentro del cual se señala:

Artículo Único.- *Se delegan en la Dirección General de Normatividad Mercantil de la Secretaría de Economía, las facultades que a continuación se indican:*

(…)

d. Recibir, analizar y dar respuesta a todo tipo de trámites y promociones relacionados con los "Terceros legalmente autorizados" a los que hace referencia la NOM-151-SCFI-2002, "Prácticas comerciales-Requisitos que deben observarse para la conservación de mensajes de datos" para cotejar la migración de información a un medio digital, para su conservación con base en la norma;

e. Establecer criterios y procedimientos mediante la emisión de lineamientos para la migración de información a que hace referencia el inciso anterior;

En conclusión, dado que en el ámbito fiscal, comercial, financiero y en el derecho común se admiten como pruebas con la misma validez las imágenes archivadas en MD si se cumple con la normatividad, resulta para las empresas costoso e ineficiente el almacenar los originales en papel. Pero para que la digitalización produzca confianza y certeza jurídica en los comerciantes es necesario que sean emitidos los lineamientos que regulan el proceso de migración de papel a data y especifique los requisitos, facultades y obligaciones de la figura del TLA.

Una vez alcanzada la digitalización, la conservación del papel no tendrá sentido en la mayoría de los casos, por lo que su destrucción será posible; sin embargo, el riesgo de destruir la documentación correría a cargo de la decisión de la empresa o entidad. Se debe establecer la relación costo-beneficio del proceso de digitalización y comparar el escenario actual con soporte en papel con el escenario futuro evaluando elementos como: recurso humano, infraestructura para el resguardo, la receptividad al cambio que tengan los operadores de los documentos, etc.

Las citadas reformas a la legislación y la creación de nuevas disposiciones en materia de las TIC fueron impulsadas con el objeto de apoyar al desarrollo comercial del país, permitiendo soluciones que reduzcan costos tanto para las empresas como para la administración pública. Es por todo lo anterior que la destrucción de documentos físicos con posterioridad a su digitalización y conservación conforme a la NOM-151, resulta una gran estrategia de optimización de procesos apegada a Derecho, debiendo las autoridades administrativas y judiciales aceptar y promover el uso de los documentos digitalizados reconociendo su fuerza y validez jurídica.

4.5.1. Sentencia que declara nula la NOM-151-SECOFI-2002 y su entrada en vigor.

El 21 de abril del 2006, la parte actora, Banco Santander Serfin, S.A., Institución de Banca Múltiple, Grupo Financiero Santander Serfin demandó la nulidad de la NOM-151, publicada en el DOF el 4 de junio del 2002 y, la *Resolución por la que se da a conocer la fecha de entrada en vigor de la NOM-151*, publicada en el DOF el 19 de diciembre del 2005, ambas emitidas por la Secretaría de Economía, por conducto de la Dirección General de Normatividad Mercantil[317]; la cual correspondió conocer a la Cuarta Sala Regional Metropolitana del Tribunal Federal de Justicia Fiscal y Administrativa quien declaró la validez de la citada NOM-151.

Inconforme la parte actora demandó el amparo y protección federal de la cual conoció el Segundo Tribunal Colegiado en Materia Administrativa del Primer Circuito, quien mediante sentencia del 19 de mayo de 2011 lo concedió para efecto de que la Sala respectiva decretara la nulidad lisa y llana al actualizarse la hipótesis prevista en el artículo 51, fracción IV, de la Ley Federal de Procedimiento Contencioso Administrativo, consistente en que los actos impugnados (la NOM-151 y su entrada en vigor) fueron dictados en contravención a las disposiciones aplicables.

En los considerandos la Sala señaló que el anteproyecto presentado por la SE y antecedente de la Norma Oficial Mexicana impugnada contraviene lo dispuesto por el artículo 45 de la Ley Federal de Metrología y Normalización (LFMN), el cual dispone lo siguiente:

[317] Resolución de fecha 13 de julio de 2011 dictada por la Cuarta Sala Regional Metropolitana del Tribunal Federal de Justicia Fiscal y Administrativa en el expediente número: 12598/06-17-04-6 promovido por Banco Santander Serfin, S.A., Institución de Banca Múltiple, Grupo Financiero Santander Serfin, que demanda la nulidad de la Norma Oficial Mexicana NOM-151-SCFI-2002: "Prácticas comerciales: Requisitos que deben observarse para la conservación de mensajes de datos", expedida por la Secretaría de Economía.

Articulo 45.- *Los anteproyectos que se presenten en los comités para discusión se acompañarán de una manifestación de impacto regulatorio, en la forma que determine la Secretaría, que* ***deberá contener una explicación sucinta*** *de la finalidad de la norma, de las medidas propuestas****, de las alternativas consideradas y de las razones por las que fueron desechadas,*** *una comparación de dichas medidas con los antecedentes regulatorios,* ***así como una descripción general de las ventajas y desventajas y de la factibilidad técnica de la comprobación del cumplimiento con la norma.*** *Para efectos de lo dispuesto en el artículo 4A de la Ley Federal de Procedimiento Administrativo, la manifestación debe presentarse a la Secretaría en la misma fecha que al comité.*

(Énfasis añadido)

Cuando la norma pudiera tener un amplio impacto en la economía o un efecto sustancial sobre un sector específico, la manifestación deberá incluir un análisis en términos monetarios del valor presente de los costos y beneficios potenciales del anteproyecto y de las alternativas consideradas, así como una comparación con las normas internacionales. Si no se incluye dicho análisis conforme a este párrafo, el comité o la Secretaría podrán requerirlo dentro de los 15 días naturales siguientes a que se presente la manifestación al comité, en cuyo caso se interrumpirá el plazo señalado en el artículo 46, fracción I.

Cuando el análisis mencionado no sea satisfactorio a juicio del comité o de la Secretaría, éstos podrán solicitar a la dependencia que efectúe la designación de un experto, la cual deberá ser aprobada por el presidente de la Comisión Nacional de Normalización y la Secretaría. De no existir acuerdo, estos últimos nombrarán a sus respectivos expertos para que trabajen conjuntamente con el designado por la dependencia. En ambos casos, el costo de la contratación será con cargo al presupuesto de la dependencia o a los particulares interesados. Dicha solicitud podrá hacerse desde que se presente el análisis al comité y hasta 15 días naturales después de la publicación prevista en el artículo 47, fracción I. Dentro de los 60 días naturales siguientes a la contratación del o de los expertos, se deberá efectuar la revisión del análisis y entregar comentarios al comité, a partir de lo cual se computará el plazo a que se refiere el artículo 47, fracción II.

(Énfasis añadido)

El artículo 45 de la LFMN dispone claramente los elementos que debe contener el anteproyecto que se presente de la NOM-151, de manera que, en la especie, esta última es ilegal por omitir por completo hacer una descripción general de las ventajas y desventajas de la misma y una descripción o explicación sucinta de la factibilidad técnica de la comprobación del cumplimiento de aquella, pues del análisis del anteproyecto ofrecido como prueba, al cual se otorga valor probatorio pleno en términos del artículo 46 de la Ley Federal de Procedimiento Contencioso Administrativo, no consta manifestación alguna en dicho sentido.

Por otra parte, por lo que hace al elemento de las “Alternativas consideradas”, la Sala estimó que la NOM impugnada también es ilegal, pues si bien es cierto que el anteproyecto de la misma contiene un apartado en tal sentido, del análisis que se hace del mismo se desprende que no se hace referencia a ninguna alternativa, ni tampoco se indican los motivos por los cuales las mismas fueron desechadas, sino que únicamente se indica que con la NOM propuesta se tendrán diversos beneficios, pero sin indicar las alternativas posibles, ni las razones de hecho y

de derecho por las cuales las mismas se desestiman. En efecto, en dicho apartado de "Alternativas Consideradas" se asentó lo siguiente:

> ***2.1 Alternativas consideradas:***
> *Los comerciantes están obligados a conservar por un plazo mínimo de diez años los originales de aquellos mensajes de datos en que se consignen contratos, convenios o compromisos que den nacimiento a derechos y obligaciones.*
>
> *Para efectos de la conservación o presentación de originales, en el caso de mensajes de datos, se requerirá que la información se haya mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y sea accesible para su ulterior consulta.*
>
> *Lo anterior, tomando en consideración que existen en nuestro país usuarios de Internet que constituyen una importante alternativa de negocios para las empresas que realizan o planean realizar comercio electrónico. Dichos usuarios constituyen además un sector del mercado donde existe un potencial de negocio sin precedente, debido a que está conformado por usuarios con poder adquisitivo, facilidad para realizar transacciones en línea y experiencia en el uso de la red.*

Por otra parte, la NOM impugnada fue publicada con un cambio distinto al considerado en los comentarios aceptados y formulados al proyecto de dicha norma general, debido a que en los comentarios se recomendó y aceptó que se definiera como *Compromiso: a cualquier acuerdo de voluntades diferente del contrato y del convenio, que genere derechos y obligaciones;* sin embargo, en la NOM publicada se definió *Compromiso: a cualquier acto jurídico diferente del contrato y del convenio, que genere derechos y obligaciones*. En efecto, como constata con la comparación que se hace entre la NOM oficial impugnada publicada en el DOF el día 4 de junio de 2002 y en los comentarios hechos valer publicados en el DOF el 20 de mayo de 2002, dicha diferencia existe:

Norma Oficial Mexicana publicada en el Diario Oficial de la Federación el 4 de junio de 2002	
*3.14 Compromiso. A cualquier acto jurídico diferente del **contrato o del convenio**, que genere derechos y obligaciones Comentario aceptado por el grupo de trabajo y publicado en el Diario Oficial de la Federación el día 20 de mayo de 2002.*	*3.14 Compromiso: a cualquier **acuerdo de voluntades diferente del contrato** y del convenio, que genere derechos y obligaciones.*

Finalmente, la NOM impugnada es ilegal por violentar lo dispuesto por el artículo 28, fracción VI, del Reglamento de la LFMN, al no indicarse en el texto de la misma, si la evaluación de conformidad podrá ser realizada por personas acreditadas y aprobadas por las dependencias competentes.

> ***Artículo 28.*** *Para los efectos de los artículos 41 y 48 de la Ley, el contenido de las normas oficiales mexicanas, incluidas las que se expidan en caso de emergencia, se ajustará a lo siguiente: (…)*
> *VI. Deberán señalar si la evaluación de la conformidad podrá ser realizada por personas acreditadas y aprobadas por las dependencias competentes, y cuando exista concurrencia de competencias,*

contener la mención expresa de las autoridades que llevarán a cabo dicha evaluación o vigilarán su cumplimiento.(…)

Del análisis del artículo transcrito, se concluye que el Reglamento de la LFMN es muy claro al indicar que toda NOM debe contener el señalamiento expreso de que la evaluación de la conformidad podrá ser realizada por personas acreditadas y aprobadas por las dependencias competentes y cuando exista concurrencia de competencias de las autoridades que llevarán a cabo dicha evaluación o vigilancia de su cumplimiento.

En ese tenor, si bien es cierto que en el apartado 6 "Vigilancia" de la NOM Mexicana impugnada se indica que "La vigilancia de la NOM estará a cargo de la SE conforme a sus atribuciones y la legislación aplicable"; también es cierto que no se hace mención alguna, ni en dicho apartado, ni en ninguna parte de dicha norma general, de las personas acreditadas y aprobadas por dicha dependencia competente que efectuarán la evaluación de la conformidad de la NOM.

En efecto, una de las dos consecuencias inmediatas que tuvo este procedimiento fueron:

a) La publicación del Acuerdo por el que se delegan facultades a la Dirección General de Normatividad Mercantil en materia de evaluación de la conformidad de la *Norma Oficial Mexicana NOM-151-SCFI-2002, prácticas come*rciales-requisitos que deben observarse *para la conservación de mensajes de datos* y otros servicios de firma electrónica competencia de la SE, publicado en el DOF el 10 de noviembre de 2006[318].
b) La publicación del Anteproyecto Norma Oficial Mexicana *NOM-151-SCFI-2015 Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos* (Anteproyecto de NOM-151-SECOFI-2015).

4.5.2. Anteproyecto de NOM-151-SECOFI-2015 del 25 de noviembre de 2015.

La falta de actualización durante el periodo de vida de la constancia de los elementos de seguridad electrónica en la conservación de los MD y digitalización de documentos que considera la NOM-151-SECOFI-2002 provoca vulnerabilidad con el paso del tiempo ante posibles delitos cibernéticos. Por ello, la modernización de la regulación nacional es indispensable para asegurar la integridad y autenticidad de los MD por periodos prolongados de tiempo respecto a protocolos internacionales, lo que mejorará el nivel en los elementos de seguridad electrónica de las constancias de la conservación de MD y digitalización de documentos.

Asimismo, los riesgos persistentes respecto a la falsificación de datos personales, fraudes, estafas, extorsión y robo de información, motivan la consideración reformas y modificaciones a la actual Norma Oficial Mexicana. Por ejemplo, de los incidentes cibernéticos denunciados en 2013, aproximadamente 39% fueron contra instituciones académicas, 31% contra instituciones gubernamentales, 26% contra entidades del sector privado y 4% contra otras entidades.

[318] Accesible en: http://dof.gob.mx/nota_detalle.php?codigo=4937232&fecha=10/11/2006, consultada el 3 de mayo de 2014.

De ahí que el pasado 25 de Noviembre de 2015 en el portal oficial de la Comisión Federal de Mejora Regulatoria (COFEMER)[319] sometiera a consulta pública el *Anteproyecto Norma Oficial Mexicana NOM-151-SCFI-2015: Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos* (Anteproyecto de NOM-151-SECOFI-2015). La razón de su emisión consiste en que se advirtió que desde la publicación de la Norma vigente ha transcurrido más de cinco años sin que se haya realizado modificaciones y/o adecuaciones a la misma, por lo que la SE consideró necesario a efecto de cumplimentar lo establecido en el artículo 51, cuarto párrafo de la Ley Federal sobre Metrología y Normalización, actualizar los elementos de datos y la digitalización de documentos en términos de lo dispuesto por el CCo.

Asimismo, la SE identificó la problemática que hace necesaria la actualización del marco regulatorio, al adecuar el contenido de la Norma vigente, que permite el cumplimiento de la obligación a cargo de los comerciantes que utilicen MD para realizar actos de comercio, de conservar el plazo establecido en el CCo y cuyo contenido debe mantenerse íntegro e inalterado a partir del momento en que se generó por primera vez en su forma definitiva, debiendo ser accesible para su posterior consulta, así como la digitalización de documentos.

Las *Unidades Económicas*[320] son las encargadas de conservar los MD, así como la digitalización de documentos en términos de los dispuesto en los artículos 33, 38 y 49 del CCo. En el reciente censo económico de 2014 del Instituto Nacional de Estadística y Geografía (INEGI) se tienen contabilizadas 4'230,745 Unidades Económicas en el país, mismas que están distribuidas principalmente en el Estado de México (12.6 %), Distrito Federal (9.8 %), Jalisco (7.4 %), Puebla (5.9 %) y Veracruz (5.7 %)[321].

En este sentido, la rápida evolución de los sistemas computacionales así como las amenazas a la seguridad informática y protección de datos, ha ocasionado que las regulaciones se vuelvan obsoletas en un lapso de tiempo muy breve, poniendo en riesgo las seguridad de los datos y restando confianza en las transacciones comerciales entre las Unidades Económicas. Así el

[319] A la COFEMER le corresponde supervisar el diseño de las nuevas regulaciones, promover la transparencia en su elaboración a través de la consulta pública y garantizar que éstas brindan mayores beneficios que costos para la sociedad. Para realizar estas actividades, la COFEMER mediante el Sistema de Manifestación de Impacto Regulatorio, permite que las dependencias y organismos descentralizados de la APF puedan interactuar con la Comisión, a fin de realizar la creación y envió de sus anteproyectos de regulaciones acompañados del formulario de Manifestación de Impacto Regulatorio (MIR) para luego poner estos anteproyectos a consulta pública a través de un portal donde se podrá buscar anteproyectos, realizar comentarios o recibir notificaciones acerca de anteproyectos o dependencias y finalmente que la COFEMER pueda dictaminarlos; accesible en: http://cofemersimir.gob.mx/mirs/39200, consultada el 6 de diciembre de 2015.

[320] Las Unidades Económicas "son las unidades estadísticas sobre las cuales se recopilan datos, se dedican principalmente a un tipo de actividad de manera permanente, combinando acciones y recursos bajo el control de una sola entidad propietaria o controladora, para llevar a cabo producción de bienes y servicios, sea con fines mercantiles o no. Se definen por sector de acuerdo con la disponibilidad de registros contables y la necesidad de obtener información con el mayor nivel de precisión analítica". Definición del Instituto Nacional de Estadística y Geografía, para la Encuesta mensual sobre establecimientos comerciales, 2007, accesible en: http://www.inegi.org.mx/lib/glosario/paginas/contenido.aspx?id_nivel=01030000000000&id_termino=289&id_capitulo=16&g=een&c=10614&s=est&e=, consulta del 9 de diciembre de 2015.

[321] Con base en el Censo Económico 2014 del INEGI, accesible en http://www.inegi.org.mx/est/contenidos/proyectos/ce/ce2014/default.aspx, consulta del 9 de diciembre de 2015.

aumento de los delitos cibernéticos[322] ha ido a la alza. De acuerdo a datos de la División Científica de la Policía Federal, los incidentes de seguridad cibernética aumentaron 113% de 2012 a 2013. Los datos preliminares para 2014 sugieren un aumento aún más pronunciado, aproximadamente el 39% fueron contra instituciones académicas, 31% contra instituciones gubernamentales, 26% a entidades del sector privado y 4% a otras entidades[323].

Igualmente, se detectaron incrementos de los incidentes relativos a amenazas persistentes avanzadas contra medianas empresas y el uso de códigos maliciosos a fin de *hackear* información a usuarios para luego intentar extorsionarlos. A mayor abundamiento, incrementó el uso de malware que emplea encriptaciones de seguridad complejas para atacar a los servidores de pequeñas empresas, lo que tiene un impacto cada vez mayor en el sector productivo. Los incidentes de seguridad cibernética más denunciados abarcan el uso de *malware, phishing, hackeos,* vandalismo y las intrusiones en sistemas. Los incidentes de fraudes de comercio electrónico, las estafas, los fraudes a la banca electrónica y la extorsión son los más frecuentes[324].

De los datos y consideraciones anteriores se advirtió la necesidad de que la NOM-151-SECOFI-2002 vigente sea adecuada a los cambios tecnológicos que se hayan generado en la materia; dicha adecuación pretende lograr, a través del establecimiento de requisitos mínimos de los MD resultantes de las digitalizaciones, procedimientos de migración de soporte fisco a un medio electrónico, incluyendo en, el formato niveles de calidad, condiciones técnicas y estándares aplicables conforme al apéndice de documentos modificatorios que se evaluará en los siguientes párrafos. Asimismo, los programas informáticos para la conservación de los MD y los equipos para la digitalización deberán cumplir con los métodos que se describen en los apéndices 7 y 8 -que en el Anteproyecto son sustituidos por los apéndices A y B.

Cabe mencionar que el proceso de digitalización deberá ser controlado por un tercero legalmente autorizado (TLA), que constará que dicha migración se realice íntegra e inalterablemente tal y como se generó por primera vez en su forma definitiva, para lo cual emitirá una constancia de conservación.

Para hacer frente a dicha problemática, la SE elaboró este Anteproyecto de NOM-151-SECOFI-2015 (ver Apéndice IV: Anteproyecto NOM-151-SCFI-2015), que actualiza la NOM-151-SECOFI-2002, vigente por más de diez años. El anteproyecto incluye métodos para la conservación de MD así como de los equipos para la digitalización a que se refieren los Apéndices 7 y 8 del Anteproyecto.

Además, se insiste en que el proceso de digitalización deberá ser controlado por un tercero legalmente autorizado, que constatará que dicha migración se realice íntegra e

[322] Es el robo o manipulación de datos o servicios por medio de piratería o virus, el robo de identidad y fraudes en el sector bancario o del comercio electrónico.
[323] Ver "Tendencias de Seguridad Cibernética en América Latina y el Caribe", OEA-Symantec, junio de 2014, accesible en: https://www.symantec.com/.../b-cyber-security-trends-report-lamc.pdf, p. 68, consulta de 9 de diciembre de 2015.
[324] Ídem, p. 69.

inalterablemente tal y como se generó por primera vez en su forma definitiva. El tercero legalmente autorizado deberá ser un PSC acreditado para tales efectos. Finalmente, el instrumento legal propuesto tiene como objetivo considerar la factibilidad técnica de la comprobación del cumplimiento de la norma propuesta, así como de la existencia de infraestructura técnica para ello.

El 8 de enero de 2016, con fundamento en los artículos 69-E, 69-G y 69-J de la Ley Federal de Procedimiento Administrativo, la Comisión Federal de Mejora Regulatoria (COFEMER) expidió el primer dictamen de valoración de la propuesta de NOM[325], el cual no es definitivo e incluye la *Manifestación de Impacto Regulatorio* (MIR)[326] , pero en él refiere varios puntos de relevancia, entre ellos:

- Se incluye además de la propuesta de la "digitalización", la de "correo electrónico certificado[327]".
- Sus disposiciones generales obligan a los comerciantes a observar los métodos que se describen en sus apéndices denominados "A Normativo: Constancia conservación de MD" y "B Normativo: Digitalización de documentos en soporte físico", a fin de conservar los MD, así como para la digitalización de toda o parte de la documentación en soporte físico relacionada con sus negocios. La información que se desee conservar se podrá almacenar en uno o varios archivos diferentes y/o en una o varias computadoras.
- Los requisitos mínimos de los MD resultantes de las digitalizaciones, procedimiento de migración de soporte físico a un medio electrónico, incluyendo el formato, niveles de calidad, condiciones técnicas y estándares aplicables, se determinan en el apéndice 8 del proyecto de Norma Oficial Mexicana. Mientras que los programas informáticos para la conservación de los MD así como los equipos para digitalización, deberán cumplir con los métodos que se describen en los apéndices 7 y 8 citados.
- La constancia de emisión de la firma electrónica avanzada por un PSC o Autoridad Certificadora observarán los términos establecidos en el *A Normativo: Constancia conservación de MD*. El almacenamiento de las constancias de conservación así como los documentos digitalizados a los que se refiere el presente proyecto quedarán en control del usuario pudiendo contratar para su administración a terceros.
- Se establecen nuevas obligaciones en los artículos. 4.1, 4.4, 5.1 del anteproyecto para estar en concordancia con lo establecido en los proyectos internacionales de seguridad como son el *RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) y RFC 5816 ESSCertIDv2 Update for RFC 1361*, mismos que establecen que la seguridad en la conservación de los MD y digitalización de documentos debe ser a lo largo del

[325] http://www.cofemersimir.gob.mx/expediente/18066/emitido/39931/COFEME, consulta del 9 de enero de 2016.

[326] Publicada en el DOF el 26 de julio de 2010 y sus modificaciones.

[327] Correo Electrónico Certificado se envía como correo normal, sin embargo en el proceso es protegido, resguardado y certificado, aumentando la seguridad desde emisor hasta el receptor garantizando que no ha sido alterada la información. El Correo Electrónico Certificado garantiza la identidad y aceptación del emisor, la autenticidad e integridad del mensaje así como la disponibilidad y seguridad de los documentos de archivo electrónico. El Certificado se puede validar con un simple clic desde el mismo cliente de correo del usuario o introduciendo el ID del documento en el portal de la institución, además debe señalase que se lleva un registro de los accesos al mensaje. Algunos países que utilizan el correo electrónico certificado son: Estados Unidos, Francia, Reino Unido, España, Alemania, Australia, Brasil, Costa Rica y Colombia.

tiempo, las herramientas consideradas tienen, entre otras cualidades, la de permitir una renovación de la vigencia más allá de 10 años.

- En los apéndices A y B del Anteproyecto se describen los requisitos a seguir para la obtención de la constancia conservación de MD y digitalización de documentos en soporte físico, respectivamente.
- Se establecen los métodos que deben observar los comerciantes para conservar los MD así como para la digitalización de toda o parte de la documentación en soporte físico relacionada con sus negocios, mismo que se describe en los apéndices A y B. Lo anterior, con el objetivo de mejorar los protocolos de seguridad en la materia de la presente norma.
- El anteproyecto se encuentra armonizado con las normas y lineamientos internacionales, según el nivel de riesgo del producto en particular.
- Se incluyen definiciones de aquellos conceptos que se utilizarán a lo largo del texto de la norma.
- No se establece un esquema de sanciones específico, la verificación y vigilancia se enmarcan en el sistema establecido en la Ley Federal de Protección al Consumidor, su Reglamento, la Ley Federal de Metrología y Normalización y su Reglamento. Además, no se observan los procedimientos propuestos para su cumplimiento.

4.6. Proyecto de Iniciativa de Decreto por el que se reforman y adicionan diversas disposiciones del Código de Comercio y del Código Penal Federal del 4 de noviembre de 2015

En los próximos días, la Iniciativa de Proyecto de Decreto por el que se reforman y adicionan diversas disposiciones del CCo y del Código Penal Federal enviada por la H. Cámara de Diputados del Congreso de la Unión[328], será publicada y vigente; dada la relevancia del tema se detalla a continuaciones los motivos y artículos a adicionar y, en su caso, a reformar.

a) Se reforma el CCo para:

i) Establecer nuevos mecanismos que permitan que los "comerciantes" optimicen su "contabilidad" a través del uso de medios digitales para la conservación de la documentación relacionada con la empresa.
ii) Adicionar un capítulo denominado *"*De la Digitalización*"*. En términos generales, los "comerciantes" podrán digitalizar sus documentos en el formato que determine, y tendrán que ser certificados por un PSC acreditados por la SE.
iii) Fijar en la "Norma Oficial" los lineamientos sobre la digitalización y conservación de MD (la información generada, enviada, recibida o archivada por medios electrónicos, ópticos o

[328] Decreto por el que se reforman y adicionan diversas disposiciones del Código de Comercio y del Código Penal Federal, documento de la Comisión de Comercio y Fomento Industrial de la Cámara de Senadores, publicado el 4 de noviembre de 2015, accesible en: http://sil.gobernacion.gob.mx/Archivos/Documentos/2016/03/asun_3342045_20160303_1456849421.pdf, consultado: 31 de noviembre de 2015.

cualquier otra tecnología).
iv) Otorgar mayores facultades a los actuales "PSC", con la finalidad de incrementar su oferta de productos y servicios.
iii) Estructura de la reforma:

Código de Comercio	
Tema: Contabilidad Mercantil.	Artículos 34, 38 y 46 Bis.
Tema: Digitalización de Documentos.	Artículos 89, 89 bis, 95 bis 1, 95 bis 2, 95 bis 3, 95 bis 4, 95 bis 4 y 95 bis 5.
Tema: Prestadores de Servicios de Certificación	Artículos 100, 101, 102, 108, 110.

b) Adicionar una fracción VII, al artículo 246, del Código Penal Federal para sancionar al PSC, cuando realice actividades sin acreditación la correspondiente.

Código Penal Federal	
Tema: Falsificación de Documentos	Artículos 246, fracción VII

Finalidad de la reforma por áreas:

a) Reducir la cantidad de insumos necesarios para el adecuado cumplimiento de sus obligaciones en materia de conservación de documentos.

Código de Comercio	
Texto Vigente	**Texto** **Minuta adaptada por las Cámaras de Diputados y Senadores**
CAPITULO III De la Contabilidad Mercantil Artículo 34.- **Cualquiera que sea el sistema de registro que se emplee, se deberán llevar debidamente encuadernados, empastados y foliados el libro mayor y, en el caso de las personas morales, el libro o los libros de actas. La encuadernación de estos libros podrá hacerse a posteriori, dentro de los tres meses siguientes al cierre del ejercicio; sin perjuicio de los requisitos especiales que establezcan las leyes y reglamentos fiscales para los registros y documentos que tengan relación con las obligaciones fiscales del comerciante.**	**CAPITULO III** **De la Contabilidad Mercantil** (Énfasis en negritas es nuestro) **Artículo 34.** Cualquiera que sea el sistema de registro que se emplee, **los comerciantes deberán llevar un libro mayor y, en el caso de las personas morales, el libro o los libros de actas; sin perjuicio de los requisitos especiales que establezcan las leyes y reglamentos fiscales para los registros y documentos que tengan relación con las obligaciones fiscales del comerciante.** **Los comerciantes podrán optar por conservar el libro mayor y sus libros de actas en formato impreso, o en medios electrónicos, ópticos o de**

	cualquier otra tecnología, siempre y cuando, en estos últimos medios se observe lo establecido en la norma oficial mexicana sobre digitalización y conservación de mensajes de datos que para tal efecto emita la Secretaría. **Tratándose de medios impresos, los libros deberán estar encuadernados, empastados y foliados. La encuadernación de estos libros podrá hacerse a posteriori, dentro de los tres meses siguientes al cierre del ejercicio.**
Artículo 38.- **El comerciante deberá conservar, debidamente archivados, los comprobantes originales de sus operaciones, de tal manera que puedan relacionarse con dichas operaciones y con el registro que de ellas se haga, y deberá conservarlos por un plazo mínimo de diez años.**	**Artículo 38.** El comerciante deberá conservar, debidamente archivados, los comprobantes originales de sus operaciones, **en formato impreso, o en medios electrónicos, ópticos o de cualquier otra tecnología, siempre y cuando, en estos últimos medios se observe lo establecido en la norma oficial mexicana sobre digitalización y conservación de mensajes de datos que para tal efecto emita la Secretaría**, de tal manera que puedan relacionarse con dichas operaciones y con el registro que de ellas se haga, y deberá conservarlos por un plazo mínimo de diez años.

b) Introducir en sus negocios los avances tecnológicos en materia de digitalización, y conservación de documentos en formato electrónico a fin de ser eficientes los procesos, ahorrar espacio, costos de impresión y fotocopiado, y brindar mayor agilidad en los tiempos de respuesta a las solicitudes de información que les sean requeridas por las autoridades, tanto administrativas, como en su caso, las judiciales.

Código de Comercio	
Texto Vigente	Texto **Minuta adaptada por las Cámaras de Diputados y Senadores**
TÍTULO SEGUNDO: De Comercio Electrónico **CAPITULO I:** De los Mensajes de Datos Artículo 89.- **Las disposiciones de este Título regirán en toda la República Mexicana en asuntos del orden comercial, sin perjuicio de lo dispuesto en los tratados internacionales de los que México sea parte.** **Las actividades reguladas por este Título se someterán en su interpretación y aplicación a los**	**Artículo 89.-** **(…)**

principios de neutralidad tecnológica, autonomía de la voluntad, compatibilidad internacional y equivalencia funcional del Mensaje de Datos en relación con la información documentada en medios no electrónicos y de la Firma Electrónica en relación con la firma autógrafa. **En los actos de comercio y en la formación de los mismos podrán emplearse los medios electrónicos, ópticos o cualquier otra tecnología. Para efecto del presente Código, se deberán tomar en cuenta las siguientes definiciones:** Certificado: **Todo Mensaje de Datos u otro registro que confirme el vínculo entre un Firmante y los datos de creación de Firma Electrónica.** Datos de Creación de Firma Electrónica: **Son los datos únicos, como códigos o claves criptográficas privadas, que el Firmante genera de manera secreta y utiliza para crear su Firma Electrónica, a fin de lograr el vínculo entre dicha Firma Electrónica y el Firmante.** Destinatario: **La persona designada por el Emisor para recibir el Mensaje de Datos, pero que no esté actuando a título de Intermediario con respecto a dicho Mensaje.** Emisor**: Toda persona que, al tenor del Mensaje de Datos, haya actuado a nombre propio o en cuyo nombre se haya enviado o generado ese mensaje antes de ser archivado, si éste es el caso, pero que no haya actuado a título de Intermediario.** Firma Electrónica: **Los datos en forma electrónica consignados en un Mensaje de Datos, o adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al Firmante en relación con el Mensaje de Datos e indicar que el Firmante aprueba la información contenida en el Mensaje de Datos, y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio.** Firma Electrónica Avanzada o Fiable: **Aquella Firma Electrónica que cumpla con los requisitos contemplados en las fracciones I a IV del artículo 97.**	**Digitalización: Migración de documentos impresos a mensaje de datos, de acuerdo con lo dispuesto en la norma oficial mexicana sobre digitalización y conservación de mensajes de datos que para tal efecto emita la Secretaría.** **(…)** **Prestador de servicios de certificación**: La persona o institución pública que preste servicios relacionados con firmas electrónicas, expide los certificados **o presta servicios relacionados como la conservación de mensajes de datos, el sellado digital de tiempo y la digitalización de documentos impresos, en los términos que se establezca en la norma oficial mexicana sobre digitalización y conservación de mensajes de datos que para tal efecto emita la Secretaría.** **(…)** **Sello digital de tiempo: el registro que prueba que un dato existía antes de la fecha y hora de emisión del citado Sello, en los términos que se establezca en la norma oficial mexicana sobre digitalización y conservación de mensajes de datos que para tal efecto emita la Secretaría.** **(…)**

En aquellas disposiciones que se refieran a Firma Digital, se considerará a ésta como una especie de la Firma Electrónica. Firmante: **La persona que posee los datos de la creación de la firma y que actúa en nombre propio o de la persona a la que representa.** **Intermediario: En relación con un determinado Mensaje de Datos, se entenderá toda persona que, actuando por cuenta de otra, envíe, reciba o archive dicho Mensaje o preste algún otro servicio con respecto a él.** Mensaje de Datos: **La información generada, enviada, recibida o archivada por medios electrónicos, ópticos o cualquier otra tecnología.** Parte que Confía: **La persona que, siendo o no el Destinatario, actúa sobre la base de un Certificado o de una Firma Electrónica.** Prestador de Servicios de Certificación: **La persona o institución pública que preste servicios relacionados con Firmas Electrónicas y que expide los Certificados, en su caso.** Secretaría: **Se entenderá la Secretaría de Economía.** Sistema de Información: **Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma Mensajes de Datos.** **Titular del Certificado: Se entenderá a la persona a cuyo favor fue expedido el certificado.**	
Artículo 89 bis.- **No se negarán efectos jurídicos, validez o fuerza obligatoria a cualquier tipo de información por la sola razón de que esté contenida en un Mensaje de Datos.**	**Artículo 89 bis.-** No se negarán efectos jurídicos, validez o fuerza obligatoria a cualquier tipo de información por la sola razón de que esté contenida en un Mensaje de Datos. **Por tanto, dichos mensajes podrán ser utilizados como medio probatorio en cualquier diligencia ante autoridad legalmente reconocida, y surtirán los mismos efectos jurídicos que la documentación impresa, siempre y cuando los mensajes de datos se ajusten a las disposiciones de este Código y a los lineamientos normativos correspondientes.**
Sin Correlativo	**Capítulo I Bis** **De la Digitalización** **Artículo 95 bis 1.** Para el caso de los servicios de digitalización se estará a lo siguiente:

	a. En todo caso, los documentos podrán ser digitalizados en el formato que determine el comerciante. b. Una vez concluida la digitalización del documento, deberá acompañarse al mismo, así como a cada uno de los anexos que en su caso se generen, la firma electrónica avanzada del comerciante, y del prestador de servicios de certificación que ejecutó las actividades de digitalización, en caso de que así haya sido. c. Cuando un prestador de servicios de certificación realice la digitalización de un documento, habrá presunción legal sobre el adecuado cumplimiento de las disposiciones legales y normativas relativas a dicho proceso, salvo prueba en contrario. d. La información que en virtud de acuerdos contractuales quede en poder de un prestador de servicios de certificación, se regirá por lo dispuesto en la Ley Federal de Protección de Datos Personales en posesión de los Particulares. e. En todo caso, el prestador de servicios de certificación que ejecutó las actividades de digitalización deberá mantener la confidencialidad de la información, salvo por mandato judicial.
Sin Correlativo	**Artículo 95 bis 2.** En materia de conservación de mensajes de datos, será responsabilidad estricta del comerciante mantenerlos bajo su control, acceso y resguardo directo, a fin de que su ulterior consulta pueda llevarse a cabo en cualquier momento.
Sin Correlativo	**Artículo 95 bis 3.** En el caso de documentos digitalizados o almacenados por prestadores de servicios de certificación, se necesitará que éstos cuenten con acreditación para realizar sus actividades a que hace referencia el artículo 102 de este Código.
Sin Correlativo	**Artículo 95 bis 4.** En caso que los servicios de digitalización sean contratados a un prestador de servicios de certificación, éste presumirá la buena fe del contratante, así como la legitimidad de los documentos que le son confiados a digitalizar, limitándose a reflejarlos fiel e íntegramente en los medios electrónicos que le sean solicitados, bajo las penas en que incurren aquellos que cometen delitos en materia de falsificación de documentos. Contra la entrega de la información digitalizada y su correspondiente cotejo, el contratante deberá firmar una cláusula de satisfacción del servicio prestado, y proceder a adjuntar su firma electrónica avanzada a la información.

	Si el contratante no adjunta su firma electrónica avanzada a la información digitalizada, ésta no podrá surtir efecto legal alguno, y será de carácter meramente informativo. Asimismo, el prestador de servicios deberá implementar el mecanismo tecnológico necesario, a fin de que, una vez digitalizado y entregado el documento electrónico a satisfacción del cliente, éste no pueda ser modificado, alterado, enmendado o corregido de modo alguno, en los términos que se establezca en la norma oficial mexicana sobre digitalización y conservación de mensajes de datos que para tal efecto emita la Secretaría.
Sin Correlativo	**Artículo 95 bis 5.** Se presumirá que aquellos prestadores de servicios de certificación que ofrezcan el servicio de almacenamiento de mensajes de datos, cuentan con los medios tecnológicos suficientes para garantizar razonablemente a los contratantes que la información bajo su control podrá ser ulteriormente consultada en cualquier tiempo, a no ser que existan causas demostradas de fuerza mayor o que no sean imputables al Prestador de Servicios autorizado.
Sin Correlativo	**Artículo 95 bis 6.** Para los efectos de este Título, la Secretaría tendrá las siguientes facultades: I. Expedir y revocar las acreditaciones como Prestadores de Servicios de Certificación a que se refieren los artículos 95 Bis 3,100 y 102 de este Código; y II. Podrá verificar en cualquier tiempo el adecuado desarrollo de las operaciones de los prestadores de servicios de certificación.

c) Otorgar mayores facultades a los actuales PSC como, la emisión de sellos digitales de tiempo (Registro que prueba que un dato existía antes de la fecha y hora de emisión del citado Sello), la conservación de MD, y la digitalización de documentación impresa.

En la reforma del 27 de agosto de 2003, se incluyó dentro del *Título Segundo: De Comercio Electrónico*, un *Capítulo III: De los Prestadores de Servicios de Certificación.* De conformidad con lo dispuesto por el artículo 100 del CCo podrán ser PSC, previa acreditación ante la Secretaría de Economía.

- Los notarios públicos y corredores públicos;
- Las personas morales de carácter privado, y
- Las instituciones públicas, conforme a las leyes que les son aplicables.

Asimismo, se estableció que la facultad de expedir Certificados por parte de los PSC, no conlleva fe pública por sí misma, así los notarios y corredores públicos podrán llevar a cabo certificaciones que impliquen o no la fe pública, en documentos en papel, archivos electrónicos, o en cualquier otro medio o sustancia en el que pueda incluirse información.

En este sentido, la modificación que se plantea propone ampliar este esquema, al establecer que los PSC al prestar servicios relacionados, como la conservación de MD, el sellado digital de tiempo, o la digitalización de documentos impresos, así como fungir en calidad de tercero legalmente autorizado conforme a lo que se establezca en la norma oficial mexicana, no conllevan fe pública por sí misma.

Código de Comercio	
Texto Vigente	Texto Minuta adaptada por las Cámaras de Diputados y Senadores
CAPITULO III De los Prestadores de Servicios de Certificación **Artículo 100.-** Podrán ser Prestadores de Servicios de Certificación, previa acreditación ante la Secretaría: I. Los notarios públicos y corredores públicos; II. Las personas morales de carácter privado, y III. Las instituciones públicas, conforme a las leyes que les son aplicables. La facultad de expedir Certificados no conlleva fe pública por sí misma, así los notarios y corredores públicos podrán llevar a cabo certificaciones que impliquen o no la fe pública, en documentos en papel, archivos electrónicos, o en cualquier otro medio o sustancia en el que pueda incluirse información.	CAPITULO III De los Prestadores de Servicios de Certificación (Énfasis en negritas es nuestro) **Artículo 100. …** I. a III. … Las facultades de expedir certificados o de prestar servicios relacionados, como la conservación de mensajes de datos, el sellado digital de tiempo, o la digitalización de documentos impresos, así como fungir en calidad de tercero legalmente autorizado conforme a lo que se establezca en la norma oficial mexicana, no conllevan fe pública por sí misma, así, los notarios y corredores públicos podrán llevar a cabo certificaciones que impliquen o no la fe pública, en documentos en papel o mensajes de datos. Quien aspire a obtener la acreditación como prestador de servicios de certificación, podrá solicitarla respecto de uno o más servicios, a su conveniencia.
Artículo 101.- Los Prestadores de Servicios de Certificación a los que se refiere la fracción II del artículo anterior, contendrán en su objeto social las actividades siguientes: I. Verificar la identidad de los usuarios y su vinculación con los medios de identificación electrónica;	**Artículo 101.** Los prestadores de servicios de certificación a los que se refiere la fracción II del artículo anterior, contendrán en su objeto social las actividades siguientes, según corresponda y de acuerdo con el servicio que pretenda ofrecer: I. a II. …

II. Comprobar la integridad y suficiencia del Mensaje de Datos del solicitante y verificar la Firma Electrónica de quien realiza la verificación; III. Llevar a cabo registros de los elementos de identificación de los Firmantes y de aquella información con la que haya verificado el cumplimiento de fiabilidad de las Firmas Electrónicas Avanzadas y emitir el Certificado, y IV. Cualquier otra	III. Llevar a cabo registros de los elementos de identificación de los Firmantes y de aquella información con la que haya verificado el cumplimiento de fiabilidad de las Firmas Electrónicas Avanzadas y emitir el Certificado; IV. Expedir sellos digitales de tiempo para asuntos del orden comercial; V. Emitir constancias de conservación de mensajes de datos; VI. Prestar servicios de digitalización de documentos; y VII. Cualquier otra actividad no incompatible con las anteriores.
Artículo 102.- Los Prestadores de Servicios de Certificación que hayan obtenido la acreditación de la Secretaría deberán notificar a ésta la iniciación de la prestación de servicios de certificación dentro de los 45 días naturales siguientes al comienzo de dicha actividad. A) Para que las personas indicadas en el artículo 100 puedan ser Prestadores de Servicios de Certificación, se requiere acreditación de la Secretaría, la cual no podrá ser negada si el solicitante cumple los siguientes requisitos, en el entendido de que la Secretaría podrá requerir a los Prestadores de Servicios de Certificación que comprueben la subsistencia del cumplimento de los mismos: I. Solicitar a la Secretaría la acreditación como Prestador de Servicios de Certificación; II. Contar con los elementos humanos, materiales, económicos y tecnológicos requeridos para prestar el servicio, a efecto de garantizar la seguridad de la información y su confidencialidad; III. Contar con procedimientos definidos y específicos para la tramitación del Certificado, y medidas que garanticen la seriedad de los Certificados emitidos, la conservación y consulta de los registros;	**Artículo 102.** Los Prestadores de Servicios de Certificación que hayan obtenido la acreditación de la Secretaría deberán notificar a ésta la iniciación de la prestación de los servicios a que hayan sido autorizados, dentro de los 45 días naturales siguientes al comienzo de dicha actividad. A) Para que las personas indicadas en el artículo 100 puedan ser Prestadores de Servicios de Certificación, se requiere acreditación de la Secretaría, la cual podrá otorgarse para autorizar la prestación de uno o varios servicios, a elección del solicitante, y no podrá ser negada si éste cumple los siguientes requisitos, en el entendido de que la Secretaría podrá requerir a los Prestadores de Servicios de certificación que comprueben la subsistencia del cumplimento de los mismos: I. Solicitar a la Secretaría la acreditación como Prestador de Servicios de Certificación y, en su caso, de los servicios relacionados, como la conservación de mensajes de datos, el sellado digital de tiempo, y la digitalización de documentos; II. Contar con los elementos humanos, materiales, económicos y tecnológicos requeridos para prestar los servicios, a efecto

IV. Quienes operen o tengan acceso a los sistemas de certificación de los Prestadores de Servicios de Certificación no podrán haber sido condenados por delito contra el patrimonio de las personas o que haya merecido pena privativa de la libertad, ni que por cualquier motivo hayan sido inhabilitados para el ejercicio de su profesión, para desempeñar un puesto en el servicio público, en el sistema financiero o para ejercer el comercio; V. Contar con fianza vigente por el monto y condiciones que se determinen en forma general en las reglas generales que al efecto se expidan por la Secretaría; VI. Establecer por escrito su conformidad para ser sujeto a Auditoría por parte de la Secretaría, y VII. Registrar su Certificado ante la Secretaría. B) Si la Secretaría no ha resuelto respecto a la petición del solicitante, para ser acreditado conforme al artículo 100 anterior, dentro de los 45 días siguientes a la presentación de la solicitud, se tendrá por concedida la acreditación.	de garantizar la seguridad de la información y su confidencialidad; III. Contar con procedimientos definidos y específicos para la prestación de los servicios, y medidas que garanticen la seriedad de los Certificados, la conservación y consulta de los registros, si es el caso; IV. a VII. … B) …
Artículo 108.- Los Certificados, para ser considerados válidos, deberán contener: I. La indicación de que se expiden como tales; II. El código de identificación único del Certificado; III. La identificación del Prestador de Servicios de Certificación que expide el Certificado, razón social, su domicilio, dirección de correo electrónico, en su caso, y los datos de acreditación ante la Secretaría; IV. Nombre del titular del Certificado; V. Periodo de vigencia del Certificado; VI. La fecha y hora de la emisión, suspensión, y renovación del Certificado; VII. El alcance de las responsabilidades que asume el Prestador de Servicios de Certificación, y	**Artículo 108.** Los Certificados, para ser considerados válidos, deberán contener: I. a II. … III. La identificación del Prestador de Servicios de Certificación que expide el Certificado, razón social, su nombre de dominio de Internet, dirección de correo electrónico, en su caso, y los datos de acreditación ante la Secretaría; IV. a VIII. …

VIII. La referencia de la tecnología empleada para la creación de la Firma Electrónica.	
Artículo 110.- El Prestador de Servicios de Certificación que incumpla con las obligaciones que se le imponen en el presente Capítulo, previa garantía de audiencia, y mediante resolución debidamente fundada y motivada, tomando en cuenta la gravedad de la situación y reincidencia, podrá ser sancionado por la Secretaría con suspensión temporal o definitiva de sus funciones. Este procedimiento tendrá lugar conforme a la Ley Federal de Procedimiento Administrativo.	**Artículo 110.** El Prestador de Servicios de Certificación que incumpla con las obligaciones que se le imponen en este Código, el reglamento o la norma oficial mexicana sobre digitalización y conservación de mensajes de datos que para tal efecto emita la Secretaría, previa garantía de audiencia, y mediante resolución debidamente fundada y motivada, tomando en cuenta la gravedad de la situación y reincidencia, podrá ser sancionado por la Secretaría con suspensión temporal o definitiva de sus funciones. Este procedimiento tendrá lugar conforme a la Ley Federal de Procedimiento Administrativo.

Que el Código Penal Federal (En adelante, CPF) tiene por objeto la regulación de:

- Los delitos del orden federal;
- Los delitos que se inicien, preparen o cometan en el extranjero, cuando produzcan o se pretenda que tengan efectos en el territorio de la República; o bien, por los delitos que se inicien, preparen o cometan en el extranjero, siempre que un tratado vinculante para México prevea la obligación de extraditar o juzgar, y
- Los delitos cometidos en los consulados mexicanos o en contra de su personal, cuando no hubieren sido juzgados en el país en que se cometieron.

Así el artículo 7 del CPF señala que “delito” es el acto u omisión que sancionan las leyes penales, y este es instantáneo, permanente o continuo, y continuado.

Para el caso que nos ocupa, la Colegisladora propone sancionar al PSC que realice actividades sin contar con la respectiva acreditación de la Secretaría de Economía.

Código Penal Federal	
Texto Vigente	Texto Minuta adaptada por las Cámaras de Diputados y Senadores
CAPITULO IV Falsificación de documentos en general Artículo 243.- El delito de falsificación se castigará, tratándose de documentos públicos, con prisión de cuatro a ocho años y de doscientos a trescientos	

sesenta días multa. En el caso de documentos privados, con prisión de seis meses a cinco años y de ciento ochenta a trescientos sesenta días multa. Artículo 246.- También incurrirá en la pena señalada en el artículo 243: I.- El funcionario o empleado que, por engaño o sorpresa, hiciere que alguien firme un documento público, que no habría firmado sabiendo su contenido; II.- El Notario y cualquier otro funcionario público que, en ejercicio de sus funciones, expida una certificación de hechos que no sean ciertos, o da fe de lo que no consta en autos, registros, protocolos o documentos; III.- El que, para eximirse de un servicio debido legalmente, o de una obligación impuesta por la ley, suponga una certificación de enfermedad o impedimento que no tiene como expedida por un médico cirujano, sea que exista realmente la persona a quien la atribuya, ya sea ésta imaginaria o ya tome el nombre de una persona real, atribuyéndoles falsamente la calidad de médico o cirujano; IV.- El médico que certifique falsamente que una persona tiene una enfermedad u otro impedimento bastante para dispensarla de prestar un servicio que exige la ley, o de cumplir una obligación que ésta impone, o para adquirir algún derecho; V.- El que haga uso de una certificación verdadera expedida para otro, como si lo hubiere sido en su favor, o altere la que a él se le expidió; VI.- Los encargados del servicio telegráfico, telefónico o de radio que supongan o falsifiquen un despacho de esa clase, y VII.- El que a sabiendas hiciere uso de un documento falso o de copia, transcripción o testimonio del mismo, sea público o privado.	Artículo 246. También incurrirá en la pena señalada en el artículo 243: I. a V. .... VI. Los encargados del servicio telegráfico, telefónico o de radio que supongan o falsifiquen un despacho de esa clase; VII. El prestador de servicios de certificación que realice actividades sin contar con la respectiva acreditación, en los términos establecidos por el Código de Comercio y demás disposiciones aplicables, y VIII. El que a sabiendas hiciere uso de un documento falso o de copia, transcripción o testimonio del mismo, sea público o privado.
Artículo 246. También incurrirá en la pena señalada en el artículo 243: I. a V. .... VI. Los encargados del servicio telegráfico, telefónico o de radio que supongan o falsifiquen un despacho de esa clase; VII. El prestador de servicios de certificación que realice actividades sin contar con la respectiva acreditación, en los términos establecidos por el Código de Comercio y demás disposiciones aplicables, y	

VIII. El que a sabiendas hiciere uso de un documento falso o de copia, transcripción o testimonio del mismo, sea público o privado.	

4.7. Reforma y adiciones a la Ley General de Sociedades Mercantiles del 14 de marzo de 2016

El pasado 14 de marzo de 2016, se reformó el párrafo segundo del artículo 1o.; el párrafo primero del artículo 20; la denominación del Capítulo XIV para quedar como: *De la sociedad por acciones simplificada*, los artículos 260, 261, 262, 263 y 264; se adicionan una fracción VII al artículo 1o.; un párrafo quinto al artículo 2o., y se recorren los subsecuentes; un segundo párrafo al artículo 5o.; los artículos 265, 266, 267, 268, 269, 270, 271, 272 y 273 de la Ley General de Sociedades Mercantiles[329].

Básicamente, la Ley General de Sociedades Mercantiles incorpora la "Sociedad por Acciones Simplificada" a la que define como a aquella que se constituye con una o más personas físicas que sólo están obligadas al pago de sus aportaciones representadas en acciones; pero en ningún caso las personas físicas que la integren podrán ser simultáneamente accionistas de otro tipo de sociedad mercantil si su participación les permite tener el control de la sociedad o de su administración.

Con la S.A.S. es sencillo, rápido y económico crear una empresa en México, pues uno de los requisitos es que el o los accionistas cuenten con certificado de FEA vigente, pues en ningún caso se exigirá el requisito de escritura pública o formalidad adicional.

Debe señalarse que con la legislación anterior el costo promedio para crear una empresa era de 20,000 pesos y el trámite tardaba hasta seis días, en el mejor de los casos, ahora se hará en 24 horas y de manera gratuita, pues el proceso se puede hacer vía Internet y sin pago de los servicios profesionales de un abogado, contador o administrador para asesorarse y constituir su empresa. Además antes se requerían dos socios para constituir una sociedad, en tanto que ahora se puede hacer con uno y sin necesidad de un capital mínimo.

De manera detallada el capítulo XIV señala a partir del artículo 260 que la S.A.S. es aquella que se constituye con una o más personas físicas que solamente están obligadas al pago de sus aportaciones representadas en acciones, y que para que surta efectos ante terceros deberá inscribirse en el Registro Público de Comercio.

Los ingresos totales anuales de una sociedad por acciones simplificada no podrá rebasar de 5 millones de pesos. En caso de rebasar el monto respectivo, la sociedad por acciones simplificada deberá transformarse en otro régimen societario; además, la denominación se formará

[329] Decreto por el que se reforman y adicionan diversas disposiciones de la Ley General de Sociedades Mercantiles, publicado en el DOF el 14 de marzo de 2016, accesible en:http://dof.gob.mx/nota_detalle.php?codigo=5429707&fecha=14/03/2016, consultado el 14 de marzo de 2016.

libremente, con la abreviatura “S.A.S" por las siglas: *Sociedad por Acciones Simplificada* y bajo los siguientes lineamientos (artículo 262):

- Que haya uno o más accionistas;
- Que el o los accionistas externen su consentimiento para constituir una *Sociedad por Acciones Simplificada* bajo los estatutos sociales que la Secretaría de Economía ponga a disposición mediante el sistema electrónico de constitución;
- Que alguno de los accionistas cuente con la autorización para el uso de denominación emitida por la Secretaría de Economía, y
- Que todos los accionistas cuenten con **certificado de firma electrónica avanzada** vigente reconocido en las reglas generales que emita la Secretaría de Economía conforme a lo dispuesto en el artículo 263 de la LGSM.
- En ningún caso se exigirá el requisito de escritura pública, póliza o cualquier otra formalidad adicional, para la constitución de la sociedad por acciones simplificada.

El sistema electrónico de constitución estará a cargo de la Secretaría de Economía y se llevará por medios digitales mediante el programa informático establecido para tal efecto.

El procedimiento de constitución se llevará a cabo de acuerdo con las siguientes bases:

- Se abrirá un folio por cada constitución;
- El o los accionistas seleccionarán las cláusulas de los estatutos sociales que ponga a disposición la Secretaría de Economía a través del sistema;
- Se generará un contrato social de la constitución de la sociedad por acciones simplificada firmado electrónicamente por todos los accionistas, usando el certificado de firma electrónica vigente a que se refiere la fracción IV del artículo 262 de esta Ley, que se entregará de manera digital;
- La Secretaría de Economía verificará que el contrato social de la constitución de la sociedad cumpla con lo dispuesto en el artículo 264 de la LGSM, y de ser procedente lo enviará electrónicamente para su inscripción en el Registro Público de Comercio;
- El sistema generará de manera digital la boleta de inscripción de la sociedad por acciones simplificada en el Registro Público de Comercio;
- La utilización de fedatarios públicos es optativa;
- La existencia de la sociedad por acciones simplificada se probará con el contrato social de la constitución de la sociedad y la boleta de inscripción en el Registro Público de Comercio;

Los estatutos sociales únicamente deberán contener los siguientes requisitos, además de los contenidos en las fracciones I, II, III, IV, V, VI, y VII del artículo 264:

- La forma y términos en que los accionistas se obliguen a suscribir y pagar sus acciones;
- El número, valor nominal y naturaleza de las acciones en que se divide el capital social;

- El número de votos que tendrá cada uno de los accionistas en virtud de sus acciones;

- El objeto de la sociedad, y
- La forma de administración de la sociedad.
- El o los accionistas serán subsidiariamente o solidariamente responsables, según corresponda, con la sociedad, por la comisión de conductas sancionadas como delitos.
- Denominación; Nombre de los accionistas; Domicilio de los accionistas; Registro Federal de Contribuyentes de los accionistas;
- Correo electrónico de cada uno de los accionistas; Domicilio de la sociedad;
- Duración de la sociedad;
- Los contratos celebrados entre el accionista único y la sociedad deberán inscribirse por la sociedad en el sistema electrónico establecido por la Secretaría de Economía conforme a lo dispuesto en el artículo 50 Bis del CCo.
- Todas las acciones deberán pagarse dentro del término de un año contado desde la fecha en que la sociedad quede inscrita en el Registro Público de Comercio.
- Cuando se haya suscrito y pagado la totalidad del capital social, la sociedad deberá publicar un aviso en el sistema electrónico establecido por la Secretaría de Economía.
- La Asamblea de Accionistas es el órgano supremo de la sociedad por acciones simplificada y está integrada por todos los accionistas quienes llevarán un libro de registro de resoluciones. Cuando la sociedad por acciones simplificada esté integrada por un solo accionista, éste será el órgano supremo de la sociedad.
- La representación de la sociedad por acciones simplificada estará a cargo de un administrador, función que desempeñará un accionista.
- Cuando la sociedad por acciones simplificada esté integrada por un solo accionista, éste ejercerá las atribuciones de representación y tendrá el cargo de administrador.
- Se entiende que el administrador, por su sola designación, podrá celebrar o ejecutar todos los actos y contratos comprendidos en el objeto social o que se relacionen directamente con la existencia y el funcionamiento de la sociedad.
- La toma de decisiones de la Asamblea de Accionistas será mediante voto sobre los asuntos por escrito o por medios electrónicos si se acuerda un sistema de información de acuerdo con lo dispuesto en el artículo 89 del CCo, ya sea de manera presencial o fuera de asamblea.
- La Asamblea de Accionistas será convocada por el administrador de la sociedad, mediante la publicación de un aviso en el sistema electrónico establecido por la Secretaría de Economía con una antelación mínima de cinco días hábiles y con el orden del día.
- El administrador publicará en el sistema electrónico de la SE, el informe anual sobre la situación financiera de la sociedad y a falta de presentación de la situación financiera durante dos ejercicios consecutivos dará lugar a la disolución de la sociedad.
- En lo que no contradiga las disposiciones de la S.A.S le son aplicables a la sociedad por acciones simplificada las disposiciones de la sociedad anónima así como lo relativo a la fusión, la transformación, escisión, disolución y liquidación de sociedades.

El decreto entró en vigor a los seis meses contados a partir de su publicación.

4.8. Incorporación de la FEA en la Administración Pública Federal antes de la Ley FEA.

A pesar de su naturaleza eminentemente mercantil, los trabajos de la CNUDMI en materia de firmas electrónicas y digitales resultarían útiles no solamente en el ámbito comercial; fue así como el régimen uniforme creado por la CNUDMI brindó ideas a los Estados que hacia el año 2001 estaban deseosos de reglamentar en materia de firmas electrónicas en ámbitos diferentes del comercio, particularmente sobre el uso de firmas electrónicas en las relaciones gobierno-gobierno (por ejemplo, en materia de comunicaciones gubernamentales) y en las relaciones gobierno-ciudadano (por ejemplo, para facilitar al ciudadano la realización de trámites vía Internet).

En México los conceptos y reglas desarrollados en las Leyes Modelo fueron acogidos en principio en las legislaciones civil y comercial, sin embargo modelos de firmas electrónicas basados en la criptografía asimétrica han sido también incorporados por diversas entidades gubernamentales.

En seguimiento a la recepción de las Leyes Modelo de la CNUDMI/UNCITRAL, el gobierno federal, con el propósito de contar con un instrumento que definirá una estrategia de desarrollo que orientará a las instituciones gubernamentales para aprovechar las tecnologías de la información y comunicaciones en la mejora de su gestión, elaboró la Agenda de Gobierno Digital[330]. Con ella se impulsó el desarrollo del Gobierno Digital desde dos frentes, tanto el aumento en el uso de trámites y servicios digitales como al hacer eficientes las operaciones. Entre las cuales se encuentran:

- Dar continuidad a la revisión y adecuación del marco normativo relacionados con Tecnologías de la Información y Comunicaciones.
- Promover la digitalización de trámites y servicios gubernamentales integrados para facilitar el acceso al ciudadano, con líneas de acción como son el impulso del uso generalizado de la FEA para crear certeza y seguridad en los trámites así como servicios digitales y homologar los portales de Internet del gobierno.
- Promover el desarrollo del Gobierno Digital mediante la vinculación con los gobiernos y organismos nacionales e internacionales, la industria, la academia y la sociedad, con líneas de acción como el fortalecimiento de los mecanismos de vinculación con los Poderes de la Unión, los Organismos Constitucionales Autónomos[331] y los órdenes de gobierno.
- Elevar el nivel de cooperación, asistencia técnica e intercambio de mejores prácticas con los estados y municipios, así como con la academia, la industria y los organismos internacionales.

De tal forma que las entidades y dependencias de la APF que comenzaron a emplear la FEA fueron:

[330] El 16 de enero de 2009 se publicó en el DOF el **Acuerdo por el que se da a conocer la Agenda de Gobierno Digital**, el cual entró en vigor el día siguiente al de su publicación.
[331] Incluidas las universidades públicas.

1. Servicio de Administración Tributaria (SAT),
2. Secretaría de la Función Pública (SFP)
3. Secretaría de Economía (SE)
4. Secretaría de Relaciones Exteriores (SER)
5. Secretaría de Gobernación (SEGOB)
6. Secretaría de Medio Ambiente y Recursos Naturales (SEMARNAT)
7. Comisión Nacional del Sistema de Ahorro para el Retiro (CONSAR)
8. Instituto Mexicano del Seguro Social (IMSS)

* Banco de México (Banxico)

Lo anterior, implicó una importante labor de homologación de procesos, estándares, leyes y regulaciones administrativas, que ubicaron a México en el lugar 37 de 192 en la evaluación general de la *Encuesta de Naciones Unidas sobre e-Gobierno de 2008*[332].

El proceso cronológico de cómo México integró la FEA al interior del gobierno federal se suscitó en el año 2000 mediante la Ley Federal de Procedimiento Administrativo (LFPA), hoy vigente, que da cabida a través de una interpretación extensiva del uso de firmas electrónicas en el ámbito gubernamental[333]. La reforma apuntada autorizó a las dependencias y organismos descentralizados de la APF a recibir las promociones y solicitudes que fueran presentadas por los ciudadanos a través de medios de comunicación electrónica. Para efectos de este estudio resulta importante destacar que la reforma a la LFPA incorporó la equivalencia funcional entre las firmas autógrafa y electrónica[334] y, precisó que los documentos presentados por medios de comunicación electrónica producirían los mismos efectos que las leyes otorgan a los documentos firmados de forma autógrafa y que tendrían el mismo valor probatorio (artículo 69-C de la LFPA).

Es así como el gobierno mexicano con los conceptos desarrollados por la CNUDMI/UNCITRAL facilitó el desarrollo de varios esquemas de ICP; los cuales aportaron los detalles y necesidades específicas de seguridad.

Inmediatamente después de la reforma a la LFPA, la Secretaría de la Función Pública (SFP) tomó un papel crítico como tercero confiable realizando funciones de certificación con respecto de lo que esta ley llamaba el "medio de identificación electrónica".

El acuerdo emitido por la entonces Secretaría de Contraloría y Desarrollo Administrativo, que sentó las bases para la operación del sistema CompraNET (Sistema Electrónico de Contrataciones Gubernamentales), la SFP emitió certificados digitales para establecer la identificación electrónica de una dependencia, entidad, entidad federativa, o de un licitante

[332] United Nations Public Administration Network (UNPAN). UN e-Government Survey 2008: from e-Government to Connected Governance, December 2007, New York, p. 29, accesible en http://unpan1.un.org/intradoc/groups/public/documents/un/unpan028607.pdf, consultado el 2 de noviembre de 2014.
[333] Reformas a la LFPA del 30 de mayo de 2000.
[334] La reforma autorizó a cada dependencia u organismo a identificar los trámites que podían ser realizados por esta vía y publicar las reglas relativas al otorgamiento de firmas electrónicas y certificaciones (artículo 69-C).

que interviniera en el Sistema CompraNET[335]. Esta aplicación de firmas electrónicas en un "sistema cerrado" resultó un éxito.

En 2008, todas las dependencias y entidades que integran la APF, las administraciones de las 32 entidades federativas y 565 municipios operaban en CompraNET; el sistema registró más de 25 mil licitaciones públicas, de las cuales el 47% se realizaron vía electrónica; mientras que en materia de licitaciones federales, siete de cada diez compras que el gobierno federal realiza las hace por medios electrónicos[336].

Luego, en 2002, le fue encomendada a la SFP la función de desempeñar nuevamente un rol de ARC, con relación al sistema de certificación de los medios de identificación electrónica que los servidores públicos utilizan para realizar su declaración de situación patrimonial. El acuerdo que creó el Sistema Electrónico de Recepción de Declaraciones Patrimoniales (conocido también como DeclaraNET) le encomendó la expedición de certificados que ampararan los medios de identificación electrónica utilizados por los servidores públicos para realizar su declaración patrimonial en el sistema[337].

Para efectos de evidenciar la penetración del concepto de FEA – concepto que en 2000 no había aparecido aún en la legislación mexicana– a nivel gubernamental, resulta importante señalar que a partir de 1 de junio de 2009, la SFP empezará a emitir certificados de firma electrónica basados en métodos de ICP de FEA[338]; en consecuencia, los certificados de firmas electrónicas que fueron emitidas al amparo del acuerdo que creó el sistema DeclaraNET estarán vigentes únicamente hasta diciembre de 2009; a partir de dicha fecha, todos los funcionarios públicos deberán utilizar una FEA para presentar su declaración patrimonial y dicha firma deberá estar amparada por un certificado digital emitido por la SFP.

La SFP también ha impulsado, desde 2002, el uso de firmas electrónicas en las relaciones gobierno-ciudadano. Un acuerdo administrativo emitido en ese año permitió a la SFP consolidarse como una ARC en materia administrativa. En cumplimiento de su encomienda de

---

[335] Véase el Acuerdo por el que se establecen las disposiciones para el uso de medios remotos de comunicación electrónica, en el envío de propuestas dentro de los procedimientos de licitación pública que celebren las dependencias y entidades de la Administración Pública Federal, así como en la presentación de las inconformidades por la misma vía, publicado en el Diario Oficial de la Federación del 9 de agosto de 2000.

[336] Disponible en: http://portal.funcionpublica.gob.mx:8080/wb3/wb/SFP/discurso_211008, consultado el 16 abirl de 2010.

[337] Véase el artículo 38 de la LFPA; consultar también el **Acuerdo que establece las normas que determinan como obligatoria la presentación de las declaraciones de situación patrimonial de los servidores públicos, a través de medios de comunicación electrónica**, publicado el 19 de abril de 2002 en el Diario Oficial de la Federación (el cual quedará abrogado el primero de junio de 2009, véanse los artículos transitorios del **Acuerdo que determina obligatoria la presentación de las declaraciones de situación patrimonial de los servidores públicos federales, por medios de comunicación electrónica, utilizando para tal efecto, firma electrónica avanzada**, publicado en el Diario Oficial de la Federación del 25 de marzo de 2009), para que la presentación de las declaraciones de situación patrimonial de los servidores públicos obligados, se realice de manera expedita y sencilla, así como para simplificar y mejorar las acciones de registro y seguimiento correspondientes, a cargo de esta Secretaría, lo cual se ha venido operando a través del Sistema Electrónico de Recepción de Declaraciones Patrimoniales (DeclaraNET).

[338] En este sentido lo precisa el Acuerdo que determina como obligatoria la presentación de las declaraciones de situación patrimonial de los servidores públicos federales, por medios de comunicación electrónica, utilizando para tal efecto, firma electrónica avanzada, publicado en el Diario Oficial de la Federación del 25 de marzo de 2009.

coordinar el desarrollo administrativo de las dependencias y organismos descentralizados para lograr simplificaciones administrativas, la SFP estableció procedimientos de certificación del medio de identificación electrónica que los particulares empezaban a utilizar conforme a las reglas que ya eran emitidas por dependencias y organismos descentralizados, al amparo de la reforma a la LFPA del año 2000[339]. Esta normatividad ha permitido que numerosas autoridades empleen algún tipo de firmas electrónicas para diversos usos, tanto en relaciones gobierno-gobierno como gobierno-ciudadano[340].

De los trabajos realizados en 2006 por la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico a iniciativa de la SFP se encuentran los *Lineamientos para la operación, funcionalidad, comunicación y seguridad de los sistemas automatizados de control de gestión*, expedido por la SFP y la SHCP, publicado en el DOF el 24 abril de 2006, cuyo objeto es establecer las directrices que deberán observar las Dependencias y Entidades de la APF para la operación, funcionalidad, comunicación y seguridad de los sistemas automatizados de control de gestión, que permitan homologar, estandarizar y hacer compatible el uso entre ellas, mediante la utilización de medios y firma electrónicos en el intercambio de información, a fin de:

- Mejorar la gestión y trámites de los asuntos administrativos mediante el uso de medios electrónicos;
- Contar con un único sistema automatizado de control de gestión por cada dependencia o entidad;
- Asegurar la confidencialidad, integridad y resguardo de la información acorde a los ordenamientos legales aplicables;
- Permitir la intercomunicación entre los sistemas de control de gestión con que cuenten las Dependencias y Entidades;
- Utilizar la firma electrónica avanzada como medio de autenticación del documento electrónico gubernamental y como método alternativo a la firma autógrafa, y
- Disminuir sustancialmente el uso de papel y mensajería.

Posteriormente, se expidió el trabajo realizado por el Archivo General de la Nación denominado *Lineamientos para la creación y uso de Sistemas Automatizados de Gestión y Control de Documentos*, publicado en el DOF el 3 de julio de 2015, el cual es más completo, funcionan y minucioso que los lineamientos referidos en el párrafo anterior.

Lo anterior es así, porque estos Lineamientos son de observancia obligatoria para las dependencias y entidades señaladas en la Ley Orgánica de la Administración Pública Federal, incluidas la Presidencia de la República, los órganos administrativos desconcentrados, y la

[339] Véase el Acuerdo por el que se establecen las disposiciones que deberán observar las dependencias y los organismos descentralizados de la Administración Pública Federal, para la recepción de promociones que formulen los particulares en los procedimientos administrativos a través de medios de comunicación electrónica, así como para las notificaciones, citatorios, emplazamientos, requerimientos, solicitudes de informes o documentos y las resoluciones administrativas definitivas que se emitan por esa misma vía, publicado en el Diario Oficial de la Federación del 17 de enero de 2002.
[340] Una lista completa de los trámites a realizar vía electrónica están accesibles en: http://www.tramitanet.gob.mx/index.html, consultada el 14 de abril de 2009.

Procuraduría General de la República; y porque entre las funcionalidades mínimas con la que deberá cumplir dicho sistema automatizado de gestión y control de documentos se encuentran tres relacionadas con la FEA:

a) Permitir el firmado electrónico e incorporación de la FEA de documentos conforme a lo establecido en la LFEA y demás disposiciones aplicables;
b) Generar la carátula de expediente para su impresión o uso electrónico y prever la incorporación de la FEA, cuando la información esté clasificada como reservada o confidencial en los términos de la legislación en materia de transparencia, protección de datos y acceso a la información pública gubernamental; y
c) Controlar el acceso al Sistema, al menos, por medio de una clave de usuario y contraseña predeterminados, en su caso, por autenticación observando lo previsto en la LFEA, su Reglamento, el Manual Administrativo de Aplicación General en materia de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información (MAAGTICSI) y demás disposiciones que resulten aplicables.

En otro orden de ideas, en el ámbito mercantil, la SE es la encargada de actuar como ARC, facultad fue regulada por el CCo. La SE opera como entidad de certificación en transacciones que involucran firmas electrónicas simples y también firmas electrónicas avanzadas, y en relaciones tanto gobierno-ciudadano, gobierno-gobierno y como coordinador de los PSC.

Posteriormente, se encargó de esta Agenda la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico (CIDGE) del que se hablará en el subcapítulo correspondiente.

Hasta el 23 de mayo de 2013 los cinco proveedores que se encuentran acreditados ante la SE como PSC habilitados son:[341]

1.	ADVANTAGE SECURITY, S. DE R.L. DE C.V.	● Emisión de Certificados publicado en el DOF (13/12/2005) ● Conservación de mensajes publicado en el DOF (08/10/2007) ● Sellos Digitales de Tiempo publicado en el DOF (30/07/2008)
2.	PSC WORLD, SA.C.V.	● Emisión de Certificados publicado en el DOF (15/12/2005)
3.	CECOBAN	● Emisión de Certificados publicado en el DOF (19/09/2008) ● Conservación de mensajes publicado en el DOF (19/09/2008) ● Sellos digitales de tiempo publicado en el DOF (07/10/2010)
4.	EDICOMUNICACIONES MEXICO S.A C.V.	● Emisión de Certificados publicado en el DOF (07/05/2009) ● Conservación de mensajes publicado en el DOF (07/05/2009) ● Sellos Digitales de Tiempo publicado en el DOF (01/03/2010)
5.	SEGURIDATA S.A DE C.V.	● Emisión de Certificados publicado en el DOF (20/06/2011) ● Conservación de mensajes publicado en el DOF (14/12/2011) ● Sellos Digitales de Tiempo publicado en el DOF (14/12/2011)

[341] Datos registrados en la página oficial de la SE para la inscripción de Prestadores de Servicios de Certificados, visible en http://www.firmadigital.gob.mx/tabla.html, fecha de consulta, 2 de enero de 2016.

Con respecto al uso de FEA en un proceso del gobierno para volverlo más eficiente, se debe señalar la automatización de la operación del RPCS de la SE por medio del Sistema Integral de Gestión Registral (SIGER), mismo que opera bajo una estructura de ICP mediante el uso de firmas electrónicas avanzadas. El SIGER ha permitido la reducción de tiempo en la inscripción en el RPC de documentos de diecinueve días a un día.

Finalmente, en materia de relaciones gobierno-ciudadano vinculadas con el comercio, existen cuando menos dos funciones relativas a trámites de los ciudadanos.

- **a)** La SE realiza una función como certificadora de firmas electrónicas simples en trámites relacionados con la importación y exportación de productos, así como la operación automatizada del Registro Nacional de Inversiones Extranjeras (RNIE)
- **b)** La SE como ARC tiene la facultad exclusiva para coordinar la actuación de los PSC que emitan certificados conforme al CCo (artículo 107)[342]. En consecuencia, las entidades que consideren que cuentan con los requisitos humanos, materiales, económicos y tecnológicos para prestar servicios de certificación en el ámbito comercial deben solicitar la acreditación de la SE y obtener la certificación correspondiente[343].

En materia fiscal, los casos en que las leyes fiscales establezcan para los contribuyentes la obligación de presentar documentos, salvo disposición en contrario, esta deberá entenderse como la obligación de presentar un documento digital.

El CFF considera documento digital, todo MD que contiene información o escritura generada, enviada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología. Los documentos digitales referidos en el párrafo anterior deberán contener la FEA del firmante y, adicionalmente, el certificado que confirme el vínculo entre el firmante y los datos de creación de dicha FEA. A partir de 2005 el uso de FEA es obligatorio.

En el entendido de que las firmas electrónicas avanzadas garantizan la integridad de los documentos digitales y, de conformidad con el principio de equivalencia funcional, una FEA, amparada por un certificado vigente, producirá los mismos efectos y tendrá el mismo valor probatorio que las leyes le otorgan a la firma autógrafa en documentos físicos.

A efecto de crear las firmas electrónicas avanzadas, los contribuyentes deben acudir ante el SAT o cualquier PSC autorizado por Banxico. En todos los casos, el SAT vigilará y participará activamente en el proceso de verificación de la identidad de los contribuyentes que crean una FEA.

De esta manera los contribuyentes pueden remitir documentos digitales ante las autoridades

[342] Los servicios de certificación relacionados con firmas electrónicas en el ámbito del sector financiero no son coordinados por la SE (artículo 106 del Código de Comercio).
[343] Entre los servicios que pueden ser acreditados se encuentran el servicio de expedición de certificados digitales, los servicios relacionados con la NOM 151 y los servicios de estampado de tiempo.

fiscales. Cada vez que un contribuyente haga tal remisión, recibirá un acuse de recibo con sello digital, mismo que permitirá al contribuyente acreditar que el documento en comento fue recibido por la autoridad correspondiente. El sello digital muestra la fecha y hora en que el documento fue recibido e identifica a la dependencia que recibió el documento.

Al 30 de junio de 2008 el SAT había expedido 1'944,417 certificados digitales a 1'506,137 contribuyentes, de los cuales 74% fueron personas físicas y 26% personas morales. La optimización de este proceso representa ahorros del 50% al 90% en costos de operación, administrativos y almacenamiento[344].

El Banco Central de México (en adelante Banxico) como órgano constitucionalmente autónomo, funge también como ARC en un esquema de ICP regulado en la Circular 26/2008[345]. La Circular 26/2008 prevé la existencia de una Agencia Certificadora que, autorizada por Banxico, preste servicios de certificación en el sistema *Infraestructura Extendida de Seguridad (IES[346])* mediante la expedición de certificados digitales[347].

El IES provee una operación segura y eficiente tanto en los sistemas de pagos como en la comunicación a través de mensajes electrónicos protegidos mediante algoritmos de criptografía asimétrica (clave pública y privada), esto es, el Banxico posee una infraestructura que administra y distribuye las claves públicas en forma ágil y con la confianza de que cada correlación de clave pública y usuario implica necesariamente la corroboración de la identidad de los usuarios con base en la comparecencia física y presentación de documentación oficial.

En el modelo general de organización para la administración de las claves públicas y los certificados digitales de Banxico, se aprecia que los participantes de la IES son:

- Agencia Registradora Central: ARC
- Agencias Registradoras: AR's
- Agencias Certificadoras: AC's
- Agentes Certificadores: AgC's o terceros de confianza.
- Usuarios

---

344 Disponible en: http://ciapem.hidalgo.gob.mx/descargables/ponencias/viernes/12AB%20-%20SAT%20NoraCaballero.pdf, publicado el 16 de abril de 2009, consulta del 3 de enero de 2015.

345 Véase la Circular 26/2008 relativa a las Reglas a las que deberán sujetarse las Instituciones de Banca Múltiple y Casas de Bolsa en relación con las solicitudes de autorización y consulta que formulen al Banco de México a través del Módulo de Atención Electrónica, publicada en el Diario Oficial de la Federación del 25 de junio de 2008. De conformidad con los artículos transitorios, las reglas entraron en vigor el 30 de junio de 2008 y a partir del 2 de enero de 2009 las solicitudes de autorización o consulta y entrega de información adicional que las casas de bolsa e instituciones de banca múltiple formulen a Banxico se tramitarán y atenderán exclusivamente a través del MAE, salvo que dichas entidades no estén en posibilidad de ajustarse a los dispuesto en las reglas, en cuyo caso debieron notificarlo y justificar tal circunstancia a la gerencia correspondiente a más tardar el 31 de diciembre de 2008.

346 Ver http://www.banxico.org.mx/sistemas-de-pago/servicios/firma-electronica/documentacion/%7B3946A28C-DEF6-1CD8-2353-DD5E63EA1323%7D.pdf, consultado el 2 de mayo de 2015.

347 El certificado digital es un MD firmado electrónicamente por la Agencia Certificadora que lo haya emitido, que confirma el vínculo entre la identidad del titular y los respectivos Datos de Verificación de Firma Electrónica.

Las principales funciones que desempeñan cada uno de los participantes de la IES se describen a continuación:

Agencia Registradora Central (ARC):

- Normar y administrar la IES de acuerdo con las políticas que establezca el Banco de México.
- Crear su propio certificado digital y certificar a las AR's y AC's.
- Garantizar la unicidad de las claves públicas del sistema.
- Administrar la base de datos de las claves públicas correspondientes a los certificados digitales que las AR's tengan registradas en sus bases de datos y mantener una liga con las AC's que los expidieron.
- Difundir su clave pública y las claves públicas de las AR's y AC's a través de la página que el Banco de México tiene en la red mundial (Internet) que se identifica con el nombre de dominio www.banxico.org.mx.
- Establecer, administrar y mantener las medidas que garanticen la seguridad del sistema.

Agencias Registradoras (AR's):

- Registrar certificados digitales siempre y cuando la ARC confirme la unicidad de las claves públicas.
- Administrar las bases de datos con los certificados digitales registrados, tanto vigentes como históricas.
- Proporcionar a los usuarios que lo soliciten a través de medios electrónicos, información respecto de certificados digitales.
- Revocar certificados digitales en los supuestos previstos en las disposiciones aplicables e informar de la revocación a la AC que los haya emitido, así como, divulgar dichas revocaciones de conformidad con las reglas emitidas por la ARC.

Agencias Certificadoras (AC's):

- Emitir certificados digitales.
- Emitir los certificados digitales de las personas que les presten los servicios de AgC's y acreditarlos como tales.
- Solicitar a la AR que corresponda, la revocación de los certificados digitales que haya emitido, en los supuestos previstos en las disposiciones aplicables o cuando los usuarios, directamente o a través de un AgC, lo soliciten.
- Auxiliarse de AgC's en la realización de sus funciones, de conformidad con las disposiciones aplicables.
- Responder por los daños y perjuicios que, con motivo de la realización de sus actividades, ocasione por negligencia en el proceso de certificación, de conformidad con las disposiciones aplicables.
- Responder por los actos que realicen sus AgĆs, así como de los daños y perjuicios que éstos generen en el cumplimiento de sus funciones, de conformidad con lo previsto en las disposiciones aplicables.

Agentes Certificadores (AgC's):

- Auxiliar a la AC en la realización de sus funcione s de conformidad con las disposiciones aplicables.
- Verificar la identidad de los solicitantes que desean obtener certificados digitales, con base en los documentos oficiales que éstos les presenten.
- Informar al solicitante de un certificado digital sus derechos y obligaciones.
- Recibir y verificar el requerimiento de certificado digital elaborado por el solicitante.
- Obtener una declaración con firma autógrafa del solicitante en la que manifieste su conformidad con las reglas sobre el uso de firma electrónica.
- Proporcionar al solicitante de un certificado digital los medios necesarios para la generación de datos de creación y verificación de su firma electrónica.
- Emitir el precertificado correspondiente y solicitar el respectivo certificado digital a la AC que corresponda.
- Entregar al titular su certificado digital registrado y obtener la carta de aceptación del referido certificado digital en la que conste su firma autógrafa.
- Informar, en su caso, al titular de la revocación de su certificado digital.

Usuarios:

- Solicitar su certificado digital a una AC directamente o a través de un AgC, presentando su requerimiento digital y los documentos oficiales para su identificación, así como en su caso, la carta de solicitud correspondiente.
- Ser informado de sus derechos y obligaciones y manifestar su conformidad con las disposiciones aplicables a la firma electrónica.
- Establecer, en secreto y en forma individual, su frase de seguridad con la que podrá cifrar su clave privada para protegerla.
- Generar, en secreto y en forma individual, su par de claves (pública y privada) y su requerimiento, así como, los archivos correspondientes.
- Recibir la carta de aceptación de su certificado digital en la que conste su firma autógrafa y su certificado digital ya registrado.
- Mantener en un lugar seguro su clave privada.
- Recordar su frase de seguridad así como su *Challenge Password* y mantenerlos en secreto.
- Solicitar a la AR a través de medios electrónicos, la información de los certificados digitales de aquellos usuarios con los que tiene una relación operativa.
- Tener acceso a un servicio que le permita revocar, en línea, su certificado digital en cualquier momento.
- Ser informado por la AC o, en su caso, por un AgC, de las reglas, procedimientos y características generales de los servicios de certificación y de los certificados digitales.

Además a través de la ICP se regulan las solicitudes, la cuales son: MD con la firma electrónica

de un representante[348], que las casas de bolsa e instituciones de banca múltiple realizan a Banxico a través del Módulo de atención electrónica (MAE)[349].

En las disposiciones generales se establece que el uso conforme a las reglas que hagan tanto las casas de bolsa como las instituciones de banca múltiple sustituirá para todos los efectos legales a la firma autógrafa, teniendo el mismo valor probatorio de conformidad con las disposiciones aplicables.

En el contexto internacional, la Administración Pública Española a través del artículo 81 de la *Ley de Acompañamiento a los Presupuestos Generales* de 1998, habilitó a la Fábrica Nacional de Moneda y Timbre para la prestación de los servicios técnicos y administrativos necesarios para garantizar la seguridad, validez y eficacia de la emisión y recepción de comunicaciones así como documentos a través de técnicas y medios electrónicos, informáticos y telemáticos en el ámbito de las relaciones entre las Administraciones y entre el administrado y la Administración; con ello, la Fabrica se constituye legamente en certificador digital en las relaciones entre administrados y Administración y entre las Administraciones entre sí.[350]

4.9. Ley de Firma Electrónica Avanzada y su Reglamento.

El 11 de enero de 2012, la SFP publicó el decreto de expedición de la LFEA, nueve años después de la última reforma de 29 de agosto de 2003 al CCo en materia de MD, FEA y prestadores de servicios de certificación; empero su vigencia comenzó a partir del 4 de julio del 2012, seis meses después de su expedición en atención a que su artículo sexto transitorio estableció que las dependencias y entidades debían remitir a la SFP el plan de instrumentación para el uso de la FEA, en los que se contemplaron los distintos actos en los que era o no factible el uso de la misma, esto es en los actos de las comunicaciones, trámites, servicios, actos jurídicos y administrativos, así como procedimientos administrativos.

En vinculación con lo anterior, el 28 de mayo del 2012 la SFP publicó el Documento Técnico de Interoperabilidad de los Sistemas Automatizados de Control de Gestión (DTISACG), que en relación con otras disposiciones hicieron jurídicamente posible el envío y recepción de oficios y comunicados electrónicos entre dependencias y entidades de la APF, y desarrolló un gobierno que funciona sin papel, promesas del Gobierno Digital. Entre estos instrumentos legales y técnicos están[351]:

---

[348] Persona física facultada por la Entidad (según se define en la Circular 26/2008), para firmar electrónicamente las solicitudes en nombre y representación de ésta, así como para realizar las acciones que competen a un operador (persona física autorizada por la Entidad para tener acceso al MAE para en su nombre, entre otras actividades, ingresar solicitudes e información adicional.

[349] A través del MAE las casas de bolsa e instituciones de banca múltiple pueden: ingresar solicitudes a Banxico y documentación adicional, consultar electrónicamente los requerimientos de información adicional, dar seguimiento al trámite de respuesta y conocer la respuesta.

[350] Davara Rodríguez, Miguel Ángel: Manual de derecho informático, 2008, 10. ed., Cizur Menor (Navarra): Thomson Aranzadi, p. 495.

[351] Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico (CIDGE), "Instrumentación de la Ley de Firma Electrónica Avanzada", Junio 2015, disponible en: http://cidge.gob.mx/menu/ejes-de-trabajo/digitalizacion-del-gobierno/gobierno-sin-papel/firma-electronica-avanzada/instrumentacion-ley-de-firma-electronica-avanzada/, fecha de consulta 4 julio de 2015.

- El oficio del DTISACG[352] y DTISACG con los Anexos 1 y 2,
- La Ley de Firma Electrónica Avanzada (LFEA),
- El Reglamento de la Ley de Firma Electrónica Avanzada (RLFEA),
- El Esquema de Interoperabilidad y de Datos Abiertos de la APF (EIDA).

Las disposiciones anteriores se sustentan y alinean al:

- Plan Nacional de Desarrollo 2013-2018
- Programa para un Gobierno Cercano y Moderno (PGCM)
- La Estrategia Digital Nacional

El DTISACG tiene relación directa con el artículo 10 de la LFEA[353], al establecer una plataforma de interoperabilidad para el intercambio de oficios electrónicos jurídicamente válidos, contribuye al cumplimiento de una obligación establecida en la LFEA para que las dependencias y entidades de la APF hagan uso de MD y acepten la presentación de documentos electrónicos con la FEA.

Creemos que el beneficio de obtener la FEA de acuerdo con la LFEA consiste en que de acuerdo con las reformas al CFF, publicadas en el Diario Oficial el 28 de junio y 27 de diciembre de 2006, todos los contribuyentes están obligados a tramitarla y para ello deberán acudir al SAT a solicitar el certificado de la FEA. Por lo que aprovechar dicha trámite para obtenerla permite a los funcionarios utilizarla también como una herramienta al servicio de funcionarios públicos y ciudadanos para realizar trámites a diario con el gobierno.

Asimismo, cuando entró en vigor el Decreto por el que se establece la Ventanilla Única Nacional de fecha 3 de febrero de 2015, la FEA se convierte en un medio de identificación digital al momento de interactuar con el gobierno.

La CIDGE está coordinada por la SFP, el órgano estratégico permanente creado para tal efecto, con fundamento en el Acuerdo Presidencial publicado en el DOF el 9 de diciembre del 2005 para promover y consolidar el uso y aprovechamiento de las Tecnologías de la Información y Comunicaciones (TIC) en la APF, creó mecanismos de coordinación entre las dependencias y entidades, así como los grupos de participación que se muestran en el Modelo Mexicano de Gobierno de TIC.

En este sentido, se logró conjugar los trabajos de los distintos representantes de la Presidencia de la República, SFP, la SE, SHCP, al responsabilizarlos conjuntamente de la expedición de las

[352] Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico (CIDGE), "oficio del DTISACG por el titular de la Unidad de Gobierno Digital de la Secretaría de la Función Pública", disponible en:http://cidge.gob.mx/wp-content/uploads/2013/03/Oficio-DTISACG_UGD-409-442-2012_28May2012.pdf/, fecha de consulta 4 julio de 2015.

[353] Artículo 10 LFEA. "Las dependencias y entidades en las comunicaciones y, en su caso, actos jurídicos que realicen entre las mismas, harán uso de mensajes de datos y aceptarán la presentación de documentos electrónicos, los cuales deberán contar, cuando así se requiera, con la firma electrónica avanzada del servidor público facultado para ello."

disposiciones generales para su adecuado cumplimiento.

Además, la CIDGE fomenta las *Agendas Digitales de los Estados de la República Mexicana* como marcos rectores para el desarrollo y crecimiento de un país, generalmente se encuentran integradas por un conjunto de herramientas basadas en el uso de las Tecnologías de la Información y Comunicaciones, estructuradas en normas, estrategias, acciones y proyectos concretos, transversales y específicos, con el fin de hacer eficiente el trabajo gubernamental y mejorar los trámites y servicios que se entregan a la sociedad[354].

Imágenes recabadas de la página gubernamental: www.cidge.gob.mx, fecha de consulta: 1 de mayo de 2015.

En consecuencia, todas las dependencias y entidades de acuerdo a sus necesidades y el volumen de actividad de los actos reportados incorporaron en sus sistemas informáticos las herramientas tecnológicas o aplicaciones que permiten utilizar la FEA, por lo que no existe una aplicación informática única para su uso.

La CIDGE creó una Subcomisión de FEA[355,] que se encargó coordinar las acciones necesarias para la homologación, implantación y uso de la FEA en la APF.

En 2006 la SFP estableció los lineamientos para la homologación de los certificados de FEA que actualmente utilizan la propia SFP, la SE y el SAT, de manera que toda la APF opere sobre una misma infraestructura de tecnología denominada *Infraestructura Tecnológica de FEA* (en adelante ITFEA)[356]; los lineamientos emitidos indican también los requisitos que otras entidades –como estados, municipios y organismos constitucionales autónomos – deben cumplir para que las entidades que ya participan en la ITFEA reconozcan los certificados expedidos por ellas, de esa manera se espera gradualmente que las comunicaciones entre las autoridades se realicen por esta vía.

El resultado de todos estos trabajos de la autoridad fue la sistematización de los rubros tratados

[354] Para ver los documentos donde se abordan temáticas de Tecnologías de la Información y Comunicaciones o Gobierno Digital de los Estados de la República Mexicana: visitara el sitio de la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico (CIDGE) disponible en: http://cidge.gob.mx/menu/ejes-de-trabajo/estados-y-municipios/agendas-digitales, consulta 1 de junio de 2015.

[355] La Comisión está integrada por los titulares de la SE, la SFP y del SAT.

[356] Véase el Acuerdo Interinstitucional por el que se establecen los Lineamientos para la homologación, implementación y uso de la firma electrónica avanzada en la Administración Pública Federal, publicado en el Diario Oficial de la Federación (DOF) del 24 de agosto de 2006.

por la LFEA:

Ley de Firma Electrónica Avanzada DOF. 11 de enero de 2012		
a)	Artículos 1 a 6	**Título Primero: Disposiciones Generales**. Capítulo Único
b)	Artículos 7 a 9	**Título Segundo: De la Firma Electrónica Avanzada.** Capítulo I: Del Uso y Validez de la Firma Electrónica Avanzada
c)	Artículos 10 a 16	Capítulo II: De los Documentos Electrónicos y de los Mensajes de Datos
d)	Artículos 17 a 20	**Título Tercero: Del Certificado Digital:** Capítulo I: De la Estructura y Procedimientos del Certificado Digital
e)	Artículos 21 a 22	Capítulo II: Derechos y Obligaciones del Titular del Certificado Digital
f)	Artículos 23 a 27	Capítulo III: De las Autoridades Certificadoras
g)	Artículos 28 a 30	Capítulo IV: Del Reconocimiento de Certificados Digitales y de la Celebración de Bases de Colaboración y Convenios de Colaboración o Coordinación
h)	Artículo 31	**Título Cuarto: De las Responsabilidades y Sanciones**. Capítulo Único
	Transitorios: del 1º al 6º	

Las observaciones, análisis y conclusiones de los rubros de la LFEA son:

1. Ante la heterogeneidad de disposiciones se publicó la regulación del uso, servicios y homologación de la FEA a nivel de entidades y dependencias de la APF. La homologación de las FEA's era indispensable, dado que las primeras regulaciones en materia de firmas electrónicas fueron emitidas por los estados de Jalisco, Sonora, Chipas, Hidalgo y Querétaro[357] y cada una de ellas era distinta.
2. Su finalidad es regular la FEA que, a través de medios de comunicación electrónica, utilicen los servidores públicos y los particulares, en las comunicaciones, trámites, prestación de servicios, actos y procedimientos administrativos
3. Reitera lo ya dispuesto por el CCo en relación a que la información que utilice la FEA es equiparable a los documentos impresos con firma autógrafa, tendiendo igual valor probatorio y, en consecuencia, produce los mismos efectos que las leyes otorgan a estos documentos.
4. Se precisó que dicha ley no sería aplicable a las materias fiscales, aduanera y financiera (bancaria y bursátil); y añade que en lo correspondiente a actos de comercio e inscripciones en el Registro Público de Comercio, el uso de la FEA lo prevé el CCo sin perjuicio de la aplicación de esta Ley.
5. En la APF, la FEA inicia una nueva etapa, al permitir reducir el uso de papeles y oficios. Se brinda certeza jurídica con un modelo de control de gestión electrónica, el cual elimina los

[357] Un caso representativo es la Ley sobre el uso de medios electrónicos y firma electrónica para el Estado de Guanajuato y sus Municipios, en vigor desde el 1 de noviembre de 2004 cuyo objetivo fue fomentar el uso de medios electrónicos en las relaciones entre los poderes ejecutivo, legislativo y judicial, organismos autónomos especializados, municipios y cualquier dependencia o entidad del Estado.

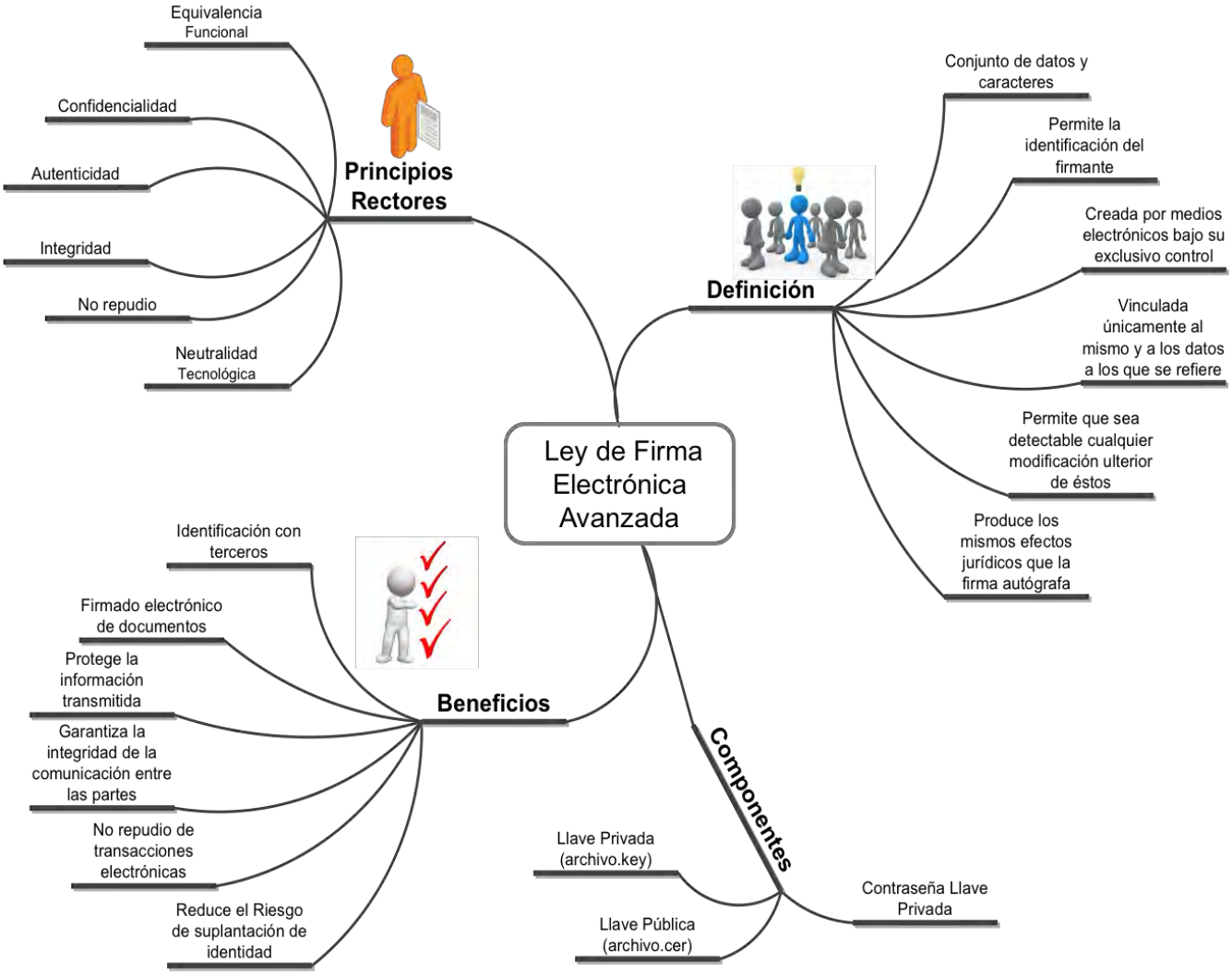
costos asociados a una gestión en papel.

6. Las organizaciones de la APF que sustituyan la firma autógrafa por la FEA reducirán significativamente costos en espacios para mantener archivos, costos de traslado al llevar un documento de una oficina a otra y costos asociados a la digitalización de documentos.
7. Esta firma aumentará el aprovechamiento de tecnologías de información y comunicaciones a través de la sistematización y digitalización de los trámites y servicios administrativos para la gestión pública, brindando una mejor atención a los ciudadanos al agilizar, simplificar y transparentar las operaciones que realicen con las dependencias gubernamentales.
8. Los beneficios de la FEA se extienden a las empresas y los ciudadanos al permitir utilizar legalmente la FEA en sus operaciones.
9. El valor agregado de implementar la FEA en los distintos actos, es que reguló de manera uniforme el uso de la firma electrónica en todas las dependencias y entidades de la APF a partir del año 2013, mejoró la calidad de los servicios en la APF, benefició en tiempo y costo de las operaciones tanto para el ciudadano como para el Gobierno:

    - Firma de documentos: Permite utilizar documentos firmados avanzadamente como Instrumentos Públicos de plena validez legal.
    - Seguridad en correos electrónicos: Permite cifrar sus correos dotando de confidencialidad a toda la información que envía.
    - Proporcionar validez legal a sus correos: Otorga validez legal a los correos y documentos firmados con firma electrónica.
    - Autenticación robusta: Se puede utilizar su certificado para autenticarse en forma robusta a en Intranet o portales institucionales.
    - Canales cifrados seguros: Se puede utilizar los certificados para establecer VPN entre equipos y usuarios.
    - Usuarios y beneficiarios

10. La CIDGE a través de la instrumentación de la FEA por parte de las Dependencias y Entidades de la APF, obliga a publicar en sus respectivas páginas web, los actos en relación a las actividades de comunicaciones, trámites, servicios, actos jurídicos y administrativos así como los procedimientos administrativos en los que es factible el uso de la FEA.
11. Como secuencia del inciso anterior, la SFP en coordinación con las dependencias y entidades deberán de integrar y actualizar un catálogo respecto de los diversos actos de la APF en los que es factible el uso de la FEA el cual deberá de publicar en su página Web cada una de las Instituciones, dicho catálogo deberá permitir el enlace con las ventanillas de acceso electrónico de las dependencias y entidades en las que se encuentran previstos los actos en que puede emplearse la FEA.

Es importante señalar que la SE y el SAT prestan servicios y recepción de trámites por medios electrónicos, y esta última es la principal emisora de certificados de firma electrónica, con casi tres millones 300 mil certificados realizados.



Mapa conceptual de la LFEA[358]

DIFERENCIAS ENTRE FIRMA ELECTRÓNICA AVANZADA, FIRMA ELECTRÓNICA Y FIRMA DIGITAL DE ACUERDO A NUESTR NORMATIVIDAD		
Código de Comercio	Ley de FEA	NOM-151
Firma Electrónica Avanzada o Fiable	**Firma Electrónica Avanzada**	**Firma Electrónica**
La que cumpla con los requisitos de las fracciones I a IV del artículo 97. En aquellas disposiciones que se refieran a Firma Digital, se considerará a ésta como una especie de la Firma Electrónica.	Conjunto de datos y caracteres que permite la identificación del firmante, que ha sido creada por medios electrónicos bajo su	A los datos en forma electrónica consignados en un mensaje de datos, o adjuntados, o lógicamente asociados al mismo, que puedan ser utilizados para identificar al

[358] Fuente de la Imagen: SAT, *La Evolución de la Firma Electrónica, en Nuevos servicios digitales del SAT*, Diapositivas de la Expo feria 2015, 16 de Diciembre de 2015, World Trade Center, Ciudad de México, accesible en: http://www.sat.gob.mx/innovacionestecnologicas/Paginas/a/documentos/EvolucionFirmaElectronica.pptx, consultado el 17 de diciembre de 2015.

Artículo 97: *(…)* *La Firma Electrónica es Avanzada o Fiable si cumple los siguientes requisitos:* *I. Los Datos de Creación de la Firma corresponden exclusivamente al Firmante;* *II. Los Datos de Creación de la Firma estaban, en el momento de la firma, bajo el control exclusivo del Firmante;* *III. Es posible detectar cualquier alteración de la Firma Electrónica hecha después del momento de la firma, y* *IV. Respecto a la integridad de la información de un Mensaje de Datos, es posible detectar cualquier alteración de ésta hecha después del momento de la firma.* Sin perjuicio de la posibilidad de que cualquier persona demuestre de cualquier otra manera la fiabilidad de una Firma Electrónica; o presente pruebas de que una Firma Electrónica no es fiable.	exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos, la cual produce los mismos efectos jurídicos que la firma autógrafa	firmante en relación con el mensaje de datos e indicar que dicho firmante aprueba la información recogida en el mensaje de datos. La firma electrónica establece la relación entre los datos y la identidad del firmante.
Firma Electrónica	**Firma Electrónica**	**Firma Digital**
Datos en forma electrónica consignados en un Mensaje de Datos, o adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al Firmante en relación con el Mensaje de Datos e indicar que el Firmante aprueba la información contenida en el Mensaje de Datos, y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio.	No la menciona	Firma electrónica que está vinculada al firmante de manera única**,** permitiendo así su identificación, creada utilizando medios que aquél pueda mantener bajo su exclusivo control, estando vinculada a los datos a que se refiere de modo que cualquier cambio ulterior de los mismos sea detectable. La firma digital **es una especie** de f**irma electrónica** que garantiza la autenticidad e integridad y la posibilidad de detectar cualquier cambio ulterior.

Ahora bien, en cuento al Reglamento se muestra este cuadro esquemático.

Reglamento de la Ley de Firma Electrónica Avanzada DOF. 21 de marzo de 2014		
a)	Artículos 1 a 7	Capítulo I: Disposiciones generales
b)	Artículos 8 a 14	Capítulo II: Del uso de la Firma Electrónica Avanzada
c)	Artículos 15 a 17	Capítulo III: De los derechos y obligaciones de los titulares de los Certificados Digitales

d)	Artículos 18 a 22	Capítulo IV: De las Autoridades Certificadoras
e)	Artículos 23 a 27	Capítulo V: De las bases y convenios de colaboración o coordinación
f)	**Transitorios (1º y 2º)**	

Las observaciones principales al Reglamento de Ley de Firma Electrónica Avanzada (RLFEA) son:

- Establecer las normas reglamentarias para el uso, los servicios y homologación de las FEA's.
- Las dependencias y entidades de la APF deberán informar a la SFP los Actos en los que han integrado el uso de la FEA.
- Existen actos en los que no es factible el uso de la FEA por disposición de Ley, esto son aquéllos en los que una disposición legal exija la firma autógrafa de los servidores públicos o de los particulares.
- Las dependencias y entidades determinarán en las disposiciones administrativas que rijan sus procedimientos, los Actos en los que se deberá usarse la FEA, especificándolo en cada etapa del proceso que corresponda.
- En términos del artículo 4 de la Ley, las dependencias y entidades de la APF no usarán la FEA a menos que la SFP emita un dictamen cuando el Oficial Mayor o equivalente de una la dependencias y entidades acredite con la información y documentación que acompañe a su solicitud, que el uso de la FEA en el Acto de que se trate no representa alguna mejora en los tiempos de atención o en la calidad del servicio, mayor eficiencia, transparencia o incremento en la productividad ni reducción de costos. El dictamen tendrá la temporalidad que determine la Secretaría, la cual no podrá exceder de dos años, y podrá prorrogarse siempre que la Dependencia o Entidad así lo solicite y acredite que subsisten las causas que motivaron su emisión.
- La SFP emitirá su dictamen en un plazo de veinte días hábiles, contados a partir del día siguiente de la presentación de la solicitud por parte de las dependencias y entidades, acompañada de la documentación que acredite los supuestos establecidos en el párrafo anterior.
- Las dependencias y entidades podrán emitir, de manera justificada, el Acto que corresponda utilizando la firma autógrafa en lugar de la FEA, en casos en que medie una situación de emergencia o urgencia. Para tales efectos dichas autoridades deberán remitir un escrito a la Secretaría en un plazo de ocho días hábiles siguientes a la firma del Acto correspondiente, en el que se funde y motive la situación de emergencia o urgencia por la que no fue posible utilizar la FEA en los términos de la Ley.
- Sólo se considerarán casos de emergencia o urgencia los acontecimientos inesperados por los que sea indispensable emitir el Acto de que se trate con firma autógrafa.
- La SFP, en el ámbito de su competencia, estará facultada para interpretar las disposiciones del presente Reglamento para efectos administrativos, no comerciales.
- Las dependencias y entidades deberán incorporar en sus sistemas informáticos, las herramientas tecnológicas o aplicaciones que permitan utilizar la FEA, para cumplir con ello, emitirán Disposiciones Generales que establecerán los requerimientos técnicos mínimos que deberán tener los sistemas informáticos, así como las herramientas tecnológicas o aplicaciones.

Ahora bien, respecto al uso específico de la FEA:

- Las dependencias y entidades en las comunicaciones y actos jurídicos que realicen entre las mismas, harán uso de MD y aceptarán la presentación de documentos electrónicos, los cuales deberán contar, cuando así se requiera, con la FEA del servidor público facultado para ello.
- La manifestación expresa de la conformidad que expresen los particulares o sus representantes se realizará preferentemente por medios electrónicos y utilizando la FEA en el *Sistema de Trámites Electrónicos* de la dependencia o entidad que corresponda.
- Para los efectos de las notificaciones que emitan la dependencia o la entidad en *Tablero Electrónico*, los días hábiles se considerarán de veinticuatro horas, el cual estará sincronizado a la hora oficial para los Estados Unidos Mexicanos, generada por el *Centro Nacional de Metrología.*
- El acuse de recibo electrónico deberá contener un sello digital que permita dar plena certeza sobre la fecha y hora de recepción, así como del registro de los documentos electrónicos, asociados a dicho acuse de recibo.
- El aviso sobre la imposibilidad para consultar el *Tablero Electrónico* o abrir los documentos electrónicos, se podrá efectuar mediante su registro en el *Tablero Electrónico*; por correo electrónico dirigido a la dirección de correo electrónico del servidor público que se señale en el Sistema de Trámites Electrónicos como responsable del Acto de que se trate, o mediante escrito con firma autógrafa dirigido al servidor público que se mencione como responsable del Acto de que se trate y presentado en el domicilio del mismo que se señale en el *Sistema de Trámites Electrónicos.*
- La SFP determinará los Lineamientos en los que cada dependencia y entidad creará y administrará un sistema de trámites electrónicos que establezca el control de accesos, los respaldos y la recuperación de información, con mecanismos confiables de seguridad, disponibilidad, integridad, autenticidad, confidencialidad y custodia.
- El acuse de recibo electrónico deberá contener un sello digital que permita dar plena certeza sobre la fecha y hora de recepción, así como del registro de los documentos electrónicos, asociados a dicho acuse de recibo.
- La SFP determinará en los Lineamientos a que se refiere el segundo párrafo del artículo 13 de la LFEA, las especificaciones técnicas que debe contener el sello digital, así como los medios para que los particulares verifiquen la autenticidad de los acuses de recibo electrónicos con sello digital, incluyendo los documentos electrónicos asociados al referido acuse de recibo. Hasta el día de hoy y dada la omisión de expedición de los Lineamientos referidos, a continuación se transcribe el segundo párrafo del artículo 13 de dicha Ley:

  > *Artículo 13. (…)*
  > *La Secretaría emitirá los lineamientos conducentes a efecto de dar cumplimiento a lo dispuesto en este artículo.*

- La impresión de los documentos electrónicos suscritos con FEA emitidos por las dependencias y entidades de la APF, contendrá una cadena de caracteres asociados al

documento electrónico original de que se trate, así como asociados a la FEA y, en su caso, al sello digital que permita comprobar la autenticidad de su contenido y, cuando corresponda, el momento de su recepción.

- Cuando los particulares o, en su caso, las personas autorizadas por los mismos, en la realización de los actos previstos en la Ley, no señalen una dirección de correo electrónico para recibir MD y documentos electrónicos o existan elementos que permitan presumir que la proporcionada es incorrecta, las dependencias y entidades de la APF considerarán como dirección de correo electrónico la contenida en el certificado digital del particular.

De los derechos y obligaciones de los titulares de los Certificados Digitales

- Las Autoridades Certificadoras deberán poner a disposición de los interesados en obtener certificados digitales, la información relativa a los derechos y obligaciones que adquieren como titulares de un certificado digital. también dará a conocer en su página web los derechos y obligaciones a que aluden los artículos 21 y 22 de la Ley y entregar un documento conteniendo los mismos al titular del certificado digital al momento de su emisión.
- Las Autoridades Certificadoras incluirán en su página web los servicios digitales y, en su caso, proporcionarán medios de acceso a éstos desde sus instalaciones para los usuarios, a fin de facilitar a los titulares de certificados digitales el cumplimiento de sus obligaciones.

De las Autoridades Certificadoras:

- Las dependencias y entidades distintas a la SFP, SE y SAT, así como los prestadores de servicios de certificación interesados en ser autoridad certificadora deberán contar con el dictamen favorable de la SFP, quien lo remitirá en un plazo de cuarenta y cinco días hábiles a partir del día siguiente de la presentación de la solicitud y la documentación adjunta que acredite los requisitos establecidos en las Disposiciones Generales. Cuando se reciba una solicitud que no reúna los requisitos establecidos en la Ley, el Reglamento y las Disposiciones Generales, la SFP le requerirá la documentación, si no la entrega será desechado el trámite para obtener el carácter de Autoridad Certificadora y tendrán que transcurrir al menos treinta días hábiles a partir de la fecha en que se notifique el desechamiento, a efecto de que pueda solicitar el inicio de un nuevo trámite. Para los efectos de la emisión del dictamen, la SFP podrá solicitar el apoyo de la SE y del SAT, en el ámbito de sus respectivas atribuciones.
- La SFP publicará y mantendrá actualizada en su página web, una relación de las Autoridades Certificadoras.
- Las autoridades certificadoras llevarán un registro de los certificados digitales que emitan y de los que revoquen, así como proveer los servicios de consulta a los interesados, a fin de que cualquier consulte a través de medios electrónicos o ante las AC, el registro de certificados digitales emitidos por las mismas.
- En las disposiciones generales se establecerán las medidas y controles de seguridad que deberán adoptar las Autoridades Certificadoras para evitar la falsificación, alteración o uso indebido de certificados digitales a que se refiere la fracción III del artículo 25 de la Ley y,

en general, para dar cumplimiento a las demás obligaciones previstas en el citado precepto.

- La SFP podrá suspender y revocar el reconocimiento otorgado a una Autoridad Certificadora, cuando esta sea un PSC, a través del procedimiento para revocar el instrumento que le reconozca tal carácter, tendrá lugar conforme a la Ley Federal de Procedimiento Administrativo, cuando de manera voluntaria así lo solicite, cuando incumpla las obligaciones previstas en la Ley, o deje de cumplir los requisitos señalados en las Disposiciones Generales para tener el carácter de Autoridad Certificadora.
- La Secretaría le notificará a la Autoridad Certificadora las causas que motivaron la suspensión de su reconocimiento y deberá abstenerse de emitir certificados digitales de manera inmediata, los cuales seguirán vigentes y serán administrados por la Autoridad Certificadora que al efecto determine la Secretaría, con el propósito de asegurar la continuidad en el uso de los mismos. Asimismo, la Secretaría determinará, de acuerdo con lo establecido en las Disposiciones Generales, el destino que se dará a los registros y archivos correspondientes. En el caso de que alguna Autoridad Certificadora ya no desee tener ese carácter, deberá solicitarlo mediante documento electrónico enviado a la dirección de correo electrónico que con ese propósito señale la Secretaría, con al menos sesenta días hábiles de anticipación, para el efecto de que ésta autorice la administración, por otra Autoridad Certificadora, de los certificados digitales emitidos y asegurar la continuidad en el uso de los mismos, así como para determinar, conforme a lo establecido en las disposiciones generales, el destino que se dará a los registros y archivos correspondientes.

De las bases y convenios de colaboración o coordinación

- La SE, el SAT y las demás Autoridades Certificadoras deberán remitir a la SFP una copia de las bases o convenios de colaboración que suscriban para la prestación de Servicios relacionados con la FEA, a fin de publicar en su Página web, un listado de las bases o convenios de colaboración que se suscriban entre las Autoridades Certificadoras.
- Para el reconocimiento de *Certificados Digitales Homologados* a que se refiere el artículo 29 de la Ley, la SFP, SE y SAT, según corresponda, deberán verificar previamente a la celebración de los convenios de coordinación o colaboración correspondientes, que los certificados digitales de que se trate cumplan con el número de serie; la autoridad certificadora que lo emitió; algoritmo de firma; vigencia; nombre del titular del certificado digital; dirección de correo electrónico del titular del certificado digital; Clave Única del Registro de Población (CURP) del titular del certificado digital; clave pública; que su vigencia no sea mayor a cuatro años; y que los procedimientos que se sigan para el registro de datos y verificación de elementos de identificación, emisión, renovación y revocación de certificados digitales, sean consistentes con los principios rectores de equivalencia funcional, autenticidad, integridad, neutralidad tecnológica, no repudio y confidencialidad.
- El resultado de la verificación a que se refiere el párrafo anterior se hará constar en un dictamen técnico, que se emitirá dentro de los cuarenta y cinco días hábiles siguientes a la recepción de la solicitud que haya presentado la Autoridad Certificadora interesada.
- Si el dictamen técnico resulta favorable, la SFP, SE y SAT, según corresponda, lo remitirá junto con el proyecto de convenio de colaboración, a las otras dos Autoridades

Certificadoras, para solicitar su opinión. El plazo para emitir dicha opinión es de veinte días hábiles, posteriores a la recepción de la solicitud de opinión correspondiente.

- En los convenios de coordinación o colaboración que se celebren para el reconocimiento de *Certificados Digitales Homologados,* la SFP, la SE o el SAT deberán pactar su terminación anticipada cuando se detecte que en la emisión, renovación, revocación y verificación de validez de dichos certificados se incumple con los principios rectores de equivalencia funcional, autenticidad, integridad, neutralidad tecnológica, no repudio y confidencialidad. Asimismo deberán incluir el compromiso de la otra parte contratante para proporcionar la información y dar las facilidades que permitan constatar que los *Certificados Digitales Homologados* no han perdido ese carácter.
- La SE y el SAT comunicarán a la SFP sobre la conclusión de la vigencia o la terminación anticipada de los convenios de coordinación que hubieren suscrito, dentro de los diez días hábiles siguientes a la conclusión o terminación anticipada, para el efecto de que a través de la página web de la SFP se informe de ello a las demás Autoridades Certificadoras.
- El reconocimiento de *Certificados Digitales Homologados* concluirá al término de la vigencia del convenio de coordinación o en la fecha en que se formalice su terminación anticipada, según corresponda, salvo que en el propio convenio se hubiere establecido algún mecanismo que permita mantener el reconocimiento de dichos Certificados Digitales hasta la fecha de su vencimiento.
- Para el reconocimiento de Certificados Digitales expedidos fuera de la República Mexicana, la SFP, SE y el SAT observarán el mismo procedimiento citado anteriormente y además suscribirán el instrumento jurídico conforme a las disposiciones aplicables procedentes.
- La SFP vigilará que las dependencias y entidades de la APF que hayan obtenido el carácter de Autoridad Certificadora cumplan con las obligaciones establecidas en la Ley, en este Reglamento y en las demás disposiciones aplicables. A tal efecto, podrá realizar las visitas de verificación que sean necesarias para el ejercicio de su función de control.

4.9.1. Excepción en materia Fiscal

Previo a abordar la materia fiscal, haremos referencia a las excepciones en general a la LFEA, En este contexto, de acuerdo con el artículo 4 de la LFEA, la firma electrónica no se aplicará en materia fiscal, aduanera y financiera, para estar en condiciones de responder de manera más ágil a las condiciones cambiantes de la economía mexicana, así como a la regulación específica con la que cuentan sus trámites y servicios.

Si un trámite fiscal, aduanero o financiera regula que para la presentación de la documentación se tiene que utilizar FEA del autor, se entenderá que forzosamente se deberá emplear esa FEA en razón de que existe una norma especial que la regula y por tanto queda exceptuado de las disposiciones de la LFEA. En conclusión, cuando no lo prohíba ningún ordenamiento jurídico, tratándose de las materias antes referidas, se entenderá que sí se podrán presentar documentos digitales y contener la FEA del autor.

4.9.1.1. Concepto, origen fundamento legal de la Facturación electrónica.

Una factura es un documento que comprueba la realización de una transacción comercial entre un comprador y un vendedor. La factura responsabiliza al vendedor a entregar el servicio o producto y obliga al comprador a realizar el pago de acuerdo a lo especificado en dicha factura.

El SAT, por primera vez, a través de la regla 2.14.1 de la Resolución de Miscelánea Fiscal (RMF) estableció que a partir del mes de julio de 2002, los contribuyentes obligados a realizar pagos mensuales dejarían de hacerlo en papel para efectuarlo mediante Internet.

Posteriormente, el 5 de enero de 2004 publicó en el DOF el esquema del Comprobante Fiscal Digital, lo que implicó que se reformara el CFF, específicamente se agregó en el Título Segundo un Capítulo Segundo denominado: "De los Medios Electrónicos", que refiere el uso de la Firma Electrónica Avanzada para los trámites fiscales, la cual, si bien es opcional en 2004, se hace obligatoria para gran parte de los contribuyentes desde 2005 y otorga la posibilidad de utilizar facturas electrónicas para amparar sus operaciones de venta.

Los principales artículos aplicables a las materias que nos ocupan, que faculta el uso de FEA, independientemente de que cada dependencia o entidad deberá acordar las disposiciones administrativas que rijan sus procedimientos, los actos en los que se deberá usar la FEA y especificar en qué etapa del procedimiento se puede aplicar.

En materia fiscal, los artículos 17-C, 17-D, 18 y 31 del CFF establecen:

> ***Artículo 17-C.*** *Tratándose de contribuciones administradas por organismos fiscales autónomos, las disposiciones de este Código en materia de medios electrónicos sólo serán aplicables cuando así lo establezca la ley de la materia.*
>
> ***Artículo 17-D.-*** *Cuando las disposiciones fiscales obliguen a presentar documentos, estos deberán ser digitales y contener una firma electrónica avanzada del autor, salvo los casos que establezcan una regla diferente. Las autoridades fiscales, mediante reglas de carácter general podrán autorizar el uso de otras firmas electrónicas.*
> *Para los efectos mencionados en el párrafo anterior, se deberá contar con un certificado que confirme el vínculo entre un firmante y los datos de creación de una firma electrónica avanzada, expedido por el Servicio de Administración Tributaria cuando se trate de* ***personas morales*** *y de los sellos digitales previstos en el artículo 29 de este Código, y por un* ***prestador de servicios de certificación autorizado por el Banco de México cuando se trate de personas físicas.*** *El Banco de México publicará en el Diario Oficial de la Federación la denomin ación de los prestadores de los servicios mencionados que autorice y, en su caso, la revocación correspondiente.*
> *En los documentos digitales, una firma electrónica avanzada amparada por un certificado vigente sustituirá a la firma autógrafa del firmante, garantizará la integridad del documento y producirá los mismos efectos que las leyes les otorgan a los documentos con firma autógrafa, teniendo el mismo valor probatorio.*
> *(…)* **(Énfasis añadido)**
>
> ***Artículo 18.-*** *Toda promoción dirigida a las autoridades fiscales, deberá presentarse mediante documento digital que contenga firma electrónica avanzada. Los contribuyentes que*

exclusivamente se dediquen a las actividades agrícolas, ganaderas, pesqueras o silvícolas que no queden comprendidos en el tercer párrafo del artículo 31 de éste Código, podrán no usar firma electrónica avanzada. El Servicio de Administración Tributaria, mediante reglas de carácter general, podrán determinar las promociones que se presentarán mediante documento impreso. (…).

Artículo 31.- *Las personas deberán presentar las solicitudes en materia de registro federal de contribuyentes, declaraciones, avisos o informes, en documentos digitales con firma electrónica avanzada a través de los medios, formatos electrónicos y con la información que señale el Servicio de Administración Tributaria mediante reglas de carácter general, enviándolas a las autoridades correspondientes o a las oficinas autorizadas, según sea el caso, pagar mediante transferencia electrónica de fondos. Cuando las disposiciones fiscales establezcan que se acompañe un documento distinto a escrituras o poderes notariales, y éste no sea digitalizado, la solicitud o el aviso se podrán presentar en medios impresos. (…)*

Las facturas electrónicas se ven reguladas por los artículos 37 a 41 del Reglamento del CFF y 94 de la Ley del Impuesto sobre la Renta (LIR).

El Servicio de Administración Tributaria, mediante reglas de carácter general, podrá autorizar a las organizaciones que agrupen a los contribuyentes que en las mismas reglas se señalen, para que a nombre de éstos presenten las declaraciones, avisos, solicitudes y demás documentos que exijan las disposiciones fiscales.

Por lo que respecta al comercio electrónico, el inciso “VI: Comercio” de las divisiones de las áreas de trabajo de la OECD asuntos fiscales (CTPA), señala los desafíos y oportunidades para los sistemas comerciales con nuevos modelos empresariales a los que es difícil aplicar los principios fiscales que rigen al comercio tradicional, sobre todo al aplicar correctamente los impuestos al consumo a las transacciones electrónicas transfronterizas, tal es el caso de los productos que pueden ser suministrados en formato electrónico y no físico, por lo que ha sido necesario celebrar foros donde se reúnan funcionarios de las administraciones económicas y fiscales de los gobiernos de los estados miembros para el intercambio de ideas respecto a los impuestos directos que se adaptan a la definición de establecimiento permanente a través de los primeros comentarios sobre el artículo 5 del *Modelo de Convenio Fiscal* de 2001 ahora *Convención modelo de las Naciones Unidas sobre la Doble Tributación*, mejor conocida como (Convención Modelo de las Naciones Unidas). Mientras que para los impuestos sobre el consumo, atribuye la imposición de acuerdo con el principio de gravamen en el país de destino, habiéndose aprobado y publicado directivas sobre la aplicación de este principio.

En este rubro se sugiere revisar las Resoluciones de Misceláneas Fiscales (RMF) publicadas anualmente en el DOF así como sus modificaciones, las cuales, para el tema fiscal de referencia empiezan a tener impacto a partir de la RMF del 30 de mayo de 2002.

El pasado 3 de diciembre de 2015 se realizó un convenio de colaboración entre la Confederación Nacional de Gobernadores (CONAGO) y SHCP a efecto de implementar la FIEL en trámites y servicios en las Entidades de la República Mexicana. Previo a la suscripción de este convenio, la

FIEL solo se podía utilizar para trámites con el gobierno federal (actualmente la FIEL es usada por 8.8 millones de contribuyentes), sin embargo la mayoría de las gestiones que debe realizar la población es ante las administraciones estatales y municipales.

Por ello, algunos de los compromisos para avanzar en el uso de la FIEL en las entidades federativas son:

a) Instalarles módulos para la emisión de firma electrónica, a cargo del Servicio de Administración Tributaria (SAT),
b) Brindarles asistencia técnica y consultoría para que desarrollen las plataformas de los trámites electrónicos, y
c) Habilitarles la firma electrónica en teléfonos inteligentes a partir de 2016.

Luego, el 31 de mayo de 2004 el SAT publicó el *Anexo 20 de la Resolución de Miscelánea Fiscal* (RMF) con el primer estándar técnico del Comprobante Fiscal Digital (CFD) y el reconocimiento de la factura electrónica, a través de ella se regulan los requisitos para personas físicas o morales que desee emitir dichos comprobantes.

La factura electrónica en México es la representación digital de un tipo de Comprobante Fiscal Digital por Internet (CFDI), que actualmente está apegada a los estándares definidos por el SAT en el vigente Anexo 20 de la Segunda Resolución de Modificaciones a la Resolución Miscelánea Fiscal (RMF) para 2015, publicada el 14 y 22 de mayo de 2015[359], respectivamente, los cuales consisten en ser generada, transmitida y resguardada empleando herramientas electrónicas.

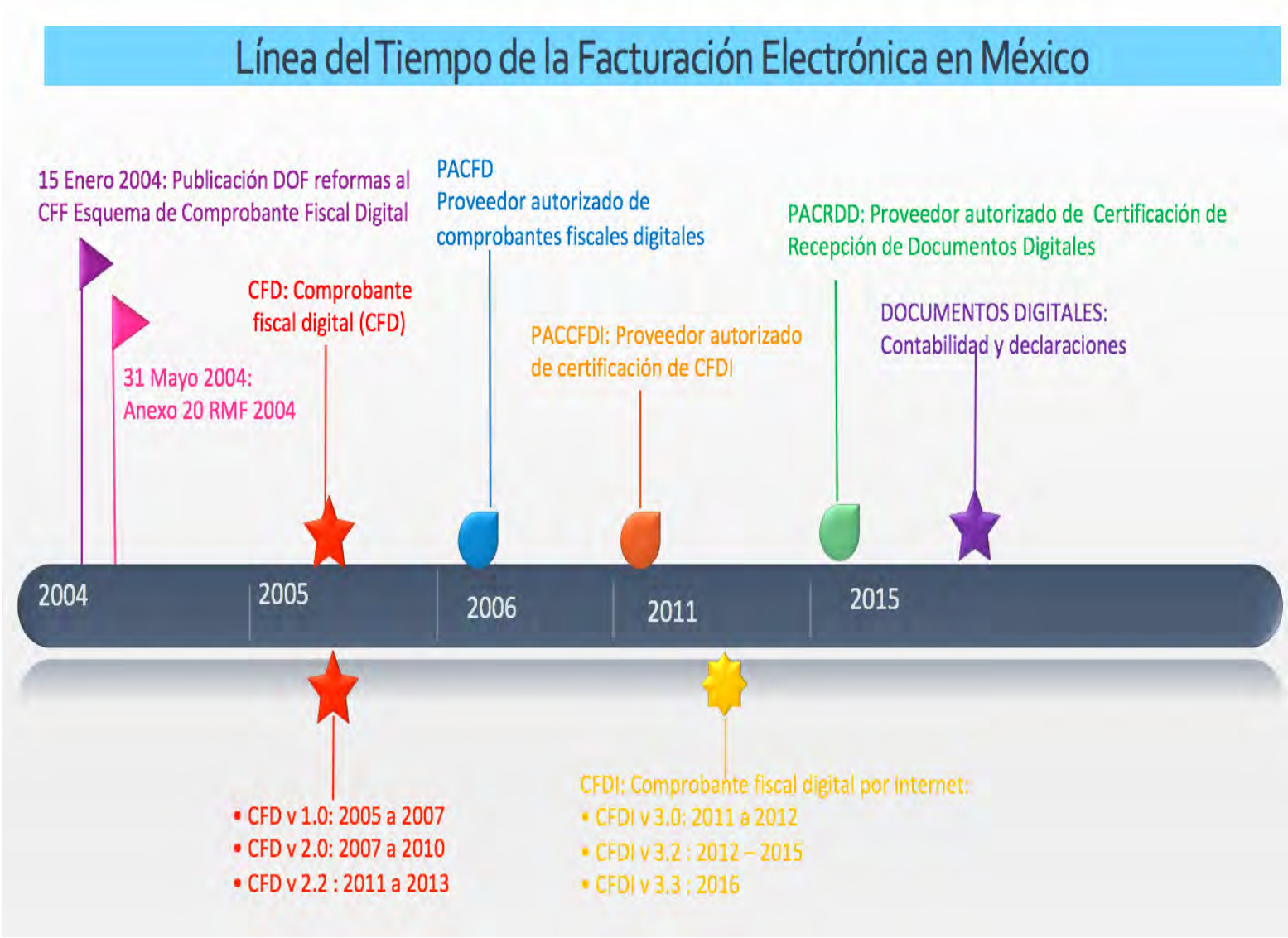
En este sentido, el SAT señala que la factura electrónica:

> *Es un tipo de CFDI y se define como un documento digital con validez legal, que utiliza estándares técnicos de seguridad internacionalmente reconocidos, para garantizar la integridad, confidencialidad, autenticidad, unicidad y no repudio del documento.* [360]

Por su parte, en el ámbito comercial la factura electrónica es un documento, de acuerdo al artículo 48 del CCo, en los siguientes términos:

> ***Artículo 48.*** *Tratándose de las copias de las cartas, telegramas y otros documentos que los comerciantes expidan, así como de los que reciban que no estén incluidos en el artículo siguiente, el archivo podrá integrarse con copias obtenidas por cualquier medio: mecánico, fotográfico o electrónico, que permita su reproducción posterior íntegra y su consulta o compulsa en caso necesario.*

[359] Accesible en http://www.sat.gob.mx/informacion_fiscal/normatividad/Paginas/resolucion_miscelanea_2015.aspx, consulta 2 de diciembre de 2015.
[360] Definición del glosario del SAT en línea, disponible en: http://www.sat.gob.mx/informacion_fiscal/glosario/Paginas/glosario_f.aspx, fecha de consulta: 1 de enero de 2015.


Línea del Tiempo de la Facturación Electrónica en México
15 Enero 2004: Publicación DOF reformas al CFF Esquema de Comprobante Fiscal Digital
31 Mayo 2004: Anexo 20 RMF 2004
CFD: Comprobante fiscal digital (CFD)
PACFD Proveedor autorizado de comprobantes fiscales digitales
PACCFDI: Proveedor autorizado de certificación de CFDI
PACRDD: Proveedor autorizado de Certificación de Recepción de Documentos Digitales
DOCUMENTOS DIGITALES: Contabilidad y declaraciones
2004
2005
2006
2011
2015
• CFD v 1.0: 2005 a 2007
• CFD v 2.0: 2007 a 2010
• CFD v 2.2 : 2011 a 2013
CFDI: Comprobante fiscal digital por internet:
• CFDI v 3.0: 2011 a 2012
• CFDI v 3.2 : 2012 – 2015
• CFDI v 3.3 : 2016

Por último, no queremos dejar de señalar que, actualmente, el SAT ofrece el servicio de emisión de Factura Electrónica de Nómina a los trabajadores a través de la aplicación Mis cuentas [361] es a través de alguna de las siguientes dos opciones:

a) Si es ante el Servicio de Administración Tributaria son:
- RFC y contraseña o firma electrónica.
- RFC de cada uno de los trabajadores.

b) Si es ante el Instituto Mexicano del Seguro Social son:
- Estar inscrito y contar con tu registro patronal.
- Contar con la prima de riesgo de trabajo asignada de acuerdo con tu actividad.
- Alta previa de tus trabajadores y contar con su número de seguro social.

La aplicación no cuenta con un límite para emitir las facturas electrónicas que se requieran, siempre y cuando se trate de un patrón que cumpla las políticas que se indican en la aplicación.

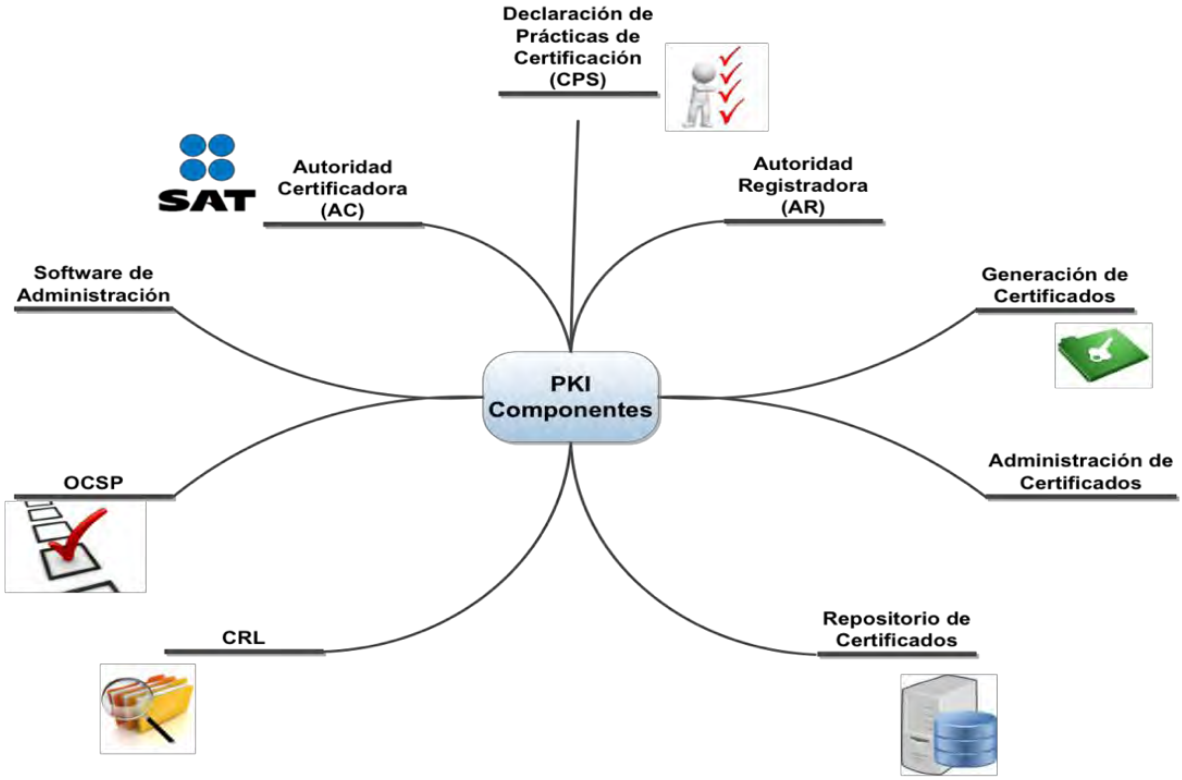
4.9.1.2. Actores en la facturación electrónica.

Mediante el uso de los certificados digitales se permite el cifrado o encriptación de un mensaje de datos, en términos coloquiales lo que una llave cierra, la otra lo abre y viceversa.

Para posibilitar la generación, administración, revocación, uso y validación de certificados digitales en la emisión y recepción de CFDI, intervienen los siguientes actores:

a) Autoridad Raíz o Autoridad Reguladora Central (Ej. Banxico y Órganos Constitucionales Autónomos): Controla la generación de certificados digitales para la Autoridad Certificadores.
b) Autoridad Certificadora (AC): Es la entidad de confianza responsable de emitir y revocar os certificados digitales, se trata del SAT
c) Contribuyentes: Titulares de certificados
d) Proveedores Autorizados de Certificación (PAC). Son quienes consultan el estatus de certificados, validan estructura del XML, y timbran el documento para envío al emisor y a la autoridad destinataria.
e) Terceras Partes de Confianza, en las que se podrá tener confianza en el certificado digital de un usuario al que previamente no se conoce si dicho certificado está avalado por una tercera parte en la que sí se confía.

[361] Accesible en https://rfs.siat.sat.gob.mx/PTSC/RFS/menu/, consultado el 8 de octubre de 2015.



Ejemplo de los componentes de la Infraestructura de Clave Pública del SAT[362]

La factura electrónica desde sus orígenes considera la participación de PAC, que son participantes indispensables para:

a) Disminuir la inversión gubernamental en la implementación de un modelo digital de comprobación fiscal,
b) Incorporar al modelo de factura electrónica del 100% de la base de contribuyentes en tiempos récord,
c) Procesar altos volúmenes transaccionales de operación,
d) Abastecer al mercado de usuarios de soluciones de cumplimiento con valores agregados,
e) Agilizar la migración hacia nuevas versiones de esquemas técnicos que permiten la mejora continua del modelo.

Dado estos participantes, no se puede falsificar una FIEL, en razón de que la tecnología que se utiliza para crear los certificados digitales que conforman la misma no permite falsificaciones.

A continuación se exhibe una tabla cronológica de la evolución de la FIEL:

[362] SAT, La Evolución de la Firma Electrónica, en Nuevos servicios digitales del SAT, Diapositivas de la Expo feria 2015, 16 de Diciembre de 2015, World Trade Center, Ciudad de México, accesible en: http://www.sat.gob.mx/innovacionestecnologicas/Paginas/a/documentos/EvolucionFirmaElectronica.pptx, consultado el 17 de diciembre de 2015.

2004

- Nace la Factura Electrónica y se publica el primer estándar tecnológico de la Factura Electrónica en México
- El SAT implementa la FIEL para su uso en los portales de servicios al Contribuyente.
- Inicio de Operaciones con AC de longitud 2048 y algoritmo criptográfico MD5.
- Firma de Convenio con Banxico para que la AC del SAT forme parte de la Infraestructura Extendida de Seguridad de Banxico.

2005

- Inicio de los Comprobantes Fiscales Digitales para la Facturación Electrónica.

Entre 2005 y 2010 se emitieron 1,133,213,763 comprobantes.
Dictamen Fiscal
Pedimentos Aduanales
Expediente Integral del Contribuyente

2006

- Aviso autoimpresores
- Renovación FIEL por Internet
- Declaranet con FIEL (Secretaria de la Función Pública)

2007

- Constitución de Sociedades (Secretaria de Relaciones Exteriores)
- Decreto INMEX (Secretaria de Economía)
- Condonación de Créditos Fiscales
- Devoluciones IVA >= $25,000

2008

- Devoluciones automáticas ISR >=$10,000
- OCSP para consulta de certificados
- Firma convenio SAT- CIAPEM
- Actualización tecnológica de certificados de AC longitud 2048 y algoritmo criptográfico SHA1.

2009

- Homologación de servicios Fiel a nivel Federal
- Declaración Anual de Personas Morales

2011

- Evoluciona la figura del Proveedor de Servicios al modelo PAC para el timbrado/certificación de CFDI.

2012

- Se promulgó la Ley de Firma Electrónica Avanzada para dar el sustento jurídico a los actos realizados por los Ciudadanos y las empresas ante los organismos del Gobierno Federal.
- Se emitieron 2,981,685,982 CFDI's

2013

- La Estrategia Digital Nacional (EDN) establece a la FIEL como el medio de Identificación, Autenticación y Autorización para la Ventanilla Única Nacional (gob.mx).
- Se emitieron 3,765,030,126 de CFDI's.

2014

- Estándar CFDI
  - Todas las facturas electrónicas en México se alinean al esquema CFDI v3.2.
  - Inicia la nómina electrónica.
  - Buzón Tributario
  - Se agrega al esquema las retenciones electrónicas e información de pagos.

2015

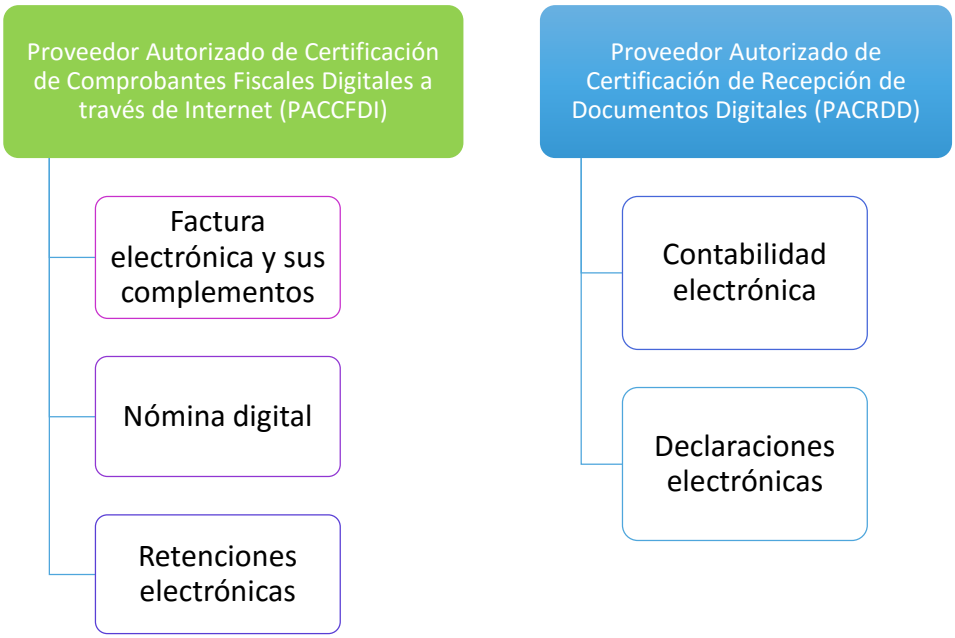
- Servicios Fiscales Digitales Integrales
  - Nace la figura del PACRDD.
  - Inicia la contabilidad electrónica.
  - Se agrega al esquema del sellado las declaraciones.

Simplificación del proceso de renovación de FIEL por internet.

- Implementación de un proceso de autorización electrónica basado en TOTP para personas físicas que tienen FIEL
- Actualización tecnológica de certificados de AC longitud 4096 y algoritmo criptográfico SHA2-256.
- A octubre de este año se han emitido 4,777,984,935 CFDI´s.
- Se promueve el cambio de significado fiscal de la FIEL a un significado ciudadano llamado e.firma.

Los PAC son una referencia que engloba a tres organizaciones:

a) Empresas autorizadas, reguladas y auditadas por la autoridad fiscal para la oferta de servicios de tributación digital.
b) Prestadoras de servicios de comunicación digital certificada: Autenticación, no repudio, confidencialidad e integridad de los datos.
c) Empresas respaldadas con inversiones superiores a los 10mdp y garantía ante la Tesorería de la Federación (TESOFE), para acreditar su solvencia técnica y jurídica.



4.9.1.3. Procedimiento descriptivo de facturación electrónica

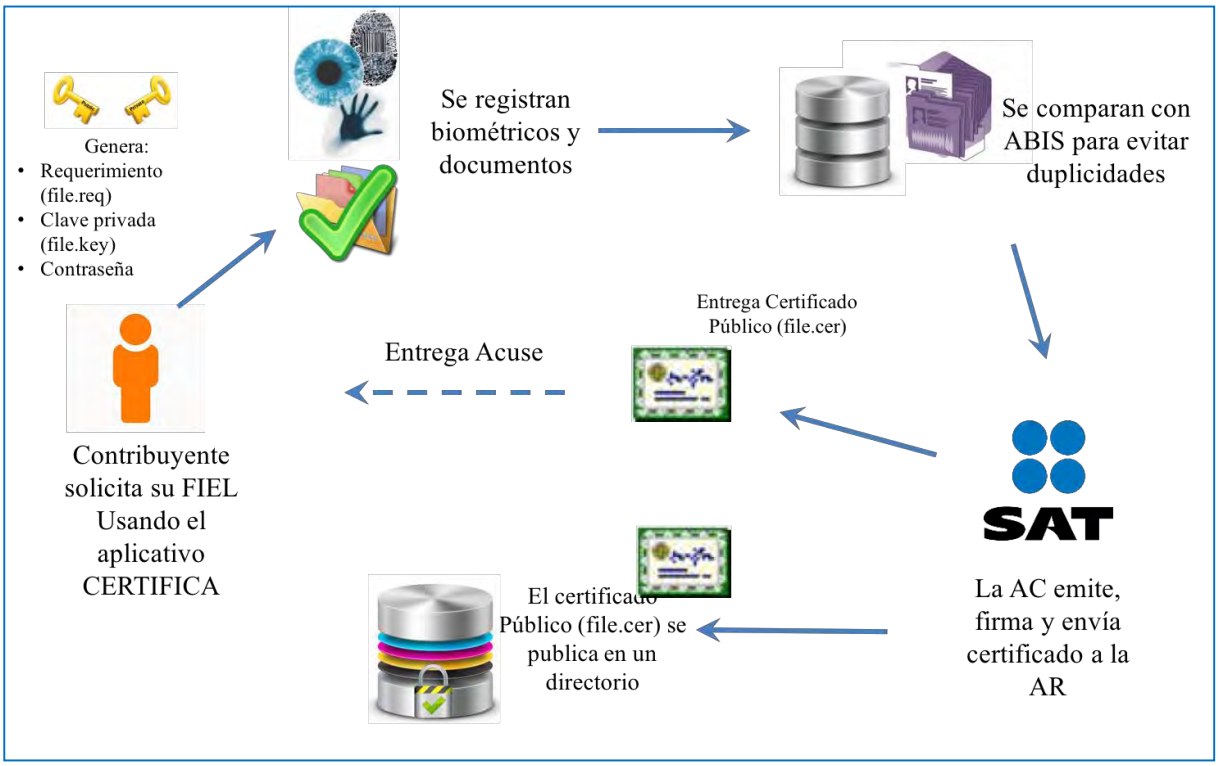
La emisión de una factura electrónica consiste en la expedición de un documento electrónico con sello digital y folios, haciendo uso de una llave privada, la información contenida en cada factura es encriptada, guardada y enviada a su destinatario vía internet, quien al recibir el archivo, la podrá desencriptar con el uso de su llave pública, incluso recibirla y registrada automáticamente por sus sistemas de planificación de recursos empresariales *Enterprise Resource Planning* (ERP) e imprimirlo en caso de que el destinatario no cuente con un sistema ERP.[363]

A dicho documento se le adjunta la FEA y un sello digital que avalan su origen y otorga validez ante el SAT, una cadena original que funciona como un resumen del contenido de la factura, y un folio que indica el número de la transacción. Además se le acompañan certificados de FEA y

[363] Arredondo Barrera, Luis H. et al. Los negocios electrónicos por Internet, en Bastidas, Ma. Teresa; Novoa, Jorge y Pérez, Alfonso (coord.). La firma y la factura electrónicas: Entorno jurídico, fiscal e informático. Ed. Instituto Mexicano de Contadores Públicos (IMCP), 2004, México D.F., p. 78.

de sellos digitales que tienen una validez de dos años, lo cual hace más difícil desencriptar una llave.

Un CFDI es utilizado por el comprador y por el vendedor como comprobante ante las autoridades y en las auditorías internas. El Anexo 20 de la Segunda Resolución de Modificaciones a la Resolución Miscelánea Fiscal para 2015[364], publicada el 14 de mayo de 2015 señala el estándar para conformar correctamente una factura digital es un documento XML integrado por los datos del emisor de la factura, el receptor de la misma, los conceptos e impuestos. El sistema de facturación electrónica funciona con llaves públicas y privadas de 1024 bits del algoritmo RSA, que requieren más de 70 años con las computadoras más potentes y un presupuestos de más de 100 millones de dólares para quebrar este algoritmo.



Descripción del procedimiento de Facturación[365]

El trámite ante el SAT consiste en otorgar a cada contribuyente de un par de claves, una pública y otra privada, además de un certificado digital que avala la identidad del contribuyente especificando sus datos fiscales además de su llave pública.

Una factura electrónica contiene dos firmas electrónicas, una otorgada por el emisor del

[364] Véase Diario Oficial de la Federación en línea: http://dof.gob.mx/nota_detalle.php?codigo=5393397&fecha=22/05/2015, fecha de consulta

[365] SAT, La Evolución de la Firma Electrónica, en Nuevos servicios digitales del SAT, Diapositivas de la Expo feria 2015, 16 de Diciembre de 2015, World Trade Center, Ciudad de México, accesible en: http://www.sat.gob.mx/innovacionestecnologicas/Paginas/a/documentos/EvolucionFirmaElectronica.pptx, consultado el 17 de diciembre de 2015.

comprobante fiscal utilizando su clave privada para signar la factura; y la otra, de un tercero autorizado que firma los datos de fecha, hora del timbrado, identificador de la transacción así como la primera firma del CFDI, ambas firmas están inmersas en un nodo de la factura digital que se le denomina timbre fiscal digital. En este sistema se utilizan dos certificados digitales: uno que acredita la clave pública que conforma a la **Fi**rma **El**ectrónica (avanzada) denominada FIEL por el SAT y de un contribuyente y otro u otros para sellar digitalmente facturas digitales.

La FIEL es un mecanismo de criptografía de clave pública que permite firmar digitalmente trámites en los procesos en línea que provee el SAT; uno de ellos es el de firmar el requerimiento para que se otorgue el certificado de sello digital para emitir facturas electrónicas. Para la plataforma de facturación electrónica propuesta se propone adoptar el mecanismo de autenticación de dos vías o mutuo, el cual está definido en el protocolo y permite que ambas partes que intervienen en la comunicación posean un certificado digital, en este caso la FIEL del lado del contribuyente, y un certificado digital del lado del servidor. De esta forma se establece un canal seguro entre la aplicación del contribuyente y la plataforma de facturación[366].

En el esquema de facturación digital desde 2010, la autenticación en los sistemas del SAT se puede realizar mediante el uso de la Clave de Identificación Electrónica Confidencial (CIEC), que está formada por el RFC del contribuyente y una contraseña asociada. Este mecanismo sirve para tramitar la FIEL y los Certificados de Sello Digital. Existe también otra manera de autenticación consistente en el empleo la FIEL desde una aplicación que se ejecuta en la computadora del contribuyente.

Los mecanismos de acceso a la FIEL que robustecen la seguridad del resguardo de la clave privada y facilitar su acceso a ésta, es el uso biométricos para su acceso mediante dispositivos que nos permitan:

- Reconocimiento de firma autógrafa (duración, presión y rúbrica de la firma autógrafa).
- Reconocimiento de voz (tesitura).
- Reconocimiento de huellas dactilares.
- Reconocimiento de retina.

Estos elementos permitirían la reconstrucción de la clave simétrica para el acceso a la clave privada de FIEL.

Lamentablemente el sistema de facturación electrónica del SAT no ha previsto una plataforma que considere el envío y recepción de los comprobantes fiscales digitales (CFDI), independientemente de que se precise que se pueden intercambiar electrónicamente acuses de recibo; no obstante, no se señala un esquema formal de envío, recepción ni acuse; ante esta ausencia, los contribuyentes envían por correo electrónico los comprobantes digitales a

[366] Véase SAT, "Tu Firm@: Firma Electrónica Avanzada", disponible en ftp://ftp2.sat.gob.mx/asistencia_ftp/publicaciones/folletos2006/ABCfea.pdf, fecha de consulta: 1 de enero de 2015.

aquellos que se les emite dicha factura digital.

Es interesante señalar que el SAT registró como marca nominativa la FIEL, la cual fue inscrita y concedida en la clase 38 de la Clasificación Niza[367], que corresponde a la materia de telecomunicaciones, en el tipo de clase 9, esto es, acceso a servicios de software en línea, del periodo que va del 20 de julio de 2011 al 30 de marzo de 2021[368].

A partir del 1º de junio 2015, el SAT descontinuó el programa Solicitud de Certificado Digital (SCD), mejor conocido por su acrónimo SOLCEDI con el que se obtenían los archivos *.req y .key* y se implementó un nuevo programa denominado CERTIFICA que sustituyó al anterior para integrar las nuevas disposiciones técnicas de los archivos FIEL y los Certificados Sellos Digitales (CSD) publicadas en el DOF el 22 de Mayo de 2015[369], dichas modificaciones del certificado digital de la FIEL y los CSD son:

a) La longitud de las llaves de los certificados de la FIEL y de los CSD que eran de 1024 bits pasa a ser de 2048 bits.
b) Se integra el algoritmo SHA-256[370] para utilizado con estas nuevas llaves de 2048 bits para firmar un certificado digital.

Los costos del servicio de certificación impactan en la expansión del uso de la FEA en el país. Su comercialización por una Prestadora de Servicios de Certificación (PSC) o Agencia Certificadora habilitada por la SE[371], determina sus precios para emitirlos considerando 3

[367] La Ley de la Propiedad Industrial establece en su Artículo 93 que las marcas se registrarán en relación con productos o servicios determinados según la clasificación que establezca su reglamento. Mientras que el artículo 59 del reglamento establece que la clasificación de productos y servicios a que se refiere el mencionado Artículo 93 de la Ley de la Propiedad Industrial será la Clasificación Internacional de Productos y Servicios para el Registro de las Marcas (Clasificación de Niza) vigente, establecida en virtud del Arreglo de Niza.
El Arreglo de Niza relativo a la Clasificación Internacional de Productos y Servicios para el Registro de las Marcas del 15 de junio de 1957, revisado en Estocolmo en 1967 y en Ginebra en 1977, y modificado en 1979, se promulgó en México mediante decreto publicado en el Diario Oficial de la Federación el 10 de abril de 2001.
[368] Ver el expediente: 1167173 y el número de registro 1228613 en el Instituto Mexicano de la Propiedad Industrial (IMPI).
[369] Véase anexo 20 de la Segunda Resolución de Modificaciones a la Resolución Miscelánea Fiscal para 2015, publicada el 14 de mayo de 2015.
[370] SHA-2 dio origen a varios tipos de hash, incluye un significante número de cambios respecto a su predecesor, SHA-1; y consiste en un conjunto de cuatro funciones hash de 224, 256, 384 o 512 bits. Es un tipo de hash criptográfico sucesor del SHA-1, con una de las funciones de hash más fuertes disponibles y es una herramienta en línea a través e la cual cualquiera puede fácilmente generar hashes.
Los cambios respecto a su predecesor SHA-1 consisten en un conjunto de cuatro funciones hash de 224, 256, 384 o 512 bits. El Algoritmo SHA-256 genera un tamaño mixto de 256 bits (32 bytes) un hash casi único. Hash es una función de una manera - que no se puede descifrar de regreso. Esto hace que sea adecuado para la validación de contraseñas, desafiar la autenticación de hash, sabotearlo y generar firmas digitales.
[371] Datos registrados en la página oficial de la SE para la inscripción de Prestadores de Servicios de Certificados, visible en http://www.firmadigital.gob.mx/tabla.html, fecha de consulta, 24 de noviembre de 2014.

factores[372]:
a) el tipo de certificado;
b) el tipo de acreditación; y
c) las condiciones comerciales.

El impacto de los mercados de los certificados muestra una diversidad, desde los certificados baratos en que la autoridad de certificación se limita a comprobar ciertos aspectos proporcionados por el solicitante on-line, hasta otros más caros con otras medidas de seguridad como solicitar al titular de la clave pública y privada se presente de manera física con los documentos que le acrediten personalidad.

De inicio el contribuyente emplea la plataforma del SAT —llamada CERTIFICA, que sustituyó al antes denominado SOLCEDI (Solicitud de certificados digitales) — a fin de generar dos archivos, cuya aplicación genera:

I. La llave privada (archivo electrónico con extensión ***.key**) y su respectiva contraseña de acceso, la CIEC, que es un mecanismo de acceso, formado por su RFC y una contraseña elegida por el contribuyente.
II. El archivo de requerimiento (archivo electrónico con extensión ***.req**) que contiene la llave pública.
III. Se resguarda el archivo de requerimiento en un disco compacto o en dispositivo USB, y se le entrega al SAT el día de la cita programada, junto con la documentación para personas físicas[373] o personas morales[374]
IV. Al finalizar el trámite recibirá una copia de su certificado digital (extensión ***.cer**) grabada en el disco compacto o en el dispositivo USB con el que presentó su archivo de requerimiento. Con dicho certificado se comprueba que el individuo que tiene una FIEL es dueño de esa firma. En consecuencia, será un requisito para establecer la validez de un documento digital.
V. Una vez generado este archivo debe "ensobretar" el requerimiento utilizando su FIEL para crear un archivo denominado así: ensobretado **(.sdg).** Para esto, hay que volver a utilizar el programa CERTIFICA accediendo en la opción "Ensobreta Sellos". Al tener el archivo de requerimiento ensobretado el usuario podrá enviarlo al SAT a través de su página oficial en la sección "Envío de Solicitud de Sellos Digitales".

La aplicación CERTIFICA se utiliza para que el contribuyente pueda generar su archivo de requerimiento de Certificado de Sello Digital, su Clave Privada y el Ensobretado. Todos sus datos

[372] La información de dicha empresa está disponible en http://www.pscworld.com/pscworld, consulta del 3 de noviembre de 2014.
[373] Acta de nacimiento, carta de naturalización o documento migratorio vigente e Identificación oficial
[374] Copia certificada del poder general para actos de dominio o de administración; Acta constitutiva y Identificación oficial del representante legal.

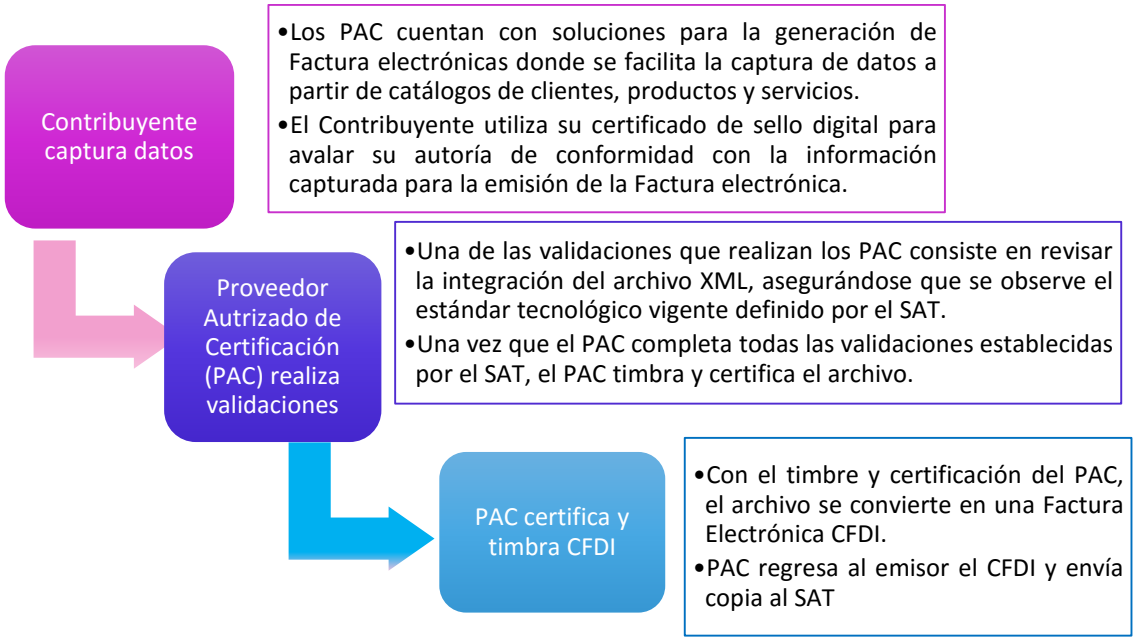
deben ser resguardados en un lugar seguro, sólo el archivo ensobretado es el que se envía al SAT a través de su página web en un archivo especial (*.sdg).

En suma los archivos que debe tener el contribuyente son:

- Archivo de requerimiento, contiene su llave pública: ***.req***
- Archivo de la clave privada*:* ***.key***
- Certificado de la FIEL que identifica al contribuyente con su llave pública: **.cer**

Los servicios de PKI que ofrece el SAT a través de sus servicios electrónicos CERTIFICA, CERTISAT y OCSP son:

- Identificación de los solicitantes de certificados digitales
- Generación de certificados digitales
- Emisión de certificados digitales
- Gestión de certificados digitales
- Validación de certificados digitales (OCSP)



4.9.1.4. Fundamento y concepto de certificado de sello digital para la emisión de facturas electrónicas

Un certificado digital es un documento electrónico que asocia una clave pública con la identidad de su propietario. Los certificados de la FIEL están basados en RFC5280 con estructura X509 V, además partir del 30 de mayo de 2015 los certificados tienen una longitud de 2048 y algoritmo criptográfico SHA2-256.

Los certificados de sello digitales son hijos de la FIEL, al ser expedidos con la FIEL, se encuentran intrínsecamente ligados al titular de la firma electrónica avanzada y se estructuran con la misma tecnología. No obstante, su uso es específico, por lo que el ámbito de su aplicación está constreñido a determinadas funciones, con lo que se facilitan tareas operativas sin poner en riesgo la seguridad de la propia FIEL.

Al igual que la FIEL, están compuestos de dos archivos electrónicos integrados por un par de llaves expedidas al titular del certificado:

- Llave pública: archivo .cer
- Llave privada: archivo. Key

Aunque el marco conceptual de los certificados y las autoridades de certificación o prestadores de servicios de certificación en general, o del SAT en particular, es un tema abordado en el próximo subcapítulo 3.4., es importante abocarnos a los certificados digitales fiscales, su empleo y validez por parte del SAT.

El fundamento legal de los Certificados de Sello Digital para la emisión de Factura Electrónica son los artículos 29, 17-D, 17-G, 17-I y 17-J del CFF.

> ***Artículo 29.****-Cuando las leyes fiscales establezcan la obligación de expedir comprobantes fiscales por los actos o actividades que realicen, por los ingresos que se perciban o por las retenciones de contribuciones que efectúen, los contribuyentes deberán emitirlos mediante documentos digitales a través de la página de Internet del Servicio de Administración Tributaria. Las personas que adquieran bienes, disfruten de su uso o goce temporal, reciban servicios o aquéllas a las que les hubieren retenido contribuciones deberán solicitar el comprobante fiscal digital por Internet respectivo.*
> *Los contribuyentes podrán optar por el uso de uno o más certificados de sellos digitales que se utilizarán exclusivamente para la expedición de los comprobantes fiscales mediante documentos digitales. El sello digital permitirá acreditar la autoría de los comprobantes fiscales digitales por Internet que expidan las personas físicas y morales, el cual queda sujeto a la regulación aplicable al uso de la firma electrónica avanzada.*
> *Los contribuyentes podrán tramitar la obtención de un certificado de sello digital para ser utilizado por todos sus establecimientos o locales, o bien, tramitar la obtención de un certificado de sello digital por cada uno de sus establecimientos. El Servicio de Administración Tributaria establecerá mediante reglas de carácter general los requisitos de control e identificación a que se sujetará el uso del sello digital de los contribuyentes.*
> *La tramitación de un certificado de sello digital sólo podrá efectuarse mediante formato electrónico que cuente con la firma electrónica avanzada de la persona solicitante. (…)*

Mientras que en la parte correspondiente a los certificados de sello digital, los artículos 17-D, 17-G, 17-I y 17-J del CFF establecen:

> ***Artículo 17-D****.- Cuando las disposiciones fiscales obliguen a presentar documentos, estos deberán ser digitales y contener una firma electrónica avanzada del autor, salvo los casos*

que establezcan una regla diferente. Las autoridades fiscales, mediante reglas de carácter general, podrán autorizar el uso de otras firmas electrónicas.
Para los efectos mencionados en el párrafo anterior, se deberá contar con un certificado que confirme el vínculo entre un firmante y los datos de creación de una firma electrónica avanzada, expedido por el Servicio de Administración Tributaria cuando se trate de personas morales y de los sellos digitales previstos en el artículo 29 de este Código, y por un prestador de servicios de certificación autorizado por el Banco de México cuando se trate de personas físicas. El Banco de México publicará en el Diario Oficial de la Federación la denominación de los prestadores de los servicios mencionados que autorice y, en su caso, la revocación correspondiente. (…)

***Artículo 17-G**.- Los certificados que emita el Servicio de Administración Tributaria para ser considerados válidos deberán contener los datos siguientes:*
***I.** La mención de que se expiden como tales. Tratándose de certificados de sellos digitales, se deberán especificar las limitantes que tengan para su uso.*
(…)
***Artículo 17-I**.- La integridad y autoría de un documento digital con firma electrónica avanzada o sello digital será verificable mediante el método de remisión al documento original con la clave pública del autor.*

***Artículo 17-J**.- El titular de un certificado emitido por el Servicio de Administración Tributaria, tendrá las siguientes obligaciones:*
***I.** Actuar con diligencia y establecer los medios razonables para evitar la utilización no autorizada de los datos de creación de la firma.*
***II.** Cuando se emplee el certificado en relación con una firma electrónica avanzada, actuar con diligencia razonable para cerciorarse de que todas las declaraciones que haya hecho en relación con el certificado, con su vigencia, o que hayan sido consignados en el mismo, son exactas.*
(…)

Un inconveniente es que dichos certificados no están disponibles en un repositorio de certificados mediante el cual cualquiera pudiera obtener un certificado que le interese, como por ejemplo el de los contribuyentes que le emitieron facturas digitales, para poder verificar los comprobantes recibidos. Para el correcto uso y funcionamiento de los certificados digitales es necesario de la incorporación de la Infraestructura de Llave Pública (PKI), la cual es una combinación de software, tecnologías de cifrado, y servicios que permiten proteger la seguridad de las transacciones de información en un sistema distribuido. Debido a que el SAT asume el papel de una autoridad certificadora —ya que genera los certificados digitales y también cumple con tareas de afiliación de los contribuyentes—, el SAT podría hacer uso de PKI para un buen funcionamiento en cuanto a poner a disposición de los contribuyentes los certificados digitales de los demás, así como las listas de revocación.

4.9.1.5. Diferencias entre sello digital y la certificación de sello digital del SAT.

El sello digital o sello del SAT es el sello que se genera para un comprobante a partir del Certificado de Sello Digital (CSD) del SAT que recibió un PAC para tales efectos.

Mientras que la Certificación o timbrado digital del SAT es la cadena original del complemento de certificación del CFDI, donde se encuentra el XML y la representación impresa del CFDI. Dicha cadena contiene los siguientes datos:

a) Versión del Timbre del CFDI.
b) Identificador Único Universal o *Universally Unique Identifier* (UUID)[375]
a) Fecha del Timbrado.
b) Sello Digital del CFDI = CSD Emisor + Cadena Original Primaria.
c) Número de Certificación del SAT= CSD del SAT que tiene un PAC en su resguardo.

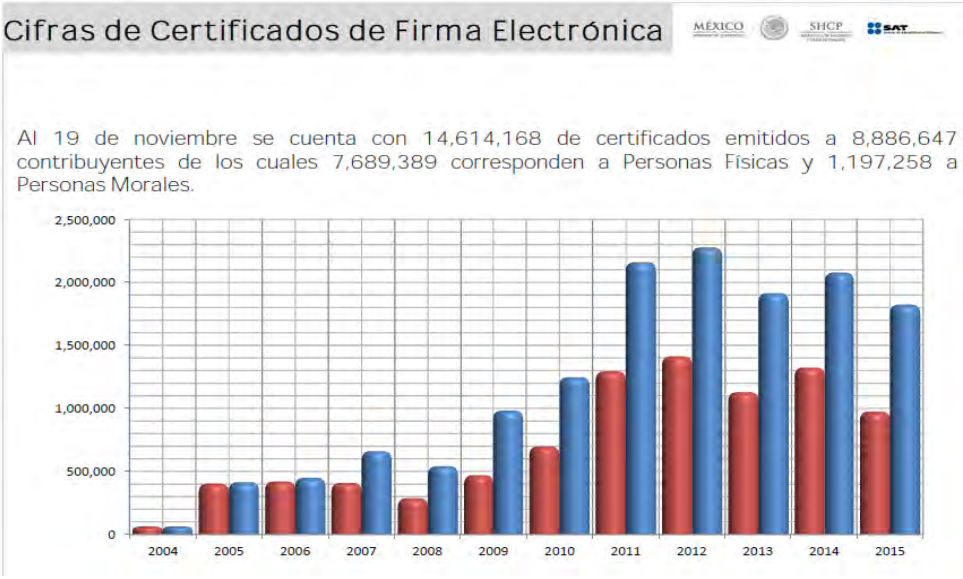


Gráfico del SAT[376]

[375] Para identificar la validez de los folios digitales o comprobantes fiscales digitales por Internet se utiliza el UUID, que es el código identificador estándar que se utiliza en el proceso de construcción de un software cuyo formato facilita un código sin una coordinación central te lo genere. En materia fiscal, el SAT autoriza que los PAC asignan los UUID al momento de realizar la validación del documentos digitales, a fin de que el SAT se libere de la tarea de otorgarlo a los contribuyentes como antes lo hacía.
El UUID está formado por una cadena compuesta por 32 dígitos hexadecimales (del 0 al 9 y las primeras 6 letras del alfabeto) que se muestran en grupos de 5 dígitos separados por guiones como por ejemplo: 560a8451-a29c-41d4-a716-544676554400 La cantidad de caracteres hace muy complicada la digitalización y búsqueda por medio de este código, por lo que para poder verificar si el UUID o Folio Fiscal del CFDI debe estar escrito con mayúsculas porque sino será imposible hacerlo desde el sitio https://verificacfdi.facturaelectronica.sat.gob.mx. Ejemplo: 4A1B43E2-1183-4AD4-A3DE-C2DA787AE56A = Valido

[376] SAT, La Evolución de la Firma Electrónica, en Nuevos servicios digitales del SAT, Diapositivas de la Expo feria 2015, 16 de Diciembre de 2015, World Trade Center, Ciudad de México, accesible en: http://www.sat.gob.mx/innovacionestecnologicas/Paginas/a/documentos/EvolucionFirmaElectronica.pptx, consultado el 17 de diciembre de 2015.

4.9.1.6. Cifras y datos de la FIEL del SAT.

Se han emitido 11, 416,948 de certificados digitales, de los cuales:

- 9,686,111 corresponden a personas físicas
- 1,730,837 corresponden a personas morales

Diariamente se generan poco más de 4 mil nuevos certificados con su biometría respectiva y se reciben 2 millones de consultas al Protocolo de Estatus de Certificados en Línea u *Online Certificate Status Protocol* (OCSP).

La arquitectura del OCSP en el SAT contempla alta disponibilidad, cuenta con balanceos en su capa de presentación y en la capa de procesamiento además de estar en dos diferentes Centros de Datos.

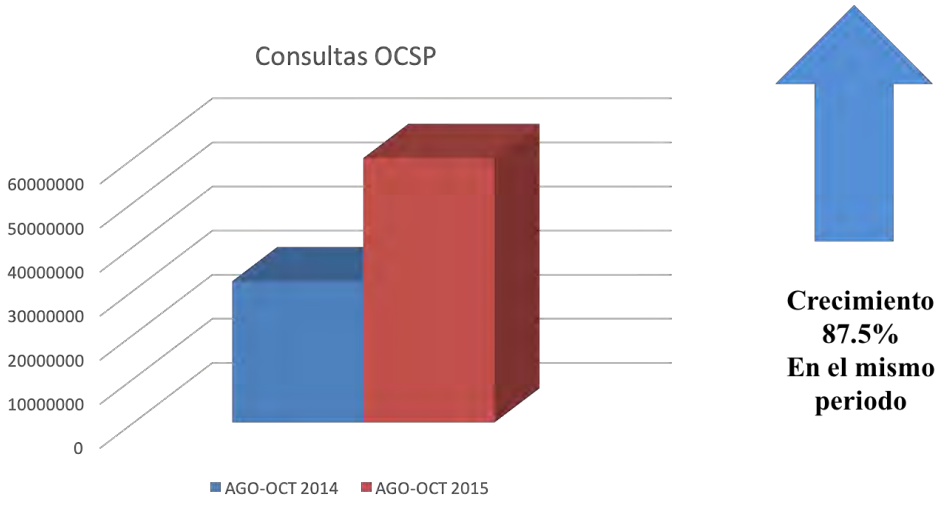


Gráfico del SAT[377]

4.9.1.7. Convenios de Colaboración del SAT.

Ha sido un gran acierto que el SAT haya considerado signar Convenios de Colaboración cuyo objeto es el reconocimiento de certificados de Firma electrónica emitidos por el SAT, a fin de que entidades y dependencias de la Administración Pública Federal, Local y Municipal puedan aprovechar los certificados expedidos por el SAT[378]. Como resultado, la autoridad solicitante signataria tendrá contar con el servicio de consulta del estado de revocación del certificado de Firma Electrónica Online Certificate Status Protocol, el cual será liberado una vez que se haya

[377] SAT, La Evolución de la Firma Electrónica, en Nuevos servicios digitales del SAT, Diapositivas de la Expo feria 2015, 16 de Diciembre de 2015, World Trade Center, Ciudad de México, accesible en: http://www.sat.gob.mx/innovacionestecnologicas/Paginas/a/documentos/EvolucionFirmaElectronica.pptx, consultado el 17 de diciembre de 2015.

[378] https://www.gob.mx/cidge/acciones-y-programas/convenio-para-el-uso-de-la-firma-electronica-avanzada

firmado el Convenio de Colaboración.

Las dependencias, entidades federativas y municipios tendrán los siguientes beneficios:

- Actualización de procedimientos para incorporar la Firma Electrónica en sus trámites.
- Verificar la autenticidad de los certificados de Firma Electrónica
- Consultar el estado de los certificados de Firma Electrónica de sus servidores públicos.
- Promover y difundir la adopción y uso de la Firma Electrónica del SAT.

El SAT ha publicado a través del Foro de Servicios Tributarios para el Gobierno Federal, un procedimiento de cinco pasos para la Colaboración eficiente:

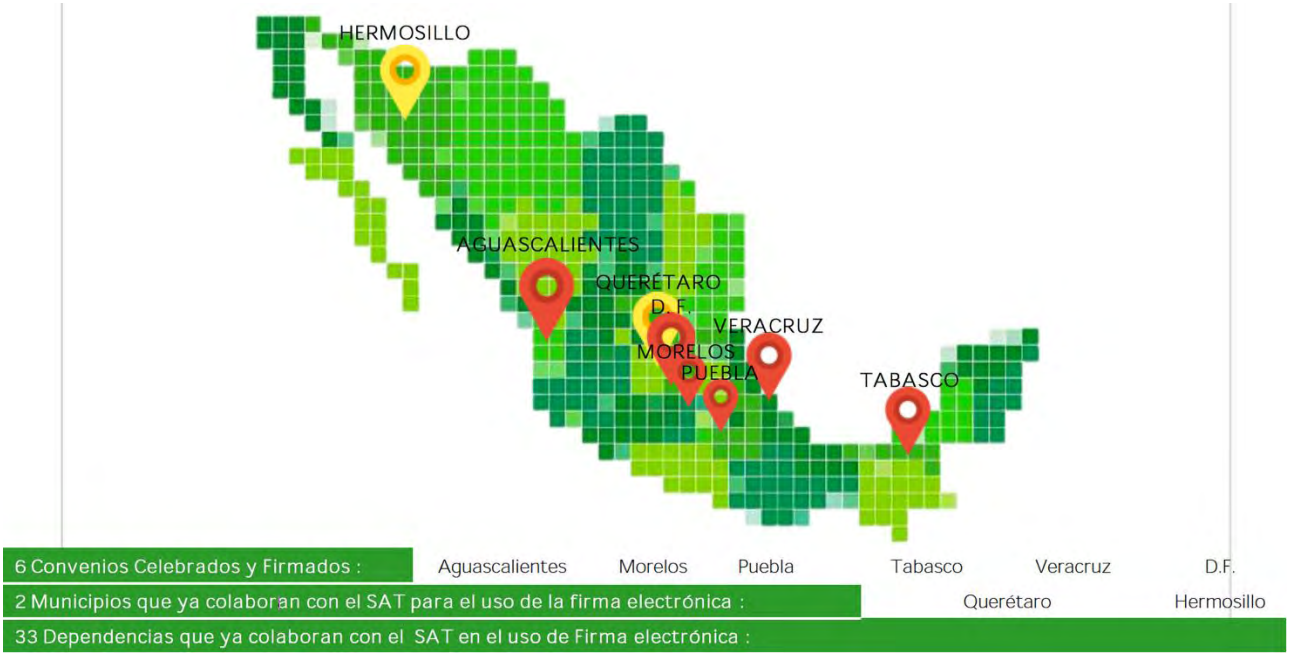
1. El SAT se acerca a las Dependencias, Entidades Federativas y Municipios, para ofrecer el Convenio de Colaboración del certificado de e.firma.
2. Reunión Normativa
3. Firma del Convenio
4. Reuniones Técnicas
5. Implementación del servicio

Luego hace permite que la autoridad interesada, descargue tres documentos del sitio web respectivo[379], a saber:

a) **Convenio Tipo de Colaboración.-** El presente convenio permite a los Estados y Municipios establecer las acciones necesarias y los mecanismos de colaboración para el uso de los servicios relacionados con la firma electrónica avanzada que presta actualmente el SAT.
b) **Anexo único de Convenio de Colaboración.-** En este anexo se establecen los requerimientos técnicos para el uso del *Online Certificate Status Protocol* (OCSP), del SAT, y se definirán los enlaces de las áreas tecnológicas tanto del SAT como del Estado o Municipio.
c) **Volumetría de los Servicios de nombre de la dependencia o entidad**.- En este anexo se integrará toda la información relativa a la volumetría[380] de servicios de la Entidad Federativa o el Municipio, para conocimiento del SAT. (Ver el Convenio tipo de colaboración, el Anexo único y la Volumetría en el Apéndice V)

[379] Acciones y Programas publicados por CIDGE, tres documentos accesibles para descargar en https://www.gob.mx/cidge/acciones-y-programas/convenio-para-el-uso-de-la-firma-electronica-avanzada, consultada el 2 de diciembre de 2015.
[380] Es la consulta que realiza la Dependencia y/o Entidad Federativa con la finalidad de corroborar si un certificado digital de firma electrónica "e.firma" emitido por el SAT es o no válido y con esto estar en posibilidad de realizar el servicio o trámite que la Dependencia y/o Entidad Federativa tenga implementado.

Convenios de Colaboración del SAT con Entidades Federativas[381]



Por lo que hace a las entidades y dependencias que han signado un convenio de colaboración en materia de Firma Electrónica Avanzada, se encuentra las siguientes:

1. Secretaría de Comunicaciones y Transportes (SCT)
2. Secretaría de Desarrollo Social (SEDESOL)
3. Secretaría de Economía (SE)
4. Secretaría de Energía (SENER)
5. Secretaría de Gobernación (SEGOB)
6. Secretaría de la Función Pública (SFP)
7. Secretaría de Marina (SEMAR)
8. Secretaría de Relaciones Exteriores (S.R.E.)
9. Secretaría de Turismo (SECTUR)
10. Secretaría del Medio Ambiente y Recursos Naturales (SEMARNAT)
11. Secretaría de Trabajo y Previsión Social (STPS)
12. Comisión Nacional del Agua (CONAGUA)
13. Instituto Mexicano del Seguro Social (IMSS)
14. Petróleos Mexicanos (PEMEX)
15. Banco de México (BANXICO)
16. Centros de Integración Juvenil, A.C. (CIJ)
17. Colegio Nacional de Educación Profesional Técnica (CONALEP)
18. Comisión Federal de Competencia Económica (COFECE)

[381] SAT. Convenios de Colaboración en Materia de Firma Electrónica, Ciudad de México, 27 de Noviembre de 2015, 9ª diapositva de la presentación pública de SHCP, accesible en http://www.sat.gob.mx/ForoTributarioDeServiciosElectronicos2015/Paginas/Documentos/ConveniosColaboracion_FirmaElectronica.pdf, consultado el 28 de noviembre de 2016.

19. Comisión Federal de Telecomunicaciones (COFETEL)
20. Comisión Nacional de Acuacultura y Pesca (CONAPESCA)
21. Comisión Nacional de Seguridad Nuclear y Salvaguardias (CNSNS)
22. Servicio de Administración y Enajenación de Bienes (SAE)
23. Comisión Reguladora de Energía (CRE)
24. Comité de Informática de la Administración Pública Estatal y Municipal A.C. (CIAPEM)
25. Consejo Nacional de Ciencia y Tecnología (CONACYT)
26. DICONSA, SA DE CV
27. Instituto Mexicano de la Propiedad Industrial (IMPI)
28. Instituto Nacional Electoral (INE)
29. Poder Judicial de la Federación (PJF)
30. Policía Federal
31. Registro Agrario Nacional (RAN)
32. Servicio Nacional de Sanidad, Inocuidad y Calidad Agroalimentaria (SENASICA)
33. Tribunal Federal de Justicia Fiscal y Administrativa (TFJFA)

A finales de 2014, 25 Entidades de la APF habían formalizado Convenio de Colaboración para uso del servicio de OCSP.

Actualmente 30 Entidades de la Administración Pública Federal tienen formalizado Convenio de Colaboración para uso del servicio de OCSP, donde 24 entidades y dependencias de la APF están gestionando este Convenio.

Para 2016 se prevé que la mayoría de las poco más de 200 Dependencias de la APF estén formalizando el Convenio de Colaboración.

4.9.2. Excepción en materia Aduanera

El sistema de facturación electrónica del SAT se extiende a la materia aduanal, con la finalidad de que entre ellos exista un mecanismo de articulación directo entre los contribuyentes naturales y jurídicos.

Los artículos 6, 9 A y 160, fracción VII, de la Ley Aduanera establecen:

> ***Artículo 6.-*** *Cuando las disposiciones de esta Ley obliguen a transmitir o presentar información ante la autoridad aduanera, ésta deberá transmitirse a través del sistema electrónico aduanero mediante documento electrónico o digital, según se exija, empleando la firma electrónica avanzada o el sello digital, en los términos y condiciones que establezca el Servicio de Administración Tributaria mediante reglas. Recibido el documento electrónico o digital, el citado sistema generará el acuse respectivo. El Servicio de Administración Tributaria podrá determinar los casos en los que la información deba presentarse a través de medios distintos al electrónico o digital. (…)*
> ***Artículo 9 A.-*** *(…)*
> *La notificación deberá contener la firma electrónica avanzada del funcionario competente, la cual producirá los mismos efectos que la firma autógrafa, de conformidad con el artículo 17-D del Código Fiscal de la Federación.*

Artículo 160.- *El agente aduanal deberá cubrir los siguientes requisitos para operar: (…)*
VI. Realizar los actos que le correspondan conforme a esta Ley en el despacho de las mercancías, empleando el sistema electrónico y la firma electrónica avanzada que le asigne el Servicio de Administración Tributaria.

Breves disposiciones que en resumen señalan que la FIEL será el medio reconocido para realizar trámites aduanales.

4.9.3. Excepción en materia Financiera

El que la LFEA exceptúe de su aplicación la materia financiera, obliga a realizar una delimitación de las normas que integran el derecho financiero, las materias el legislador juzgó no conveniente la aplicación de la FEA son:

a) Derecho Bancario
b) Derecho Bursátil
c) Derecho de Seguros
d) Derecho de Seguros y Derecho de Financiero.

La clasificación anterior permite a su vez determinar las legislaciones especializadas que integran cada materia del derecho:

- Ley de Instituciones de Crédito.
- Ley del Mercado de Valores.
- Ley del Banco de México.
- Ley de Fondos de Inversión (antes Ley de Sociedades de Inversión)
- Ley General de Organizaciones y Actividades Auxiliares del Crédito.
- Ley para Regular las Agrupaciones Financieras (antes Ley General de Instituciones y Sociedades Mutualistas de Seguros y la Ley Federal de Instituciones de Fianzas.

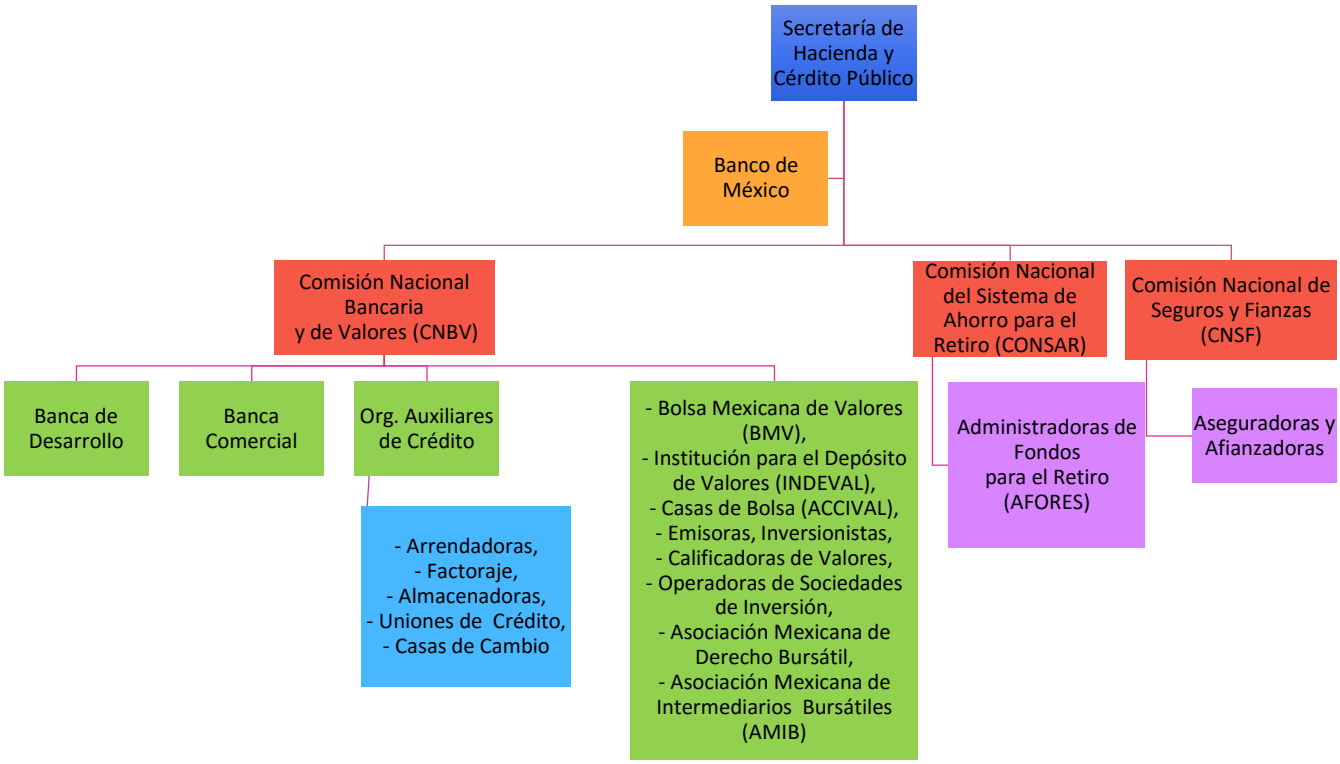
)

Sin duda, el derecho y sistema financiero mexicano, supone una serie de elementos, legislación y políticas a emplear un tanto complejas, ya que la materia de estudio es de carácter bursátil, bancario, económico y financiero en sí mismo. En este sentido, Jesús de la Fuente Rodríguez, en el Derecho Financiero se encarga de evaluar los:

(…) aspectos jurídicos de las instituciones de crédito y casa de bolsa. En un sentido amplio, se define como el conjunto de las legislaciones de instituciones de crédito y bursátiles que regulan la creación, organización, funcionamiento y operaciones de las entidades bancarias y de valores, así como los términos en que intervienen las autoridades financieras y la protección de los intereses del público. También incluye las legislaciones de seguros, fianzas, organizaciones y actividades auxiliares del crédito, de ahorro y crédito popular y Ley para Regular las Agrupaciones Financieras que forman parte del Derecho Financiero. [382]

[382] Citado en Gamboa Montejano, Claudia. Derecho Financiero Mexicano: Estudio teórico conceptual, antecedentes, derecho comparado y opiniones especializadas (1ª parte), 2009, México, Centro de Documentación, Información y Análisis de la Cámara de Diputados, LXI Legislatura, p. 4.

A continuación se esquematiza la conformación del sistema financiero mexicano.[383]



Dado que la Ley de Instituciones de Crédito no se pronuncia respecto a la FEA y que las instituciones de crédito no son reguladas por la LFEA, las *Disposiciones de carácter general aplicables a las instituciones de crédito (*conocida como *Circular Única de Bancos)*, publicada en el DOF el 02 de diciembre de 2005, define a la Firma Electrónica Avanzada o Fiable en su artículo 1º, numeral LXXI, como *la firma electrónica avanzada o fiable a que se refiere el Código de Comercio*, el cual se relaciona con el artículo 307 de la Circular:

> ***Artículo 307.-*** *Las Instituciones, para la contratación de los servicios de Banca Electrónica con sus clientes, adicionalmente a lo previsto en el Artículo 306 anterior, se sujetarán a lo siguiente:*
> *I. Deberán obtener el consentimiento expreso mediante firma autógrafa de sus clientes, previa identificación de estos o bien, mediante* ***firma electrónica avanzada o fiable*** *de sus clientes, siempre y cuando estas se sujeten a lo establecido en el Código de Comercio para estos efectos. En todo caso, podría utilizarse alguna otra forma de contratación, tratándose de los servicios siguientes:*
> *a) Pago móvil.*
> *b) Aquellos ofrecidos a través de Cajeros Automáticos y Terminales Punto de Venta, cuando estos se refieran exclusivamente a la operación de Cuentas Bancarias de los Niveles 1 a 3.*
> *c) Los previstos en la fracción V de este artículo.*
> *d) Banca Móvil, Banca por Internet, Banca Telefónica Audio Respuesta y Banca Telefónica Voz a Voz, cuando estén asociados a Cuentas Bancarias de Niveles 1 a 3, según corresponda, y sean para realizar operaciones diferentes a las previstas en el Artículo 313 de las presentes disposiciones.*
> *e) Los contratados a través de Cajeros Automáticos y Terminales Punto de Venta, siempre y cuando*

[383] Suárez Dávila, Francisco y Díaz, Juan Luis. Reestructuración del sistema financiero, 1988, 1a ed., México, FCE-Secretaria de Hacienda y Crédito Publico, p. 50-88.

estos servicios sean utilizados para realizar operaciones monetarias de Mediana Cuantía. Para dicha contratación, las Instituciones deberán solicitar a los Usuarios un segundo Factor de Autenticación de las Categorías 3 o 4 a que se refiere el Artículo 310 de estas disposiciones. Asimismo, las Instituciones deberán prever que las propias Instituciones asumirán los riesgos y por lo tanto los costos de las operaciones realizadas a través de los servicios antes mencionados que no sean reconocidas por los Usuarios. Las reclamaciones derivadas de estas operaciones deberán ser abonadas a los Usuarios a más tardar cuarenta y ocho horas posteriores a la reclamación.
II. (...)

(Énfasis añadido)

Por otro lado, la Ley del Mercado de Valores, abrogada en el DOF el 30 de diciembre de 2005, establecía en la segunda parte de la fracción II del artículo 91:

***Artículo 91**.- Como consecuencia del contrato de intermediación bursátil:*
(…)
II.- A menos que en el contrato se pacte el manejo discrecional de la cuenta, las instrucciones del cliente para la ejecución de operaciones concretas o movimientos en la cuenta del mismo, podrán hacerse de manera escrita, verbal o telefónica, debiéndose precisar en todo caso el tipo de operación o movimiento, así como el género, especie, clase, emisor, cantidad, precio y cualquiera otra característica necesaria para identificar los valores materia de cada operación o movimiento en la cuenta.
*Las partes podrán convenir libremente el uso de carta, telégrafo, télex, telefax o cualquier **otro medio electrónico**, de cómputo o de telecomunicaciones para el envío, intercambio o en su caso confirmación de las órdenes de la clientela inversionista y demás avisos que deban darse conforme a lo estipulado en el contrato, así como los casos en que cualquiera de ellas requiera cualquiera otra confirmación por esas vías.*

(Énfasis añadido)

La vigente Ley de Mercado de Valores secunda dicha conveniencia pero en la fracción II del artículo 200:

***Artículo 200.-** Como consecuencia del contrato de intermediación bursátil:*
(…)
II. A menos que en el contrato se pacte el manejo discrecional de la cuenta, las instrucciones del cliente para la ejecución de operaciones específicas o movimientos en la cuenta del mismo, podrán hacerse de manera escrita, verbal, electrónica o telefónica, debiéndose precisar en todo caso el tipo de operación o movimiento, así como el género, especie, clase, emisor, cantidad, precio y cualquiera otra característica necesaria para identificar los valores materia de cada operación o movimiento en la cuenta.
*Las partes podrán convenir libremente el uso de **cualquier medio de comunicación, para el envío, intercambio o, en su caso, confirmación de las órdenes de la clientela inversionista** y demás avisos que deban darse conforme a lo estipulado en el contrato, así como los casos en que cualquiera de ellas requiera otra confirmación por esas vías.*

(Énfasis añadido)

Ambas legislaciones, la bancaria y la de valores, exhiben que los contratos por medios electrónicos no podían ser solo peculiares del CCo.

Por otra parte, en materia de Instituciones de Fianzas, a través del *Decreto por el que se reforman, adicionan y derogan diversas disposiciones en materia financiera y se expide la Ley para Regular las Agrupaciones Financieras*, publicado en el DOF el 10 de enero de 2014, Ley que suple a dos legislaciones, la Ley Federal de Instituciones de Fianzas y la Ley General de Instituciones y Sociedades Mutualistas de Seguros.

Al respecto la ley de referencia considera en un solo artículo la FEA:

> ***Artículo 282.-****Los valores objeto de depósito en instituciones para el depósito de valores, podrán ser representados en títulos múltiples o en un solo título que ampare parte o la totalidad de los valores materia de la emisión y del depósito.* ***Tales títulos podrán emitirse de manera electrónica en forma de mensaje de datos con firma electrónica avanzada de acuerdo con lo establecido en el Código de Comercio y de conformidad con las disposiciones de carácter general que emita el Banco de México,*** *que comprendan, entre otros aspectos, los títulos que podrán emitirse utilizando medios electrónicos, así como las características específicas y de seguridad que deberán reunir para tales efectos. Los títulos que se encuentren emitidos en medios impresos, podrán sustituirse de manera electrónica en los términos del presente párrafo de conformidad con las disposiciones de carácter general que emita el Banco de México.*
>
> ***(Énfasis añadido)***

En cuanto hace a la Ley de Fondos de Inversión y la Ley General de Organizaciones y Actividades Auxiliares del Crédito tampoco existe un pronunciamiento en relación con la FEA.

Figura: Infraestructura Extendida de Seguridad (aplicable a las Instituciones de Crédito)

4.10. FIEL en el actual Gobierno Federal y FEA en Organismos y Órganos Constitucionales Autónomos.

Actualmente, las dependencias y entidades del Gobierno Federal, de conformidad con el Plan Nacional de Desarrollo 2013-2018 (PND: 2013-2018), se encuentran incorporando paulatinamente en sus plataformas la FIEL, no la FEA, para la realización de trámites digitales gubernamentales.

Antes de adentrarnos en el tema a que de la FIEL en el actual gobierno federal y los Organismos Constitucionales Autónomos (OCA), resulta necesario enunciar estos últimos. Los primeros OCA que se precisaron en la CPEUM son:

1) Banco Central o Banco de México (artículo 28 párrafo sexto);
2) Instituto Federal Electoral (artículo 41, fracción III), hoy Instituto Nacional Electoral (INE);
3) Comisión Nacional de los Derechos Humanos (artículo 102, apartado B, del primer al cuarto párrafo);
4) Universidad Nacional Autónoma de México (artículo 3º, fracción VII) [384].

Cronológicamente, después la Constitución integró ocho Órganos Constitucionales Autónomos (OgCA) pero que no son Federales y, por ende, no se denominaron OCA, ello en razón de que la CPEUM marcó una diferencia entre organismos y órganos:

I. Las organizaciones de los pueblos y comunidades indígenas (artículo 2).
II. Universidades e instituciones de educación superior, de acuerdo con las leyes respectivas (artículo 3, fracción VII).
III. Tribunales agrarios (artículo 27, fracción XIX).
IV. Tribunales de lo contencioso-administrativo, que en la ley respectiva es denominado Tribunal Federal de Justicia Fiscal y Administrativa (artículo 73, fracción XXIX-H).
V. Entidad de fiscalización superior de la Federación o Auditoría Superior de la Federación como la ley respectiva la denomina (artículo 74, fracción II).
VI. Autoridades estatales encargadas de organizar y de resolver las controversias en las elecciones, en las entidades federativas, que en forma genérica son conocidas como Institutos y Tribunales Electorales (artículos 116, fracción IV, inciso c) y 122, apartado C, base primera, fracción V, inciso f).
VII. Tribunales locales de lo contencioso administrativo (artículo 116, frac. V).
VIII. El Estatuto de Gobierno del Distrito Federal, expedido por el Congreso de la Unión, reconoce autonomía a entidades como el Tribunal de lo Contencioso Administrativo, los órganos político-administrativos conocidos como delegaciones políticas, el Instituto y el Tribunal Electorales.

Luego, más recientemente se incluyeron en la CPEUM los OCA's enlistados a continuación:

5) Instituto Nacional de Estadística, Geografía e Información (INEGI),
6) Comisión Federal de Competencia Económica (CFCE),

[384] El lector advertirá que la numeración termina aquí con el número "4)" y a partir del párrafo posterior al subsecuente, continua con el "5)", pues los organismos

7) Instituto Federal de Telecomunicaciones (IFT),
8) Instituto Nacional de Evaluación Educativa (INEE),
9) Instituto Nacional de Acceso a la Información y Protección de Datos (INAI),
10) Consejo Nacional de Evaluación de la Política de Desarrollo Social (CONEVAL)
11) Fiscalía General de la República (FGR).

Por lo que actualmente existen once OCA's y ocho OgCA's.

Órganos Constitucionales Autónomos:
Específicamente, en relación con la FEA, los Organismos Constitucionales Autónomos acuden a la generación de los datos de activación de la clave de su ACR, que es una combinación de cierto número de tarjetas inteligentes, las cuales operan bajo el esquema de compartir el secreto. A detalle el uso de la FEA en sus trámites cotidianos son:

Banco de México y la Firma Electrónica Avanzada.

Banco de México ha aprovechado la infraestructura conjunta de emisión y consulta de certificados digitales para desarrollar productos y servicios que tengan seguridad basada en la firma electrónica.

El Comprobante Electrónico de Pago (CEP) es un documento electrónico que permite verificar que un pago del SPEI se haya abonado en la cuenta beneficiaria. Esta información está firmada electrónicamente por el banco que recibe el pago.

Un software de la FIEL expedido por Banco de México es el *WebSec®,* que es una aplicación desarrollada por el propio y dota de seguridad a documentos electrónicos mediante el uso claves privadas y certificados de FIEL; sus funcionalidades son:

a) Firmado y verificación de documentos electrónicos: Se firman y verifican no solo los elementos criptográficos involucrados, sino que también se valida la autenticidad y vigencia del certificado involucrado en la firma electrónica del documento en cuestión.
b) Cifrado y descifrado: La información que se considere confidencial puede cifrarse auxiliándose de la clave privada y el certificado de FIEL.
c) Creación y apertura de sobres: Un sobre en el WebSec es un documento electrónico que tiene un signatario (lo que permite corroborar la autenticidad, integridad y no repudio de la información) y uno o varios destinatarios. La información contenida en el sobre está cifrada para cada uno de los destinatarios (lo que provee de confidencialidad a la información ahí contenida).

Utiliza la FEA a través de los siguientes trámites:

a) La infraestructura de clave pública del Sistema de Pagos mexicano es denominada

Infraestructura Extendida de Seguridad (IES)[385]*,* es un sistema diseñado y administrado por Banco de México quien cuenta con una tabla de certificados de la IES que muestra aquellos que pertenecen a la Agencia Raíz, a las Agencias Certificadoras y Registradoras, así como los de las Autoridades Registradoras Autorizadas (ARA's), con el detalle de su número de serie e institución a la que pertenece.

b) El Banco de México diseñó y desarrolló un sistema de cómputo denominado WebSec con el propósito de proveer las siguientes operaciones sobre documentos electrónicos:
   I. Creación y verificación de firmas electrónicas.
   II. Creación de ensobretados[386] y apertura de los mismos.
   III. Cifrado y descifrado de información.
   IV. Descarga de software versión 2.2.0
   V. Huella digital SHA1: a1:62:a4:c8:cb:51:ca:3b:97:fe:1f:be:ca:7d:d4:f3:1e:2f:f6:c7
   VI. Huella digital SHA256: 0d:9d:68:66:18:2e:62:25:6c:21:ae:4e:25:45:21:76:61:9a:98:13:26:c7:84:3a:93:9c:44:06:d7:f6:70:22

Instituto Nacional Electoral (INE)

Utiliza la FEA para los trámites que especifíca el Acuerdo del Consejo General del Instituto Federal Electoral por el que se aprueba el Reglamento para el uso y operación de la Firma Electrónica Avanzada en el Instituto Federal Electoral, publicado en el DOF el 14 de noviembre de 2013 así como el Acuerdo de la Junta General Ejecutiva del Instituto Federal Electoral, por el que se aprueban los Lineamientos para la Implementación de la Firma Electrónica Avanzada en el Instituto Federal Electoral, publicado en el DOF el 7 de mayo de 2014 (Ver los Lineamientos en el Apéndice VI).

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

Utiliza la FEA a través de los siguientes trámites:

- El sistema electrónico para la recepción y envío de respuesta por parte de los funcionarios de entidades y dependencias encargados de las Unidades de Enlace emplea la FIEL de los funcionarios.
- El artículo 89, fracción I, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP)[387] permite que se reconozca la identidad del titular

[385] El sistema de IES se complementa en la regulación contenida en el Reglamento Interior del Banco de México, también se regula a través de la Disposiciones de carácter general aplicables a las instituciones de crédito (Circular Única de Bancos), Publicada en el DOF el 02 de diciembre de 2005, accesible en: http://www.cnbv.gob.mx/Paginas/NORMATIVIDAD.aspx, consultado el 2 de marzo de 2015 y las Circulares: Telefax 6/2005, Telefax 6/2005 B y 23/2010 "Reglas para operar como Agencia Registradora y/o Agencia Certificadora en la Infraestructura Extendida de Seguridad".

[386] "Ensobretar" es envolver electrónicamente el requerimiento (.req) utilizando la FIEL para crear un archivo denominado así: ensobretado (.sdg).

[387] **Artículo 89.** Los derechos ARCO se ejercerán:

de los derechos de Acceso, Rectificación, Corrección y Oposición (ARCO) a través de la Firma Electrónica Avanzada.
- Actualmente se encuentran en aprobación los Lineamientos para el uso y operación de la Firma Electrónica Avanzada en el sistema electrónico de INAI PRODATOS, accesible en https://www.datospersonales.org.mx/ para presentación de solicitudes de protección de derechos ARCO y de denuncias.

Finalmente, los siguientes organismos no cuentan con regulación sobre Firma Electrónica Avanzada:

- Comisión Nacional de los Derechos Humanos (CNDH):
- Comisión Federal de Competencia Económica (COFECE):
- Instituto Federal de Telecomunicaciones (IFT)

Ahora bien, las entidades y dependencias de la APF y los OCA´s que van avantes en el tema de uso y operación con la FEA se encuentran:

Archivo General de la Nación (AGN) de la Secretaría de Gobernación.

- En coordinación con Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), la SFP emitió y publicó en el DOF el 3 de julio de 2015 los *Lineamientos para la creación y uso de sistemas automatizados de gestión y control de documentos* a fin de establecer las bases para la creación y uso de sistemas automatizados de gestión y control de documentos. De esta forma obliga a las entidades y dependencias a que toda Unidad de TIC´s cuente con un sistema automatizado que permita el firmado electrónico e incorporación de la FEA de documentos conforme a lo establecido en la Ley de Firma Electrónica Avanzada.
- Actualmente se encuentra en liberación el Sistema de Administración de Archivos (SAA) con la FEA, que es un sistema electrónico de gestión de archivos que incorpora la Firma Electrónica Avanzada a fin de que los servidores públicos firmen los documentos institucionales que tramitan. Dicho sistema adopta a cabalidad los Lineamientos citados.

Secretaría de Economía.

Utiliza la FEA a través de los siguientes trámites:

a) Programa tu empresa: www.tuempresa.gob.mx

I. Por el titular, previa acreditación de su identidad, a través de la presentación de copia de su documento de identificación y habiendo exhibido el original para su cotejo. También podrán ser admisibles los instrumentos electrónicos por medio de los cuales sea posible identificar fehacientemente al titular, u otros mecanismos de autenticación permitidos por otras disposiciones legales o reglamentarias, o aquéllos previamente establecidos por el responsable. La utilización de firma electrónica avanzada o del instrumento electrónico que lo sustituya eximirá de la presentación de la copia del documento de identificación, y

b) Sistema Integral de Gestión Registral (SIGER) para la inscripción de actos mercantiles en el Registro Público de Comercio y en el Registro Único de Garantías Mobiliarias.
c) Sellos digitales de tiempo conforme a NOM-151-SCFI-2002.
d) Constancias de conservación conforme a NOM-151-SCFI-2002.
e) Autorización de uso de denominaciones o razones sociales tanto para la creación de sociedades de naturaleza mercantil y sociedades y/o asociaciones de naturaleza civil.
f) Solicitudes de autorización de uso o modificación de denominaciones o razones sociales.
g) Presentación del *Aviso de Liberación de Denominaciones o Razones*.
h) Obtención y descarga de los documentos que contienen las autorizaciones de uso de denominaciones o razones sociales autorizadas.
i) Modificación del régimen jurídico, o en su caso del fedatario público o servidor público que fueron elegidos para formalizar la creación o modificación de la Sociedad o Asociación correspondiente.

Instituto Mexicano de la Propiedad Intelectual (IMPI).
Utiliza la FEA a través del *Portal de Pagos y Servicios Electrónicos* del IMPI (PASE) y emplea la FIEL al realizar el llenado, pago, firma y envío de la solicitud de Registro de figuras de propiedad intelectual.

Secretaría de la Función Pública.

Utiliza la FEA a través de los siguientes trámites:

a) Portal único de trámites, información y participación ciudadana: www.gob.mx
b) CompraNET: www.compranet.funcionpublica.gob.mx
c) DeclaraNET: www.declaranet.gob.mx
d) Registro Único de Personas Acreditadas: www.rupa.gob.mx
e) Proyecto coordinado por el SAT y SFP, cuyo objetivo es facilitar el Pago de Derechos, Productos y Aprovechamientos (DPAs) de todas las entidades y dependencias de la APF, mejor conocido como e-5CINCO: www.e5cinco.segob.gob.mx
f) Autenticación de certificados digitales y de mensajes y validación de documentos con FIEL en el portal de la función publica
g) Instituto de Administración y Avalúos de Bienes Nacionales (INDAABIN), órgano desconcentrado de la Secretaría de la Función Pública, lanzó el Sistema Automatizado de Avalúos Electrónicos con el uso de la FIEL:
http://www.indaabin.gob.mx/Paginas/default.aspx

Secretaría de Salud

Utiliza la FEA a través del Expediente Electrónico Clínico de conformidad con la NOM-004-SSA3-2012 Norma Oficial Mexicana del Expediente Clínico posibilitan el uso de la plataforma del Sistema de Información de Registro Electrónico para la Salud (SIRES) para permitir la FIEL del profesional de la salud para que pueda ingresar toda aquella información que determine el Prestador de Servicios de Salud.

Instituto Mexicano del Seguro Social:

Utiliza la FEA a través de los siguientes trámites:

a) Para altas de trabajadores y trámites de los patrones: www.imss.gob.mx/servicios/linea/Pages/default.aspx
b) Para el Acceso al Sistema Único de Dictamen a través de Internet (SUDINET) para contador público autorizado para los siguientes trámites para: 1. Registro del Contador Público Autorizado (CPA); 2. Dictamen; 3. Consulta de Dictamen; y 4. Importar Avisos presentados por escrito.
c) Para el Sistema IMSS desde su Empresa (IDSE) hace posible el empleo de la FIEL para realizar trámites y actuaciones electrónicas por Internet a través de un Certificado Digital, Número Patronal de Identificación Electrónica (NPIE), usuario y contraseña, mismos que se obtienen al realizar la Solicitud de Certificado Digital.

Sociedad Hipotecaria Federal, S.N.C., (SHF):
Utiliza la FEA para el proceso de validación y registro de avalúos electrónicos: www.shf.gob.mx, por conducto de la Institución financiera perteneciente a la Banca de Desarrollo.

Instituto Nacional de Desarrollo Social (INDESOL):
Utiliza la FEA a través del Programa de Coinversión Social se otorgar apoyos a proyectos sociales, específicamente la FIEL permite la captura y envío del proyecto: http://indesol.gob.mx/programas/coinversion-social/

Tribunal Federal de Justicia Fiscal y Administrativa:
Utiliza la FEA para el trámite del Juicio en Línea del Tribunal Federal de Justicia Fiscal y Administrativa admite certificados de la FIEL expedidos por el SAT. Esta plataforma permite la consulta remota de expedientes, con una clave de acceso y una contraseña, y que las partes interesadas pueden conocer el estado procesal del juicio las 24 horas del día, los 365 días del año, con la seguridad que entraña el uso de la FIEL para validar las promociones de las partes y actuaciones de los funcionarios jurisdiccionales: www.tff.gob.mx/index.php/juicio-en-linea-video-0

4.11. Firma Electrónica Certificada en el Poder Judicial Federal.

4.11.1. El Consejo de la Judicatura Federal: La FESE (2007)

El Pleno del Consejo de la Judicatura Federal (CJF) como órgano encargado de la administración, vigilancia, disciplina y de la carrera judicial del Poder Judicial de la Federación (PJF), con excepción de la Suprema Corte de Justicia de la Nación (SCJN) y el Tribunal Electoral del Poder Judicial de la Federación (TE), en sesión plenaria del 3 de julio de 2007 expidió el Acuerdo General 21/2007 para la asignación, certificación y uso de la Firma Electrónica para el Seguimiento de Expedientes (FESE). El acuerdo determinó los mecanismos de aplicación

informática necesarios para controlar el flujo de información, creó una instancia denominada Unidad para el Control de Certificación de Firmas a fin de determinar la clave personal de la FESE y establecer las modalidades de la información remitida y consultada con esas claves.

En términos generales, fue un acuerdo de observancia obligatoria para las partes, los terceros interesados, los auxiliares de la administración de justicia o personas autorizadas por los órganos jurisdiccionales que tuvieran acceso al expediente electrónico de su interés contenido en el sistema, para la recepción de promociones que formularan en los procedimientos jurisdiccionales a través del sistema electrónico, así como para las notificaciones, citatorios, emplazamientos, requerimientos, solicitudes de informes o documentos y las resoluciones definitivas que se emitan por esa misma vía.

Para certificar documentos de acreditación, registro y entrega de firma electrónica se creó la figura de un autorizado con los atributos de certificación, que podía ser el secretario del órgano jurisdiccional designado por el Presidente del Tribunal Colegiado de Circuito, titular del Tribunal Unitario de Circuito o del Juzgado de Distrito, pues dichos secretarios cuentan con la calidad de certificadores de la documentación que acreditan a un solicitante además contaban con la facultad de registrar y entregar la firma electrónica a las personas autorizadas al acceso a los expedientes en los que fueran partes, terceros interesados, auxiliares de la administración de justicia o personas que por razones legales o laborales debieran intervenir en ellos.

Asimismo, la citada *Unidad para el Control de Certificación de Firmas* (que posteriormente se convirtió en la actual *Unidad del PJF para el Control de Certificación de Firmas*), elaboró manuales e iniciativas para la aplicación generalizada de las actuaciones jurisdiccionales y administrativas. Dicha Unidad estaba integrada con los secretarios autorizados para certificar firmas de los órganos jurisdiccionales, y como su coordinador fungió el Secretario Técnico de Desarrollo y el Titular de la Dirección General de Estadística y Planeación Judicial.

La FESE contaba con una clave que identificaba a la persona que enviaba o recibía cualquier comunicado a través de los medios electrónicos como el Sistema de Información Electrónica (SIE) del CJF. Al ser una firma que se utilizaría, el SIE creaba las propias claves de manera automática y confidencial, previa solicitud de formato por las partes que aparecía en el portal del CJF a la cual le seguía una consulta a fin de revisar si era parte autorizada en el asunto en que se actuaba.

El procedimiento para la obtención de la FESE, era el siguiente:

a) El particular solicitaba por escrito ante el órgano jurisdiccional donde esté radicado su asunto, la generación de su FESE.
b) El órgano jurisdiccional y, excepcionalmente, la Unidad para el Control para Certificación de Firmas emitía respuesta a la solicitud, una vez que el interesado cumplía con los requisitos establecidos en el Acuerdo, se emitía y el interesado, previa identificación, la recibirá en el órgano jurisdiccional correspondiente.
c) La FESE era única e intransferible.

d) Antes de generar la clave electrónica a las instituciones públicas o a los particulares, el órgano jurisdiccional o la *Unidad para el Control de Certificación de Firmas*, debía cerciorarse de la identidad y personalidad de los mismos, utilizando cualquier medio admitido en derecho.

e) Una vez obtenida la clave electrónica, las personas debían incorporar su FESE, en sustitución de la autógrafa, en las promociones y solicitudes de trámites electrónicos que así lo requieran.

f) Para renovarla se seguía el procedimiento inicial. Y, cuando era el caso, el interesado informaba vía electrónica cuando había revocado o limitado las facultades a su representante legal.

La constancia de certificación de la fecha, hora e identidad del remitente por el secretario del órgano jurisdiccional autorizado, debía realizarse en términos del artículo 210-A del Código Federal de Procedimientos Civiles[388], bajo la responsabilidad del órgano jurisdiccional. El tablero electrónico de cada órgano jurisdiccional estaba disponible para consulta en la dirección del sitio web: www.dgepj.cjf.gob.mx[389].

Cada órgano jurisdiccional era responsable, previo envío-recepción de cualquier documento o trámite electrónico realizado por una persona física o moral en el sistema electrónico correspondiente, de desplegar una declaración o carta de aceptación en la que se manifestara su consentimiento para la recepción de actuaciones electrónicas a fin de dar cumplimiento a lo dispuesto por los artículos 319 y los 320[1] del CFPC

Las promociones o solicitudes enviadas en horas y días hábiles para el órgano jurisdiccional y viceversa de los órganos jurisdiccionales para con los autorizados para consulta del sistema de información electrónica a través del FESE se tenían por recibidas o surtían sus efectos el mismo día y hora.

Finalmente, se aprobó un formato de solicitud de FESE que consiste en escrito de solicitud, aceptación y consecuencias de uso en el Sistema de Información Electrónica (ver Apéndice VII. Formato de solicitud de la FESE).

4.11.2. El Poder Judicial Federal y la nueva Ley del Amparo: FIREL (2013)

Con motivo de la heterogeneidad en tres tipos de firmas electrónicas distintas en el PJF (CJF, TE y SCJN), con motivo de la expedición del *Decreto de la Ley de Amparo, reglamentaria de los*

[388] **Artículo 210-A.-** Se reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología. Para valorar la fuerza probatoria de la información a que se refiere el párrafo anterior, se estimará primordialmente la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas obligadas el contenido de la información relativa y ser accesible para su ulterior consulta. Cuando la ley requiera que un documento sea conservado y presentado en su forma original, ese requisito quedará satisfecho si se acredita que la información generada, comunicada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología, se ha mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y ésta pueda ser accesible para su ulterior consulta. (Artículo adicionado DOF 29-05-2000).

[389] Dirección General de Estadística Judicial es un órgano jurídico administrativo del Consejo de la Judicatura Federal.

artículos 103 y 107 de la CPEUM publicada el 2 de abril de 2013, los tres órganos expidieron el Acuerdo General conjunto número 1/2013, en el que se establece una Firma Electrónica Certificada del Poder Judicial de la Federación (FIREL) y el 4 de julio de 2014 se concierta el *Acuerdo General 34/2014 del Pleno del CJF para regular los expedientes electrónicos a través de las bases de la firma y del expediente electrónicos a disposición de los justiciables por el PJF,* el cual es el instrumento vigente a través del cual se ingresa al Sistema Electrónico para presentar medios de impugnación (demandas), se envían promociones y/o documentos, reciben comunicaciones, notificaciones y/o documentos oficiales, así como se consultan acuerdos, resoluciones y sentencias relacionadas con los asuntos competencia de la SCJN, el Tribunal Electoral, de los Tribunales de Circuito y de los Juzgados, y produce los mismos efectos que la firma autógrafa, tomando en cuenta el multicitado artículo 3º de la Ley de Amparo. Con lo anterior, valga decir que se abrogó el Acuerdo General 21/2007 del Pleno del CJF.

Particularmente, los artículos Tercero[390] y Décimo Primero Transitorios[391] de la nueva Ley de Amparo, obligó a la SCJN, TE, CJF a participar conjuntamente para la integración de un sistema de Firma Electrónica Certificada del Poder Judicial Federal (PJF), a través de sistemas informáticos de emisión de firma electrónica y expediente electrónico que funcionaran en todo el PJF.

Así, con fundamento en el artículo 17, párrafo segundo de la CPEUM, el cual dispone que toda persona tiene derecho a que se le administre justicia por tribunales que estarán expeditos para impartirla en los plazos y términos que fijen las leyes, emitiendo sus resoluciones de manera

---

[390] "**Artículo 3o**. En el juicio de amparo las promociones deberán hacerse por escrito.
Podrán ser orales las que se hagan en las audiencias, notificaciones y comparecencias autorizadas por la ley, dejándose constancia de lo esencial. **Es optativo para el promovente presentar su escrito** en forma impresa o **electrónicamente.**
Las copias certificadas que se expidan para la substanciación del juicio de amparo no causarán contribución alguna.
Los escritos en forma electrónica se presentarán mediante el empleo de las tecnologías de la información, utilizando la Firma Electrónica conforme la regulación que para tal efecto emita el Consejo de la Judicatura Federal.
La Firma Electrónica es el medio de ingreso al sistema electrónico del Poder Judicial de la Federación y producirá los mismos efectos jurídicos que la firma autógrafa, como opción para enviar y recibir promociones, documentos, comunicaciones y notificaciones oficiales, así como consultar acuerdos, resoluciones y sentencias relacionadas con los asuntos competencia de los órganos jurisdiccionales.
En cualquier caso, sea que las partes promuevan en forma impresa o electrónica, los órganos jurisdiccionales están obligados a que el expediente electrónico e impreso coincidan íntegramente para la consulta de las partes.
El Consejo de la Judicatura Federal, mediante reglas y acuerdos generales, determinará la forma en que se deberá integrar, en su caso, el expediente impreso.
Los titulares de los órganos jurisdiccionales serán los responsables de vigilar la digitalización de todas las promociones y documentos que presenten las partes, así como los acuerdos, resoluciones o sentencias y toda información relacionada con los expedientes en el sistema, o en el caso de que éstas se presenten en forma electrónica, se procederá a su impresión para ser incorporada al expediente impreso. Los secretarios de acuerdos de los órganos jurisdiccionales darán fe de que tanto en el expediente electrónico como en el impreso, sea incorporada cada promoción, documento, auto y resolución, a fin de que coincidan en su totalidad. El Consejo de la Judicatura Federal, en ejercicio de las facultades que le confiere la Ley Orgánica del Poder Judicial de la Federación, emitirá los acuerdos generales que considere necesarios a efecto de establecer las bases y el correcto funcionamiento de la Firma Electrónica.
No se requerirá Firma Electrónica cuando el amparo se promueva en los términos del artículo 15 de esta Ley."

[391] **Transitorio Décimo Primero.** El Consejo de la Judicatura Federal expedirá el Reglamento a que hace referencia el artículo 3o del presente ordenamiento para la implementación del Sistema Electrónico y la utilización de la firma electrónica. Asimismo el Consejo de la Judicatura Federal dictará los acuerdos generales a que refieren los artículos 41 Bis y Bis 1 del presente decreto, para la debida integración y funcionamiento de los Plenos de Circuito. Las anteriores disposiciones deberán emitirse en un plazo de noventa días a partir de la entrada en vigor del presente Decreto.

pronta, completa e imparcial, fue posible que cada uno de tres órganos citados emitan las Disposiciones Generales que sienten las bases para el uso más eficaz y eficiente de las tecnologías de la información disponibles; sin menoscabo de generar certeza a las partes dentro de los juicios constitucionales sobre los mecanismos para acceder a un expediente electrónico y los efectos de ello, especialmente en materia de notificaciones, máxime si el legislador amplió el derecho de acceso efectivo a la justicia en la Ley de Amparo, al contemplar el uso de dichas tecnologías en la tramitación del juicio de amparo, específicamente el uso de una firma electrónica y la integración del expediente electrónico.

De conformidad con lo previsto en el artículo 3o. de la Ley de Amparo, la Firma Electrónica que establezca el PJF será el medio de ingreso al sistema electrónico del PJF, como opción para enviar y recibir promociones, documentos, comunicaciones y notificaciones oficiales, así como consultar acuerdos, resoluciones y sentencias relacionadas con los asuntos competencia de los órganos jurisdiccionales, y producirá los mismos efectos que la firma autógrafa, siendo conveniente que la regulación que rija la referida firma sea uniforme en la SCJN y en el CJF, lo que brindará mayor certeza a los justiciables y permitirá un uso más eficiente y eficaz de los recursos públicos asignados a esos órganos constitucionales.

Imagen extraída del sitio web: https://www.uncocefi.cjf.gob.mx/cjfUser/

Dentro de los Conceptos relevantes del Acuerdo General 34/2014 están:

Agente Certificador: El servidor público por conducto del cual actuará la *Unidad para el Control de Certificación Firmas (*UNCOCEFI) para tramitar la emisión, renovación y revocación de Certificados Digitales de la FIREL:

- Áreas administrativas: Las unidades administrativas y los órganos auxiliares del CJF;
- Certificado Digital de la FIREL: El Documento Electrónico emitido por la UNCOCEFI que asocia de manera segura y fiable la identidad del Firmante con una llave pública,

permitiendo con ello identificar quién es el autor o emisor de un Documento Electrónico o MD remitido mediante el uso de la FIREL;

- Certificado Intermedio del Consejo: El certificado digital emitido al Consejo por la Autoridad Certificadora Raíz del PJF, a partir del cual la UNCOCEFI generará los certificados digitales de la FIREL para los usuarios finales;
- Certificado OCSP: El certificado digital emitido por el Consejo para el uso del protocolo de la verificación en línea del estado de los certificados digitales de la FIREL emitidos por el propio Consejo;
- Certificado Raíz del PJF: El certificado digital único emitido por la Unidad del PJF para el Control de Certificación de Firmas, que sirve de base a la infraestructura de firma electrónica de los órganos del PJF y da origen a los certificados intermedios, los que a su vez servirán para generar los certificados digitales de la FIREL que emitan las Unidades de Certificación correspondientes;
- Certificado TSA: El certificado digital emitido por el Consejo para el uso de los sellos de tiempo;
- Clave de Acceso a la Llave Privada del Certificado Digital de la FIREL: La cadena de caracteres alfanuméricos del conocimiento exclusivo del titular de un certificado digital de la FIREL, que le permite utilizar la Llave Privada para firmar un documento electrónico o, en su caso, para acceder a diversos sistemas que establezca el Consejo;
- Llave Privada: Los datos que el Firmante genera de manera secreta y bajo su estricto control Artículo 4.

El Certificado Intermedio del CJF deberá ser emitido por la Autoridad Certificadora Raíz del PJF y quedará resguardado en un módulo criptográfico (HSM) con nivel de seguridad FIPS1402, nivel 3. Con fundamento en este certificado se emitirán los certificados digitales de la FIREL a los usuarios finales.

El certificado digital de la FIREL únicamente podrá ser solicitado y emitido a personas físicas con independencia de que éstas sean representantes de personas morales públicas o privadas, cuya solicitud se realizará exclusivamente por el interesado, sin que dicho trámite pueda efectuarse mediante apoderado o representante legal. Para obtenerlo, el interesado ingresará a la dirección http://www.pjf.gob.mx/firel/, disponible en el sitio web del Consejo y de la Dirección General de Estadística Judicial; accederá al vínculo denominado FIREL y completará el procedimiento establecido en las Políticas para la obtención y uso de la FIREL.

La renovación deberá efectuarse dentro de los 30 días anteriores a la conclusión de su vigencia. Si en ese lapso no se renueva el Certificado Digital de la FIREL correspondiente, éste caducará y el interesado deberá formular una nueva solicitud.

La UNCOCEFI será la responsable de llevar a cabo los procedimientos para la emisión, renovación, revocación y consulta de los certificados digitales de la FIREL, por sí o, en los términos de la normativa aplicable, por conducto de los agentes certificadores que la auxilien. Los certificados digitales emitidos por dicha Unidad deberán cumplir con las especificaciones

referidas en el estándar X.509 definido por la Unión Internacional de Telecomunicaciones de la Organización de Naciones Unidas.

Asimismo, los sistemas informáticos del Consejo reconocerán plenamente los certificados digitales emitidos por la SCJN y el Tribunal Electoral del PJF.

Con independencia de los convenios relativos a la FIREL y al expediente electrónico, el Consejo podrá celebrar convenios de coordinación con los Poderes Ejecutivo y Legislativo Federales; los organismos y órganos constitucionales autónomos; los gobiernos de las entidades federativas, los municipios y los órganos político-administrativos del Distrito Federal; y los Poderes Judicial y Legislativo de los estados y los órganos respectivos del Distrito Federal, a fin de que éstos en sus trámites internos utilicen los certificados digitales de la FIREL emitidos por el Consejo (Ver el Apéndice VIII: Políticas de Operación del Uso de la FEA emitida por el CJF).

4.11.3. Acuerdo General conjunto 1/2015 de la SCJN y del CJF.

El 1º de diciembre de 2015 se publicó en el DOF el Acuerdo General Conjunto 1/2015 de la Suprema Corte de Justicia de la Nación y del Consejo de la Judicatura Federal, que regula los servicios tecnológicos relativos a la tramitación electrónica del juicio de amparo, las comunicaciones oficiales y los proceso de oralidad penal en los Centros de Justicia Penal Federal, a fin de contemplar destacadamente el uso de las TIC que den certeza a las partes dentro de los juicios de amparo y los juicios de oralidad penal sobre los mecanismos para acceder a los expedientes electrónicos así como capetas digitales, los efectos de las notificaciones electrónicas y el uso de firmas electrónicas para ello.

Si bien el *Acuerdo General conjunto número 1/2013 de la Corte, el TE y el CJF* citado en el punto anterior continua vigente, sí se abroga *el Acuerdo General conjunto número 1/2014 de la SCJN y el CJF* por el que se regula la integración de los expedientes impreso y electrónico, y el acceso a éste, así como las notificaciones por vía electrónica, mediante el uso de la FIREL, a través del sistema electrónico del Poder Judicial de la Federación previsto en el artículo 3o. de la Ley de Amparo.

De conformidad con dicho Acuerdo, se conforma el Sistema Electrónico del Poder Judicial de la Federación con los siguientes sistemas:

I. Sistema Electrónico de la SCJN;
II. Portal de Servicios en Línea del Poder Judicial de la Federación;
III. Sistema de recepción, registro, turno y envío de asuntos utilizado por las Oficinas de Correspondencia Común, y
IV. Sistema Integral de Seguimiento de Expedientes.

El primero únicamente tendrá aplicación en la SCJN y los tres últimos en los Juzgados de Distrito y Tribunales de Circuito, así como en los Centros de Justicia Penal Federal y en el CJF.

Los puntos que se abordan en el Acuerdo versan sobre los siguientes puntos:

a) El Sistema Electrónico de la SCJN,
b) La integración del expediente impreso y electrónico en la SCJN,
c) El acceso al expediente electrónico en la SCJN,
d) La notificación por vía electrónica en la SCJN,
e) La manifestación expresa para solicitar la recepción de notificaciones por vía electrónica,
f) Las notificaciones electrónicas,
g) Las bitácoras de notificaciones electrónicas en la SCJN,
h) Las promociones por vía electrónica en la SCJN,
i) La interposición de recursos por vía electrónica en la SCJN,
j) Los servicios electrónicos del CJF,
k) La tramitación electrónica del juicio de amparo en los Juzgados de Distrito y Tribunales de Circuito,
l) El Portal de Servicios en Línea del PJF en el juicio de amparo electrónico,
m) La presentación de demandas de amparo indirecto en términos del artículo 15 de la Ley de Amparo,
n) El Sistema de recepción, registro, turno y envío de asuntos utilizado por las oficinas de correspondencia común en el Juicio de Amparo Electrónico,
o) El *Sistema Integral de Seguimiento de Expedientes en el Juicio de Amparo Electrónico,*
p) Las comunicaciones oficiales electrónicas, y
q) Los Servicios en línea en los Centros de Justicia Penal Federal.

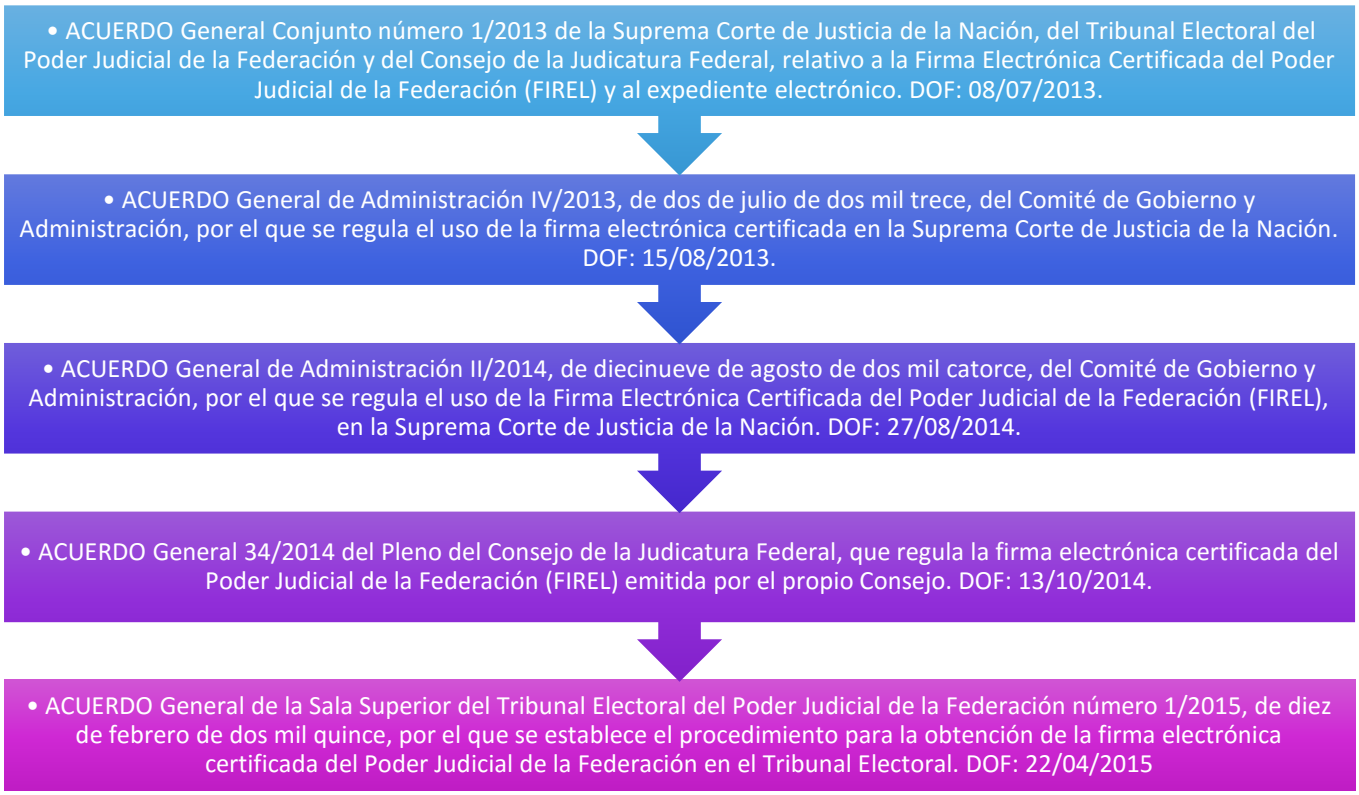
Finalmente, debemos señalar que el Tribunal Superior de Justicia del Distrito Federal usa el servicio de Sistema Integral de Resoluciones (SICOR)[392] que ofrece la oportunidad para los justiciables de:

a) Conocer de manera expedita los acuerdos, a través de dispositivos electrónicos, sin tener que desplazarse a las instalaciones de los Juzgados, con la certeza de que la información de las resoluciones es correcta;
b) Consultar en línea el estado del proceso de los asuntos; y

[392] http://www.poderjudicialdf.gob.mx/es/PJDF/registro_SICOR, consultado el 2 de noviembre de 2015.

c) Ahorrar tiempo en la transcripción de las resoluciones y costos de traslado. No obstante, el SICOR es única y exclusivamente para fines informativos, razón por la que no surte ninguna clase de efectos jurídicos.

Cronología de los Acuerdos Generales conjuntos del PJF



CAPÍTULO V. INCORPORACIÓN DE LA CONTRATACIÓN ELECTRÓNICA SEGURA EN EL DERECHO INTERNACIONAL PRIVADO MEXICANO.

En el ámbito internacional, México y la mayoría de los países, elijen las reglas más apegadas sus intereses cuando se originan controversias en contratos internacionales considerando a las siguientes opciones:

a) Eligen la creación de una normativa específica, se trata de una autorregulación o *Lex Mercatoria*.

b) Eligen las reglas de Derecho Internacional Privado en razón de su capacidad para cumplir adecuadamente la función de solucionar problemas que son regulares. En este contexto, existen dos convenciones de las Naciones Unidas que resultan imprescindibles para las contrataciones internacionales así como cuatro instrumentos de la Cámara de Comercio Internacional (CCI):

b.1) Convención sobre Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales: Armonización legislativa en la Contratación Electrónica
b.2) Convención de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías (Viena, 1980)
b.3) Cláusulas contractuales 2004 de la Cámara de Comercio Internacional (CCI) para el comercio electrónico (e. ICC TERMS 2004)
b.4) Actualización, interpretación y correcta utilización de los Términos Internacionales de Comercio (INCOTERMS)

c) Eligen no pactar ley aplicable e invariablemente se acude a las normas de derecho internacional privado a fin de conocer qué ley regula la contratación así como los criterios a seguir, entre estos se encuentran son tres:

c.1) Rígidos (se enf*oca* en el lugar de ejecución, lugar de celebración);
c.2) Flexibles (se enfoca en el *proper law of the contract*) o,
c.3) Intermedios (se enfoca en que el legislador da pautas para determinar la ley aplicable, como en la Convención de Roma de 1980).

En suma, consideramos que la *Lex Mercatoria* a que se refiere el inciso "a)" es el ideal para abordar la contratación electrónica segura en el Derecho Internacional Privado Mexicano aunando la *Lex Informática,* lo que da como resultado una LEX ELECTRO-MERCATORIA o LEX INFO-MERCATORIA.

5.1. Convención de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías (Viena, 1980).

La Convención de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías (CNUCCIM) fue un proyecto iniciado por la CNUDMI y hace presente la unificación a escala internacional de una parte extensa del derecho mercantil y con ello atraer una mayor participación en un régimen uniforme de compraventa internacional.

Lo anterior, aun cuando la Convención no regula todas las cuestiones legales que pueden originarse en relación con la compra-venta internacional, pues han surgido otras convenciones que norman distintos elementos de la compraventa.

La CNUCCIM comprende 101 artículos e inició su vigencia en México siete años después, cuando la Cámara de Senadores la aprobó, sin reservas, publicándose en el DOF el 12 de noviembre de 1987; y, de acuerdo con el artículo 99-2 de la Convención, inició su vigencia el 1º de enero de 1989.

El objeto de la CNUCCIM es disminuir impedimentos en relación a la elección del derecho aplicable al comercio internacional, a través de la creación de normas sustantivas modernas e

imparciales que rigen los derechos y obligaciones de las partes en contratos de compraventa internacionales.

Se trata de 84[393] Estados parte de la Convención, que hacen presente más de dos terceras partes del comercio internacional de mercaderías.

La Convención regula los contratos de compraventa internacional si:

a) Ambas partes tienen sus establecimientos en Estados contratantes, o
b) El derecho internacional privado prevé la aplicación de la ley de un Estado contratante —a menos que el Estado contratante al ratificarla la Convención haya declarado que no se sujetará a ello.

La autonomía de las partes establecida en la CNUCCIM permite que las partes pacten excepciones a cualquier norma de la Convención, o excluir por completo su aplicación en favor de otro ordenamiento.

Por otro lado, la Convención no regula los aspectos relativos a la validez del contrato o los efectos del contrato sobre la propiedad de las mercaderías vendidas, que serán normadas por el derecho internacional privado (artículo 4). Asimismo, los sectores que no estén contempladas por la CNUCCIM, se resolverán de acuerdo a sus propios principios generales o bien por los proporcionados por la ley aplicable en razón del derecho internacional privado.

Harry M. Flechtner, hace un excelente análisis de los temas más relevantes que asienta la CNUCCIM[394]:

a) Interpretación de los acuerdos entre las partes;
b) Función de las prácticas establecidas entre las partes y de los usos internacionales;
c) Características, duración y revocabilidad de las ofertas;
d) Modalidades, plazos y eficacia de la aceptación de las ofertas;
e) Efectos de las tentativas de añadir o modificar los términos de una aceptación;
f) Modificaciones de los contratos de compraventa internacional;
g) Obligaciones del vendedor respecto de la calidad de las mercaderías y del momento y el lugar de entrega;
h) Lugar y fecha de pago;
i) Obligaciones del comprador de recibir las mercaderías entregadas, examinarlas y notificar cualquier incumplimiento que se alegue;
j) Acciones del comprador en caso de incumplimiento del contrato por el vendedor, incluidos los derechos a exigir la entrega, reclamar la reparación o la sustitución de las mercaderías si éstas

[393] Véase Situación actual de la Convención de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías (Viena, 1980), accesible en : http://www.uncitral.org/uncitral/es/uncitral_texts/sale_goods/1980CISG_status.html, fecha de consulta 31 de diciembre de 2015.
[394] Flechtner, Harry M., Convención de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías, 2010, United Nations Audiovisual Library of International Law, pp. 1-4, accesible en: www.un.org/law/avl, consultada el 14 de diciembre de 2014.

no fueran conformes al contrato, declarar resuelto el contrato, ser indemnizado por los daños y perjuicios y rebajar el precio si las mercaderías no fueran conformes al contrato;

k) *Acciones del vendedor en caso de incumplimiento del contrato por el comprador, incluidos los derechos a exigir al comprador que reciba las mercaderías o pague el precio, declarar resuelto el contrato y ser indemnizado por los daños y perjuicios;*
l) *Transmisión del riesgo sobre las mercaderías vendidas;*
m) *Incumplimiento previsible del contrato;*
n) *Percepción de intereses por sumas adeudadas;*
o) *Exoneración de responsabilidad por falta de cumplimiento, incluso en supuestos de fuerza mayor;*
p) *Obligaciones de conservar las mercaderías que deben ser enviadas o devueltas a la otra parte.*

Al respecto, la CNUCCIM señala que no es necesaria la forma escrita para los contratos de compraventa internacional que regula, pero realizando una interpretación conjunta con la CNUUCECI, se puede hacer uso de métodos electrónicos de comunicación en los contratos internacionales, la formación del contrato por medios automatizados de comunicación, el momento y el lugar en que las comunicaciones electrónicas se consideran emitidas y recibidas, la determinación de ubicación de las partes que utilizan comunicaciones electrónicas y los criterios para establecer una equivalencia funcional entre la comunicación y la autenticación en formato electrónico e impreso.

Como se advierte de lo anterior, las leyes modelo y las convenciones proyectadas por la CNUDMI funcionan de manera integral e interactúan con esta Convención.

Finalmente, las reglas de la Convención son aplicadas e interpretadas por los tribunales y órganos arbitrales nacionales competentes para conocer de las controversias que surgen en las transacciones sujetas a la Convención.

5.2. Convención sobre Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales: Armonización legislativa en la Contratación Electrónica

5.2.1. Campo de aplicación y principios generales.

La Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales de 2005 (CNUUCECI) refiere que el ámbito de aplicación de la utilización de las comunicaciones electrónicas relativas al cumplimiento de un contrato, se apoya del artículo 1º de la Convención de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías (CNUCCIM) relativo en que las partes del contrato tienen su residencia habitual o establecimiento en estados distintos.

Lo anterior implica que un contrato internacional puede interpretarse a través de una visión restringida o amplia de acuerdo a su ubicación; en el primer caso, se considere el factor extranjero —ubicación del establecimiento de las partes en estados diferentes— en el segundo caso, que considera factores más relevantes no basados en aquella.

Para la CNUUCECI es suficiente manifestar que los estados donde se ubican los establecimientos de las partes son parte de la Convención si incluyen la declaración a que se refiere el artículo 19:

> ***Artículo 19.*** *(…) todo Estado parte en la Convención podrá declarar que la misma sólo se aplicará cuando los estados en los que las partes* ***tengan su establecimiento sean estados contratantes*** *de dicha Convención, o cuando las partes* ***hayan convenido que su régimen sea aplicable.***
>
> **(Énfasis añadido)**

Ahora bien, dos elementos en el ámbito geográfico deben analizarse: el primero, el de comunicación electrónica, y segundo, el de establecimiento.

La *comunicación* de acuerdo con artículo 4 (a) de la CNUUCECI es toda exposición, declaración, reclamación, aviso o solicitud, incluida una oferta y la aceptación de una oferta, que las partes hagan o decidan hacer con la formación o el cumplimiento de un contrato.

Mientras que por *comunicación electrónica el* artículo 4 (b) refiere que es toda comunicación que las partes hagan por medio de MD.

Por lo que hace al segundo, el establecimiento es *todo lugar donde una parte mantiene un centro de operaciones no temporal para realizar una actividad económica distinta del suministro transitorio de bienes o servicios desde determinado lugar* [395]*,* y no se considera establecimiento un lugar por el mero hecho de que en él estén ubicados los equipos y tecnología que sirvan de soporte para el sistema de información utilizado por una de las partes para la formación de un contrato o donde ellas puedan tener acceso a dicho sistema de información[396].

Asimismo en el numeral 5 del artículo 6 se establece que el hecho de que una parte haga uso de un nombre de dominio o de una dirección de correo electrónico vinculados a cierto país, no crea la presunción de que su establecimiento se encuentra en dicho lugar.

La **pluralidad de establecimientos** lo señala el artículo 6 numeral 2 de la CNUUCECI –de su definición depende la aplicación de la Convención– **es el que tenga la relación más estrecha con el contrato**, teniendo en cuenta las circunstancias conocidas o previstas por las partes en cualquier momento antes de la celebración del contrato o al concluirse éste. Igualmente, en caso de ausencia de establecimiento, se estará a la **residencia habitual**, reglas éstas que ya habían sido incorporadas en el artículo 10 de la CNUCCIM (énfasis añadido).

Por otra parte, el numeral segundo del artículo 1º de la Convención que nos ocupa señala que no se tendrá en cuenta el hecho de que las partes tengan sus establecimientos en distintos estados cuando ello no resulte del contrato ni de los tratos entre las partes, ni de la información revelada por las partes en cualquier momento antes de la celebración del contrato o al

[395] Artículo 4 "h" de la CNUUCECI.
[396] Artículo 6 numeral 4 de la CNUUCECI.

concluirse éste. Tal disposición se reproduce en el artículo 1º párrafo 2 de la CNUCCIM razón por la que la jurisprudencia ha considerado que el carácter internacional del contrato debe ser evidente para las partes al momento de celebrarlo, pudiendo en consecuencia argumentar que el carácter internacional del contrato no es evidente, debiendo para ello probar su afirmación[397].

La CNUUCECI menciona en general a los contratos internacionales sin dirigirse a algún tipo de operación particular, no obstante, sí incluyó normas jurídicas para las transacciones electrónicas internacionales de bienes materiales. Luego, precisó que para la aplicación de la Convención había dos excepciones:

a. No se tendrá en cuenta la nacionalidad ni la naturaleza civil o mercantil de la operación (artículo 1º numeral 3), pero no se aplicará a los contratos concluidos con fines personales, familiares o domésticos (el artículo 2º).

Al abarcar el mayor número de transacciones sin tener en cuenta el carácter civil o comercial de las partes o del contrato, implícitamente aplica la Convención a operaciones de carácter empresarial, dejando fuera a todas las operaciones del consumidor; por ende, si el vendedor no estuvo informado de que las mercaderías se compraban para un uso doméstico o de consumo antes de la celebración del contrato o en el momento de su celebración, la aplicación de la Convención a las transacciones de compraventa internacional podría ser aplicable.

b) No es aplicable a las operaciones de mercados de capitales, bursátiles y divisas, títulos crediticios, tales como letras de cambio, pagarés, cartas de porte, conocimientos de embarque o resguardos de almacén, etc., pero se aplicará a cualquier otro tipo de operaciones internacionales concertadas por medios electrónicos, entre las cuales podrían estar las operaciones de compraventa, comercio compensatorio o *countertrade,* operaciones de intermediación, incluidas agencia, concesión, distribución, etc. (artículo 2 de la CNUUCECI).

El ámbito temporal de la CNUUCECI es las *comunicaciones electrónicas* cursadas a partir de la fecha de entrada en vigor de la Convención respecto de cada Estado contratante (artículo 24).

En cuanto a los principios generales de la contratación internacional establecido por la CNUUCECI, entre ellos autonomía de la voluntad, los principios generales y reglas de derecho internacional privado.

El principio de autonomía de la voluntad es similar al artículo 6 de la CNUCCIM, al establecer que *las partes podrán excluir la aplicación de ella o exceptuar o modificar los efectos de cualquiera de sus disposiciones* . En este caso, se está aludiendo a la autonomía de la voluntad,

[397] Oviedo Albán, Jorge, Convención de las Naciones Unidas sobre la utilización de comunicaciones electrónicas en contratos internacionales, en International Law Review Colombia, Derecho Internacional Bogotá, Colombia, N° 7: 11-59, enero-mayo de 2006.

tanto en sentido material como conflictual, toda vez que los contratantes podrán no sólo determinar el contenido del contrato, sino también excluir la aplicación de la Convención. No obstante, las partes deben cuidarse a la hora de redactar cláusulas de exclusión ambiguas, como por ejemplo señalar a un derecho nacional "en general", y la Convención fuere parte de dicho derecho[398].

Además, dicha autonomía de la voluntad material podrá expresarse por medios electrónicos o por medios físicos tradicionales.

Por otra parte, en cuanto hace a los principios interpretativos, se consideró su carácter internacional, la uniformidad en su aplicación, la buena fe (artículo 5). Asimismo integra dos mecanismos de los cuales se pueden valer los intérpretes: a) los principios generales de la Convención, o la ley aplicable nacional o internacional; y b) los usos y prácticas que se lleguen a derivar de las operaciones electrónicas.

Ahora, en cuanto a los principios de la contratación electrónica, la Convención reconoce expresamente los siguientes:

a) Equivalencia funcional
b) Neutralidad tecnológica
c) Libertad de forma y de prueba
d) No alteración del derecho preexistente en obligaciones y contratos

5.2.2. Formación del Contrato.

A fin de facilitar la formación del contrato, lo hemos dividido en cinco puntos:

a) Oferta y aceptación
b) Tiempo y lugar de envío y recepción de las comunicaciones
c) Sistemas automatizados y formación del contrato
d) Firma electrónica
e) Error en las comunicaciones electrónicas

a) Oferta y aceptación

Implícitamente, es posible expresar la oferta y aceptación por medios electrónicos pues aun cuando la CNUUCECI no hace referencia ello, sí acepta el principio de equivalencia funcional de los actos electrónicos establecida en la LMCE. Lo anterior se refuerza con el artículo 8º de la Convención, que establece que no se negará validez ni fuerza ejecutoria a una comunicación o contrato por la sola razón de que estén en forma de comunicación electrónica.

[398] Cfr. Oviedo Albán, Jorge. Convención de las Naciones Unidas sobre la utilización de comunicaciones electrónicas en contratos internacionales, en International Law Review Colombia, Derecho Internacional Bogotá, Colombia, N° 7: 11-59, enero-mayo de 2006, p. 34.

Los requisitos de la oferta quedan regulados por las normas o instrumentos jurídicos que resulten aplicables, en razón del principio de no alteración del derecho preexistente en obligaciones y contratos, v.gr. se pueden aplicar los preceptos de la CNUCCIM.

También se regula por la Convención, la *invitación para presentar ofertas*:

> ***Artículo 11.*** *Toda propuesta de celebrar un contrato presentada por medio de una o más comunicaciones electrónicas* ***que no vaya dirigida a una o varias partes determinadas****, sino que sea generalmente accesible para toda parte que haga uso de sistemas de información, así como toda propuesta que haga uso de aplicaciones interactivas para hacer pedidos a través de dichos sistemas, se considerará una invitación a presentar ofertas, salvo que indique claramente la intención de la parte que presenta la propuesta de quedar obligada por su oferta en caso de que sea aceptada.*
>
> **(Énfasis añadido)**

Cuya interpretación es que cuando se hace una oferta de bienes o servicios a través de Internet a un número de personas ilimitado, se aplica el principio de que la empresa que anuncia así sus bienes o servicios está invitando a los que acceden al sitio web donde se encuentran las ofertas; y por ende, tales las ofertas no son en principio vinculantes.

b) Tiempo y lugar de envío y recepción de las comunicaciones

La CNUUCECI no precisa el momento en que se perfeccionará el contrato, sino el momento en que cada comunicación se entiende enviada o recibida, por lo que las leyes sustantivas lo determinarán. Esto no hace más que reafirmar el principio de no alteración del derecho preexistente en las obligaciones, por lo que es posible aplicar las nacionales o internacionales que regulen dicho tema.

Las comunicaciones son expedidas en el momento en que salgan de un sistema de información que esté bajo el control del iniciador o quien la envíe a nombre suyo, y en caso de que la comunicación no haya salido de un sistema de información que esté por él controlado o por la parte que la envíe a su nombre, en el momento en que se reciba, lo cual se entenderá en el momento en que pueda ser recuperada por el destinatario en una dirección electrónica por él designada (artículo 10).

Igualmente se señala, que la comunicación se tendrá por expedida en el lugar en que el iniciador tenga su establecimiento, y recibida, en el lugar en que el destinatario tenga el suyo, todo lo cual resulta importante para saber en qué sitio producen efectos los actos jurídicos, lo que también puede tener implicaciones en la determinación de reglas aplicables conforme al derecho internacional privado e incluso reglas de índole procesal.

c) Sistemas automatizados y formación del contrato

Los contratos pueden perfeccionarse mediante la interacción de un sistema automatizado de mensajes y una persona física, o por la interacción de sistemas automatizados de mensajes:

Artículo 12. *No se negará validez ni fuerza ejecutoria a un contrato que se haya formado por la interacción entre un sistema automatizado de mensajes y una persona física, o por la interacción de sistemas automatizados de mensajes, por la simple razón de que ninguna persona física haya revisado uno de los distintos actos realizados a través de los sistemas o el contrato resultante de tales actos ni haya intervenido en ellos.*
(…).

La persona en cuyo nombre estaba programada la computadora es responsable de todos los mensajes generados por la máquina porque ésta no tiene voluntad propia. Sin olvidar que un sistema automatizado puede iniciar, responder o interactuar con otras partes o sus agentes electrónicos una vez que ha sido activado por una parte.

d) Firma electrónica.

Por su relevancia en nuestra investigación, a continuación se transcribe el artículo 9 de la CNUUCECI, el cual es una reproducción del artículo 7º de la LMCE, fundamento de nuestra regulación en el CCo.

Artículo 9. Requisitos de forma*.*
1. Nada de lo dispuesto en la presente Convención obligará a que una comunicación o un contrato tenga que hacerse o probarse de alguna forma particular.

2. Cuando la ley requiera que una comunicación o un contrato conste por escrito, o prevea consecuencias en el caso de que eso no se cumpla, una comunicación electrónica cumplirá ese requisito si la información consignada en su texto es accesible para su ulterior consulta.

*3. Cuando la ley requiera que una comunicación o un contrato sea **firmado** por una parte, o prevea consecuencias en el caso de que no se firme, ese requisito se dará por cumplido respecto de una comunicación electrónica:*

*a) Si se utiliza un método para determinar la **identidad** de esa parte y para indicar la **voluntad** que tiene tal parte respecto de la información consignada en la comunicación electrónica; y*
b) Si el método empleado:

*i) O bien es tan **fiable** como sea apropiado para los fines para los que se generó o transmitió la comunicación electrónica, atendidas todas las circunstancias del caso, inclusive todo acuerdo aplicable; o*
ii) Se ha demostrado en la práctica que, por sí solo o con el respaldo de otras pruebas, dicho método ha cumplido las funciones enunciadas en el apartado a) supra.

(Énfasis añadido)

4. Cuando la ley requiera que una comunicación o un contrato se proporcione o conserve en su forma original, o prevea consecuencias en el caso de que eso no se cumpla, ese requisito se tendrá por cumplido respecto de una comunicación electrónica:

a) Si existe alguna garantía fiable de la integridad de la información que contiene a partir del momento en que se generó por primera vez en su forma definitiva, en cuanto comunicación electrónica o de otra índole; y
b) Si, en los casos en que se exija proporcionar la información que contiene, esta puede exhibirse a la persona a la que se ha de proporcionar.

5. Para los fines del apartado a) del párrafo 4:

a) Los criterios para evaluar la integridad de la información consistirán en determinar si se ha mantenido completa y sin alteraciones que no sean la adición de algún endoso o algún cambio sobrevenido en el curso normal de su transmisión, archivo o presentación; y
b) El grado de fiabilidad requerido se determinará teniendo en cuenta la finalidad para la que se generó la información, así como todas las circunstancias del caso.

e) Error en las comunicaciones electrónicas

Cuando una persona física cometa error al introducir los datos de una comunicación electrónica con el sistema automatizado de mensajes de otra parte, y éste no permita la corrección, se podrá retirar la comunicación, siempre que se notifique a la otra parte tan pronto como sea posible y si además no se ha utilizado los bienes o servicios recibidos en virtud del contrato ni se ha obtenido ningún beneficio material o valor de ellos. Así, el numeral 14 de la CNUUCECI reza:

Artículo 14. *Error en las comunicaciones electrónicas*
1. Cuando una persona física cometa un error al introducir los datos de una comunicación electrónica intercambiada con el sistema automatizado de mensajes de otra parte y dicho sistema no le brinde la oportunidad de corregir el error, esa persona, o la parte en cuyo nombre ésta haya actuado, tendrá derecho a retirar la parte de la comunicación electrónica en que se produjo dicho error, si:
a) La persona, o la parte en cuyo nombre haya actuado esa persona, notifica a la otra parte el error tan pronto como sea posible después de haberse percatado de éste y le indica que lo ha cometido; y si
b) La persona, o la parte en cuyo nombre haya actuado esa persona, no ha utilizado los bienes o servicios ni ha obtenido ningún beneficio material o valor de los bienes o servicios, si los hubiere, que haya recibido de la otra parte.
2. Nada de lo dispuesto en el presente artículo afectará a la aplicación de regla de derecho alguna que regule las consecuencias de un error cometido, a reserva de lo dispuesto en el párrafo 1.

5.2.3. Cláusulas contractuales para el comercio electrónico de la ICC (*ICC eTerms 2004*)

Para completar el tema del comercio electrónico seguro en materia internacional no se puede pasar por alto las cláusulas contractuales publicadas en 2004 por la Cámara de Comercio Internacional (CCI), más conocidos por su abreviatura: ICC eTerms 2004.

Los ICC eTerms 2004[399] están diseñados para mejorar la seguridad jurídica de los contratos celebrados por medios electrónicos, para proporcionar dos cláusulas cortas (ver transcripción inglés-español en el cuadro que se muestra a continuación), fáciles de incorporar en los contratos, que dejan claro que ambas partes tienen la intención de vincularse en un contrato electrónico. Tales términos no afectan la materia objeto del contrato, no interfieren en modo alguno con otro término que se encuentre dentro del contrato, a menos que se pacte lo contrario; simplemente, facilitan los procedimientos y el uso de medios electrónicos en la celebración de un contrato y, además, pueden ser utilizados en y para cualquier contrato que incluya la venta u otra disposición de bienes, derechos o servicios.

ICC eTerms 2004	
Inglés	**Español[400]**
A. Article 1 - E-commerce agreement *The parties agree:* *1.1 that the use of electronic messages shall create valid and enforceable rights and obligations between them; and* *1.2 that to the extent permitted under the applicable law, electronic messages shall be admissible as evidence, provided that such electronic messages are sent to addresses and in formats, if any, designated either expressly or implicitly by the addressee; and* *1.3 not to challenge the validity of any communication or agreement between them solely on the ground of the use of electronic means, whether or not such use was reviewed by any natural person.*	***A. Artículo 1 - Acuerdo de comercio electrónico*** *Las partes acuerdan:* *1.1 Que el uso de mensajes electrónicos generará derechos y obligaciones válidas y exigibles entre ellas; y* *1.2 Que en la medida en que lo permita la legislación aplicable, los mensajes electrónicos serán admisibles como prueba, siempre que dichos mensajes electrónicos sean enviados a direcciones y en los formatos, que en su caso, sean designados, expresa o implícitamente por el destinatario; y* *1.3 No impugnar la validez de cualquier comunicación o acuerdo entre ellos por el mero hecho de la utilización de medios electrónicos, independientemente de que dicha utilización fue revisado por cualquier persona física.*
Article 2 - Dispatch and Receipt *2.1 An electronic message is deemed1 to be:* *(a) dispatched or sent when it enters an information system outside the control of the sender; and* *(b) received at the time when it enters an information system designated by the addressee.* *2.2 When an electronic message is sent to an information system other than that designated by the addressee, the electronic message is deemed to be received at the time when the addressee becomes aware of the message.* *2.3 For the purpose of this contract, an electronic message is deemed to be dispatched or sent at the place where the sender has its place of business and is deemed to be received at the place where the addressee has its place of business.*	***A. Artículo 2 - Envío y Recepción*** *2.1 Un mensaje electrónico se considerará que:* *(a) Es expedido o enviado cuando entre en un sistema de información fuera del control del remitente; y* *(b) Es recibido en el momento en que entre en un sistema de información designado por el destinatario.* *2.2 Cuando un mensaje electrónico se envía a un sistema de información distinto del designado por el destinatario, el mensaje electrónico se considerará recibido en el momento en que el destinatario tenga conocimiento del mensaje.* *2.3 Para efectos de este contrato, un mensaje electrónico se tendrá por expedido o enviado en el lugar donde el emisor tiene su lugar de trabajo y se considerará que se ha recibido en el lugar donde el destinatario tenga su domicilio comercial.*

[399] ICC eTerms 2004, Cámara de Comercio Internacional (CCI), accesible en http://iccwbo.org/, consultado el 3 de mayo de 2015.

[400] La traducción al español es nuestra.

Finalmente, se recomienda encarecidamente que se estudie la *ICC Guide for eContracting*[401] o *Guía de CCI para la contratación electrónica*, cuyo contenido está integrado como se muestra a continuación:

ICC Guide for eContracting	
Inglés	**Español**[402]
B.1 How to apply ICC eTerms 2004	*B.1 Cómo aplicar ICC eTerms 2004*
B.2 The legal validity of ICC eTerms 2004	*B.2 La validez legal de ICC eTerms 2004*
B.3 The limits of ICC E-Terms 2004	*B.3 Los límites de ICC eTerms 2004*
B.4 Who contracts on your behalf?	*B.4 Quién contrata en tu nombre?*
B.5 With whom are you contracting?	*B.5 Con quién estás contratando?*
B.6 Constructing an electronic contract	*B.6 La elaboración de un contrato electrónico*
B.7 Technical Specifications	*B.7 Especificaciones Técnicas*
B.8 Protecting Confidentiality	*B.8 Protección de la confidencialidad*
B.9 Technical Breakdown and Risk Management	*B.9 Fallo técnico y gestión de riesgo*

5.2.4. Inclusión de los Términos Internacionales de Comercio (INCOTERMS)

La finalidad de toda negociación comercial es que se cumpla, cuestiones como la seguridad y el traslado de una mercancía llegue a su destino debe realizarse con el menor número de contingencias.

Por tal razón, cada una de las cláusulas del contrato electrónico deben ser sencillas, concretas y seguras, uno de los mejores medios para lograrlo es utilizar los Incoterms de la Cámara de Comercio Internacional (CCI), cuya definición está protegida por copyright de la CCI.

Cuando los contratantes hacen referencia específica a uno de los INCONTERMS o *International Commerce Terms* de la CCI, prácticamente no existen interpretaciones equivocas relativas a los términos usados, y por ende, evita la generación de conflictos entre las partes.

Los INCOTERMS regulan la distribución de documentos, las condiciones de entrega de la mercancía, la distribución de costos de la operación y la distribución de riesgos de la operación; no obstante, quedan fuera de su regulación, las cláusulas internas de un contrato de compra y venta, la situación de la mercancía, el traspaso de propiedad, la garantía, la concreción de pago y el incumplimiento de compromisos del contrato de compra, entre otras.

En suma los Incoterms son normas para la interpretación de los términos comerciales utilizados en las transacciones internacionales, elaboradas por la Cámara de Comercio Internacional.

[401] ICC Guide for eContracting, Cámara de Comercio Internacional (CCI), accesible en http://iccwbo.org/, consultado el 3 de mayo de 2015.
[402] La traducción al español es nuestra.

Existen trece categorías básicas o términos estandarizados (EXW, FCA, FOB, FAS, CFR, CIF, CPT, CIP, DAF, DES, DEQ, DDU, DDP) que facilitan el comercio internacional al permitir que agentes de diversos países se entiendan entre sí[403]:

1) **EXW: (Ex-works, ex-factory, ex-warehouse, ex-mill)**
   El vendedor ha cumplido su obligación de entrega al poner la mercadería en su fábrica, taller, etc. a disposición del comprador. No es responsable ni de cargar la mercadería en el vehículo proporcionado por el comprador ni de despacharla de aduana para la exportación, salvo acuerdo en otro sentido. El comprador soporta todos los gastos y riesgos de retirar la mercadería desde el domicilio del vendedor hasta su destino final.

2) **FCA: (*Free Carrier* - Franco Transportista - libre transportista)**
   El vendedor cumple con su obligación al poner la mercadería en el lugar fijado, a cargo del transportista, luego de su despacho de aduana para la exportación. Si el comprador no ha fijado ningún punto específico, el vendedor puede elegir dentro de la zona estipulada el punto donde el transportista se hará cargo de la mercadería. Este término puede usarse con cualquier modo de transporte, incluido el multimodal.

3) **FOB: (*Free On Board* - Libre a bordo)**
   Va seguido del puerto de embarque, ej. FOB Algeciras. Significa que la mercadería es puesta a bordo del barco con todos los gastos, derechos y riesgos a cargo del vendedor hasta que la mercadería haya pasado la borda del barco, con el flete excluido. Exige que el vendedor despache la mercadería de exportación. Este término puede usarse solamente para el transporte por mar o vías acuáticas interiores.

4) **FAS: (*Free Alongside Ship* - Libre al costado del buque)**
   La abreviatura va seguida del nombre del puerto de embarque. El precio de la mercadería se entiende puesta a lo largo (costado) del navío en el puerto convenido, sobre el muelle o en barcazas, con todos los gastos y riesgos hasta dicho punto a cargo del vendedor. El comprador debe despachar la mercadería en aduana. Este término puede usarse solamente para el transporte por mar o vías acuáticas interiores.

5) **CFR: (*Cost & Freight* - Costo y Flete)**
   La abreviatura va seguida del nombre del puerto de destino. El precio comprende la mercadería puesta en puerto de destino, con flete pagado pero seguro no cubierto. El vendedor debe despachar la mercadería en Aduana y solamente puede usarse en el caso de transporte por mar o vías navegables interiores.

6) **CIF: (*Cost, Insurance & Freight* - Costo, Seguro y Flete)**
   La abreviatura va seguida del nombre del puerto de destino y el precio incluye la mercadería puesta en puerto de destino con flete pagado y seguro cubierto. El vendedor contrata el

[403] Acota Roca, Felipe. INCOTERMS: Términos de Compra-Venta Internacional, 1ª ed., 1989, México, D.F., Ed. ISEF, p. 3-31; Para más información visitar el sitio de la Confederación de Asociaciones de Agentes Aduanales de la República Mexicana: http://www.caaarem.mx/.

seguro y paga la prima correspondiente. El vendedor sólo está obligado a conseguir un seguro con cobertura mínima.

7) **CPT: (*Carriage paid to* -Transporte Pagado Hasta)**
   El vendedor paga el flete del transporte de la mercadería hasta el destino mencionado. El riesgo de pérdida o daño se transfiere del vendedor al comprador cuando la mercadería ha sido entregada al transportista. El vendedor debe despachar la mercadería para su exportación.

8) **CIP: (*Carriage and Insurance Paid to* - Transporte y Seguro pagados hasta)**
   El vendedor tiene las mismas obligaciones que bajo CPT, pero además debe conseguir un seguro a su cargo.

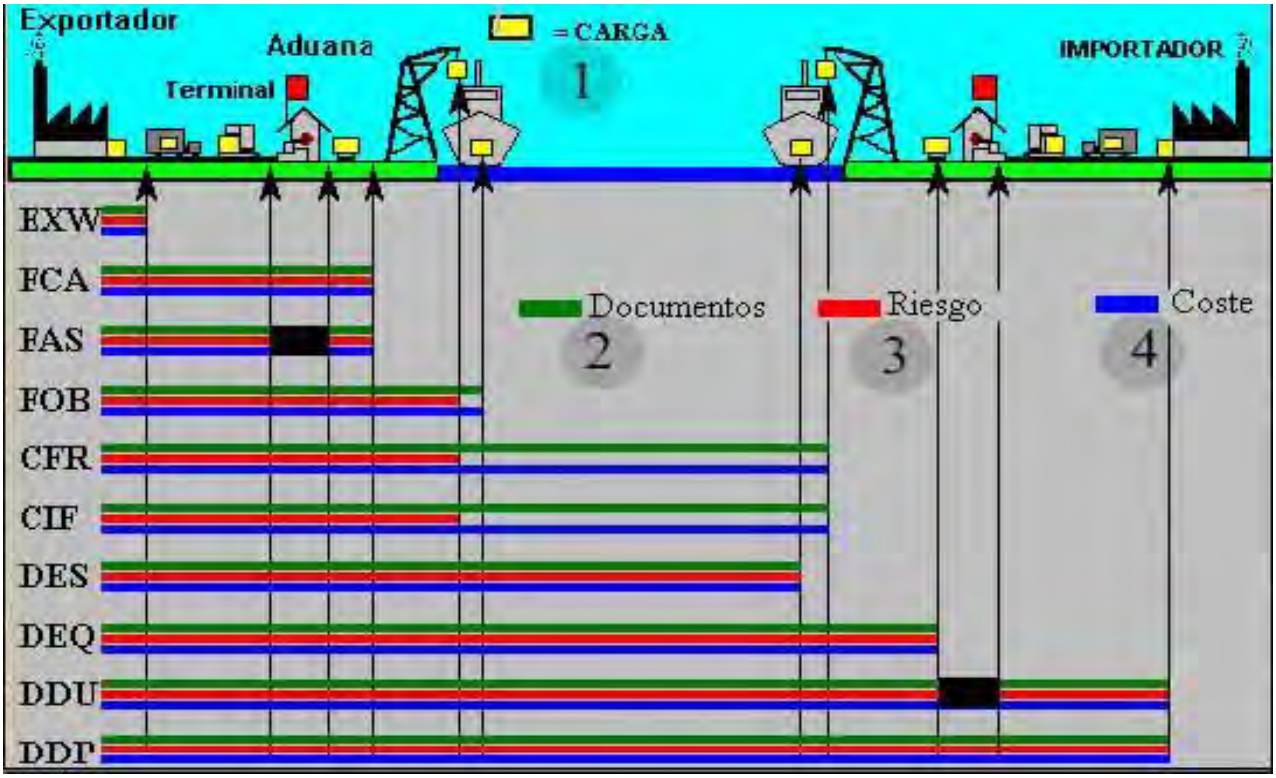
9) **DAF: (*Delivered at Frontier* - Entregado en frontera)**
   El vendedor cumple con su obligación cuando entrega la mercadería, despachada en aduana, en el lugar convenido de la frontera pero antes de la aduana fronteriza del país colindante. Es fundamental indicar con precisión el punto de la frontera correspondiente.

10) **DES: (*Delivered ex Ship* - Entregada sobre buque)**
    El vendedor cumple con su obligación cuando pone la mercadería a disposición del comprador a bordo del buque en el puerto de destino, sin despacharla en aduana para la importación.

11) **DEQ: [*Delivered ex Quay (Duty Paid)* - Entregada en muelle (derechos pagados)]**
    El vendedor cumple con su obligación cuando pone la mercadería a disposición del comprador sobre el muelle en el puerto de destino convenido, despachada en aduana para la importación.

12) **DDU: (*Delivered Duty Unpaid* - Entregada derechos no pagados)**
    El vendedor cumple con su obligación cuando pone la mercadería a disposición del comprador en el lugar convenido en el país de importación. El vendedor asume todos los gastos y riesgos relacionados con la entrega de la mercadería hasta ese sitio (excluídos derechos, cargas oficiales e impuestos), así como de los gastos y riesgos de llevar a cabo las formalidades aduaneras.

13) **DDP:(*Delivered Duty* Paid - Entregada derechos pagados)**
    El vendedor asume las mismas obligaciones que en D.D.U. más los derechos, impuestos y cargas necesarias para llevar la mercadería hasta el lugar convenido.



Gráfica de Incoterms[404]

[404] Imagen de BusinessCol.com, Accesible en http://www.businesscol.com/comex/incoterms.htm, consultada el 3 de mayo de 2015.

CAPÍTULO VI. ALTERNATIVAS Y CONSIDERACIONES PARA LA CONSAGRACIÓN DE LA FIRMA ELECTRÓNICA AVANZADA EN EL COMERCIO ELECTRÓNICO

6.1. Propuesta de reforma constitucional y Proyecto de Ley General de Firma Electrónica Avanzada.

La propuesta relativa a medios electrónicos se hace desde la visión de *lege ferenda*[405]. Los antecedentes que sustentan tal sugerencia de reforma e iniciativa de Ley se fundan en los antecedentes constitucionales relativos a la incorporación de las TIC en la Carta Magna.

Primeramente, el 11 de julio de 2013 se adicionaron diversos párrafos e incisos del artículo 6o de la CPEUM, que son de especial relevancia porque incorporan las TIC's y las telecomunicaciones a nivel constitucional, especialmente del tercer párrafo, al inciso A, fracción V, inciso B, fracción I, en relación con su transitorio Décimo Cuarto del Decreto, los cuales establecen:

> ***Artículo 6º.*** *(…)*
> *El Estado garantizará el derecho de acceso a las* ***tecnologías de la información y comunicación****, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de* ***banda ancha e internet****. Para tales efectos, el Estado establecerá condiciones de competencia efectiva en la prestación de dichos servicios.*
> *(…)*
> ***Inciso A:***
> *(…)*
> ***V.*** *Los sujetos obligados deberán preservar sus documentos en archivos administrativos actualizados y publicarán, a través de los* ***medios electrónicos disponibles****, la información completa y actualizada sobre el ejercicio de los recursos públicos y los indicadores que permitan rendir cuenta del cumplimiento de sus objetivos y de los resultados obtenidos.*
> *(…)*
> ***Inciso B:***
> ***I. (…)***
> *B. En materia de radiodifusión y telecomunicaciones:*
> *I. El Estado garantizará a la población su integración a la sociedad de la información y el conocimiento, mediante una política de inclusión digital universal con metas anuales y sexenales.*
> *(…)* ***(Énfasis añadido)***
>
> ***Transitorio Décimo Cuarto.*** *El Ejecutivo Federal tendrá a su cargo la política de* ***inclusión digital universal****, en la que se incluirán los objetivos y metas en materia de infraestructura, accesibilidad y conectividad,* ***tecnologías de la información y comunicación, y habilidades digitales,*** *así como los programas de gobierno digital, gobierno y datos abiertos, fomento a la inversión pública y privada en aplicaciones de telesalud, telemedicina y Expediente Clínico Electrónico y* ***desarrollo de aplicaciones, sistemas y contenidos digitales, entre otros aspectos.***

[405] Locución latina que significa "para una futura reforma de la ley" o "con motivo de proponer una ley".

Dicha política tendrá, entre otras metas, que por lo menos 70 por ciento de todos los hogares y 85 por ciento de todas las micros, pequeñas y medianas empresas a nivel nacional, cuenten con accesos con una velocidad real para descarga de información de conformidad con el promedio registrado en los países miembros de la Organización para la Cooperación y el Desarrollo Económicos. Esta característica deberá ser ofrecida a precios competitivos internacionalmente.
El Instituto Federal de Telecomunicaciones deberá realizar las acciones necesarias para contribuir con los objetivos de la política de inclusión digital universal.

Asimismo, el Ejecutivo Federal elaborará las ***políticas de radiodifusión y telecomunicaciones del Gobierno*** *Federal y realizará las acciones tendientes a* ***garantizar el acceso a Internet de banda ancha*** *en edificios e instalaciones de las dependencias y entidades de la Administración Pública Federal. Las entidades federativas harán lo propio en el ámbito de su competencia.*

(Énfasis añadido)

De las transcripciones anteriores, se advierte que la CPEUM es omisa en precisar la necesidad de inserción de un párrafo relativo a garantizar el valor y reconocimiento probatorio de las TIC, en particular, de los medios electrónicos, en términos de una Ley Reglamentaria, lo cual tiene, desde luego, implicaciones jurídicas. De tal forma que la citada ley establecería que los medios electrónicos otorguen seguridad jurídica en la valoración de los medios electrónicos.

La primera implicación sería en qué artículo se anexaría, además de la correspondiente adición al artículo 73, fracción XVII constitucional para que se le otorgue al Congreso de la Unión, la facultad de regular la materia.

En este sentido, se sugiere agregar dicho párrafo como un tercero del artículo 16 constitucional:

Toda persona tiene derecho a que se le reconozca el uso y valor de los medios electrónicos, la cual se sujetará a la Ley Reglamentaria respectiva.

La adición constitucional propuesta en el artículo 16 constitucional conjugaría el énfasis y relevancia de los medios electrónicos, la priorización del desarrollo de Internet, la *infotecnología*[406] y, en general, de todas las TIC y de la SIC; por ende, la adición consolidaría el fomento de aquellas ya están incluidas por legislador.

En tanto que el artículo 73, se adicionarían una frase al final del testo de la fracción XVII:

Artículo 73. *El Congreso tiene facultad:*
(…)
XVII. *Para dictar leyes sobre vías generales de comunicación, tecnologías de la información y la comunicación, radiodifusión, telecomunicaciones, incluida la banda ancha e Internet, postas y correos, y sobre el uso y aprovechamiento de las aguas de jurisdicción federal* ***así como del reconocimiento de su valor probatorio.***

[406] Es la utilización de las TIC en el sistema educativo.

El uso acorde de las TIC exige a las naciones identificar los mecanismos y variables a considerar en una estrategia digital. A guisa de ejemplo, varios países andinos ya incluyeron varias disposiciones de las TIC a nivel constitucional, a saber:

Bolivia, en la primera parte de la Constitución, establece las bases fundamentales del estado, derechos, deberes y garantías que se inserta en el título 1, "Derechos fundamentales y garantías", Capítulo VI, "Educación, interculturalidad y derechos culturales", sección IV, "Ciencia, tecnología e investigación":

> ***Artículo 103****: El Estado garantizará el desarrollo de la ciencia y la investigación científica, técnica y tecnológica en beneficio del interés general. Se destinarán los recursos necesarios y se creará el sistema estatal de ciencia y tecnología.*
> *El Estado asumirá como política la implementación de estrategias para incorporar el conocimiento y aplicación de nuevas tecnologías de información y comunicación.*

Colombia, en el *Capítulo II: De los Derechos Sociales, Económicos y Culturales,* el artículo 71 menciona lo siguiente:

> *La búsqueda del conocimiento y la expresión artística son libres. Los planes de desarrollo económico y social incluirán el fomento a las ciencias y, en general, a la cultura. El Estado creará incentivos para personas e instituciones que desarrollen y fomenten la ciencia y la tecnología y las demás manifestaciones culturales y ofrecerá estímulos especiales a personas e instituciones que ejerzan estas actividades.*

Perú, establece en el artículo 2 constitucional que *toda persona tiene derecho a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.*

Por otro lado y previo al análisis de la segunda propuesta de este trabajo, es indispensable y, por demás pertinente, señalar las similitudes y diferencias entre las leyes federales y las leyes generales, para establecer los motivos por los cuales se propone una Ley General a la par de la Ley Federal ya expedida.

En este orden, las similitudes de leyes federales y generales son creadas de acuerdo con las competencias atribuidas en la CPEUM por el Poder Legislativo Federal y regulan asuntos de interés nacional.

Por lo que respecta a sus diferencias, la Ley General —cuyo apelativo y uso en México es más antiguo que el de una Ley Federal— implica una competencia concurrente y establece obligaciones y facultades en cada uno de los tres niveles de gobierno (federal, estatal y municipal).

Cabe señalar que el Pleno de la Suprema Corte de Justicia de la Nación al resolver la acción de inconstitucionalidad número 119/2008[407] se pronunció sobre este tema y señaló que aun cuando técnicamente la Federación y las entidades federativas están a la par en cuanto a su orden jurídico, como excepción a esta regla se encuentran las Leyes Generales, cuyo objeto es la distribución de competencias en materias concurrentes.

Curiosamente, históricamente la materia que ha sido regulada por Leyes Generales es la mercantil, ejemplos de ello son: la Ley General de Instituciones de Crédito, la Ley General de Títulos y Operaciones de Crédito, la Ley General de Sociedades Mercantiles, Ley General de Sociedades Cooperativas y la Ley General de Sociedades de Interés Público[408]. Algunos ejemplos de otras materias son la reciente Ley General de Transparencia y Acceso a la Información Pública, la Ley General de Población, Ley General de Salud y la Ley General de Bienes Nacionales.

En tanto las Leyes Federales son aquellas cuyo ámbito de aplicación personal es todo el territorio nacional y su vigilancia se realiza por autoridades federales como las entidades y dependencias de la Administración Pública Gubernamental, la otrora Procuraduría General de la República ahora la Fiscalía General de la Federación; cuyos ejemplos son la Ley Federal de Procedimiento Administrativo, La Ley Federal de Responsabilidades Administrativas de los Servidores Públicos y la Ley Federal de Presupuesto y Responsabilidad Hacendaria. En otros casos las leyes federales normalmente tienen su origen en un señalamiento de una disposición Constitucional, tal como la Ley de Amparo.

Nuestra Ley de Firma Electrónica Avanzada es de orden público y de acuerdo con su artículo 3, están sujetos a ella: I. Las dependencias y entidades; II. Los servidores públicos de las dependencias y entidades que en la realización de los actos a que se refiere esta Ley utilicen la firma electrónica avanzada, y III. Los particulares, en los casos en que utilicen la firma electrónica avanzada en términos de esta Ley; por ende, una Ley Federal no es de competencia concurrente, esto es, no establece obligaciones y facultades en cada uno de los tres niveles de gobierno.

Ahora bien, el motivo por el cual se propone esta alternativa para la consagración del uso de la FEA, como una herramienta de consentimiento y valor probatorio en todo el derecho mexicano, por medio de una Iniciativa de Ley General de Firma Electrónica Avanzada, es que sea una regulación de competencia concurrente de los tres órdenes del gobierno mexicano para el sector público.

Por ello, todas las disposiciones relacionadas con la LFEA, a saber, su Reglamento, el Reglamento del CCo en materia de Prestadores de Servicios de Certificación y las Reglas Generales a las que deberán sujetarse los prestadores de servicios de certificación así como el Acuerdo que las modifican, estarán homologadas.

---

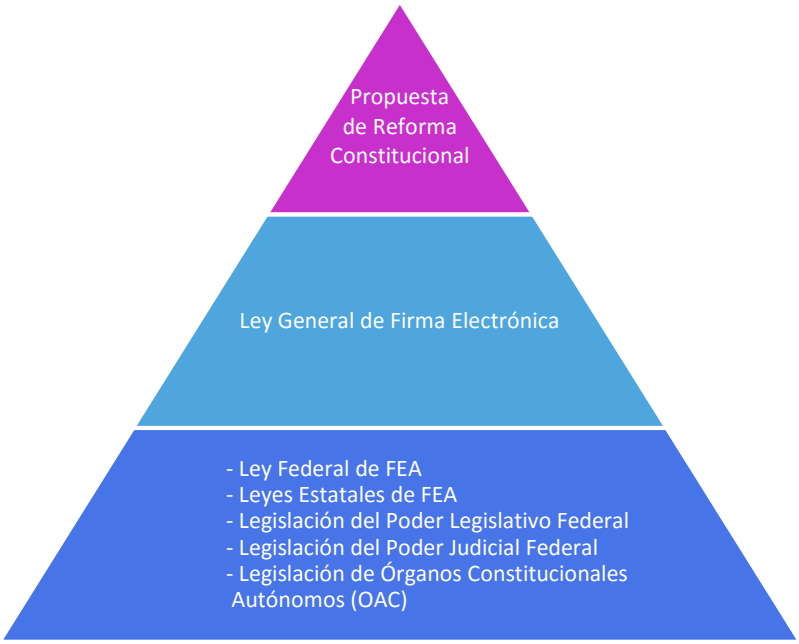
[407] Novena Época; Pleno de la SCJN, Semanario Judicial de la Federación y su Gaceta, Tomo XXX, Diciembre de 2009, página 850.

[408] González Oropeza, Manuel. Conceptualización Histórica de la terminológica legislativa, Soberanes Fernández, José Luis (coord.), en Memoria del III Congreso de Historia del Derecho Mexicano (1983), 1984, México, Ed. UNAM, p. 343.

Por lo que hace a la regulación del consentimiento y valor probatorio de los documentos electrónicos, se encuentran disposiciones en sólo algunos códigos civiles y procesales civiles de los Estados de la República.

Entre las contradicciones y problemáticas que resolvería una Ley General de FEA se encuentran:

a) Los inconvenientes de homologación conceptual (diferentes y nuevos conceptos que se contraponen con otra regulación, confusión de principios normativos).
b) Diversas normativas aplicables (excepciones a la Ley).
c) Representaciones complicadas de conservación de MD.
d) Esquemas de digitalización que niegan destrucción del original.
e) Inclusión del Poder Judicial y Poder Legislativo Federales, de los OCA así como los tres poderes de las entidades federativas y municipios.
f) Limitada información de los aspectos legales de las TIC.
g) Incertidumbre de abandonar la cultura del papel a cambio del procesamiento, almacenamiento, portabilidad, ubicuidad y herramientas de escritura digital, tanto por parte del gobierno como de los gobernados.
h) Miedo al uso de la "Ecoescritura" al otorgar menor valor a la cultura sin papel.
i) Inconvenientes legales en materia sustantiva y adjetiva de la homologación en relación con conceptos, bases y procesos de aquellas.
j) Impedimentos de homologación complejos relativos al área técnica, operativa, de coordinación, interrelación, entre otros:
    - Excepciones a la regulación.
    - Esquemas complejos de conservación.
    - Esquemas de digitalización que no permiten la destrucción de la fuente original.
    - Uso incompatible con diversas autoridades (PJF, Poder Legislativo, entidades federativas, municipios, etc.).
    - Barrera a la inversión extranjera, facilidad para hacer negocios y abrir empresas.



Inserción de la Ley General en la Jerarquía del Sistema Jurídico Mexicano

La propuesta consiste en facultar al Congreso de la Unión para expedir una Ley General que desarrolle los principios y bases en materia de Firma Electrónica Avanzada de los poderes, autoridades, entidades, órganos y organismos gubernamentales de todos los niveles de gobierno, que homologará el uso de la FEA a través dela modificación de la actual LFEA cuyo objeto sea operar trámites entre entidades públicas y privadas incorporando disposiciones uniformes sobre conservación, digitalización y correo electrónico certificado.

La Ley General establecerá la obligación para que todas las autoridades del Estado Mexicano adecuen su regulación respectiva en términos de dicha ley.

Abundando en los beneficios de una Iniciativa de Ley General de Firma Electrónica Avanzada exhibimos también los siguientes:

- Reforma estructural que afianza las recientes reformas nacionales en materia de telecomunicaciones, transparencia y combate a la corrupción.
- Reforma conforme con la innovación tecnológica internacional y el fomento de la SIC.
- Avance en la consolidación de la Estrategia Digital Nacional.
- Aparejar, preparar, disponer el marco regulatorio frente al resto de los proyectos e iniciativas de Leyes Generales mexicanas pendientes de aprobarse en el Congreso de la Unión: Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados y Ley General de Archivos.
- Incluir e interrelacionar a los poderes de la unión, órganos constitucionales autónomos, entidades federativas y municipios, al adherirlos a la reforma gubernamental.
- Fluidez y simplicidad para atraer inversión y facilidad para realizar negocios.
- Certeza legal en la economía digital y seguridad jurídica nacional en el uso de los medios electrónicos.
- Concretos beneficios de conservación y preservación medioambientales con las actividades empresariales basadas en las TIC.
- Reconocimiento e identificación de las actividades y recursos asociados a las TIC que evitan gastos gubernamentales.

Finalmente, a guisa de ejemplo de la necesidad de homologación de la FEA a nivel nacional, se debe precisar que en el ámbito estatal y municipal existen las siguientes variedades de regulaciones en materia de FEA y Firma Electrónica:

No.	Estados de la República Mexicana	Nombre de la Regulación en materia de Firma Electrónica Avanzada o Firma Electrónica
1.	Aguascalientes:	Ley sobre el Uso de Medios Electrónicos para el Estado de Aguascalientes
2.	Baja California:	Ley de Firma Electrónica para el Estado de Baja California
3.	Baja California Sur:	Código Fiscal del Estado y Municipios del Estado de Baja California Sur.
4.	Campeche:	Ley de Firma Electrónica Avanzada y Uso de Medios Electrónicos del Estado de Campeche
5.	Chiapas:	Ley de Firma Electrónica Avanzada del Estado de Chiapas
6.	Chihuahua:	Código Civil y Ley del Registro Público de la Propiedad del Estado de Chihuahua
7.	Coahuila:	Ley de Mejora Regulatoria del Estado de Coahuila de Zaragoza
8.	Colima:	Ley sobre el Uso de Medios Electrónicos y Firma Electrónica para el Estado de Colima
9.	Ciudad de México[409]:	Ley de Firma Electrónica del Distrito Federal
10.	Durango:	Ley de Firma Electrónica Avanzada para el Estado de Durango.
11.	Guanajuato:	Ley sobre el Uso de Medios Electrónicos y Firma Electrónica para el Estado de Guanajuato y sus Municipios
12.	Guerrero:	Ley Número 874 que regula el uso de la Firma Electrónica Certificada del Estado de Guerrero.
13.	Hidalgo:	Ley sobre el Uso de Medios Electrónicos y Firma Electrónica Avanzada para el Estado de Hidalgo
14.	Jalisco:	Ley de Firma Electrónica Avanzada para el Estado de Jalisco y sus Municipios
15.	Michoacán:	Código de Justicia Administrativa e Iniciativa: Ley de Firma Electrónica Certificada del Estado de Michoacán de Ocampo
16.	Morelos:	Ley de Firma Electrónica del Estado Libre y Soberano de Morelos
17.	Estado de México:	Ley para el Uso de Medios Electrónicos del Estado de México.
18.	Nayarit:	Ley de Justicia y Procedimientos Administrativos del Estado de Nayarit.
19.	Nuevo León:	Ley sobre Gobierno Electrónico y Fomento al Uso de las Tecnologías de la Información del Estado.
20.	Oaxaca:	Ley de Firma Electrónica Certificada del Estado de Oaxaca
21.	Puebla:	Ley de Gobierno Digital para el Estado de Puebla y sus Municipios
22.	Querétaro:	Ley de Mejora Regulatoria del Estado de Querétaro
23.	Quintana Roo:	Ley sobre el Uso de Medios Electrónicos, Mensajes de Datos y Firma Electrónica Avanzada para el Estado de Quintana Roo.
24.	San Luis Potosí:	Ley para La Regulación de la Firma Electrónica Avanzada del Estado de San Luis Potosí.

[409] El 29 de enero de 2016, es publicó en el DOF el Decreto por el que se declaran reformadas y derogadas diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de la reforma política de la Ciudad de México.

25.	Sinaloa:	Ley de Justicia Administrativa para el Estado de Sinaloa.
26.	Sonora:	Ley sobre el Uso de Firma Electrónica Avanzada para el Estado de Sonora.
27.	Tabasco:	Ley Registral del Estado de Tabasco.
28.	Tamaulipas:	Ley de Firma Electrónica Avanzada para el Estado de Tamaulipas.
29.	Tlaxcala:	Ley de Firma Electrónica Avanzada para el Estado de Tlaxcala
30.	Veracruz:	Código de Procedimientos Administrativos para el Estado de Veracruz de Ignacio de la Llave.
31.	Yucatán:	Ley sobre el Uso de Medios Electrónicos y Firma Electrónica del Estado de Yucatán.
32.	Zacatecas:	Ley de Firma Electrónica del Estado de Zacatecas.

6.2. Definir la figura del Tercero Legalmente Autorizado

Como se ha señalado en uno de los subcapítulos anteriores de este trabajo, que el objetivo general de la NOM-151 es hacer posible un almacenamiento electrónico de los documentos, a fin de que posean la calidad de originales, y por ende, conserven íntegra su capacidad probatoria. Estos documentos podrían tener un origen electrónico, pero también proceder de una migración a partir de un medio diferente como lo es el papel y haber sido conseguidos por medio de un proceso de digitalización. Entonces, el efecto de este proceso digital, es que el valor probatorio de los documentos migrados estará supeditado por NOM-151 y por la calidad así como garantías aplicadas en dicha migración.

En cuanto hace a la autorización de la digitalización en este respecto, el punto 4.3 de la NOM-151 señala:

> *Sin perjuicio de lo que dispongan otros ordenamientos jurídicos aplicables, cuando se pretenda conservar en un medio electrónico, óptico o de cualquier otra tecnología, información derivada de un acto de comercio, que se encuentre soportada en un medio físico similar o distinto a aquéllos, los comerciantes podrán optar por migrar dicha información a una forma digital y, observar para su conservación en forma digital, las disposiciones a que se refiere la presente Norma Oficial Mexicana. La migración de la información deberá ser cotejada por un* ***tercero legalmente autorizado,*** *que constatará que dicha migración se realice íntegra e inalterablemente tal y como se generó por primera vez en su forma definitiva. El* ***tercero legalmente autorizado*** *deberá ser una persona física o moral que cuente con la capacidad tecnológica suficiente y cumpla con los requisitos legales aplicables.*
>
> **(Énfasis añadido)**

La transcripción que antecede evidencia que la NOM-151 de referencia no establece ningún procedimiento para efectuar dicha migración, ni aclara el término Tercero Legalmente Autorizado (TLC), lo cual redunda en incertidumbre e indecisión entre los candidatos a usuarios, que puede ser un obstáculo para la aplicación de la norma.

El inconveniente de no definir la figura de TLC, es que estará encargada de cotejar la migración; lo cual trae a colación dos situaciones que se traducen en las siguientes interrogantes: 1) ¿Qué es un Tercero legalmente autorizado? y 2) ¿En qué consiste el cotejo de la migración?

Puede haber dos respuestas a la primera pregunta; una, podría ser considerar que un TLA puede ser cualquier persona capacitada legalmente para dar fe pública: los notarios o corredores públicos.

La otra posible respuesta es que tomando en consideración que el proceso de acreditación para el empleo de la NOM-151 exige que quien desee optar por usarlo debe ser previamente reconocido como Autoridad de Certificación, por lo que ésta podría ser una TLC también, dado que la norma no precisó ningún otro proceso de acreditación.

La conclusión es que son los PSC acreditados para la NOM-151 quienes automáticamente ostentan también dicha calidad. Ello es así porque todo prestador de este tipo cuenta con la acreditación de su responsabilidades profesionales y técnicas y garantizan el cumplimiento de sus obligaciones a través de la suscripción de pólizas de seguro, por lo que dentro de sus funciones se puede aunar la de delegar la función de TLA a través de contrataciones privadas del PSC autorizado, quien será responsable frente al usuario o la propia administración, sin perjuicio de las reclamaciones que a su vez pueda emprender contra dicho tercero que obre incorrectamente.

En suma, creemos que por TLA debe entenderse:

- Los fedatarios Públicos
- Los PSC autorizados para aplicar la NOM-151
- Los terceros que mediante contrato obren por cuenta de los PSC autorizados para la aplicación de la NOM 151 bajo la responsabilidad y garantías de la acreditación de éste.

Por cuanto hace a la segunda interrogante, la relativa a ¿en qué consiste el cotejo de la migración? El TLA se obliga a constatar y comparar que la imagen generada es fiel expresión de su original, esto es, representa la misma calidad, fiabilidad, integridad, volumen y naturaleza del documento primario, que se traduce en el mismo grado de confianza del documento secundario generado al ser equivalente a los dígitos combinados (código binario: 0 o 1) del primer documento.

Debe aclarase que la imagen generada se obtiene de una muestra del documento primario, es decir, no se hace una revisión particular o pormenorizada de todos los documentos ya que esto no es factible, y por ende, el trabajo de cotejo de la migración de un documento debe hacerse bajo estrictos controles de calidad donde la fiabilidad se defina como no pérdida de información, ya que se podría destruir información en papel confiando en que ha sido migrada a una forma digital, lo que dañaría al usuario de la información.

Para resolver el problema de falta de definición de la figura de TLA y de en qué se basa o consiste el cotejo de la migración, se proponen estas alternativas:

a) No expedir normatividad alguna que subsane estas faltas de definición, sino realizar una consulta por parte de una PSC a la SE donde pregunte tales situaciones.
b) Garantizar que el proceso de digitalización sea una imagen fiel del original, donde la calidad de la resolución de la imagen no sea detectable a la vista, como por ejemplo la resolución de imagen de 200 puntos por pulgada (ppp).
c) El TLA tiene la obligación de cotejar que la imagen obtenida de forma individual es un fiel reflejo del original y que en el muestreo efectuado la calidad obtenida, la fiabilidad y la integridad es adecuada al volumen y naturaleza de la información, expresando dicho grado de confianza en términos numéricos así como el porcentaje de la muestra. Para dar su aprobación la calidad y la integridad de la información obtenida deberá ser del 100% en toda la muestra.
d) Emitir una regulación del proceso de digitalización certificada similar a la de la *Orden EHA/962/2007*, de fecha 10 de abril de 2007 del Ministerio de Economía y Hacienda Español así como su *Resolución de 24 de Octubre de 2007*, la cual se basa en un procedimiento de homologación certificado por la Agencia Tributaria Española para él mismo. La Orden garantiza la integridad del documento si es obtenido en un proceso informático automático en el que sin interrupción del mismo y sin intervención en momento alguno de operador se realicen, en el orden indicado, las siguientes tareas:

    - Digitalización de la factura por un medio fotoeléctrico, de modo que se obtenga un fichero en memoria del sistema asociado al dispositivo.
    - Proceso de optimización de esa imagen para garantizar su legibilidad, de modo que todo el contenido del documento original pueda apreciarse y sea válido para su gestión (umbralización, reorientación, eliminación de bordes negros, etc.).
    - Introducir en el fichero de la imagen, como metadatos, la información exigida por la Administración Tributaria que incluye la referencia identificativa de la homologación acordada, una marca de tiempo, así como el nombre y el número de versión del software de digitalización. Para la representación de metadatos, la Agencia Tributaria establece como referencia la especificación estándar denominada XMP (*Extensible Metadata Platform*).

En la práctica garantizar que este proceso sea sin interrupción y sin intervención humana es inviable, aunque las empresas encuentren caminos para acreditarlo en el momento de la homologación, y aun así, que el proceso se realice sin interrupción no garantiza la integridad, pues por ejemplo una desconfiguración del software en un proceso desasistido (como exige la norma) podría producir infinidad de imágenes defectuosas que pasarían desapercibidas.

Ahora bien, la inclusión en forma de metadatos de información concreta, exige pasar previamente un proceso de reconocimiento *óptic*o de caracteres o en inglés *Optical Character Recognition (OCR) y de mapping* de los datos, que serían cambiantes para cada tipo de documento (la Orden solo es válida para facturación, mientras que en México es para todo tipo

de documentos). Como corolario, este proceso español solo garantiza en la captura de la imagen mientras que la NOM-151 garantiza los documentos en forma de constancia, manteniendo inalterado el documento original.

6.3. Nuevos retos del archivo digital.

6.3.1. Soluciones técnicas para el archivo digital.

El éxito esperado respecto a la consagración de la FEA no se presentó en dos aspectos: 1) La aparición del mercado de tecnologías de las FEA que se originaría y con ello falló la materialización de la infraestructura de llave pública; y 2) La comunidad archivística ha desarrollado herramientas y prácticas intelectuales para la comprensión de evidencia documental electrónica pero ésta es básicamente contextual sin tomar en cuenta la comprensión de evidencia documental electrónica en su aspecto físico.

En el entendido de que los comerciantes y las dependencias y entidades de la APF están obligados a la preservación de los registros, y dado que sirven como evidencia a través de su fijación, su preservación envuelve la protección contra dos tipos de amenazas deterioro natural (que es el tema que ahora tratamos) y los intentos de modificar la información de esos registros.

En este sentido, los registros electrónicos enfrentan dos problemas:

a) El deterioro del medio y de la obsolescencia del formato, esto es, el medio óptico o magnético en que se encuentren los documentos electrónicos y MD deben ser periódicamente renovados así como también deben ser migrados los formatos en que están codificados a fin de asegurar que los documentos y MD puedan ser leídos a futuro, independientemente de la obsolescencia del hardware y software.
b) La preservación de la evidencia creada por la FEA, esto es, la conservación de los documentos o MD que acompañan a la FEA y ello evidentemente también aplica a todos los *elementos* necesarios probar el proceso de verificación de la FEA.

Las diferencias entre los documentos electrónicos y los documentos en papel se hacen explícitos a través del ciclo de vida de la FEA, que se divide en cuatro etapas:

I. Creación: La FEA es creada por el signatario y el documento firmado es enviado al destinatario;
II. Verificación inicial: Al recibir el documentos electrónico signado, el destinatario verifica la firma y si tiene éxito, procede a realizar la obligación que le corresponde de acuerdo la negociación;
III. Archivo: el documento y la firma son archivados con miras a su preservación como evidencia potencial de un futuro litigio;
IV. Litigio: Cuando el litigio se suscita, la documentación es presentada como evidencia frente al juez y la FEA es verificada nuevamente, entonces la identidad del signatario y cerciorada la integridad del documento electrónico y/o MD.

Evidentemente, la etapa número cuatro raramente ocurre y la etapa tres tiene como finalidad proveer al anterior de los elementos y pruebas necesarios llegado el caso.

Un número de problemas se presentan por el tiempo que transcurre entre la etapa dos y cuatro. Mientras que el lapso entre el paso uno y dos se puede dar en minutos y acaso días, la verificación de los registros y firma puede ocurrir en años.

Existen tres implicaciones respecto a la preservación de la FEA que deben detallarse[410]:

- **a)** Deterioro de seguridad: Como consecuencia de los avances en seguridad de la información y específicamente, en el área de criptografía, las llaves inicias de la ICP que se usaron para la firma, pueden ser, con el tiempo, vulnerables, y por ende, posibilita que se falsifiquen las firmas.
- **b)** Disponibilidad de software para la verificación: el software compatible para la verificación de las firmas debe permanecer disponible durante todo el ciclo de vida del documento electrónico y/o MD.
- **c)** Interacción entre la verificación de la de la firma y la preservación del documento: las firmas electrónicas avanzadas congelan o paralizan el documento firmado en su estado original, prohibiendo cualquier modificación a la integridad de la cadena de bits.

Esta tercera implicación significa asegurar la inteligibilidad del documento electrónico y/o MD a través del tiempo por medio de la actualización del formato lógico (por ejemplo, por medio de su migración) a fin de que permanezcan compatibles con el software disponible y el hardware necesario para decodificar y reproducirlo en pantalla o en papel.

El gran dilema se presenta en que dicha migración necesariamente invalidará las firmas adjuntas al MD o documento electrónico, es decir, se presentan dos objetivos tecnológicamente incompatibles: o se preserva la legibilidad del MD y/o documento electrónico o el de las firmas electrónicas avanzadas anexas a ellos.

Las implicaciones *a)* y *b)* son problemas que cuentan con tres posibles soluciones técnicas, estas son:

a) Servicios de Archivos de Confianza (SAC) o *Trusted Archival Services* (TAS)
b) Actualización de los sellos de tiempo de la firma o *resignature*
c) Canonización (estandarización o normalización)

[410] Blanchette Jean-François. The digital signature dilemma, Annales des Télécommunications, August 2006, Volume 61, Issue 7-8, p. 915.

5.3.1.1. Servicios de archivos de confianza

El concepto de Servicios de Archivos de Confianza (SAC) fue introducido en el contexto de la Iniciativa de Estandarización del Firma Electrónica Europea[411] (*European Electronic Signature Standardization Initiative (*EESSI por sus siglas en inglés). Un SAC refiere a un nuevo tipo de servicio comercial que puede ser ofrecido por organizaciones de profesionales en archivología emergentes cuya misión es garantizar la integridad a largo plazo de los documentos signados digitalmente, como por ejemplo la *Fédération Nationale des Tiers de Confiance* (FNTC[412]).

Se requiere diversas medidas técnicas a fin de que los servicios de archivo de confianza cumpla las expectativas, tales como: compatibilidad con el hardware y software, ya sea a través de la conservación de los equipos o realizando emulación[413]:

Los SAC deben mantener un conjunto de aplicaciones (lectores y aplicaciones de validación de firmas), sin olvidar las plataformas correspondientes (hardware, sistemas operativos, etc.) o, al menos, un emulador de este tipo de aplicaciones y/o plataformas con el fin de garantizar que el contenido de los documentos todavía se pueda ver y que la firma de estos documentos puedan validarse todavía años más tarde, incluso si la tecnología ya no está disponible en ese momento[414].

Por lo tanto, se propone que para el resolver el problema de la preservación simultánea de los documentos junto con sus firmas, los SAC actúan como museos de información tecnológica o negocios de estrategias de emulación. Esto se debe a que la migración de códigos, que es la estrategia de archivos más simple y aceptada, no está disponible para los documentos firmados digitalmente.

Ninguna institución archivística está considerando el uso de software y hardware original, ni a través de su conservación ni de su emulación, como una solución práctica para la preservación de documentos[415].

6.3.1.2. Actualización de los sellos de tiempo de la firma o *resignature*

A fin de responder a la necesidad de garantizar la integridad a largo plazo de los documentos firmados criptográficamente, EESSI elaboró un *formato de firma electrónica*[416], el cual distingue

[411] European Electronic Signature Standardisation Initiative (EESSI) Expert Team Final report, June 2003, accesible en http://www.ict.etsi.org/Working_Groups/EESSI/Index.htm, consultado 13 de noviembre de 2014.
[412] Véase: www.fntc.org, consultado el 2 de marzo de 2014.
[413] En informática, un emulador es un software que permite ejecutar programas en una plataforma (sea una arquitectura de hardware o un sistema operativo) diferente de aquella para la cual fueron creados. A diferencia de un simulador, que sólo trata de reproducir el comportamiento del programa, un emulador trata de modelar de forma precisa el dispositivo de manera que este funcione como si estuviese siendo usado en el aparato original. Cfr. www.webopedia.com/
[414] Dumortier, Jos, Van Den Eynde, Sofie, Electronic signatures and trusted archival services, in Proceedings of the DLMForum 2002, Barcelona 6-8 May 2002, Luxembourg, Office for Official Publications of the European Communities, 2002, p. 521 y ss., accesible en http://www.law.kuleuven.ac.be/icri, consultado del 4 de noviembre de 2014.
[415] Cfr. IETF, S/MIME Version 3 Message Specification —RFC 2633, Internet Engineering Task Force, 1999.
[416] Pinkas, D., Electronic Signature Formats, European Electronic Signature Standardization Initiative, ETSI TS 101 733 V1.2.2.

entre dos momentos de verificación de firma: la *validación inicial* y *validación tardía (*que corresponden respectivamente a los pasos dos y cuatro del ciclo de vida de la firma digital).

El formato para la *validación tardía* encapsula toda la información que se puede utilizar eventualmente en el proceso de validación, tales como información de revocación, marcas de tiempo, políticas de firma, etc., mientras que la *validación inicial* se utiliza para recopilar esta información con el fin de construir el formato de validación tarde.

Sin embargo, la distinción entre la validación inicial y tardía se basa en un análisis exclusivamente de la amenaza de seguridad de las firmas originadas por la decadencia de la fortaleza criptográfica. Antes de que los algoritmos, claves y otros datos criptográficos utilizados en el momento de la firma digital se debiliten y las funciones criptográficas se vuelvan vulnerables, los MD y los documentos electrónicos firmados deben contener una marca de tiempo. Lo cual se logra al utilizar algoritmos más fuertes o claves más avanzadas que las utilizadas en sello de tiempo original. El proceso de sellado de tiempo se puede repetir cada vez que la protección utilizada para una marca de tiempo anterior firma digital se debilite[417].

Es decir, el principal problema de seguridad que aquí se aborda es la posibilidad de que los avances en el criptoanálisis hagan posible deducir la clave privada de firma originales años después de su creación.

Para protegerse contra esta amenaza de obsolescencia, el formato estandarizado que propone ESSI está diseñado para establecer una marca de tiempo nueva, con algoritmos de firma y tamaños de clave apropiada a los métodos criptográficos con tecnología de última generación.

Lamentablemente, esta solución no aborda el problema de la preservación simultánea de documentos legibles y firmas verificables. De hecho, se agrava aún más, porque encierra la cadena de bits de los documentos electrónicos en una capa más profunda de firmas criptográficas.

6.3.1.3. La canonización (estandarización o normalización)

La canonicalización ofrece una respuesta al deterioro de los formatos de codificación del MD o un documento electrónico que acompaña la firma digital. En 1999 Clifford Lynch propuso la utilización de la canonicalización como estrategia de conservación para la información digital[418]. A partir de este enfoque, *Internet Engineering Task Force* (IETF), en español Grupo de Trabajo de Ingeniería de Internet, desarrolló varias especificaciones para abordar el tema de la preservación a largo plazo de las firmas criptográficas basadas en el uso de formatos canónicos.

---

[417] Library and Archives Canada (LAC), Guidelines For Records Created Under a Public Key Infrastructure Using Encryption and Digital Signatures, Ottawa, Library and Archives Canada, 2001, disponible en http://www.collectionscanada.ca

[418] Lynch, C., Canonicalization: A Fundamental Tool to Facilitate Preservation and Management of Digital Information. D-Lib Magazine, 5(9), 1999, Corporation for National Research Initiatives (CNRI), USA, accesible en http://www.dlib.org/dlib/september99/09lynch.html, consulta: 3 de diciembre de 2014.

La canonicalización o normalización (estandarización) es el proceso de conversión de datos que involucra a más de una representación en un formato estándar aprobado. Tal conversión asegura que los datos se ajusten a las normas canónicas. Esto se compara con diferentes representaciones para asegurar la equivalencia, para contar el número de estructuras de datos distintas, para imponer un orden de clasificación significativa y para mejorar la eficiencia de algoritmos, eliminando así los cálculos repetidos. La representación canónica de los datos se utiliza ampliamente optimización de motores de búsqueda (SEO), servidores web, Unicode y XML.

En materia de conservación de archivos, la canonicalización se refiere al proceso de la traducción de un texto codificado en una versión conforme con alguna definición canónica de la codificación. La utilidad percibida de canonización para firmas digitales se hace evidente en el caso de *Secure/Multipurpose Internet Mail Extensions (S/MIME),* formato creado por la IETF para la mensajería segura que define las distintas estructuras de datos que permiten firmar criptográficamente el texto plano de los mensajes de correo electrónico[419].

Este proceso se enfrenta al problema de que las firmas criptográficas no pueden tolerar ninguna modificación del mensaje original, incluso uno que implica un cambio de caracteres invisibles. Por lo tanto, el estándar S/MIME especifica que cada entidad *Multipurpose Internet Mail Extensions* debe convertirse a una forma canónica que sea representable únicamente y sin ambigüedades en el entorno en el que se creó la firma y el entorno en el que se verificará la firma. La canonicalización más común e importante es la hecha sobre el texto, que se representa a menudo en diferentes entornos[420].

La ventaja de los formatos canónicos es que realizan una migración de formato antes de que ocurra la firma digital, minimizando así el efecto de decadencia del formato lógico, así los documentos que han sido objeto de *canonicalización* son menos susceptibles a las transformaciones sencillas de la formato lógico (como la normalización de espacio en blanco), que invalida inmediatamente las firmas digitales.

6.3.2. Las respuestas de la archivología

Con la concesión de valor probatorio a las firmas digitalmente, las instituciones archivísticas de Estados Unidos, Canadá y Australia han tenido que determinar el tratamiento de los registros firmados criptográficamente. Los principales instituciones nacionales archivísticas que abordan proyectos en este tema son *National Archives and Records Administration* (NARA), *Library and Archives de Canadá*, y *National Archives of Australia* y por lo tanto han emitido directrices que tratan de asesorar a organismos oficiales, de las medidas necesarias para preservar los registros que pueden ser digitalmente firmado y eventualmente puede ser transferido a la custodia de los archiveros.

[419] IETF, S/MIME Version 3 Message Specification, Network Working Group , B. Ramsdell, Editor, Request for Comments: RFC 3851, Obsoletes: RFC 2633, Category: Standards Track , Internet Engineering Task Force, July 2004, p. 1 y 2.
[420] Ibídem, p. 4 – 6.

Asimismo, existe un proyecto de participación mundial denominado *The International Research on Permanent Authentic Records in Electronic Systems* (InterPARES) que tiene como objetivo desarrollar los conocimientos esenciales para la preservación a largo plazo de registros auténticos creados y/o mantenidos en forma digital así como proporcionar la base para las normas, políticas, estrategias y planes de acción capaz de asegurar la longevidad de este tipo de material y la capacidad de sus usuarios de confiar en su autenticidad[421].

La premisa fundamental del proyecto InterPARES y al mismo tiempo su más grande aportación es que la autenticidad no es principalmente una función de la tecnología, sino más bien, de las instituciones. A las instituciones públicas y privadas de archivo históricamente se les ha encomendado la tarea de proporcionar esta función, y siguen siendo las más reconocidas socialmente y apropiadas en organizar profesionalmente las funciones en el entorno electrónico.

Por su parte, México por conducto de la Ley Federal de Archivos (LFA) expedida en enero de 2012, no ha construido las bases de un archivo digital seguro, auténtico e íntegro, en cambio se dirige a establecer que los sujetos obligados (básicamente los tres poderes de la unión y organismos autónomos) deberán elaborar, capturar, organizar y conservar los documentos de archivo electrónico procedentes de los diferentes sistemas del sujeto obligado. Luego en el segundo párrafo del artículo 20 de esa Ley establece que en la preservación de archivos electrónicos en el largo plazo se deberá contar con la funcionalidad de un sistema de preservación en el largo plazo, el cual deberá cumplir las especificaciones que para ello se emitan. Y que cuando los sujetos obligados hayan desarrollado o adquirido herramientas informáticas de gestión y control para la organización y conservación de documentos de archivo, deberán ser adecuadas a los lineamientos a que se refiere el artículo anterior.

Mientras que en su artículo 21 siguiente dispone que el Archivo General de la Nación (AGN), en coordinación con el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) y SFP, emitirá *Lineamientos para la creación y funcionamiento de los sistemas que permitan la organización y conservación de la información de los archivos administrativos del Poder Ejecutivo Federal* de forma completa y actualizada, a fin de publicar aquélla relativa a los indicadores de gestión, ejercicio de los recursos públicos y con alto valor para la sociedad. Finalmente, añade que la autoridad que establezca las disposiciones secundarias aplicables a los sujetos obligados distintos del Poder Ejecutivo Federal deberá emitir los lineamientos que señala el presente artículo, de conformidad con las directrices que para tal efecto emita el Consejo Nacional de Archivos (CNA).

6.4. Reconoer el valor de la interoperabilidad técnica, semántica y sintáctica.

[421] The International Research on Permanent Authentic Records in Electronic Systems (InterPARES), InterPARES Project 1, 2 y 3; School of Library, Archival and Information Studies at The University of British Columbia & British Columbia, Canada, accesible en:http://www.interpares.org/, consultado el 2 de noviembre de 2014.

Prescindir de la interoperabilidad en la FEA y de los certificados digitales tiene varias consecuencias. Respecto a la primera, esto es, sobre el conjunto de estándares relacionadas para la cualificación de FEA basada en ICP, es claro que el progreso se ve dificultado cuando solo puede ser usada un tipo de tecnología de FEA en el mercado, no obstante, también es cierto que México no es sujeto activo en la creación de innovación de tecnologías de seguridad de la información así como de firmas electrónicas y digitales.

La falta de interoperabilidad en los elementos objetivos del comercio electrónico a nivel nacional e internacional es un gran obstáculo para el crecimiento del mercado y la proliferación de la FEA. Particularmente, los mercados de los PSC existente como islas de suscripción y certificación de firmas electrónicas, donde la certificación otorgada por una autoridad de certificación sólo puede ser usada para una aplicación aislada. [422]

El beneficio de que se determinen principios, criterios comunes para el desarrollo o adopción de políticas de FEA e instrumentos vinculados tales como formatos, uso de algoritmos, creación y validación de firma para documentos electrónicos, así como reglas de confianza en certificados electrónicos, sellos de tiempo y firmas longevas, incrementan la eficiencia operativa de la FEA y los certificados digitales, no sólo en el sector de la administración pública, sino también en el sector comercial[423].

Cuando se busca la interoperabilidad en la FEA e instrumentos que se vinculan a ella (certificados, sellos, archivos digitales) se están alineando políticas de acuerdo a las tendencias a nivel nacional e internacional, de tal forma que se establecen requisitos mínimos para el tratamiento nacional y transfronterizo de los documentos firmados electrónicamente por las autoridades competentes, lo que deviene en la generación de confianza en el comercio electrónico.

La interoperabilidad implica que se toman en consideración un conjunto de normas de seguridad, de organización, técnicas y legales para determinar cómo se generan, verifican y gestionan firmas electrónicas, incluyendo las características exigibles a los certificados de firma.

Para lograrlo, la SE, quien regula las actividades propias del comercio, y por ello, el uso de la FEA en el contexto mercantil, podría fomentarla, lo que en definitiva ayudaría a la gestión de la evidencia digital.

En nuestro país, el gobierno federal considera la interoperabilidad[424] como un habilitador que se refiere a la armonización del marco jurídico con la finalidad de propiciar un entorno de certeza y confianza favorables para la adopción y fomento de las TIC, cuyo impacto puede ir

[422] Cfr. Dumortier, J., Kelm, S., Nilsson, H., Skouma, G., Van Eecke, P., "The Legal and Market Aspects of Electronic Signatures", Datenschutz und Datensichering, 2004, n° 3, p. 143.
[423] En este sentido el Gobierno Federal ya recibido beneficios con la expedición del Acuerdo por el que se establece el Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal del 6 de septiembre de 2011.
[424] Gobierno Federal de la República Mexicana, Estrategia Digital Nacional, Coordinación de Estrategia Digital Nacional, noviembre de 2013, p. 28 a 30.

desde la economía digital hasta el gobierno digital. De ahí la necesidad de considerar la interoperabilidad como un área de acción a implementar en el comercio electrónico.

Ahora bien, se entiende por interoperabilidad es: *la capacidad de los equipos de diferentes fabricantes (o sistemas) para comunicarse entre sí en la misma infraestructura (o sistema) o en otro en itinerancia*[425].

Mientras que Third Generation Partnership Project (3GPP) la define como la capacidad de dos o más sistemas o componentes para intercambiar datos e usar información[426] La interoperabilidad técnica se asocia generalmente con el hardware/software componentes, sistemas y plataformas que permiten de máquina a máquina la comunicación. Este tipo de interoperabilidad a menudo se centra en la comunicación de protocolos y la infraestructura necesaria para operar a través de protocolos.

Dentro de esta interoperabilidad existen diferentes categorías, por ejemplo: la interoperabilidad técnica, la interoperabilidad sintáctica, semántica, la interoperabilidad y la interoperabilidad organizativa, e independientemente de que aquí solo nos referimos a la interoperabilidad técnica y mencionamos los diferentes tipos de interoperabilidad, porque el término interoperabilidad la mayoría de las veces se utiliza para denominar a cualquier tipo de interoperabilidad (técnica, sintáctica y semántica), excepto a la interoperabilidad organizativa.

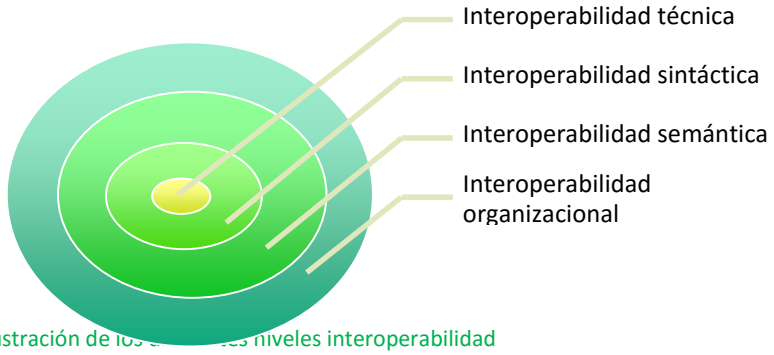


Ilustración de los [illegible] niveles interoperabilidad

El primer tipo de interoperabilidad es la técnica, ya definida con anterioridad, mientras que el segundo tipo es la *interoperabilidad sintáctica,* la cual se asocia generalmente con los formatos de datos. Ciertamente, los mensajes transferidos por los protocolos de comunicación deben tener bien definida una sintaxis y codificación, incluso si es sólo en la forma de bits tablas. Sin embargo, muchos protocolos transportan datos o contenidos, y esto se pueden representar mediante la transferencia de alto nivel de sintaxis como HTML, ASN.1 o XML.

[425] ETSI's Technical Committee TISPAN, Interoperability of Next Generation Networks (NGN), European Telecommunications Standards Institute (ETSI), accesible en: http://www.etsi.org/technologies-clusters/technologies/next-generation-networks, consultado 5 de noviembre de 2014.

[426] El 3rd Generation Partnership Project (3GPP) congrega a siete organizaciones de telecomunicaciones para el desarrollo estándares (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC). El desarrollo de sus especificaciones es de aplicación mundial en las comunicaciones móviles de 3ª generación, accesible en: www.3gpp.org/, consulta 6 de noviembre de 2014,

En tanto que la *interoperabilidad semántica* se asocia generalmente con el significado del contenido y se refiere a la interpretación humana. Por lo tanto, interoperabilidad en este nivel significa que hay un entendimiento común entre la gente respecto del significado del contenido o información que se intercambian.

Finalmente, la *interoperabilidad organizativa**,*** como su nombre lo indica, es la capacidad de las organizaciones para comunicarse con eficacia en la transferencia de datos (significativos) a pesar de que pueden estar usando una variedad de diferentes sistemas de información sobre muy diferentes infraestructuras, posiblemente a través de diferentes regiones y culturas geográficas. La interoperabilidad organizacional depende del éxito de la interoperabilidad técnica, sintáctica y semántica.

Para hacer que los servicios digitales del comercio electrónico sean interoperables primero es menester detectar los síntomas típicos que evidencian que no existe tal interoperabilidad, el ejemplo tradicional es cuando entre dos o más sistemas de comunicación algo *no funciona (como se esperaba).*

El *como se esperaba* es importante aquí porque a veces los sistemas funcionan exactamente como los estándares señalan pero están siendo utilizados para tareas para las que nunca fueron diseñado y posteriormente ya no funcionan bien. Si las normas se adaptan o se utilizan más allá de su contexto original, entonces es importante que las consecuencias para interoperabilidad se hayan comprendido y abordado. Esto es especialmente pertinente en el entorno de la normalización de múltiples organizaciones.

En términos de ingeniería, la falta de interoperabilidad se puede ejemplificar con la incapacidad de los auriculares inalámbricos habilitados que no permiten hablar desde la computadora portátil, o un componente de red que se convierte en un punto muerto durante una descarga de algún documento. En este mismo ejemplo, supongamos que el protocolo que se fijó se definió pero no especifica claramente algún aspecto del formato o contenido de los mensajes que se intercambian. Estas ambigüedades pueden variar de lo muy pequeño (a nivel de bit) a mayores (secciones completas de los mensajes) como sucede en las retransmisiones que si se repite muchas veces por un gran número de usuarios que trabajan sobre un ancho de banda limitado derivaría en retrasos en el acceso de los usuarios[427].

Los estándares son impulsados por las contribuciones de muchos individuos a partir de una amplia gama de orígenes, culturas y posiciones comerciales. En la práctica, a menudo no hay suficientes recursos para integrar las diversas contribuciones en un todo coherente consistente; por ello, se debe atender a las razones por las que un estándar puede no ser interoperable,[428] tales como:

[427] Van Der Veer, Hans y Wiles, Anthony. Achieving Technical Interoperability the European Telecommunications Standards Institute (ETSI) Approach, 3rd edition, Abril 2008, France, p. 5 y ss., accesible en http://www.etsi.org/WebSite/document/whitepapers/IOP%20whitepaper%20Edition%203%20final.pdf

[428] Íbidem, p.10.

a) **Está incompleto:** a menudo las especificaciones están incompletos (aunque no intencionadamente), aspectos esenciales para la interoperabilidad no están presentes o se especifican sólo parcialmente.
b) **Hay interfaces inadecuadas**: Las interfaces están mal consignadas o no están claramente definidas.
c) **Hay mal manejo de opciones:** Un estándar puede contener demasiadas opciones, o las opciones están mal especificados. Por ejemplo, puede haber una imprecisa comprensión de las consecuencias si no se implementan ciertas opciones. Peor aún, puede haber inconsistencias - incluso contradicciones – entre varias opciones;
d) **Hay falta de claridad:** No hay distinción al escribir un estándar, el cual debe incluir los siguiente:
   • Estar bien estructurado;
   • Distinguir entre lo que debe ser estandarizado y lo que no se debe;
   • No conceptos mezclados;
   • No especificar la misma cosa de diferentes maneras;
   • No ser confuso;
   • No ser demasiado prolijo;
   • No usar demasiada criptología.
e) **Mantenimiento deficiente**: La falta de control de versiones, indicaciones poco claras de los requisitos (obligatorios y opcionales) cubiertos por un seguro procedimientos de liberación de una norma, y solicitar el cambio laxa pueden tener un impacto negativo sobre la interoperabilidad.

Estándares incompletos y poco claros con limitadas opciones de especificación pueden contribuir a la principal causa de falta de interoperabilidad, es decir, que el implementador se ve obligado a tomar decisiones de diseño en partes críticas del sistema basado en una falta de información.

Los ejemplos anteriores por falta de interoperabilidad son bastante básicos y por lo general se pueden evitar con normas sencillas y autónomas. Sin embargo, se está convirtiendo cada vez más común para los sistemas complejos que se advierten por islas de las normas.

Las presiones comerciales prohíben especificaciones hasta el más mínimo detalle, ya sea por falta de recursos o por el deseo de dejar ciertos temas abiertos, pues se considera demasiado tiempo y es demasiado caro estandarizar la totalidad sistema. En un sistema complejo, los problemas de interoperabilidad pueden tener efectos impredecibles que posiblemente parecen muy alejados de la causa original y que puede ser muy difícil de rastrear. Estos problemas se agravan cuando ya no hay una sola fuente para las diferentes normas, sino que las normas provienen de una variedad de organismos de normalización, cada uno con su particular manera de hacer las cosas, esto es, se trata de una estandarización multiorganizacional, donde existen diferentes islas de normas con diferentes propietarios.

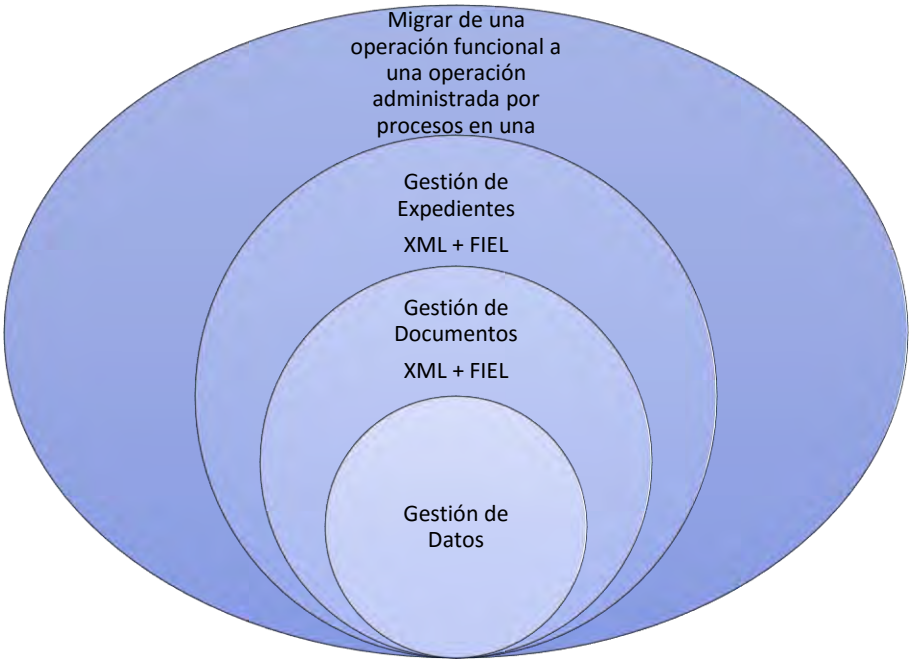
Existen varias características de por qué los productos sobre la base de algunos estándares no pueden interoperar:

a) **La falta de visión general del sistema**: en un contexto multiestándar la combinación de normas y las opciones proporcionadas por esas normas, si no está bien especificada y claramente con referencias cruzadas, puede prevenir el implementador de tener una clara visión general del sistema.
b) **El uso de normas más allá de sus propósitos originales**: cada vez es más común reutilizar normas desarrolladas en un contexto que no toma en cuenta el que se está realizando. Una norma de buena ingeniería será lo suficientemente robusta y flexible para hacer la transición. Pero en muchos casos los cambios o adiciones a la original altera la interoperabilidad. Los riesgos de que esto ocurra se puede reducir si esos cambios se hacen de una manera considerada y bien planificada: lamentablemente esto no siempre es el caso ya que las cosas se hacen a menudo de una manera ad-hoc.
c) **La variación de la calidad**: cada organización de estándares tiene sus propias reglas y cultura en cómo una norma está escrita, presentada y en el nivel de calidad técnica, lo que es confuso para los ejecutores de esas normas.

Creemos que es importante que se cree un Instituto Mexicano de Estándares de Telecomunicaciones, quien podría depender el Instituto Federal de Telecomunicaciones (IFT) o bien, ser un órgano creado con recursos gubernamentales, cuyo objetivo sea asegurar la producción de normas interoperables y actividades de normalización, especialmente en el contexto multiorganizacional y que señale que organizaciones son las adecuadas para certificar determinado tipo de especificaciones.

Finalmente, para lograr la interoperabilidad de los trámites gubernamentales digitales se requiere que los documentos digitales se encuentren alineados por lo menos en tres puntos:

a) Estar codificados en un lenguaje universal, no propietario (de uso libre) como lo es el lenguaje XML, el cual cuenta con estandarización en su estructura y es accesible a todos los usuarios. La estructura de codificación de XML son los archivos XSD que publica el gobierno en el DOF.
b) Los documentos digitales deben presentar una seguridad que garanticen su confiabilidad, veracidad, integridad y autoría a través de la firma electrónica, el sello digital y el timbre electrónico, este último estampado por un certificador autorizado. Todos estos elementos de seguridad son generados mediante unan infraestructura de llave pública (PKI) la cual está basada en la generación y administración de certificados digitales expedidos a todos los actores firmantes de documentos digitales.
c) Considerar una regulación armonizada y homogénea en el ámbito federal sobre el tema de los documentos digitales.
d) Utilizar TCP/IP (Protocolos de transmisión Internet).
e) Utilizar la interoperabilidad de servicios web (*Web Services Interoperability: WS-I)* sobre cualquier plataforma, aplicación y lenguaje de programación, a fin de integrar los estándares para ayudar al avance de los servicios web de una manera estructurada y coherente. Un ejemplo es la Arquitectura Orientada a Servicios (*SOA*) se muestra en la siguiente figura.



Para la interoperabilidad de los trámites gubernamentales digitales se requiere que los documentos digitales se encuentren alineados mínimo con dos puntos:

1. Estar codificados en un lenguaje universal, no propietario (de uso libre), con estandarización en su estructura y accesible a todos los actores. Este lenguaje es el XML. La estructura de los documentos codificados en XML se describe en archivos XSD los cuales deben ser publicados en el Diario Oficial por las autoridades y dependencias competentes en cada caso.
2. Contar con elementos de seguridad que garanticen su confiabilidad y veracidad. Los elementos de seguridad que garantizan la integridad y autoría de documentos digitales son la firma electrónica, el sello digital y el timbre electrónico, este último estampado por un certificador autorizado. Todos estos elementos de seguridad son generados mediante unan infraestructura de llave pública (PKI) la cual está basada en la generación y administración de certificados digitales expedidos a todos los actores firmantes de documentos digitales.

6.5. Tratamiento de la evidencia digital y la carga de la prueba.

Actualmente existen miles de fuentes de datos digitales, tales como los registros de las computadoras que se encuentran en el hogar, los respaldos de datos que realizan las empresas u organizaciones, los registros de un celular, los localizadores satelitales que registran la ruta de transportes, los registros de las cámaras instaladas en cualquier lugar para lograr una vigilancia segura, entre otros.

Para complicar la situación, estos datos archivados son general y rápidamente sobrescritos (*overwritten*) y no se hace ningún esfuerzo por preservarlos. En este sentido, la mayoría de los datos pueden ser obtenidos y procesados con la ayuda de hábiles técnicos a los que se les tendrá que pagar por sus servicios y, provocando que el descubrimiento digital (*electronic discovery and digital evidence*) devenga costoso y difícil.

Uno de los primeros autores que se enfocó en el registro de la evidencia digital y la administración o gestión de registros es David Brearman[429], quien define la evidencia digital como:

> *El conjunto de datos (por ejemplo los registro de palabras, números, imágenes y sonidos en realidad hechos por el creador), estructura (por ejemplo las relaciones entre cómo son empleados esos datos por el creador de registro para transmitir un significado), y el contexto (por ejemplo la relación entre los registros y la actividad de la que surgió).*

Ahora bien, existen varios tipos de evidencia digital que se deben de considerar en toda investigación digital[430]:

> *a) Los registros que son primero creados electrónicamente y existen en un formato digital; y*
> *b) Los registros electrónicos que originalmente fueron elaborados en papel y luego fueron escaneados o convertidos en un formato electrónico para facilitar su análisis, su despliegue y/o visualización ante el juez.*

Cuando el juez norteamericano Frank Easterbrook satirizó los esfuerzos por desarrollar una ley especial llamada la "ley de ciberespacio" argumentó que tales esfuerzos eran tan similares como crear la "ley de los caballos", pues en ese entonces se argumentaba que la evidencia digital debía recibir el mismo trato que cualquier tipo de evidencia[431]. A nadie le gusta el riesgo de crear nuevas reglas de descubrimiento de evidencia para el entorno virtual, pero lo cierto es que actualmente se requiere prestar atención a las variadas posibilidades de descubrimiento de evidencia en soporte material y la que se realiza en soporte digital.

Richard L. Marcus[432] estableció las diferencias más plausibles que existen entre el descubrimiento de evidencia en soporte material y digital, ellas son:

a) Las computadoras pueden reducir la carga de buscar entre materiales voluminosos.
b) Material electrónicamente almacenado contiene información que no siempre se incluye en documentos que obran soporte material o papel.
c) Los datos electrónicos pueden contener comentarios negligentes o descuidados que son más reveladores que los datos que se encuentran en soporte material o papel.
d) Los datos electrónicos pueden ser más duraderos que los que se encuentran en papel.

---

[429] Bearman, David. Archival Principles and the Electronic Office, in Electronic Evidence, p. 147.
[430] Calloway, Jim. What is electronic evidence, in Family Advocate, Vol. 28, No. 3, winter 2006, p.8.
[431] Easterbrook, Frank H. Cyberspace and the Law of the Horse, 1996 University of Chicago Legal Forum 207, p. 207- 216
[432] Marcus, Richard L. Confronting the future: Coping with discovery of electronic material, Law and Contemporary Problems, Vol. 64, No. 2/3, Complex Litigation at the Millennium (Spring - Summer, 2001), Duke University School of Law pp. 253-281

e) La búsqueda de material electrónico puede requerir buscar en muchos lugares adicionales.
f) Los problemas de preservación y despojo de datos y documentos digitales pueden multiplicarse.
g) La inspección de un sitio digital puede ser mucho más importante.
h) Expertos pueden no ser necesitados para el descubrimiento de evidencia digital.
i) El descubrimiento de evidencia digital puede ser mucho más intrusivo.
j) Las cargas de descubrir evidencia digital pueden propagarse de manera más uniforme, puedes ahora se presenta un balance entre la enorme cantidad de información que puede recoger de un empleado, la empresa y el equilibrio que tiene que haber con respecto a su privacidad.
k) El descubrimiento de evidencia digital y los desarrollos relacionados pueden alterar el modo de litigar.

6.5.1. Tipos, procesamiento y resguardo de evidencia digital.

Matthew Braid, el ex oficial australiano del *Equipo de Respuesta ante Emergencias Informáticas (CERT, del inglés Computer Emergency Response Team)* y analista de seguridad de la información estableció cinco reglas de la evidencia que deben ser tomadas en cuenta para un análisis de la evidencia digital:

I. Admisible,
II. Auténtica,
III. Completa,
IV. Fiable, y
V. Creíble.

Para utilizar estas cinco reglas relativas a la evidencia, Timothy E. Wright conjuntamente con Matthew Braid respectivamente establecieron doce pasos que se deben seguir.[433]

I. Minimizar la manipulación y la corrupción de datos originales.
Una vez que haya creado una copia maestra de los datos originales, no se debe tocar el original mismo, siempre se deben manejar copias secundarias. Los cambios realizados en los originales afectarán los resultados de cualquier análisis posterior realizado en las copias. Además se debe asegurar que no se quede ningún programa que modifique los tiempos de acceso de todos los archivos (como *tar* y *xcopy*), eliminar cualquier posible vía de cambio externo y, en general, se debe analizar la evidencia después de que ha sido recogida.

[433] Cfr. Braid, Matthew. Collecting Electronic Evidence After a System Compromise, Computer Emergency Response Team (CERT) in Australia (AusCERT) 2001, accesible en http://www.auscert.org.au/Information/Auscert_info/Papers/Collecting_Evidence_After_A_System_Compromise.html, consultado de 1 de noviembre de 2014, p. 5 y ss. Ver también: Wright, Timothy E. "The Field Guide for Investigating Computer Crime: Search and Seizure Basics (Part 3)" 28 July 2000, accesible en: http://www.symantec.com/connect/articles/field-guide-part-three, consultado el 3 de octubre de 2015.

II. Considerar cualquier cambio y mantener registros detallados de las acciones.
A veces la alteración evidencia es inevitable. En estos casos es absolutamente esencial que la naturaleza, el alcance y los motivos de los cambios sean documentados. Todo cambio debe contabilizarse, no sólo la alteración de datos, sino también la alteración física de los originales (por ejemplo la eliminación de componentes de hardware).

III. Cumplir con las cinco reglas de evidencia
Las cinco reglas (I. admisible, II. auténtica, III. completa, IV. fiable, y V. creíble) existen por una razón y si no se siguen es probable que se pierda tiempo y dinero. Son esenciales para garantizar la recopilación de pruebas con éxito.

IV. No exceder el conocimiento propio. Si no entiende bien lo que está haciendo, será más difícil para dar cuenta de los cambios que realice y puede que no ser capaz de describir qué es exactamente lo que hizo o hará. Si se encuentra fuera de su especialidad y cuenta con tiempo disponible la opción es conocer e investigar más antes de continuar, o bien buscar a alguien más que conozca el tema. La norma es nunca avanzar solo de otra forma se acabara dañando el caso.

V. Seguir las políticas de seguridad local y obtener un permiso escrito.
Durante el curso de su investigación se debe pedir al acceso a la evidencia a fin de copiar datos sensibles u obtener declaraciones de los usuarios del sistema como a los empleados. Antes de iniciar la investigación, es importante asegurarse de obtener por escrito y firmado un permiso para tener instrucciones claras sobre el alcance de la investigación.

Sin una autoridad clara para proceder, las acciones realizadas pueden ser, o ser percibidas como una violación de las políticas de seguridad de la organización y puede ser sujeto de responsabilidad. En caso de duda, hay que consultar con los encargados o personal que conozca las facultades y responsabilidades de cada uno de los empleados, incluso, solicite la obtención de la asesoría legal necesaria.

También se recomienda que la organización desarrolle políticas apropiadas y procedimientos de recogida de pruebas electrónicas para que estén en su lugar antes de la un incidente ocurrido, las cuales alinearan el proceso y ahorro de tiempo valioso antes de las pruebas.

VI. Capturar de forma precisa una imagen del sistema.
Esto se relaciona con el primer punto, se trata de capturar las diferencias entre el sistema original y para conocer en qué cambiaron los datos; y por ende, se debe ser capaz de dar cuenta de la diferencias.

VII. Prepararse para testificar
Si no se está dispuesto a declarar sobre las pruebas que se han recogido, es mejor detenerse antes de empezar a trabajar. No contar con una persona recolectora de la evidencia que valide los documentos creados durante la recopilación de pruebas proceso es tanto como contar con

un testimonio de oídas e inadmisible. Se tiene que tener presente que puede testificar en un momento posterior.

VIII. Asegurarse de que las acciones son repetibles
Nadie va a creer en la evidencia se no se pueden replicar las acciones o si no se llega a los mismos resultados en una demostración.

IX. Trabajar rápido
Cuanto más rápido se trabaja, menos probable es que los datos vayan a cambiar. Las pruebas volátiles pueden desaparecer por completo si no se recogen a tiempo y eso no quiere decir que debe apresurarse todo, todavía se tiene que recoger datos precisos y mantener un registro de sus acciones sobre la marcha. Si varios sistemas están involucrados, se debe trabajar en ellos en paralelo (un equipo de investigadores sería muy útil en este punto), pero cada sistema debe trabajarse en forma metódica. La automatización de ciertas tareas hace que la recolección proceder aún más rápido.

X. Proceder de evidencia volátil a persistente
Algunas pruebas electrónicas son más volátiles que otras; debido a esto, siempre debe tratarse de recoger en primer término la evidencia más volátil.

XI. No apagar un sistema antes de recolectar la evidencia
Nunca se debe apagar un sistema antes de recolectar la evidencia, pues no sólo perderá la evidencia volátil sino que también un atacante pudo haber instalado al inicio un software malicioso (troyanos) o un apagado de scripts. Los dispositivos *plug-and-play* pueden alterar o borrar el sistema configuración y sistemas de archivos temporales. El reinicio es aún peor, ya que puede resultar en la pérdida de más pruebas y debe evitarse a toda costa. Como regla general, hasta que se acabe con el disco comprometido y se acabe con la restitución del disco, nunca debe utilizarse como disco de arranque.

XII. No ejecutar ningún programa en el sistema afectado
Dado que el atacante puede haber dejado programas y bibliotecas de troyanos en el sistema, sin darse cuenta puede desencadenar algo que podría cambiar o destruir la evidencia buscada. Cualquier programa que utilice deberá estar en modo de lectura de medios de comunicación (como un CD-ROM o un disquete protegido contra escritura) y debe ser enlazado estáticamente.

6.5.1.1. Evidencia volátil.

No todas las pruebas en un sistema durarán largos períodos de tiempo. La duración de algunas evidencias reside en el almacenamiento (es decir, la memoria volátil) sólo mientras hay una fuente de alimentación consistente; mientras que otras evidencias almacenadas estarán cambiando continuamente. Cuando se recolectan las pruebas siempre se debe proceder de lo más volátil a lo menos volátil y, de los sistemas o máquinas más críticas a las menos, por ejemplo, no se debe perder tiempo en extraer o examinar información de una memoria

principal de una máquina sin importancia cuando existe una memoria secundaria de una máquina de gran importancia[434].

Para determinar qué pruebas recoger primero, se debe elaborar una *orden de volatilidad*, esto es, una lista de fuentes de pruebas clasificadas por la volatilidad relativa. Un ejemplo *orden de volatilidad* que precisó el mismo Matthew Braid podría ser[435]:

I. Registros y *caché*
II. Tablas de enrutamiento
III. *Arp caché*[436]
IV. Tabla de Procesos
V. Estadísticas del *kernel*
VI. Memoria Principal
VII. Sistemas de archivos temporales
VIII. Memoria Secundaria
IX. Configuración de módulos del enrutador
X. Topología de red

Una vez recogidos los datos en bruto procedentes de fuentes volátiles se puede apagar el sistema.

6.5.2. Procedimientos para recoger y analizar la evidencia digital

El procedimiento para recoger y analizar la evidencia no son simples etapas o pasos a seguir, lo que se presenta a continuación es un esquema genérico que es necesario personalizar con pasos para adaptarse a determinada situación.[437]

[434] Braid, Matthew. Collecting Electronic Evidence After a System Compromise, Computer Emergency Response Team (CERT) in Australia (AusCERT) 2001, accesible en http://www.auscert.org.au/Information/Auscert_info/Papers/Collecting_Evidence_After_A_System_Compromise.html, consultado de 1 de noviembre de 2014, pp. 7-9.

[435] Para más información sobre el tema ver: federal judicial center. The manual for complex litigation, usa, 4ª ed., 2004, pp. 300-380.

[436] En red de computadoras, el protocolo de resolución de direcciones (ARP, del inglés Address Resolution Protocol) es un protocolo de comunicaciones de la capa de enlace de datos, responsable de encontrar la dirección de hardware (Ethernet MAC) que corresponde a una determinada dirección IP. Para ello se envía un paquete a la dirección de difusión de la red que contiene la dirección IP por la que se pregunta, y se espera a que esa máquina u otra responda con la dirección Ethernet que le corresponde. Cada máquina mantiene una caché con las direcciones traducidas para reducir el retardo y la carga. ARP permite a la dirección de Internet ser independiente de la dirección Ethernet. Ver: Wikipedia, voz: "Protocolo de resolución de direcciones (ARP)" accesible en: https://es.wikipedia.org/wiki/Protocolo_de_resoluci%C3%B3n_de_direcciones, consultada el 12 de mayo de 2015.

[437] Wright, Timothy E. "The Field Guide for Investigating Computer Crime, Part 7: information Discovery - Basics and Planning" 26 February 2001, accesible en: http://www.symantec.com/connect/articles/field-guide-part-seven, consultado el 3 de octubre de 2015. En el mismo sentido ver Braid, Matthew. Collecting Electronic Evidence After a System Compromise, Computer Emergency Response Team (CERT) in Australia (AusCERT) 2001, accesible en http://www.auscert.org.au/Information/Auscert_info/Papers/Collecting_Evidence_After_A_System_Compromise.html, consultado el 1 de noviembre de 2014, p. 6 y ss.

a) Identificación de Evidencia: Se debe ser capaz de distinguir entre los datos de las pruebas y de la chatarra. Para este propósito se debe saber cuáles son los datos, dónde están y cómo se almacenan así como ser capaz de determinar la mejor manera de recuperar y almacenar cualquier evidencia encontrada.

b) Preservación de Evidencia. La evidencia encontrada se debe preservar lo más cerca posible a su estado original. Cualquier cambio realizado durante esta fase debe ser documentado y justificado.

c) Análisis de Evidencia. La evidencia almacenada debe ser analizada para extraer la información pertinente y recrear la cadena de acontecimientos. Se debe asegurar siempre que las personas que están analizando las pruebas son totalmente calificadas para hacerlo.

d) Presentación de Evidencia. Comunicar el significado de la evidencia es de vital importancia, de lo contrario no se puede hacer nada con ella. Debe ser técnicamente correcta, creíble y fácilmente comprendida por personas que no son técnicas.

e) Archivo y colección. Una vez que se ha desarrollado un plan de ataque e identificada la evidencia a recabar, es el momento de empezar a capturar los datos. El almacenamiento de datos también es importante, ya que puede afectar el cómo se percibe la información.

f) Registros (*log and logging*[438]). Se debe estar ejecutando algún tipo de función de registro del sistema. Es importante mantener señales o rastros de registros seguros y que los respalde periódicamente. Dado que los registros son generalmente fechados automáticamente una copia simple debería ser suficiente, aunque debe **firmar digitalmente y cifrar los registros** que son importantes para protegerlos de la contaminación. Los registros que se guardan localmente en el sistema afectado son susceptibles a la alteración o eliminación por un atacante.

Tener un servidor *syslog*[439] remoto y almacenar registros en un directorio adjunto o alternativo puede reducir este riesgo, a pesar de que aún es posible que un atacante para agregar entradas falsas o basura en los registros. Las auditorías periódicas y la contabilidad de un sistema son útiles no sólo para la detección de intrusos, sino también como un medio de prueba. Los mensajes y los registros de los programas como *Tripwire*[440] pueden ser utilizados para mostrar

[438] Logging o historial designa la grabación secuencial de un archivo o base de datos, de todos los acontecimientos que afectan un proceso particular (aplicación, actividad de una red informática...). El término log designa al archivo que contiene estas grabaciones, generalmente fechadas y clasificadas por orden cronológico, estos últimos permiten analizar paso a paso la actividad interna del proceso y sus interacciones con su medio. Ver voz: "Logging": accesible en: https://en.wikipedia.org/wiki/Logfile, consultada el 22 de mayo de 2015.

[439] Es un estándar de facto para el envío de mensajes de registro en una red informática IP. Por syslog se conoce tanto al protocolo de red como a la aplicación o biblioteca que envía los mensajes de registro. Un mensaje de registro suele tener información sobre la seguridad del sistema, aunque puede contener cualquier información. Junto con cada mensaje se incluye la fecha y hora del envío.

[440] Es un programa de computadora consistente en una herramienta de seguridad e integridad de datos que es útil para monitorizar y alertar de cambios en los ficheros de un sistema de ficheros. Funciona cotejando la firma digital de archivos y directorios contra una base de datos de los mismos en un instante previo.

lo que hizo un atacante. Por supuesto, usted necesita una limpia instantánea para éstos a los trabajos[441].

g) Monitoreo. Monitorear el tráfico de la red puede ser útil por muchas razones, se pueden recopilar estadísticas, atento a la actividad irregular (y posiblemente detener una intrusión antes de que suceda) y rastrear donde un atacante entra y lo que hacen; también se pueden recopilar registros de vigilancia, ya que se crean pueden mostrar información importante que podría posteriormente ser eliminada por el atacante. Esto no significa que la revisión de los registros después no vale la pena, puede ser que la falta de registros cree sospecha.

La información recopilada mientras que el tráfico de la red es monitoreada puede ser compilada en las estadísticas para definir un comportamiento normal para su sistema. Estas estadísticas se pueden utilizar como una advertencia temprana de la presencia y las acciones de un atacante.

También se puede supervisar las acciones de sus usuarios. Esto puede usarse como una de las primeras alertas del sistema, como los intentos fallidos para hacer su a *root* o la aparición repentina de usuarios desconocidos que amerita una inspección más cercana. No importa el tipo de monitoreo hecho, se debe tener mucho cuidado con transgredir leyes que podría no conocer. El monitoreo se debe limitar al tráfico o la información del usuario y dejar el contenido sin monitorear a menos que la situación lo haga necesario. También se debe mostrar una advertencia que indique que se está monitoreando cuando los usuarios inician sesión.

h) Métodos de Colección. Hay dos formas básicas de recolección: la "congelar la escena" y *honeypotting*[442] y las dos no se excluyen una a la otra, se puede obtener información congelada después o durante cualquier honeypotting. La congelación de la escena consiste en tomar una instantánea del sistema en su estado comprometida. Las autoridades necesarias deben ser notificados (por ejemplo, la policía, los equipos de incidencia de respuesta).

A continuación, se deben recopilar todos los datos importantes como la evidencia no volátil extraíble de medios de comunicación en un formato estándar y asegurarse de que los programas y utilidades utilizados para recoger los datos también se recojan en los mismos medios que los datos. Todos los datos recogidos debe tener un mensaje criptográfico digerido y los resúmenes deben compararse con el original para su verificación.

[441] Cfr. WRIGHT, Timothy E. "The Field Guide for Investigating Computer Crime, Part 6: Search and Seizure - Evidence Retrieval and Processing" 8 January 2000, accesible en: http://www.symantec.com/connect/articles/field-guide-part-six, consultado el 3 de octubre de 2015.

[442] Un honeypot o equipo trampa, es un software o conjunto de computadores cuya intención es atraer a atacantes, simulando ser sistemas vulnerables o débiles a los ataques. Es una herramienta de seguridad informática utilizada para recoger información sobre los atacantes y sus técnicas. Los honeypots pueden distraer a los atacantes de las máquinas más importantes del sistema, y advertir rápidamente al administrador del sistema de un ataque, además de permitir un examen en profundidad del atacante, durante y después del ataque al honeypot.

Honeypotting es el proceso de crear un sistema de réplica y atraer el atacante en ella para su posterior monitoreo. Un método relacionado - *sandboxing* - implica limitar lo que el atacante puede hacer, mientras que todavía en el sistema comprometido para que puedan ser monitoreados sin mucho daño adicional.

La colocación de la información engañosa y la respuesta del atacante es un buen método para determinar los motivos del atacante. Cualquier dato sobre el sistema que se refiere a la detección del atacante, no debe ser removido o encriptado, de lo contrario pueden cubrir sus huellas destruyéndola.

Honeypotting y sandboxing son recursos extremos por lo que debe ser factible poderlos realizar. También hay algunas cuestiones legales a tener en cuenta, se recomienda el asesoramiento legal.

i) Artefactos. Cada vez se ve comprometido un sistema, hay rastros, huellas o algo que dejó el atacante, ya sea fragmentos de código, programas troyanos, procesos o *sniffer*[443] corriendo los archivos de registro. Estos son conocidos como artefactos y son elementos importantes a recabar y difíciles de encontrar pero no deben analizarse en el sistema comprometido. Los programas troyanos pueden ser idénticos a los artefactos originales (tamaño de archivo, tiempos MAC, etc.).

El uso de sumas de control criptográficas permitirá determinar si los archivos se han modificado, por lo que es posible que se necesite saber la suma de comprobación del archivo original. El análisis de artefactos puede ser útil en la búsqueda de otros sistemas.

A manera de corolario, Matthew Braid creó una guía de para la recolección de evidencia en siete pasos[444], la cual se reproduce a continuación:

a) Encontrar la Evidencia. Determinar si las pruebas que busca son almacenadas. Se sugiera crear una lista que ayudará a anotar la evidencia recabada y hacer doble verificación de todo lo que se está buscando.

b) Encontrar los datos relevantes. Una vez encontrada la evidencia, se debe identificar lo que es relevante para el caso. No se aconseja una recolección excesiva pero sí se aconseja trabajar rápido.

[443] Es un programa informático que registra la información que envían los periféricos, así como la actividad realizada en una determinada computadora.

[444] Braid, Matthew. Collecting Electronic Evidence After a System Compromise, Computer Emergency Response Team (CERT) in Australia (AusCERT) 2001, accesible en http://www.auscert.org.au/Information/Auscert_info/Papers/Collecting_Evidence_After_A_System_Compromise.html, 13 p., consultada 1 de noviembre de 2014.

c) Crear una Orden de Volatilidad. A estas alturas se conoce exactamente lo que se debe reunir, por ello, el mejor fin para reunirla es a través de una orden prioritaria de volatilidad para minimizar la pérdida de evidencia.

d) Retirar los caminos externos de Cambio. Evitar alteraciones en los datos originales o evidencia, se puede crear una imagen tan exacta como sea posible.

e) Recoger la Evidencia. La recolección de las pruebas se realiza a través de herramientas adecuadas para la trabajo. A medida que se avanza, se deben reevaluar las pruebas que ya se han recogido pues se puede encontrar algo que es importante.

f) Documentar todo. Los procedimientos de recolección pueden generar nuevas interrogantes, por lo que es importante documentar todo lo hecho, entre ellas marcas de tiempo, las firmas digitales y electrónicas.

g) La Cadena de Custodia. Una vez que los datos han sido recogidos deben ser protegidos de la contaminación. Los originales nunca deben utilizarse en el examen forense sino los duplicados verificados.
Esto asegura que los datos originales permanecen limpios y permite a los examinadores probar lo más peligroso, potencialmente pruebas de datos-corrompiendo. Por supuesto, las pruebas hechas se deben hacer en una máquina host aislada y limpia para no permitir que programas del atacante tengan acceso a la red[445].

Una buena forma de asegurar los datos permanece incorrupto es mantener una cadena de custodia. Este es una lista detallada de lo que se hizo con las copias originales una vez que se recogieron.
Recuerde que este será interrogado más tarde, por lo que documentar todo. Record que encontrado los datos, cuando y donde fue transportado (y cómo), que tenía acceso a ella y lo que hicieron con él. Usted puede encontrar que su documentación termina superior a los datos que recoge, pero es necesario para probar su caso.

6.5.3. Análisis de la evidencia digital.

Una vez que los datos han sido recogidos con éxito se analizan para extraer la evidencia a presentar y reconstruir lo que sucedió realmente. En cuanto a los procedimientos de documentación de lo que se hizo, la persona encargada de ello será interrogada respecto del trabajo realizado a fin de que evidencie que los resultados son consistentes con los procedimientos realizados[446].

---

[445] Wright, Timothy E. "An Introduction to the Field Guide for Investigating Computer Crime (Part 1)" 17 April 2000, accesible en: http://www.symantec.com/connect/articles/field-guide-part-one, consultado el 3 de octubre de 2015.
[446] Ver Bantin, Philip C. Developing a strategy for managing electronic records, in The American Archivist, Vol. 61, No. 2 (Fall, 1998), pp. 328-364; y MARCUS, Richard L. Confronting the future: Coping with discovery of electronic material, Law and Contemporary Problems, Vol. 64, No. 2/3, Complex Litigation at the Millennium (Spring - Summer, 2001), Duke University School of Law pp. 253-281

a) Tiempo
Para reconstruir los acontecimientos que condujeron a su sistema está dañado debe ser capaz de crear una línea de tiempo. Esto puede ser difícil cuando se trata de computadoras con *zonas de deriva de reloj o clock drift* [447], que realizan notificaciones retardadas y horas distintas que crean confusión. En efecto, nunca se debe cambiar el reloj en un sistema afectado, al contrario se debe grabar cualquier deriva del reloj y uso de zona horaria, ya que se necesitará más tarde.

Los archivos de registro suelen utilizar las marcas de tiempo para indicar cuando se añadió una entrada y éstas deben sincronizarse para tener sentido, pues las marcas de tiempo contribuyen a la formación a la cadena de acontecimientos que deben estar representaron. Lo mejor es usar el GMT (UTC) de zona horaria al crear marcas de tiempo, pues el incidente puede implicar zonas horarias distintas a la que se está usando para trabajar, por lo que el uso de un punto de referencia común hará las cosas mucho más fácil.

b) Análisis Forense de Back-Ups
Al analizar las copias de seguridad, lo mejor es tener un host dedicado para el trabajo. Este examen a través del host debe ser seguro, limpio y aislado de cualquier red. Una vez que este sistema está disponible, se analizan las copias de seguridad, cometer errores en este punto no debería ser un problema porque simplemente se restaura la copia de seguridad Se debe asegurar que lo que se hace es repetible y siempre se obtienen los mismos resultados.

c) La reconstrucción del Ataque
Al reconstruir la cadena de acontecimientos, se deben correlacionar todas las pruebas reunidas de ahí lo relevante de las marcas de tiempo. La mejor manera de correlacionar es usar herramientas gráficas, diagramas y hojas de cálculo. Toda evidencia encontrada debe ser incluida en la reconstrucción del ataque no importa lo pequeño que sea.

En suma, la recolección de pruebas electrónicas no es un asunto trivial, se presentan muchas complejidades en el camino para decidir qué hacer y hay que ser capaz de justificar las acciones.

6.6. Considerar las Normas Mexicanas en Tecnologías de la Información que abonan a la regulación y operación de la FEA: NMX-I-289-NYCE-2013 y NMX-I-291–NYCE-2013.

Antes de realizar un análisis de las dos Normas Mexicanas en Tecnologías de la Información que abonan a la aplicación y generación de valor agregado a la Norma Oficial Mexicana *NOM-151-SCFI-2002: Prácticas comerciales: Requisitos que deben observarse para la conservación de mensajes de datos*, es indispensable hacer un análisis de la diferencia que existe entre una Norma Oficial Mexicana (NOM) y una Norma Mexicana (NMX).

[447] La deriva de reloj se refiere a varios fenómenos relacionados debido a los que un reloj no marcha exactamente a la misma velocidad que otro, lo que significa, que después de cierto tiempo la hora indicada por el reloj se irá separando (a esto se refiere la deriva) de la indicada por el otro. La citada deriva es aprovechada por las computadoras para construir generadores de números aleatorios y también puede ser utilizado para ataques de tiempo en criptografía.

Para aclarar esta distinción se acude a la noción de *normalización* que consiste en el proceso de regulación técnica, aplicable a nivel nacional e internacional, mediante el cual se consolida el conocimiento de los sectores privado y público, en diferentes sectores tanto privado como público (por ejemplo en materia de medio ambiente en general, seguridad al usuario, información comercial, salud, prácticas de comercio, industrial y laboral) y establecen las características técnicas que un producto, proceso o servicio deberían cumplir, y se publican en una norma, que se emite para su cumplimiento a nivel nacional.

Existen tres tipos principales de normas que reconoce y regula la Ley Federal de Metrología y Normalización (LFMN): las Normas Oficiales Mexicanas (NOM), las Normas Mexicanas (NMX) y las Normas de Referencia (NFR), aquí nos referiremos a las primeras dos, pero definimos las tres.

Las Normas Oficiales Mexicanas (NOM) se caracterizan por:

a) Sus códigos empiezan con NOM, por ejemplo: *NOM-151-SCFI-2002*.
b) Son de carácter obligatorio, es decir que de no cumplirse hay repercusiones.
c) Establecen reglas, especificaciones, características y atributos técnicos aplicables a productos, procesos o servicios, especialmente cuando:
    - Los productos (o sus envases o embalajes), procesos o servicios puedan constituir un riesgo para la seguridad o salud de las personas animales o vegetales o el medio ambiente en general.
    - Están relacionadas con los instrumentos para medir, los patrones de medida y sus métodos de medición, verificación, calibración y trazabilidad.
    - Tienen que ver con los símbolos o tecnicismos a emplearse en cierta área.
    - Se requieren especificaciones, criterios y procedimientos para proteger la salud de las personas y medio ambiente.
    - Se relacionan con la información comercial que deben llevar los envases de los productos.
    - Tienen que ver con las denominaciones de origen.
    - Se requieren para proteger las vías de comunicación y seguridad de sus usuarios.
    - Tiene que ver con el manejo y transporte de materiales y residuos peligrosos.
d) Si una NOM no se cumple por una empresa, la PROFECO y/u otras autoridades o dependencias de gobierno pueden sancionarla (multas y penas administrativas) o inmovilizar los productos que oferta.
e) Su fundamento son los artículos 40 a 51 de la Ley Federal de Metrología y Normalización (LFMN), especialmente a continuación reproducimos los artículos 43 y 51.

Artículo 43.- *En la elaboración de normas oficiales mexicanas participarán, ejerciendo sus respectivas atribuciones, las dependencias a quienes corresponda la regulación o control del producto, servicio, método, proceso o instalación, actividad o materia a normalizarse.*

Artículo 51.- *Para la modificación de las normas oficiales mexicanas deberá cumplirse con el procedimiento para su elaboración.*
Cuando no subsistan las causas que motivaron la expedición de una norma oficial mexicana, las dependencias competentes, a Iniciativa propia o a solicitud de la Comisión Nacional de Normalización, de la Secretaría o de los miembros del comité consultivo nacional de normalización correspondiente, podrán modificar o cancelar la norma de que se trate sin seguir el procedimiento para su elaboración.
(…)
Las normas oficiales mexicanas deberán ser revisadas cada 5 años a partir de la fecha de su entrada en vigor, debiendo notificarse al secretariado técnico de la Comisión Nacional de Normalización los resultados de la revisión, dentro de los 60 días naturales posteriores a la terminación del período quinquenal correspondiente. De no hacerse la notificación, las normas perderán su vigencia y las dependencias que las hubieren expedido deberán publicar su cancelación en el Diario Oficial de la Federación. La Comisión podrá solicitar a la dependencia dicha cancelación (…).

En tanto que las Normas Mexicanas (NMX) se caracterizan por:

a) Sus códigos empiezan por las siglas: NMX; por ejemplo: *NMX-I-289-NYCE-2013: Metodología de Análisis Forense de Datos y Guías de Ejecución*.
b) Establecen requisitos mínimos de calidad de productos y servicios para, por un lado, proteger y orientar al consumidor y, por el otro, brindar directrices de calidad que pueden ser muy importantes para un negocio y que de hecho pueden darle una ventaja respecto a sus competidores o darle la preferencia de sus clientes fortaleciendo la presencia en el mercado.
c) Son de carácter voluntario; no obstante una organización puede inconformarse con una NMX aduciendo que sigue un proceso de acreditación o certificación distinto, como con las normas de la Organización Internacional para la Estandarización o *International Organization for Standardization (ISO)*, por ejemplo el ISO 27000 en materia de seguridad de la información.
d) El fundamento legal es el artículo 54 de la LFMN:

Artículo 54.- *Las normas mexicanas, constituirán referencia para determinar la calidad de los productos y servicios de que se trate, particularmente para la protección y orientación de los consumidores. Dichas normas en ningún caso podrán contener especificaciones inferiores a las establecidas en las normas oficiales mexicanas.*

Las Normas de Referencia (NRC se caracterizan por:

a) Sus códigos empiezan por las siglas: NRC; por ejemplo: *NRF-046-PEMEX-2012: Protocolos de Comunicación en Sistemas Digitales de Monitoreo y Control*.
b) Son las que elaboran entidades de la administración pública, por ejemplo PEMEX, CFE.
c) Su fundamento legal es el primer párrafo del artículo 67 de la LFMN:

Artículo 67. *Las entidades de la administración pública federal, deberán constituir comités de normalización para la elaboración de las normas de referencia conforme a las cuales adquieran, arrienden o contraten bienes o servicios, cuando las normas mexicanas o internacionales no cubran los requerimientos de las mismas, o bien las especificaciones contenidas en dichas normas se consideren inaplicables u obsoletas. (…)*

Con estas aclaraciones, se procede a analizar las dos NMX elaboradas por NYCE[448] que abonan al uso de la FEA de manera extensiva:

a) NMX-I-289-NYCE-2013: Metodología de Análisis Forense de Datos y Guías de Ejecución *Information Technology o Forensic Methodology Data Analysis and Implementation Guidelines (NMX-I-289)*
b) NMX-I-291–NYCE-2013: Digitalización Documental con Valor Agregado Information *Technology o Added Value Document Digitizing (NMX-I-291).*

a) La NMX-I-289

Esta Norma Mexicana cubre las actividades que se requieren en materia de cómputo forense y de análisis de evidencia digital. El proceso del cómputo forense consta de cuatro etapas que comprenden las actividades necesarias para realizar una investigación que permita presentar un documento de información factual y de calidad legal para ser presentado en una instancia administrativa, civil o penal. Para ello, determina cuatro etapas que deben realizarse como mínimo después del cómputo forense en equipos de cómputo, independiente de las herramientas de las que se tenga disponibilidad :

a) Identificación y preservación de las fuentes de evidencia;
b) Adquisición de la evidencia digital;
c) Inspección y análisis de la evidencia digital; y
d) Presentación de resultados y elaboración de informe.

Bajo esta norma, toda actividad de cómputo forense se debe realizar por un laboratorio especializado con procedimientos establecidos sobre un Sistema de Gestión de Seguridad de la Información, el cual debe estar implantado, validado, certificado y funcionando. Esto ayuda a garantizar la privacidad de la información cumpliendo con la legislación vigente en nuestro País.

Para el desarrollo de las actividades del cómputo forense, esta Norma Mexicana considera la creación y uso de Procedimientos Operativos Estándar (POE), para garantizar la eficacia del personal encargado del proceso de cómputo forense.

[448] NYCE, es un organismo con 20 años de experiencia en el desarrollo de estándares y en evaluación de la conformidad de diferentes normas establecidas a nivel nacional (NOM, NMX) e internacional (ISO, IEC). Contamos con un amplio portafolio de servicios en certificación, verificación, normalización y capacitación; sitio web institucional https://www.nyce.org.mx/

Esta norma está vinculada con la diversa: NMX-I-27001-NYCE-2009: Técnicas de Seguridad: Requisitos de los Sistemas de Gestión de Seguridad de la Información.

Las etapas establecidas en esta Norma Mexicana para el cómputo forense y de análisis de evidencia digital son:

I. Etapa de identificación y preservación
II. Etapa de adquisición de la evidencia digital
III. Etapa de inspección y análisis de la evidencia digital
IV. Etapa de presentación de resultados y elaboración del informe
V. Herramientas
VI. Metodología
VII. Cadena de custodia y sus consideraciones

b) La NMX-I-291

Esta norma mexicana ofrece lineamientos para las personas que opten por migrar información de un medio físico a una forma digital, su cumplimiento debe ser cotejado por el tercero certificado al momento de la verificación del proceso de migración, así también debe realizar auditorías periódicas para brindar mayor certeza al proceso. El cumplimiento de lo establecido por ésta norma por parte de las personas y del tercero certificado pueden ser auditados por el organismo certificador en cualquier momento, previa notificación con 15 días hábiles de anticipación.

Las etapas del proceso de migración son realizadas por las personas o bien por uno o varios terceros prestadores de servicios, en nombre y por cuenta de aquél. Las personas pueden migrar su información a través de estos terceros siempre y cuando los procesos de dichos prestadores de servicios cumplan con lo establecido por la presente norma. Por lo anterior las personas pueden contratar a terceros para el cumplimiento de los requisitos y obligaciones de la presente norma.

Las personas pueden optar por migrar su información que se encuentre soportada en un medio físico a una MD, siempre y cuando esté permitido por la legislación vigente y además el proceso de migración haya sido verificado por un tercero certificado y observen para su conservación las disposiciones a las que se refiere la NOM-151-SCFI-2002 y a la presente norma.

Las personas deben contar con los mecanismos necesarios que permitan detectar si existe alguna alteración en la información migrada, desde el momento en que se generó por primera vez en su forma definitiva, esto es al momento de la migración, mediante los procedimientos y tecnologías de información que utilicen como parte de su proceso de migración.

Las personas, pueden aplicar las tecnologías de la información existentes en el mercado para su proceso de migración, siempre que dicha tecnología permita cumplir con lo que se establece en la presente norma.

Las personas deben garantizar que su proceso de migración permita que la información migrada sea accesible para su posterior consulta, implementando mecanismos de respaldo y recuperación de la información, y que permita ser verificada su integridad, sin importar el formato en el que se represente.

Queda a juicio de cada persona determinar la documentación que debe ser migrada, quedando bajo su absoluta responsabilidad resolver sobre la destrucción de la misma, sin embargo deben establecerse controles para evitar destruir un documento físico original que a simple vista presente rastros de alteración, borrado y/o sobre posición de letras, rasgos, signos, firmas, o cualquier otra característica que afecte o ponga en duda total o parcialmente el consentimiento de las partes que intervienen o el contenido de la información.

El tercero certificado debe informar a las personas los límites de responsabilidad de sus servicios.

Lineamientos del Proceso.

El proceso de migración debe cumplir como mínimo los siguientes requisitos, los cuales deben estar documentados y deben ser cotejados por el tercero certificado:

Contar con una aplicación que asegure la legibilidad del documento migrado y la futura validación de la inalterabilidad e integridad del documento migrado así como su disponibilidad y accesibilidad para su consulta posterior. En ningún caso un tercero certificado podrá llevar a cabo la prestación de los servicios de digitalización, retención, conservación y almacenamiento de aquellas personas de los cuales hubiere verificado y acreditado su proceso de migración.

Que un tercero certificado por un organismo certificador verifique que el proceso de migración se encuentre correctamente documentado y cumple dependiendo del volumen y criticidad de la información, con los niveles de seguridad, controles y aplicaciones habituales o requeridos en el sector comercial de las personas que realicen los actos de comercio adecuados para asegurar la integridad, inalterabilidad, accesibilidad de la información migrada desde el momento que se generó por primera vez en MD entendiendo por esta su forma definitiva. Se entienden cumplidos los requisitos de integridad e inalterabilidad del documento migrado salvo prueba en contra, cuando se cuente con procesos y tecnologías que permitan verificar dicha integridad e inalterabilidad, como es el caso de la FEA y surtirá pleno efecto jurídico a partir del momento de su conservación.

El Tercero Certificado.

El tercero certificado es responsable de la verificación de que el proceso de migración cumple con los presentes requisitos y que cumple con las medidas de seguridad, controles y aplicaciones que establecen las normas, tomando en cuenta el volumen y criticidad de la información a migrar. Es responsabilidad del tercero certificado es la verificación del cumplimiento de los requisitos contenidos en los puntos 4 y 5 de la NMX-I-291 por parte de la

persona que realice actos de comercio al momento de la verificación. El tercero certificado no puede emitir dentro del reporte de cumplimiento su opinión favorable a aquel proceso que no cumpla con los requisitos aquí establecidos.

El tercero certificado debe realizar el proceso de verificación de los procesos de migración que le soliciten las personas, siempre y cuando le entreguen la documentación requerida para la verificación establecida por la presente norma.

Posterior a su verificación positiva, el proceso de migración no debe sufrir modificaciones, en caso contrario deberá ser verificado de nuevo. El tercero certificado está obligado a verificar nuevamente el cumplimiento de la presente norma con un mínimo de seis meses desde el último reporte de cumplimiento de un tercero certificado.

El tercero certificado debe contar con los elementos humanos, tecnológicos y procedimientos para garantizar el cumplimiento de sus obligaciones derivadas de la presente norma. Los organismos de certificación tienen por satisfechos los elementos humanos, tecnológicos y procedimientos por parte de un solicitante cuando se cumpla lo siguiente:

Elementos humanos.

I. Un profesional en auditoría de sistemas de información y seguridad informática, que sea el responsable de evaluar y dictaminar el proceso de migración:

a) Ser licenciado o ingeniero en área de tecnologías de la información o afín, con título y cédula profesional registrados en la secretaría de educación pública;
b) Comprobar al menos dos años de experiencia en auditoría de sistemas de información, control de procesos o seguridad de sistemas de información, contar con diplomado en alguna de las áreas anteriores o, en su caso, alguna certificación como auditor certificado en sistemas de información (CISA), administrador certificado en seguridad de la información (CISM), líder auditor en las normas que se indican en los incisos A.2 y A.7 del apéndice A o equivalentes;
c) Comprobar al menos tres años de experiencia en sistemas de información que manejen procesos de migración de documentos físicos a forma digital;
d) Comprobar al menos dos años de experiencia en sistemas de conservación de MD;
e) Los requisitos establecidos en los incisos del c) al e) son acreditados con declaración ante fedatario público en la cual el profesional en auditoría de sistemas de información, manifieste bajo protesta de decir verdad y advertido de las penas en que incurren falsamente ante una autoridad diferente a la judicial que cumple con los mismos y que incluya los datos de las empresas o instituciones y fechas en las que adquirió la experiencia, sus cargos y las actividades y funciones desempeñadas;
f) La declaración referida en el punto inmediato anterior debe incluir la manifestación de que el profesional no ha sido condenado por delito contra el patrimonio de las personas ni inhabilitado para el ejercicio de la profesión, o desempeñar un puesto en el servicio público, en el sistema financiero o para ejercer el comercio.

II. Un profesional jurídico que es el responsable de revisar el cumplimiento de la legislación aplicable vigentes y emitir un dictamen legal de dicho proceso. Tiene como objetivo principal de su actividad verificar que los procesos de migración aseguren el cumplimiento normativo de la documentación que presente la persona y el cumplimiento de las leyes y de las reglamentaciones aplicables:

a) El profesional jurídico debe ser licenciado en derecho o abogado con título y cédula profesional registrados en la secretaría de educación pública;
b) Demostrar al menos dos años de experiencia en materia de procesos en materia civil y mercantil y cumplimiento;
c) Acreditar al menos un año de experiencia comprobable en actividades relacionadas con cualquier área del derecho informático o comercio electrónico;
d) Comprobar que conoce de forma general la operación de procesos de digitalización, retención, conservación y almacenamiento;
e) Los requisitos de los incisos del b) al d) pueden acreditarse con declaración ante fedatario público en la cual el profesionista jurídico manifieste bajo protesta de decir verdad y advertido de las penas en que incurren los que declaran falsamente ante una autoridad distinta a la judicial, que cumple con cada uno de los requisitos y que incluya los datos de las empresas o instituciones y fechas en las que adquirió la experiencia, sus cargos y las actividades y funciones desempeñadas;
f) La declaración referida en el punto inmediato anterior debe incluir la manifestación de que el profesional no ha sido condenado por delito contra el patrimonio de las personas ni inhabilitado para el ejercicio de la profesión, o desempeñar un puesto en el servicio público, en el sistema financiero o para ejercer el comercio;
g) El tercero certificado puede auxiliarse del personal que considere necesario para el cumplimiento de sus funciones, este personal debe contar con la declaración ante fedatario público donde manifieste bajo protesta de decir verdad y advertido de las penas en que incurren falsamente ante una autoridad diferente a la judicial que no ha sido condenado por delito contra el patrimonio de las personas ni inhabilitado para el ejercicio de la profesión, o desempeñar un puesto en el servicio público, en el sistema financiero o para ejercer el comercio.

Elementos tecnológicos y sus procedimientos

a) Debe contar con los elementos tecnológicos (equipo de cómputo y software) que le permiten verificar el cumplimiento y apego en todas las etapas de los procesos de migración de información con los presentes requisitos;
b) Debe contar como mínimo con los siguientes documentos:

b.1) Políticas de auditoría;
b.2) Prácticas de auditoría las cuales deben ser compatibles con normas y prácticas de auditoría de sistemas de información.

Obligaciones del Tercero Certificado:

a) Tramitar la certificación de esta norma;
b) Evaluar los procesos de migración que le son solicitados por escrito por las personas, de acuerdo a sus manuales de políticas y prácticas de auditoría;
c) Emitir para la persona que realice actos de comercio y para el organismo certificador un "reporte de cumplimiento", en el formato previamente autorizado por el organismo certificador, indicando si en su opinión el proceso de migración cumple razonablemente con lo establecido en la presente norma y/o en su caso, los hallazgos y observaciones pertinentes;
d) Contar con un registro actualizado de los procesos verificados el cual contiene, nombre o denominación social, domicilio, nombre del proceso y personal a cargo del proceso;
e) Debe conservar y almacenar la documentación que se generó en el proceso de verificación de migración de acuerdo a la presente norma, independientemente del resultado obtenido;
f) Dentro del reporte de cumplimiento por el tercero certificado, debe incluir un dictamen de auditoría informática y de auditoría jurídica emitido por el tercero certificado respecto del análisis y la evaluación de las aplicaciones, herramientas y validez legal de la actividad desarrollada, en el que se exprese la opinión acerca del cumplimiento de la presente norma y la normatividad vigente, por parte de la persona que realice actos de comercio.

Obligaciones del interesado en obtener la certificación:

a) Presentar la solicitud en los formatos que determine el organismo certificador;
b) Adjuntar a la solicitud:

b.1) En caso de personas morales, copia certificada de su acta constitutiva, póliza u otro instrumento público que acredite su constitución de acuerdo con las leyes mexicanas;
b.2) Póliza de seguro, cuyo monto aplicable para cada año es determinado por la secretaría con base en un análisis de las operaciones comerciales y mercantiles en las que son utilizados los certificados, monto que se da a conocer mediante publicación en el DOF;
b.3) Formato de reportes de cumplimiento;
b.4) La documentación que acredite el cumplimiento de los requisitos establecidos en la presente norma.

El Solicitante de acreditación para actuar como tercero certificado, debe proporcionar al organismo certificador, la documentación con la que acredite el cumplimiento de los requisitos en la NOM-151-SCFI-2002 y en la presente norma generales conforme a lo siguiente:

I. Tratándose de documentos públicos, en copia certificada o en copia simple con el original para cotejo, o;
II. Tratándose de documentos privados, en copia simple, y;
III. Una copia en disco compacto de toda la documentación presentada.

El organismo certificador puede en todo momento verificar que un proceso de migración cumple con la norma que se indica en el inciso A.5 del apéndice A, en materia de auditoría, con la legislación aplicable, de acuerdo con lo siguiente:

- Verificar el cumplimiento de las funciones de un tercero certificado;
- Solicitar a otro tercero certificado la verificación de algún proceso de migración; y
- Directamente revisar los procesos de migración previamente verificados por un tercero certificado.

6.7. Abatir el problema de la incorporación de condiciones generales por referencia o remisión.

Nuestro CCo no consideró la acertada modificación del artículo 5 bis publicada en la LMCE de 1996 y cuya reforma fue aprobada por la comisión en su 31° período de sesiones, en junio de 1998, que consiste en la incluir la "incorporación por remisión": y agregar que *no se negarán efectos jurídicos, validez ni fuerza obligatoria a la información por la sola razón de que no esté contenida en el mensaje de datos que se supone ha de dar lugar.*

El termino remisión en una dimensión electrónica es un avance y respuesta técnica que posibilita abrir un vínculo o hiperenlace que contienen las condiciones generales del contrato para leerla pero simultáneamente dar anuencia o no ante una interfaz para dar clic en "acepto" o "no acepto" las cláusulas mostradas.

Evidentemente sí existe equivalencia entre la entrega en papel de condiciones generales de la contratación y la puesta a disposición por vía electrónica de tales clausulas, si se negare la equivalencia dejaría de existir el comercio electrónico inmediatamente. Así pues, la incorporación de un clausulado concreto a un MD por mera referencia o remisión sí es información que viene a completar el contenido de un MD, cuando se remite al destinatario expresamente a ella o al lugar donde la misma puede ser hallada (link, correo electrónico o página web), el destinatario estará en posibilidad de conocerla, imprimirla, reproducirla o realizar una copia privada.

En cuanto a la referencia o reenvío a textos o documentos estos deben facilitarse previa o simultáneamente a la conclusión del contrato, este principio no solo implica que las condiciones generales consten por escrito, sino su documentación en el propio contrato o en documento que lo acompañe, esto podría tener otra repercusión consistente en que en los casos de contratación masiva, por contratos de adhesión sería unas veces poco práctico por la extensión de los documentos a los que se debe hacer reenvío y también debe quedar al arbitrio del juez la exigencia de todas las condiciones generales de un contrato.

El caso más relacionado con la materia que nos ocupa es el de las declaraciones de prácticas de certificación, en las que no existe en principio entrega de las mismas al cliente, pero sí una puesta a disposición de ella. Si dicha puesta a disposición permite un acceso razonable y sin un

esfuerzo adicional excesivo, esto es, la incorporación por referencia de unas declaraciones de prácticas de certificación de una autoridad cumpliría con un control de inclusión de contenidos[449].

Las cláusulas de reenvío no garantizan el conocimiento de las condiciones generales de contratación por parte del cliente, más bien, tienen otro sentido, el de asegurar el signatario conoce que le serán aplicables a su contrato un determinado tipo de condiciones generales y en qué consisten.[450]

En todo caso, una incorporación oscura o difícil puede no ser una incorporación adecuada y, por tanto, puede no ser efectiva. Igualmente, es menester que las cláusulas o condiciones incorporadas existan en el momento que la referencia tiene efecto, esto es, no es posible definir que a futuro se expedirán dichas condiciones.

Evidentemente, en el caso de que los documentos o mensajes incorporados hayan sido modificados posteriormente al reenvío, no serán considerados incorporados por referencia; previendo esto, algunas empresas que actúan como AC quienes establecen que cuando modifiquen sus declaraciones de prácticas, los suscriptores de certificados vigentes deberán aceptar el nuevo contenido o proceder a solicitar la revocación del certificado en un periodo, un ejemplo de certificados es los de la empresa VeriSign[451] y de las organizaciones que ofrecen como servicio los sellos de confianza (*trustmark*) como por ejemplo: AMIPCI.

6.8. Fortalecer la protección al consumidor en línea.

Si bien es cierto que el comercio electrónico a generado oportunidades sin precedentes entre las que se encuentran que el consumidor puede seleccionar entre una variedad de productos y servicios así como comparar la información respectiva, también es cierto que devinieron conductas de los proveedores sin precedentes, tales como causar daño a los consumidores en diferentes jurisdicciones mediante prácticas comerciales fraudulentas y engañosas, así como la evasión de la autoridad que aplica la ley.

Lo anterior genera desconfianza en los consumidores y debilita la integridad de los mercados nacionales e internacionales, por lo cual todo país debe regular la información y publicidad que llegue al consumidor, fomentar la confianza a través de información transparente y reglamentar la presencia de conductas comerciales en línea fraudulentas, engañosas o desleales con sistemas de reparación del daño.

No obstante, nuestra legislación en materia de protección al consumidor considera un apartado para enfrentar las prácticas comerciales fraudulentas y engañosas, estas fueron implementadas antes del año 2000, esto es, antes de que tales prácticas se presentaran en el ámbito

[449] Martínez Nadal, Apol·lònia: Comercio electrónico, firma digital y autoridades de certificación, 2001, 3ª ed., Madrid, Civitas, p. 136 y 137.
[450] Aguila-Real, Jesús Alfaro. Las condiciones generales de la contratación, 1. ed., 1991, Madrid, Ed. Civitas, p. 196.
[451] http://www.verisign.com/mx, fecha de consulta: 3 de noviembre de 2014.

electrónico, por lo que sus disposiciones no son siempre acertadas para enfrentar el problema de esas prácticas en el comercio electrónico.

En este contexto, quienes realizan prácticas fraudulentas, engañosas o desleales en contra de los consumidores se aprovechan de tres aspectos[452]:

a) Las limitaciones en la aplicación y observancia transfronteriza de las leyes de protección al consumidor mediante acciones tales como establecer operaciones en uno o más países y dañar a consumidores de otros;
b) Que los proveedores se encuentran dispersos en diferentes lugares y territorios, o bien su ubicación es difícil de determinar, ya que pueden operar simultáneamente desde más de un territorio;
c) Que los proveedores utilizan diversas estructuras corporativas u organizativas que les permiten mover sus operaciones o sus prácticas comerciales a varios territorios y hacer uso de varios servicios en diferentes lugares, servicios como los que provienen de otros proveedores de productos, proveedores de Internet, de mensajería *express,* servicios telefónicos, registros de nombres de dominio, apartados postales, servidores de *website*, bancos, operaciones crediticias, centros de servicios telefónicos y de procedimiento de datos, agencias de publicidad y servicios de respuesta[453].

Los contratos mercantiles electrónicos que generalmente son sujetos de negociación en nuestro país son los que tienen que ver con compras internacionales de productos o servicios que no son accesibles en México y lamentablemente, la información que puede ser considerada en un determinado momento evidencia judicial (MD y/o documentos electrónicos) generalmente no es resguardada por el consumidor por encontrarse en sistemas y redes de cómputo que, ya sea por falta de costumbre o cuidado, lo que lo deja en estado de indefensión.

A partir de estas conductas tanto de proveedores como consumidores en las redes, México a través de la multicitada reforma del 29 de mayo de 2000 instrumentó varias obligaciones del proveedor en *transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología*[454] en la LFPC, de acuerdo con las cuales los proveedores deben cumplir con:

a) Resguardar de manera confidencial la información del consumidor,
b) Utilizar elementos técnicos para brindar seguridad y confidencialidad en la transacción e informarlos al consumidor antes de la transacción,
c) Proporcionar domicilio físico, números telefónicos y medios a los que pueda acudir el propio consumidor para presentarle sus reclamaciones o solicitarle aclaraciones;
d) Evitar prácticas comerciales engañosas respecto de las características de los productos,

[452] Directrices de la OCDE para la Protección de los Consumidores de Prácticas Comerciales Transfronterizas Fraudulentas y Engañosas, 2004, trad. al español por la Procuraduría Federal del Consumidor (PROFECO), México, p.10.
[453] Directrices de la OCDE para la Protección de los Consumidores de Prácticas Comerciales Transfronterizas Fraudulentas y Engañosas, 2004, trad. al español por la Procuraduría Federal del Consumidor (PROFECO), México, p.10.
[454] Véase artículo 76 bis de la LFPC.

e) Cumplir con las disposiciones relativas a la información y publicidad de los bienes y servicios que ofrezca,

f) Respetar la decisión del consumidor en cuanto no recibir avisos comerciales,

g) No utilizar estrategias de venta o publicitarias que no proporcionen al consumidor información clara y suficiente sobre los servicios ofrecidos

En tanto que al consumidor se le otorgó el derecho a conocer toda la información sobre los términos, condiciones, costos, cargos adicionales así como formas de pago de los bienes y servicios ofrecidos por el proveedor.

No obstante, dicha regulación no fue suficiente en razón de que en la práctica comercial en línea tales previsiones son muy poco respetadas por el proveedor en razón de que no existe regulación respecto a las obligaciones específicas que se deben cumplir para abrir un negocio en Internet independientemente de los requisitos comunes para toda actividad comercial, por lo cual, además se debe añadir reglamentación de algunas obligaciones específicas del comercio electrónico, como las que proponemos a continuación:

a) Los propietarios de sitios web o tiendas virtuales deben publicar los datos e información a que se refiere el artículo 76 bis, fracción III de la LFPC, para la protección de los consumidores, tales como:

- La identificación de la empresa: incluyendo la denominación legal y el nombre o marca de comercialización; el principal domicilio geográfico de la empresa; correo electrónico u otros medios electrónicos de contacto, o el número telefónico; y, cuando sea aplicable, una dirección para propósitos de registro, y cualquier número relevante de licencia o registro gubernamental.
- Una comunicación rápida, fácil y efectiva con la empresa;
- Mecanismos de solución de disputas apropiados y efectivos;
- Servicios de atención a procedimientos legales; y
- Ubicación del domicilio legal de la empresa y de sus directivos para uso de las autoridades encargadas de la reglamentación y de la aplicación de la ley.

b) Regular ex ante el envío de correos electrónicos publicitarios no solicitados o consentidos (spam), ante la falta de precisión de la regulación de los artículos 17 y 76 bis, fracción VI, de la LFPC.

c) Regular el registro de las empresas, profesionales que cuenten con un negocio en Internet y que dispongan de archivos de carácter personal, a darse de alta ante dicho órgano, ello haría posible que las tiendas online que utilizan sistemas de pagos electrónicos y pagos con tarjeta de crédito y débito se encuentren controladas y monitoreadas. El órgano encargado de dicho registro podría ser la PROFECO y también estaría encargado del registro correspondiente de los contratos y las condiciones generales vigentes del negocio.

d) Cuando los productos y servicios se ofrezcan en sitios web de comercio se debe indicar de modo legible, a más tardar al inicio del procedimiento de compra, si se aplican restricciones de suministro, las limitaciones técnicas de los medios de comunicación, cómo son el número de caracteres en determinadas pantallas de celulares o de tiempo

en los anuncios televisivos, la funcionalidad y la interoperabilidad pertinente de contenidos digital. Donde el concepto de funcionalidad debe hacer referencia a las posibles maneras de utilizar el contenido digital, por ejemplo para el seguimiento del comportamiento de los consumidores, y referirse asimismo a la ausencia o presencia de cualquier limitación técnica, como la protección a través de la gestión de los derechos digitales o la codificación regional. Mientras que la interoperabilidad se refiere a describir la información relativa a aparatos y programas estándar con los que el contenido digital es compatible.

e) Establecer auditorías electrónicas periódicas por parte de la PROFECO para la revisión de documento de seguridad para los datos personales, y de los contratos, formularios y cláusulas necesarias para la recogida de datos.

La falta de las disposiciones propuestas en los puntos precedentes genera que la mayoría de las empresas mexicanas en línea se encuentren en la invisibilidad.

Por otra parte, es necesario que tanto la PROFECO[455] como la SE fomenten la confianza reforzando la difusión de diferentes principios[456], como lo son:

a) Que los proveedores que realicen transacciones con consumidores por medio del comercio electrónico deben proporcionar información precisa y fácilmente accesible que describa los bienes o servicios ofrecidos, de manera que permita a los consumidores tomar una decisión informada antes de participar en la transacción, y en términos que les permita mantener un adecuado registro de dicha información. Sobre todo en sitios web donde la información la mayoría de las veces no es precisa, y fácil de localizar.

b) Que antes de concluir una compra el consumidor debe ser capaz de identificar con precisión los bienes o servicios que desea comprar, de identificar y corregir cualquier error o modificación de la orden de compra; de expresar su consentimiento para realizar la compra de manera deliberada y razonada, así como de conservar un registro completo y preciso de la transacción. El consumidor debe tener el derecho de cancelar la transacción antes de concluir la compra.

c) Que se proporcione a los consumidores mecanismos de pagos seguros y fáciles de usar e información sobre el nivel de seguridad que brinden tales mecanismos.

d) Que se proporcione a los consumidores un fácil acceso a mecanismos alternativos para un justo y oportuno proceso de resarcimiento y resolución de disputas sin costos o cargos onerosos.

e) Que el comercio electrónico entre empresarios y consumidores debe conducirse de acuerdo la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

[455] Como parte de las actividades que realizan los países miembros de la International Consumer Protection and Enforcement Network (ICPEN)[455], en español, Red Internacional de Protección al Consumidor y de Aplicación de la Ley, de la que México forma parte desde 1994.

[456] Recomendación del consejo de la OCDE relativa a los lineamientos para la protección al consumidor en el contexto del comercio electrónico, 9 Diciembre 1999, trad. al español del inglés: OECD Guidelines for Consumer Protection in the Context of Electronic Commerce, Secretaría de Comercio y Fomento Industrial-Procuraduría Federal del Consumidor, México, p.

f) Que el país de manera internacional cooperar con empresarios, consumidores y sus representantes, ello a través de autoridades judiciales, legislativas y ejecutivas, mediante el intercambio de información.

Por otra parte, respecto a los contratos de suministro de agua, gas y electricidad cuando no se determina la venta de acuerdo con un volumen determinado así como los contratos sobre contenido digital que no se suministre en soporte material, deberían ser considerados como contratos de adhesión en línea con regulación particular en la LFPC.

Efectivamente, los contratos de adhesión en línea no habían sido abordados hasta ahora dada su problemática naturaleza contractual.[457] No es nada nuevo que quienes defienden la naturaleza eminentemente contractual del contrato de adhesión[458], refutan su esencia administrativa, con el argumento de que el acuerdo de personas para producir o transferir obligaciones y derechos es un elemento suficiente para configurar un contrato, pues en ningún precepto de la ley se exige como supuesto de validez la libre discusión entre las partes de sus cláusulas contractuales[459], y se amparan en tesis federal de la tercera sala de la SCJN de rubro: *Adhesión. No afecta la validez del contrato relativo la elaboración unilateral de su clausulado por una de las partes*; por conducto de la cual se afirma que un contrato de adhesión supone que una de las partes fija las condiciones a que debe sujetarse la otra en caso de aceptarlo, por ello dicha circunstancia no afecta su validez, ya que no implica la ausencia de la alternativa para aceptarlo o rechazarlo en forma total o parcial por parte de quien no interviene en su elaboración. Tesis que opaca nociones tan relevantes de doctrinarios de derecho público o administrativo como Leon-Duguit, Mauricio Hauriou y Saleilles, quienes niegan a los contratos por adhesión el carácter contractual porque en él, el oferente emite una voluntad reglamentaria y el adherente se encuentra en la imposibilidad de discutir los términos del contrato y acepta las condiciones preestablecidas o no hay tal operación jurídica, cuyo resultado no es obra de dos voluntades, es decir, la fuente obligacional es extracontractual.

Dentro de las características del contrato de adhesión están que no requieren ninguna discusión precontractual entre las personas interesadas solo requiere de su aceptación de un clausulado unilateral, por lo que debilitan el principio de la autonomía de la voluntad,[460]por lo que es

[457] Véase DE BUEN LOZANO, Néstor. La decadencia del contrato, 1965, México, p. 297 y 298; y también GUTIÉRREZ Y GONZÁLEZ, Ernesto. Derecho de las obligaciones, 13ª ed., 2002, México, Ed. Porrúa, p. 511-523.

[458] Los civilistas o contractualistas, entre ellos Planiol y Ripert, Josserand, Baudry-Lacantinerie, Colínt y Capitan, Domat así como Lafaille y Salvat arguyen que sí existe contrato porque una de las partes prerredacta el contrato y establece cláusulas obra de su sola voluntad pero mientras el contrato no se formule siempre hay una simple oferta, no hay contrato hasta que la parte ofertante o adherente lo lee y manifiesta su voluntad otorgando la aceptación. Si alguno de los contratantes no ha leído el contrato, habrá dolo, error, vicio de la voluntad en su consentimiento y podrá alegar su nulidad absoluta o relativa, según la naturaleza del vicio; pero habrá contrato.

[459] Díaz Bravo, Arturo. Contratos mercantiles, 2012, México, De Iure, p. 13 y 14. También Cfr. Arce Gargollo, Javier. Contratos Mercantiles Atípicos. VII Edición. Ed. Porrúa, México, 2000. p.75.

[460] Ernesto Gutiérrez y González, expresa: "En el tipo de este acto que denominé, guión administrativo, se apuntan entre otros: 1.- El suministro de energía eléctrica. 2.- El servicio telefónico. 3.- El transporte terrestre, aéreo o marítimo. 4.- El servicio de hotelería. "Los tratadistas de Derecho civil y los de Derecho administrativo pretenden mantener este tipo de acto jurídico en el campo del contrato, por el hecho de que tiene, en apariencia, los mismos elementos estructurales de un contrato: consentimiento y objeto. Cfr. Ernesto Gutiérrez y González Derecho de las Obligaciones, 13a Edición, Ed. Porrúa, México, 2001. pp. 5l1 -523.

menester que se proteja el interés difuso o fragmentario que beneficie a las personas y este es el trabajo que de manera infructuosa ha hecho el legislador en la LFPC.

Los contratos de adhesión se encuentran definidos en el artículo 85 de la LFPC que en lo conducente dice:

> *Se entiende por contrato de adhesión el documento elaborado unilateralmente por el proveedor, para establecer en formatos uniformes los términos y condiciones aplicables a la adquisición de un producto o la prestación de un servicio, aun cuando dicho documento no contengan todas las cláusulas ordinarias de un contrato. Todo contrato de adhesión celebrado en territorio nacional, para su validez, deberá estar escrito en español y sus caracteres tendrán que ser legibles a simple vista y en un tamaño y tipo de letra uniforme. Además,* ***no podrá implicar prestaciones desproporcionadas a cargo de los consumidores, obligaciones inequitativas o abusivas,*** *o cualquier otra cláusula o texto que viole las disposiciones de esta ley.*
>
> ***(Énfasis añadido)***

El siguiente artículo 86 bis del mismo ordenamiento federal, establece que:

> *En* ***los contratos de adhesión de prestación de servicios*** *deben incluirse por escrito o por* ***vía electrónica*** *los servicios adicionales, especiales, o conexos, que pueda solicitar el consumidor de forma opcional por conducto y medio del servicio básico. El proveedor sólo podrá prestar un servicio adicional o conexo no previsto en el contrato original si cuenta con el consentimiento expreso del consumidor, ya sea por escrito o* ***por vía electrónica***[461]***.***
>
> ***(Énfasis añadido)***

En tanto, el artículo 86 Ter de la misma Ley, asienta que el consumidor que realicé contratos de adhesión de prestación de servicios gozará de las siguientes prerrogativas:

> ***I.*** *Adquirir o no la prestación de servicios adicionales, especiales o conexos al servicio básico;*
> ***II.*** *Contratar la prestación de servicios adicionales, especiales o conexos con el proveedor que elija;*
> ***III.*** *Dar por terminada la prestación de los servicios adicionales conexos al servicio básico en el momento que lo manifieste de manera expresa al proveedor, sin que ello implique que proceda la suspensión o la cancelación de la prestación del servicio básico. El consumidor sólo podrá hacer uso de esta prerrogativa si se encontrare al corriente en el cumplimiento de todas sus obligaciones contractuales se hubiese vencido el plazo mínimo pactado; y*
> ***IV.*** *Las demás prerrogativas que señalen ésta y otras leyes o reglamentos.*
>
> *El consumidor gozará de las anteriores prerrogativas aun cuando no hubieren sido incluidas de manera expresa en el clausulado del contrato de adhesión de que se trate.*

Del análisis del anterior artículo, se advierte que no se considera un derecho del consumidor a ser informado de que tiene el derecho de desistimiento, aun cuando el artículo 50 no habla de la figura de desistimiento como tal sí refiere la figura de la rescisión del contrato pero sólo en

[461] El artículo 86 bis antes de la adición de la adición y reforma en el DOF el 5 de junio de 2000 y 4 de febrero de 2004 respectivamente, decía: En los contratos de adhesión de servicios deben incluirse por escrito en caso de existir, los servicios adicionales, especiales o conexos que pueda solicitar el consumidor en forma opcional por conducto y medio del servicio básico. **Si el consumidor omitiera alguno de esos servicios, se entenderá que no podrá hacerlo, a menos que con posterioridad, existía una solicitud específica por escrito.**

el caso en que el autor de la promoción u oferta no cumple su ofrecimiento, el consumidor debe tener el derecho a desistirse dentro de un periodo después de la aceptación de la oferta aun cuando el proveedor no cumple en los términos que estableció en su oferta, dado que en las ventas a distancia el consumidor no puede ver los bienes antes de celebrar el contrato, debe disponer de un derecho de desistimiento.

En este sentido, creemos acertada la propuesta que anexa la Directiva sobre los derechos de los consumidores respecto al establecimiento de un modelo de información sobre desistimiento y formato de desistimiento del consumidor (Ver Apéndice IX. Anexos I.A y I.B. de la Directiva 2011/83/UE del parlamento europeo y del consejo de 25 de octubre de 2011 sobre los derechos de los consumidores, por la que se modifican la Directiva 93/13/CEE del Consejo y la Directiva 1999/44/CE del Parlamento Europeo y del Consejo y se derogan la Directiva 85/577/CEE del Consejo y la Directiva 97/7/CE del Parlamento Europeo y del Consejo).

Añadiendo a lo anterior, que un contrato de adhesión es elaborado de manera masiva frente a recientes servicios de telecomunicaciones, servicios de información, de entretenimiento así como de servicios de diversas clases de energía, donde tales industrias afectan la libertad contractual al prefijar en avanzada contenidos de determinado tipo en algunos casos aun cuando el servicio es prestado para bienes o servicios indispensables para el ser humano desde una posición dominante en el mercado o en el mejor de los casos duopólica, ante la que el consumidor no puede sino aceptar.

En este contexto, el panorama no es el mismo, a partir del ingreso de las nociones de vía electrónica y el clausulado de una empresa generalmente dominante en el mercado[462], se añade mayor riesgo en los contratos de adhesión en línea. Lo anterior es así, porque normalmente a través de los contratos de adhesión se oculta un servicio privado de utilidad pública, en este sentido, el adherente actúa bajo el apremio que incluye la necesidad; esta situación normalmente puede generar renuncia de derechos, limitaciones a la responsabilidad del oferente o concesionario; caducidad con términos cortos; obligaciones adicionales; falta de información; pactos comisorios; facultades para rescindir unilateralmente; pactos leoninos; clausulas compromisorias o derogaciones a la competencia de la autoridad judicial; la mayor parte de las veces el clausulado es redactado en forma bastante ambigua.

En suma, la propuesta consiste en que cuando un contrato de adhesión que se configura por vía electrónica y al mismo tiempo versa sobre la adquisición en línea de ciertos bienes y servicios de primera necesidad, debe ser regulado en la propia LFPC, como un apartado denominado *contratos especiales de prestación de servicios en línea*.

[462] Entre las empresas que ofrecen servicios a los particulares de bienes de primera necesidad nos referimos a Telmex/Telcel, Comisión Federal de Electricidad, a negocios de hospedaje, líneas aéreas como Aeroméxico, negocios de gas doméstico como Fenosa, empresas de transporte terrestre y bancos, quienes abusan de la situación económica del consumidor adherente, no únicamente por la relación jurídica impositiva y unilateral que se genera entre las empresas oferentes y los consumidores, sino porque no es posible que éstos acuerden su derecho con aquéllas porque las clausulas de los documentos constitutivos del contrato no se otorgan al adherente y en el caso de que logren obtenerlo, se encuentran redactados en forma ambigua, en hojas separadas y con letras de imprenta pequeñas que el adherente acepta por necesidad, aunque éste no logre comprender el alcance legal del clausulado.

6.9. Respetar la privacidad y protección de datos personales en el comercio electrónico.

A) Ámbito internacional.

La importancia de comenzar con el marco internacional de la privacidad y la protección de los datos personales se justifica en el origen posterior de la regulación mexicana frente a cuatro instrumentos internacionales que lo reconocieron y normaron en primera instancia.

Los primeros dos autores y juez norteamericanos se pronunciaron respecto a este derecho, fueron Samuel Warren y Louis Brandeis, en el artículo intitulado *The right to privacy*[463], en el que anunciaron al derecho a la privacidad y cristalizaron el ejercicio de la defensa de la privacidad en los Estados Unidos de Norteamérica. Por otro lado, en 1882, el juez Cooley describía el derecho a la privacidad como "el derecho a que lo dejen en paz".

El derecho a la privacidad es un derecho humano que se encuentra regulado en cuatro instrumentos internacionales que tutelan la protección de la vida privada, donde esta última es reconocida como aquella que se desenvuelve a la vista de pocos o de otra persona.

Mientras que el instrumento internacional inicial que reguló el derecho a los datos personales fue la Declaración Universal de los Derechos Humanos de 1948 precisando que: *nadie será objeto de injerencias arbitrarias en su vida privada.* A tal normatividad se le aunó el Pacto Internacional de Derechos Civiles y Políticos de 1966: *Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación*. Luego, se sumó la Declaración sobre la utilización del progreso científico y tecnológico en interés de la Paz y en beneficio de la humanidad de 1975, la cual precisó el respeto de la vida privada; y finalmente, se incorporó a tales instrumentos la Declaración sobre el Genoma Humano y los Derechos Humanos de 1997: *Ninguna persona puede ser objeto de discriminaciones por sus características genéticas que atentan con su dignidad .*

Posteriormente, el Consejo de Europa elaboró la *Resolución o Recomendación 509* de 1968 sobre los derechos humanos y los nuevos logros científicos y técnicos a fin de estudiar las TIC y su potencial agresividad a los derechos de las personas. En suma, puso de manifiesto la posible confrontación entre derechos humanos y los nuevos logros científicos así como técnicos y, ofreció como opciones de solución, que en caso de encontrar gravámenes contra estos derechos, se debían generar recomendaciones en este tema.

Finalmente, se expidió el *Convenio número 108 del Consejo de Europa para la Protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*, del 28 de enero de 1981, el cual consideramos es el instrumento más próximo a la regulación requerida

[463] Harvard Law Review, Vol. 4, No. 5 (Dec. 15, 1890), pp. 193-220.

frente a las empresas y actividades comerciales que se basan en la utilización de datos personales de manera electrónica y su empelo por industrias intensivas de información así como nuevos modelos de negocio que se sostienen con el uso y venta de la información personal. Ante tal situación el Convenio citado, establece límites para que los datos de carácter personal puedan ser almacenados, registrados y tratados. Además, reconoce el derecho de acceso por parte de los interesados a la información que les atañe, con el derecho de cancelarlas o corregirlas cuando hayan sido procesadas indebidamente, así como la facultad de recurrir cualquier transgresión de estos derechos.

Pero, ¿qué es propiamente el derecho a la privacidad? y ¿cómo se protege? Para dar respuesta, según Ernesto Garzón Valdés, debe diferenciarse entre lo *íntimo, lo privado y lo público:*[464]*:*

> ***Íntimo.*** *Ámbito de los pensamientos propios, de la formación de decisiones, de las dudas, de lo reprimido, de lo aún no expresado.*
> ***Público.*** *Está caracterizado por la libre accesibilidad de los comportamientos y decisiones de las personas en sociedad.*
> ***Privado****. Ámbito reservado a un tipo de situaciones o relaciones interpersonales en donde la selección de los participantes depende de la libre decisión de cada individuo.*
> **(Énfasis añadido)**

De tal forma, el autor concluye que la privacidad *es el ámbito donde pueden imperar exclusivamente los deseos y preferencias individuales. Es condición necesaria del ejercicio de la libertad individual .*

Entonces, dónde queda la privacidad en Internet, sobre todo cuando existen datos personales que se pueden transferir como resultado del comercio electrónico internacional, la mayor preocupación en el tema de protección de datos transfronterizos se relaciona con los Estados Unidos de América, pues cuenta con la economía más grande del mundo y sus principales actividades comerciales son la banca, seguros, enseñanza, investigación, transportes, comercio y turismo. Su PIB es el más grande del mundo y le sigue, el de toda la Unión Europea en conjunto.

Entonces, el problema de la protección de datos con los diferentes comerciantes de diferentes países marcan la diferencia en el nivel de protección; de ahí que los Estados Unidos de América y la Unión Europea, sean sistemas jurídicos de resguarden de diferente forma tales derechos.

En este orden, hasta hoy la Corte Suprema de Estados Unidos no ha reconocido ni un derecho fundamental a la autodeterminación informativa, ni a la protección de datos. La Corte aplica conclusiones de diversas enmiendas a las restricciones de la Constitución sobre la recopilación de datos por parte del Estado en áreas específicas, sobre todo cuando se ha infringido la libertad de expresión o de prensa protegido por la Constitución.

[464] Garzón Valdés, Ernesto. Entre lo íntimo, lo privado y lo público, Cuadernillo no. 06 de la Colección de transparencia, 2015, México, Ed. IFAI, p 14 -19, accesible en http://inicio.ifai.org.mx/Publicaciones/Cuadernillo%2006%20B.pdf, consultado el 3 de mayo de 2015.

La legislación norteamericana en materia de protección de datos personales aplica la "*Doctrina de terceros*" de la Corte Suprema de Justicia, en la cual no existe una protección contra la divulgación de datos con los que cuenta el gobierno si el interesado ha dado a conocer libremente sus datos a terceros. Además, restringe la protección de datos en Norteamérica si existen datos que sean de relevancia para la seguridad nacional.

Las empresas de Estados Unidos de América, especialmente las que gozan de una posición dominante en el mercado, no reconocen la protección de datos personales o el derecho a la privacidad, y para efectos de los datos personales transfronterizos que deriven de cualquier operación comercial electrónica, los comerciantes no ofrecen a los consumidores garantías de protección debido a dos factores:

1) La política de seguridad[465] y
2) La política económica.[466]

En cambio, para la Unión Europea, el derecho a la protección de datos personales y la privacidad son un derecho fundamental que no se cuestiona y por ello la región ha puesto enorme empeño para intensificar el intercambio de datos de forma protegida a través del Atlántico. Como resultado de tal protección, los países miembros de la Unión Europea se esfuerzan en lanzar herramientas que respeten los cuatro instrumentos internacionales antes citados frente cualquier tipo de litigio.

B) Ámbito nacional.

La privacidad, en un sentido moderno, está estrechamente relacionada con la evolución técnica de procesamiento de la información que despersonaliza la relación entre los seres humanos.

Ante una privacidad en la era de la vigilancia[467], se requiere proporcionar una amplia protección de los consumidores a fin de que se vinculen a una contratación electrónica.

---

[465] El repudio de un derecho fundamental a la protección integral de los datos es una condición previa para la afirmación de la política de seguridad hecha por el gobierno de Estados Unidos la que ejerce en casi todas partes del mundo: si un derecho tan fundamental sería reconocida en los EE.UU., los ciudadanos de otros estados no pudiera razonablemente ser privado de ella. Pero esto implicaría que las medidas militares y de vigilancia de la seguridad de servicios de Estados Unidos serían puestas en cuestión en todo el mundo. Esto es cierto para las medidas de control contra los potenciales enemigos militares en los países árabes, así como para la búsqueda de datos pertinentes presumiblemente de seguridad de la Unión Europea, por ejemplo, bancarios o de pasajeros de vuelo de datos.

[466] Es innegable que las empresas estadounidenses han adquirido el dominio en el mercado de tecnología de la información a nivel mundial, pero sobre todo en Europa. No corporaciones europeas, pero compañías como Microsoft, Apple, Google o Facebook dominan el desarrollo tecnológico en el mercado de la tecnología de la información y sobre todo en Internet. Estas corporaciones tienen acceso directo a la política y el gobierno actual de Estados Unidos. Modelos de negocio centrales de estas corporaciones de Estados Unidos se basan en ignorar las estrictas normas europeas de protección de datos. Esto es especialmente cierto para la exploración de los datos del usuario, por Facebook y Google por ejemplo. Como resultado las empresas estadounidenses obtienen una ventaja competitiva en el mercado europeo a las empresas europeas, esto último sujeto a la supervisión nacional de protección de datos y más o menos rígida inspecciones de protección de datos. Las acciones de aplicación de las autoridades europeas de protección de datos frente a las políticas corporativas de las empresas estadounidenses fueron muy limitados en el pasado. Esto ha cambiado últimamente sólo por un par de acciones de ejecución relativas a las solicitudes de Google (Búsqueda, vista de la calle, Analytics) y Facebook.

[467] Témino usado por Dinah PoKempner, consejera general de Human Rights Watch.

En México, en principio se exige que se ponga a disposición del consumidor un *Aviso de Privacidad*[468] que señala la información que será recabada del consumidor, en la que se advierta que al dar su autorización se utilizarán registros electrónicos en cumplimiento a determinadas especificaciones. Si el consumidor realiza un formato de registro electrónico también debe ser informado en el aviso de privacidad de lo siguiente:

a) De cualquier derecho u opción de recibir un registro en forma no electrónica;
b) Sobre el derecho de retirar su consentimiento para recibir notificaciones electrónicas y recibir una explicación de las consecuencias y penas por dicha terminación;
c) Si el consentimiento es en relación a un aspecto en particular o para una categoría de avisos puestos a su disposición durante el curso de la relación de las partes;
d) De los procedimientos para la revocación del consentimiento y para actualizar la información que se necesita para ponerse en contacto con el consumidor por vía electrónica;
e) Sobre cómo obtener una copia en papel de un registro electrónico y si se efectuará algún cargo;
f) Los requisitos de hardware y software necesarios para el acceso y la conservación de registros; y
g) Que si confirma electrónicamente está aceptando que puede acceder a la información en forma electrónica necesaria.

Se debe precisar que la PROFECO considerará como datos personales en posesión de los particulares los que señale la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) así como su Reglamento (RLFPDPPP); y como información reservada, confidencial o comercial reservada aquella que fuere recolectada por los sujetos obligados que establezca la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG), conjuntamente con los *Lineamientos Generales para la clasificación y desclasificación de la información de las dependencias y entidades de la Administración Pública Federal (LGCDIDEAPF).*

Donde los particulares obligados a la protección de aquellos son las personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales, con excepción de:

I. Las sociedades de información crediticia en los supuestos de la Ley para Regular las Sociedades de Información Crediticia y demás disposiciones aplicables, y
II. Las personas que lleven a cabo la recolección y almacenamiento de datos personales, que sea para uso exclusivamente personal, y sin fines de divulgación o utilización comercial.

[468] Es un documento físico, electrónico o en cualquier otro formato (por ejemplo sonoro), a través del cual el responsable informa al titular sobre la existencia y características principales del tratamiento al que serán sometidos sus datos personales. A través del aviso de privacidad se cumple el principio de información que establece la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su Reglamento.

Por otra parte, el titular, o en su caso su representante legal, podrá ejercer los Derechos ARCO o de:

- **a)** Acceso
- **b)** Rectificación
- **c)** Cancelación
- **d)** Oposición

El ejercicio de cualquiera de ellos no impide el ejercicio de otro (artículo 22 de la LFPDPPP)

a) Acceso: Los Titulares tienen derecho a acceder a sus datos personales que obren en poder del Responsable, así como conocer el Aviso de Privacidad al que está sujeto el tratamiento (artículo 23 de la LFPDPPP).

La obligación de acceso se dará por cumplida cuando el Responsable ponga a disposición del Titular los datos personales en sitio, o bien, mediante la expedición de copias simples, medios magnéticos, ópticos, sonoros, visuales u holográficos, o utilizando otras tecnologías de la información que se hayan previsto en el aviso de privacidad. En todos los casos, el acceso deberá ser en formatos legibles o comprensibles para el Titular (artículo 102 del RLFPDPPP).

b) Rectificación: El Titular de los datos tendrá derecho a rectificarlos cuando sean inexactos o incompletos (artículo 24 de la LFPDPPP). La solicitud de rectificación deberá indicar a qué datos personales se refiere, así como la corrección que haya de realizarse y deberá ir acompañada de la documentación que ampare la procedencia de lo solicitado. El Responsable podrá ofrecer mecanismos que faciliten el ejercicio de este derecho en beneficio del Titular (artículo 104 del RLFPDPPP).

c) Cancelación: El Titular tendrá en todo momento el derecho a cancelar sus datos personales, previo periodo de bloqueo, mismo que equivale al plazo de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento (artículo 25 de la LFPDPPP). El bloqueo tiene como propósito impedir el tratamiento, a excepción del almacenamiento, o posible acceso por persona alguna, salvo que alguna disposición legal prevea lo contrario (artículo 108 del RLFPDPPP). Cuando los datos personales hubiesen sido transmitidos con anterioridad a la fecha de cancelación y sigan siendo tratados por terceros, el Responsable deberá hacer de su conocimiento dicha solicitud para que proceda a efectuarla también.

De resultar procedente la cancelación, el responsable deberá:

- Establecer un periodo de bloqueo.
- Atender las medidas de seguridad adecuadas para el bloqueo.
- Llevar a cabo la supresión correspondiente, una vez transcurrido el periodo de bloqueo (artículo 107 del RLFPDPPP).

Excepciones para la cancelación de datos personales:

a) Durante el cumplimiento de un contrato.
b) Los datos deban ser tratados por disposición legal.
c) Se obstaculicen actuaciones judiciales o administrativas.
d) Sean necesarios para (artículos 25 y 26 de la LFPDPPP):
   - Proteger los intereses del Titular.
   - Realizar una acción en función del interés público.
   - Cumplir con una obligación legal del Titular.
   - Sean indispensables para la atención, gestión, prevención o diagnóstico médico.

d) Oposición: El Titular tendrá derecho en todo momento a oponerse al tratamiento de sus datos personales o exigir que cese en el mismo cuando:

- Exista causa legítima y su situación específica así lo requiera.
- Requiera manifestar su oposición para el tratamiento de sus datos personales para que no se lleve a cabo el tratamiento para fines específicos (artículo 109, fracciones I y II, del RLFPDPPP).

No procederá el ejercicio del derecho de oposición en aquellos casos en los que el tratamiento sea necesario para el cumplimiento de una obligación legal impuesta al Responsable (artículo 109, párrafo segundo, del RLFPDPPP).

Los Responsables podrán gestionar listados de exclusión en los que incluyan los datos de las personas que han manifestado su negativa para que se traten sus datos personales, la inscripción del Titular a dichos listados deberá ser gratuita y se le otorgará una constancia de su inscripción (artículo 110 del RLFPDPPP).

Ejercicio de los Derechos Arco.
El Titular o su representante legal podrán ejercer ante el Responsable en cualquier momento, el derecho ARCO, respecto de sus datos personales, por el medio señalado en el aviso de privacidad (artículo 28 de la LFPDPPP). El Responsable pondrá a disposición del Titular, medios remotos o locales de comunicación electrónica u otros que considere pertinente. Asimismo, podrá establecer formularios, sistemas u otros métodos simplificados para facilitar el ejercicio de los derechos ARCO (artículo 90 del RLFPDPPP).

Si el Responsable dispone de servicios de cualquier índole para la atención a su público, podrá atender las solicitudes para el ejercicio de los derechos ARCO a través de los mismos, siempre y cuando no se contravengan los plazos establecidos en la LFPDPPP (artículo 91 del RLFPDPPP).

La solicitud deberá contener y acompañar lo siguiente:

- El nombre del Titular y domicilio u otro medio para comunicarle la respuesta a su solicitud.

- Los documentos que acrediten la identidad del Titular o, en su caso, la representación legal del Titular.
- (El Titular podrá acreditar su identidad exhibiendo copia de su documento de identificación, mismo que será cotejado con el original, o bien a través de instrumentos electrónicos u otros mecanismos de autenticación permitidos por otras disposiciones legales)
- La descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos antes mencionados.
- Cualquier otro elemento o documento que facilite la localización de los datos personales(artículo 29 de la LFPDPPP)

El Responsable debe dar respuesta en un plazo de 20 días hábiles, contados desde la fecha en que se recibió la solicitud. En su caso, deberá hacer efectivo el derecho del Titular en un plazo máximo de 15 días hábiles a partir de notificada la respuesta. Estos plazos podrán ampliarse por una sola vez (artículo 32 de la LFPDPPP y 97 del RLFPDPPP).

Si la información proporcionada en la solicitud es insuficiente, errónea o bien, no se acompañan los documentos antes señalados, el Responsable podrá requerir al Titular dentro de los 5 días siguientes a la recepción de la solicitud y éste contará con 10 días para atender el requerimiento; de no dar respuesta en dicho plazo, se tendrá por no presentada la solicitud correspondiente (artículo 96 del RLFPDPPP).

En caso de que el Titular atienda el requerimiento de información, el plazo para que el Responsable dé respuesta a la solicitud empezará a correr al día siguiente de que el Titular haya atendido el requerimiento (artículo 96 del RLFPDPPP).

El Responsable podrá negar el derecho ARCO cuando:

- El solicitante no sea el Titular de los datos personales, o el representante legal no esté debidamente acreditado.
- En su base de datos, no se encuentren los datos personales del solicitante.
- Se lesionen los derechos de un Tercero.
- Exista un impedimento legal, o la resolución de una autoridad competente, que restrinja el acceso a los datos personales, o no permita la rectificación, cancelación u oposición de los mismos.
- La rectificación, cancelación u oposición haya sido previamente realizada (artículo 34 de la LFPDPPP).

Finalmente, cabe señalar que los artículos 46, segundo párrafo, de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y 89, fracción I de su Reglamento, consideran el uso de la FEA como una forma para tener por acreditada y reconocida la identidad de los titulares de derechos ARCO.

Artículo 46.- *La solicitud de protección de datos podrá interponerse por escrito libre o a través de los formatos, del sistema electrónico que al efecto proporcione el Instituto y deberá contener la siguiente información:*
(…)
La forma y términos en que deba acreditarse la identidad del titular o bien, la representación legal se establecerán en el Reglamento.

Artículo 89. *Los derechos ARCO se ejercerán:*
I. Por el titular, previa acreditación de su identidad, a través de la presentación de copia de su documento de identificación y habiendo exhibido el original para su cotejo. También podrán ser admisibles los instrumentos electrónicos por medio de los cuales sea posible identificar fehacientemente al titular, u otros mecanismos de autenticación permitidos por otras disposiciones legales o reglamentarias, o aquéllos previamente establecidos por el responsable. La utilización de ***firma electrónica avanzada*** *o del instrumento electrónico que lo sustituya eximirá de la presentación de la copia del documento de identificación, y*
(…)

6.10. Considerar la Jurisdicción digital (*online jurisdiction*) en el Comercio Electrónico Internacional para resolución de conflictos.

Las controversias derivadas de negocios electrónicos por Internet resulta engorroso a diferencia de contratos signados en papel, en razón de conflictos de leyes en el espacio y de determinación jurisdiccional[469], porque en una parte de los contratos no se especifica la legislación aplicable a la situación específica ni tampoco la conocida clausula promisoria jurisdiccional; no obstante, tales negocios contractuales privados derivados de tratados internacionales, encuentran solución jurisdiccional con base en los tratados internacionales.

Normalmente la jurisdicción en materia de derecho internacional privado la constituye el domicilio del demandado; sin embargo, el contrato electrónico abarca situaciones especiales que dificultan determinar el domicilio del demandado. Lamentablemente ni la Ley Modelo sobre Comercio Electrónico de 1996 ni la Convención de las Naciones Unidas sobre la Utilización de la Comunicaciones Electrónicas en los Contratos Internacionales de 2005 lo determinan; por ello la doctrina propone tres opciones[470]:

i) Unificación de las reglas de conflicto;
ii) Unificación material, a través de una Convención Internacional que regule expresamente las cuestiones jurídicas vinculadas al comercio electrónico y,
iii) Asumir que Internet tiene una jurisdicción propia y dirimir todas las disputas relacionadas con Internet en un Tribunal de Arbitraje Internacional Especial o Corte Especial creada al efecto, ya sea que éstas realicen sus procedimientos exclusivamente por medios electrónicos o por medios tradicionales o en forma mixta.

[469] Wang, Faye Fangfei, (2010) Internet Jurisdiction and choice of law, edit Cambridge University Press, Cambridge, U.K. p 17-19.
[470] Cfr. Casados Borde, Alfonso Jesús. La jurisdicción mercantil y la globalización comercial. Derecho y Ciencias Sociales, Octubre 2015, No. 13, págs. 40-70, Instituto de Cultura Jurídica y Maestría en Sociología Jurídica. FCJ y S. UNLP. Véase también: Burstein M., citado por MARTÍNEZ, Luciana Paula y Menicocci, Alejandro Aldo, "Jurisdicción y ley aplicable en las relaciones jurídicas concluidas por Internet". Investigación y docencia, N° 40, p. 73., accesible en: http://www.centrodefilosofia.org.ar/IyD/iyd40_6.pdf, consultada el 20 octubre de 2015.

Dentro de alternativas enunciadas, la opción que menos dificultades ofrece es la selección de una jurisdicción especial, mediante la base de la CNUDMI/UNCITRAL. Sin embargo, habrá contratantes que no determinen jurisdicción alguna, para lo cual la ejemplificación más clara es la de la forma en que lo regula la Unión Europea:

a) Convenio de Roma de 1980 sobre Ley Aplicable en las Obligaciones Contractuales
b) Reglamento CE 44/ 2001 de 22 de diciembre de 2000, sobre Jurisdicción y Aplicación de las sentencias en materia Civil y Mercantil
c) Convenio de Bruselas de 27 de septiembre de 1968, sobre Jurisdicción y Ejecución de las sentencias en materia Civil y Mercantil.
d) Convenio de Lugano de 16 de Septiembre de 1988, sobre Jurisdicción y Ejecución de las sentencias en materia Civil y Mercantil, obligatoria para la Asociación Europea de Libre Comercio (EFTA), esto es, Noruega, Islandia, Liechtenstein y Suiza.

Específicamente a través de la opción b), el Reglamento CE 44/ 2001, se establecen tres supuestos para definir la competencia judicial internacional en materia contractual:

1. Los pactos entre las partes o los pactos de sumisión, en donde la competencia internacional va a quedar determinada en el mismo momento de la contratación internacional.
2. El domicilio del demandado (Convenios de Bruselas y Lugano)
3. El lugar donde deba cumplirse la obligación litigiosa (*Lex loci executionis).*

En los contratos de compraventa de mercaderías el Estado que tiene la jurisdicción es aquel en el que deben entregarse los bienes, y en el caso de prestación de servicios, es el Estado en donde se prestarán los servicios contratados de acuerdo con el artículo 5 (1) (a) del multicitado Reglamento 44/2001 así como el artículos 5 (1) de los Convenios de Lugano y Bruselas.

Ahora, las modalidades de los contratos electrónicos internacionales por Internet pueden presentarse en de dos formas:

A) Contratos celebrados en Internet cuyo cumplimiento es fuera de él, en el mundo "real";
B) Contratos totalmente celebrados y ejecutados en Internet.

En este mismo respecto, los E.U.A. adopta el Convenio de Bruselas de 27 de septiembre de 1968, sobre Jurisdicción y Ejecución de las sentencias en materia Civil y Mercantil y el Reglamento CE 44/ 2001[471].

La *Uniform Commercial Code* (UCC) regula la jurisdicción y la elección de los contratantes para escoger ley aplicable, por lo que tanto las transacciones nacionales como internacionales sin dudar se apegan a la autonomía de la voluntad de las partes; la misma suerte sigue la normatividad denominada Uniform Computer Transactions Act (UCITA) aunque su ámbito de

[471] Wang, Faye Fangfei, Internet Jurisdiction and choice of Law, edit. Cambridge University Press, Cambridge, UK, 2010, 13 pp.

competencia es respecto a informática, software de todo tipo y base de datos en línea, entre otros.

El Convenio de Roma de 1980 sobre Ley Aplicable en las Obligaciones Contractuales determina dos alternativas para establecer la jurisdicción aplicable a los contratos electrónicos:

> *a) En donde las partes escogen libremente la ley de aplicación a los contratos y la jurisdicción que resolverá un posible litigio (principio de autonomía de la voluntad de las partes); y*
> *b) En ausencia de la determinación anterior, la ley resuelve la laguna legal en función de la vinculación contractual más cercana, en el domicilio del demandado y en donde se realiza la ejecución de la obligación contraída.*

En 2001 la Cámara de Comercio Internacional publicó *Jurisdiction and aplicable law in electronic commerce* o *Jurisdicción y Ley aplicable en Comercio Electrónico*, para delimitar las operaciones realizadas en línea y la protección de los consumidores, pero sin considerar el área de propiedad intelectual y los e-terms 2004.

Preferencia del arbitraje a las resoluciones de órganos jurisdiccionales.

La globalización de los procesos arbitrales en material comercial así como el uso y reconocimiento entre los contratantes de los mismos ha desplazado la jurisdicción judicial. Los motivos son muchos van desde la agilidad, la reticencia a la burocratización, la privacidad, confidencialidad, la velocidad de las resoluciones, la aplicación de la justicia de fondo y no la formal, además de los siguientes[472]:

a) Una decadente impartición de justicia estatal, debido a los siguientes factores:
1) Expansión de la división del trabajo que no se corresponde con la división del trabajo habida en la judicatura;
2) El lento ritmo burocrático, que implica excesivo papeleo, rituales exagerados, complicados y complejos;
3) Dudas acerca de la imparcialidad de los jueces;
4) Formación exegética y conservadora de la judicatura;
5) Los jueces deciden a nombre del Estado y por sí;
6) Carencia de confidencialidad y privacidad del proceso; y
7) La moneda como instrumento de cambio de las operaciones comerciales debe de considerarse en relación a su valor en el tiempo del proceso y no en relación con su valor al momento del pacto.
b) Un sistema legislado fuera de época, por lo que se debe buscar una constante actualización legislativa acorde con la velocidad de la globalización comercial;
c) La imposibilidad del Estado de resolver específicos litigios inter-partes en un ámbito de confianza internacional, ya que los nacionales de un país desconfían en la judicatura del país de la contraparte;
d) Un deseo de mejor armonía entre las partes, buscando la lealtad entre ellas y resoluciones basadas en justicia, no en resoluciones formales.

[472] Silva Silva, Jorge Alberto, Arbitraje Comercial Internacional en México, 1994, Ed. Pereznieto, p. 34 a 45.

El arbitraje comercial se ha fundamentado del derecho procesal mercantil para que en la práctica se apliquen los siguientes principios:

> *I. Trato igualitario para las partes;*
> *II. Garantía de audiencia, o debido proceso; el cual requiere:*
> *a. Recibir de todas las partes los escritos en donde hacen vales sus derechos;*
> *b. Permitir a todas las partes presentar pruebas y demás medios de defensa, y darles la oportunidad de desahogar las mismas antes de emitir el laudo;*
> *c. Escuchar los alegatos de las partes aceptando recibir sus pretensiones y defensas;*
> *d. Comprobar que las partes tengan acceso a la información presentada por ambas, o sea, que accedan a toda documentación e información que contenga el proceso;*
> *e. No podrá limitar el derecho a las probanzas y a los argumentos, excepto cuando éstas busquen dilatar el proceso.*
> *III Conducción del procedimiento por parte del tribunal, garantizando la audiencia a las partes, aplicando el principio de preclusión procesal, que cierra las etapas procesales superadas para avanzar a las siguientes, y la agilidad procesal consecuente, para una resolución rápida y adecuada*[473]

6.10.1. Arbitraje online (ciberarbitraje) en el Comercio Electrónico Internacional.

Una de las opciones de la no sujeción a la jurisdicción de los tribunales judiciales es el arbitraje comercial internacional, cuyo inicio sólo requiere de una cláusula arbitral, cuya validez dependerá en última instancia de lo que dispongan los ordenamientos jurídicos nacionales.

El arbitraje ofrece las posibilidades del arbitraje tradicional y el denominado *ciberarbitraje* o *arbitraje online* cuyas características son el ahorro de costos, el innecesario traslado y la celeridad del procedimiento.

El arbitraje de la Cámara de Comercio Internacional (CCI) es el más famoso y recomienda que para acudir a su proceso de arbitraje se incluya la siguiente cláusula modelo en sus contratos.

> *Todas las desavenencias que deriven de este contrato o que guarden relación con éste serán resueltas definitivamente de acuerdo con el Reglamento de Arbitraje de la Cámara de Comercio Internacional por uno o más árbitros nombrados conforme a este Reglamento.* [474]

Asimismo, se precisa a las partes la conveniencia de indicar, en la cláusula de arbitraje, el derecho aplicable al contrato, el número de árbitros, la sede y el idioma del arbitraje. El Reglamento de arbitraje de la CCI no limita la libertad de las partes de elegir el derecho aplicable, la sede del arbitraje y el idioma del proceso arbitral.

Existen múltiples centros o instituciones de arbitraje on line, con diversos alcances. Entre ellos podemos mencionar:

---

[473] González de Cossio, Francisco,(2004) Arbitraje, edit. Porrúa, México, p 3-4.
[474] Reglamento de arbitraje de la CCI, vigente a partir del 1º de enero de 1998, accesible en http://www.sice.oas.org/dispute/comarb/icc/arbruls.asp, consultada 1 de enero de 2015.

1.	Online Ombuds accesible en http://odr.info/, Office: inició en 1996 por iniciativa de la universidad de Massachussets,
2.	Proyecto del CyberTribunal, accesible en www.cyberjustice.ca/, inició en 1998 por el Centre de recherche en droit public (CRDP) de la Facultad de Derecho de l'Université de Montreal,
3.	Proyecto Magistrado Virtual de Pittsburgh, iniciado y auspiciado por el National Center for Automated Information Research,
4.	American Arbitration Association y el Villanova Center for Information law and Policy, ambos accesibles en https://www.adr.org,
5.	Uniform Dispute Resolution Policy (UDRP) de la Internet Corporation for Assigned Names and Numbers (ICANN), accesible en seis idiomas en https://www.icann.org/es
6.	National Arbitration Forum, accesible en www.adrforum.com,
7.	Eresolution, accesible en http://eresolution.com,
8.	CPR Institute for Dispute Resolution, accesible en www.cpradr.org/, un centro de arbitraje de Nueva York,
9.	Society of Professionals in Dispute Resolution (SPIDR), accesible en https://imimediation.org/qap-profile-spidr,
10.	Cibertribunal peruano, accesible en cibertribunalperuano.org,
11.	Asociación Española de Arbitraje Tecnológico (ARBITEC), www.arbitec.org,
12.	CMAP (Centre de Médiation et d'arbitrage de Paris), accesible en www.cmap.fr,
13.	Internet Arbitrator (Georgia); accesible e https://www.net-arb.com/
14.	Conflict Information Consortium, http://conflict.colorado.edu, de la Universidad de Colorado
15.	Better Business Bureau Online, accesible en https://www.bbb.org,
16.	CyberSettle accesible en http://www.cybersettle.com,
17.	Internet Ombudsman, accesible en http://www.theinternetombudsman.com,
18.	Mediation Arbitration Resolution Services, accesible en https://www.arbresolutions.com,
19.	Résolution électronique des disputes commerciales (ECODIR), proyecto Francés accesible en: http://www.ecodir.org,
20.	Debt Resolution Forum, accesible en http://www.debtresolutionforum.org.uk,
21.	European Advertising Standards Alliance (EASA), accesible en www.easa-alliance.org,
22.	Centro de Arbitraje en línea auspiciado por la Cavecom-e (Cámara Venezolana de Comercio Electrónico), accesible en http://arbitrajeccc.org

Por otra parte existe un ejemplo de Arbitraje en línea en México:

El Centro de Arbitraje de México (CAM) que es un iniciativa del Instituto Tecnológico de Monterrey, Campus Ciudad de México, accesible en http://www.camex.com.mx/, del cual el exministro de la SCJN, Ulises-Schmill-Ordóñez es miembro del Consejo General del Centro de Arbitraje de México.

Finalmente y con el ánimo de establecer avances de nuestro país no en materia de arbitraje en línea, sino de Cibertribunales en varios Estados de la República Mexicana, se enlistan tres:

a) El Tribunal Virtual del Poder Judicial del Estado de Nuevo León.
b) El Expediente Electrónico del Poder Judicial del Estado de Querétaro.
c) El Juicio en línea del Tribunal Federal de Justicia Fiscal y Administrativa.

CONCLUSIONES

Capítulo I. Derecho del comercio electrónico.

1. Para el análisis del derecho del comercio electrónico en el ámbito nacional se requiere un pluralismo metodológico basado en la interdisciplinariedad del método socio-económico, el método del sobre-expectación de la madurez de la tecnología, el método de la adopción y aplicación comercial de las TIC así como la difusión de su innovación.
2. Para el análisis del derecho del comercio electrónico en el ámbito internacional se requiere de un pluralismo metodológico basado en el Derecho Comparado, con dos enfoques metodológicos: el histórico y la dogmática jurídica.
3. El éxito del comercio electrónico no sólo se apoya en la tecnología, sino en el encuadre, tratamiento y rumbo que se le da a dicha tecnología, cuyo abanico de posibilidades parte de las necesidades del mercado mexicano, el ofrecimiento de servicios, la forma de implementar pagos en línea, la publicidad, la protección al consumidor y más importante aún, la seguridad legal otorgada al contratar a través de los medios electrónicos.
4. La expresión legal de la globalización es el Derecho electrónico.
5. De acuerdo al Ciclo de sobre-expectación tecnológica de Gartner, el uso de la FEA se ubica en *Rampa de consolidación*, a un paso de la última fase denominada *Meseta de productividad.*
6. El cambio de soporte de papel a soporte electrónico constituye un reto para la certidumbre jurídica pero también se encuentra abastecida de variadas soluciones.
7. Para que un mensaje de datos consignados en contratos pueda considerarse legalmente válido, se debe asegurar que la información en él contenida cuente con ciertas características, a saber: integridad, atribución y accesibilidad (el recurso nemotécnico sugerido con motivo de sus vocales es: **I**nd**A**g**A**r: **I**ntegridad, **A**tribución y **A**ccesibilidad).
8. Todo sistema de información debe contar con tres características para el tratamiento de los MD: **R**ecuperabilidad, **F**iabilidad y **C**ontrol de los MD (el recurso nemotécnico sugerido en razón de sus consonantes es: RFC).

Capítulo II. Configuración, formación y cumplimiento contractual electrónico

9. El empleo de medios electrónicos para celebrar actos jurídicos es un legado jurídico trascendental, autoriza el cumplimiento y extensión de obligaciones.
10. El derecho mercantil sea inmutable, en algunos casos, la normatividad civil, se adecúa al campo mercantil, dado que el derecho comercial no debe desligarse tampoco del acto de comercio, ni olvidar su carácter federal.
11. Los contratos electrónicos como especie de los contratos, son una de las siete fuentes de las obligaciones mercantiles, además de la ley, la declaración unilateral de voluntad, la responsabilidad objetiva, el enriquecimiento ilegítimo, la gestión de negocios y el acto ilícito.
12. A las modalidades de los contratos electrónicos le son aplicables las modalidades de las obligaciones civiles pero con ciertos bemoles, en atención a que las reglas de las modalidades se presumen en materia mercantil, pero no en la materia civil y viceversa; lo mismo sucede

con los significados de algunos términos, que para el CCo representan algo distinto que para el CCiF.

13. Ante la correspondencia de la oferta y la aceptación, el contrato mercantil se perfecciona entre personas físicas y morales presentes y ausentes.

14. De conformidad con el artículo 1805 de CCiF, la oferta sin plazo entre presentes es aceptada inmediatamente, en caso de que no sea así, queda desvinculado el oferente. De conformidad con el artículo 1806 de CCiF, si la oferta se hace olvidando señalar un plazo a una persona ausente, el oferente queda obligado a sostenerla durante tres días, más el tiempo necesario para ida y vuelta regular del correo público, o del que se juzgue bastante, no habiendo correo público, según las distancias y la facilidad o dificultad de las comunicaciones.

15. Es complejo ajustar las legislaciones del siglo XX con la realidad creada por las TIC del siglo XXI, aun así, la declaración de voluntad informática por sistemas expertos está suficientemente regulada por el derecho mexicano de las obligaciones.

16. El artículo 80 del CCo dispone que los contratos celebrados por medios electrónicos, ópticos o de cualquier otra tecnología, quedan perfeccionados desde que se reciba la aceptación de la propuesta o las condiciones con que ésta fue modificada; en este sentido, el artículo 56 de la Ley Federal de Protección al Consumidor establece que las ventas a domicilio se perfeccionan 5 días a partir de la firma, entre tanto el contrato puede revocarse.

17. El *spam* o correo electrónico comercial no solicitado no sólo implica una gran molestia en las bandejas de entrada de los e-mails, sino que las pérdidas económicas, por lo que su problemática es la falta de cultura en seguridad informática.

18. La declaración de la voluntad abre un abanico de distintos momentos dentro marco del perfeccionamiento del contrato por vía electrónica, ello implica transitar el camino donde inician las negociaciones *precontractuales, contractuales y postcontractuales*, esto es, hasta el cumplimiento de la voluntad de las partes.

19. En la contratación electrónica se usa por antonomasia el *Sistema de Pagos Electrónicos Interbancarios* (SPEI) es un sistema desarrollado y operado por el Banco de México que permite al público en general realizar en cuestión de segundos pagos electrónicos, también llamados transferencias electrónicas, a través de la banca por Internet o de la banca móvil de manera casi instantánea.

Capítulo III. Contratación electrónica segura: Firma Electrónica Avanzada.

20. Existen dos clases jurídicas de firmas que deben ser reformadas, la firma a ruego y la huella digital. Cuando las personas analfabetas o los individuos que no puedan firmar usen la huella digital en documentos privados a fin de autenticar al otorgante, así como lo dispone el Código Civil, dicha huella digital no sirve como prueba de voluntariedad, por lo que lo es recomendable que cualquier acto jurídico donde intervengan tales personas se celebre de forma pública.

21. En el caso de la firma a ruego, cuando el negocio sea superior a doscientos pesos no debería tener validez en actos públicos o privados en que intervenga un mandatario al que se le haya hecho la solicitud de firmar a ruego, dado que cantidad no está actualizada.

22. Hasta antes de la expedición de la LFEA, la única normatividad federal que regulaba los MD era el Código Comercio.
23. La FEA es un conjunto de datos que se adjuntan a un mensaje electrónico, cuyo propósito es identificar al emisor del mensaje como su autor legítimo, verificar que la información no haya sido modificada y brindar seguridad a las transacciones electrónicas.
24. El proceso para lograr la seguridad de la información de la FEA es asociar una clave privada y pública a una persona, de tal forma que al utilizarla se pueda afirmar que esta persona está firmando digitalmente el documento, lo anterior se alcanza utilizando la criptografía.
25. El diseño de la FEA se basa en estándares internacionales de Infraestructura de Clave Pública (ICP) en donde se utilizan dos claves o llaves para el envío de MD: la "clave privada" que únicamente es conocida por el titular de la FEA y sirve para cifrar datos; y la "clave pública" con la que se descifran datos y que la mayoría de las veces está disponible en Internet para consulta de todos los usuarios de servicios electrónicos.
26. El esquema de confianza de terceros en la FEA provee certeza y resuelve el problema de autenticidad e integridad en las transacciones electrónicas. Sin embargo, su principal perjuicio es su complejidad, mientras más seguro sea el sistema de FEA, más complejo se torna. La complejidad de la ICP choca con la facilidad de las transacciones electrónicas. Ello explica por qué la FEA no se ha extendido como se esperaba después de los estándares tan altos de seguridad.
27. En materia de seguridad de la información es imposible descifrar un mensaje utilizando una llave que no corresponda.
28. Los beneficios en materia de seguridad de la FEA se recuerdan a través de la palabra: "AHÍNCO" la cual permite recordad sus cuatro características: **A**utenticidad; **I**ntegridad; **N**o repudio y **C**onfidencialidad**;** así como evocar que su uso requiere la emisión de certificados digitales (agente y agencia certificadora) así como el registro y administración de los certificados digitales (agencia registradora y registradora central).
29. La FEA empleada en materia mercantil asegura que los MD que envían y reciben las partes intervinientes en un acuerdo comercial corresponden a su contenido original e íntegro, sin haber sido transformados en o durante su transmisión.
30. La clave privada de cada FIEL (firma electrónica avanzada del SAT) se encuentra almacenada en un archivo y está resguardada por una frase de seguridad.
31. La seguridad del acceso a la clave privada recae en: el algoritmo de cifrado empleado y la frase de seguridad asignada por el titular del certificado de FIEL, denominada CIEC. Si la frase de seguridad es muy simple y el archivo de la clave privada queda en un lugar público, entonces podría ser vulnerada.
32. Por más seguro que sea el algoritmo empleado para resguardar la clave privada de FIEL, la vulnerabilidad e/o inaccesibilidad recae, para efectos prácticos, en la frase de seguridad CIEC, la cual si se olvida, el contribuyente no puede utilizar su clave privada y certificado de FIEL.
33. La seguridad de la clave privada y del certificado de una FEA recae en la cantidad de cálculos basada en la resolución de problemas matemáticos computacionales.
34. El avance tecnológico permite hacer cada vez más cálculos por segundo, lo que implica una disminución paulatina de la seguridad en los elementos de clave privada y certificado de

FIEL.

35. Los elementos de seguridad se van ajustando con el paso del tiempo, debido a lo anterior, las firmas realizadas con una clave privada y certificado de FIEL tienen una vigencia del certificado de la FIEL que queda determinada por periodos.

36. Los diferentes tipos de títulos de crédito que expresamente permiten el uso de la firma autógrafa pueden incluir también el uso de la FEA y del endoso, ya que la voluntad de las partes es un principio del comercio electrónico.

37. La FEA provee un alto nivel de certeza en la identidad del firmante, la integridad del documento electrónico, incluso una certeza mayor al de la firma autógrafa.

38. En las transacciones en papel la única forma de tener certeza de la identidad de las partes y de la integridad del documento es a través de la intervención de un notario público o corredor público, no así en los mensajes de datos que son seguros sin la intervención de aquellos.

39. El certificado digital de la FEA es un documento electrónico que asegura que una clave pública específica corresponde a una persona física o moral determinada, documento que está firmado electrónicamente por la agencia que certificó la identidad de tal persona.

40. Difícilmente se puede falsificar una FEA por varias razones: la tecnología que crea los certificados digitales se actualiza constantemente, la existencia de un tercero de confianza que asegura que la persona que cuenta con la llave pública es la persona propietaria de dicho certificado y la obligación que tienen los PSC de renovar por periodos específicos de los certificados digitales otorgados al titular de la FEA.

41. La FEA se estructura por medio de los certificados que son emitidos por autoridades certificadoras o prestadores de servicios de certificación que realiza una serie de comprobaciones para asegurarse de que la persona a la que va a otorgar el certificado es quien dice ser; donde el certificado es un documento electrónico, emitido por dichas figuras reconocidas por la SE, que asocian una clave pública con una persona física o moral determinada.

42. En términos de seguridad, la FEA parece estar un paso delante de las firmas autógrafas; pues mientras que aquella garantice la identidad e integridad puede compararse con firmas certificadas.

43. Las transacciones materializadas en papel tampoco están exceptuadas del riesgo. Tanto en las transacciones en papel como en las electrónicas existen riesgos de que los documentos sean alterados, las firmas forzadas y las partes del contrato nieguen haber firmado.

44. En las transacciones en papel el máximo nivel de seguridad no es requerido, pero se reserva para contratos o actos que la ley demanda valiosos para concretarlos con simples firmas autógrafas. Exactamente sucede lo mismo con la FEA, pareciera que la seguridad que proveen es excesiva para ciertos actos, pero justificable para otros; incluso las partes contratantes están dispuestas a pagar los costos de un contrato certificado para transacciones relevantes, pero no para aquellas que no muestran un riesgo evidente.

45. Desde el momento en que la FEA otorga un alto grado de seguridad, es preferida por los legisladores y es reconocida por varias legislaciones como la única que tiene el mismo valor legal que la firma manuscrita.

46. Para crear un incentivo en la adopción de la FEA en el comercio, a cada tipo de firma electrónica se le otorgó la garantía de un valor probatorio diferente, independientemente de que todas sean admisibles.

Capítulo IV. Configuración e incorporación nacional de las soluciones técnico-jurídicas del comercio electrónico en los sectores privado y público.

47. La falta de familiaridad y percepción pública en relación con los documentos electrónicos y la FEA provoca que las personas perciban riesgos en el uso de la FEA, los cuales son mínimos a comparación de la firma autógrafa.

48. Las firmas electrónicas ("a secas") responden a las necesidades del entorno electrónico porque presentan una solución al problema de identidad e integridad. Las más conocidas son los PIN's, contraseñas, dar clic en "acepto" o "no acepto", las biométricas y las más sofisticadas son las que utilizan la infraestructura de llave pública basadas en claves elípticas. Mientras que las firmas digitales pueden ser firmas electrónicas avanzadas, fiables o certificadas y varían de acuerdo al grado se seguridad ofrecido por su sistema de encriptación.

49. Independientemente de la existencia de los tres enfoques: Enfoque obligatorio o de tecnología específica; Enfoque minimalista o habilitador; y Enfoque híbrido o de doble nivel, actualmente en la regulación de las firmas electrónicas, la tendencia es evitar regulación basada en alguna tecnología en particular.

50. Los primeros años a partir de las reforma al CCo del 29 de mayo de 2000 se pensó que la firma electrónica simple y la FEA serían esquemas que convivirían únicamente en las áreas comercial, bancaria y fiscal. No obstante, los beneficios y resultados obtenidos en dichos ámbitos provocó que hubiera también una adopción y adaptación paulatina por parte de organismos constitucionales autónomos, del Poder Judicial Federal así como dependencias y entidades de la Administración Pública Federal, Estatal y Municipal.

51. Es prematuro saber la interpretación de los jueces en relación a la FEA, incluso de la firma electrónica en términos simples, dado que se ha emitido muy poca jurisprudencia en la materia mercantil.

52. Las adiciones al CCo del 29 de agosto de 2003, después de la reforma del 29 de agosto de 2000, se basaron en la expedición anterior de la Ley Modelo CNUDMI de Firma Electrónica de 2001 que está enfocada en un modelo de negocios, el cual ha sido progresivamente remplazado por un mercado más heterogéneo así como complejo, un reflejo de dicho basamento, es que se contemplan reglas muy minuciosas para los prestadores de servicios de certificación y ninguna disposición para otras categorías de proveedores de servicios, como los servicios de terceros que pueden ser contratados por la Autoridad de Certificadora, tal es el caso de proveedores de servicios confianza (*trust service providers),* proveedores de servicios de archivo *(archival services providers),* servicios de registro de correo electrónico *(registred mail services),* servicios de proveedores sellos de tiempo y estampados digitales (*time stamping providers*), así como repositorios.

53. Las Normas Mexicanas en Tecnologías de la Información NMX-I-289-NYCE-2013 y NMX-I-291–NYCE-2013, integran las lagunas e interpretan de los términos que no son claros en la parte relativa al punto *4.6. Norma Oficial Mexicana NOM-151-SCFI-2002: Prácticas comerciales: Requisitos que deben observarse para la conservación de mensajes de datos.*

54. La NOM-151-SCFI-2015 ha estado vigente por más de diez años, durante los cuales se ha detectado que ofrece cierto nivel de certidumbre en la conservación de MD, pero presenta riesgos al no contemplar la actualización de la constancia de los elementos de seguridad electrónica durante el periodo de vida de los MD, lo que provoca que la misma se vuelva vulnerable con el paso del tiempo y que en 2015 se elaborara un proyecto de NOM-151 por aprobarse.

55. En el Poder Judicial Federal se publicó el Acuerdo General de expedición de la FIREL para acelerar los trámites, notificaciones y procedimientos jurisdiccionales a través del uso de la FEA, además de incluir la protección de datos personales e información confidencial y reservada.

56. La LFEA permite identificar electrónicamente a los participantes de una actuación o comunicación, al tiempo que permite garantizar la integridad y veracidad del contenido de los MD y documentos electrónicos generados en el ámbito gubernamental.

Capítulo V. Incorporación de la Contratación Electrónica Segura en el Derecho Internacional Privado Mexicano.

57. La *Lex Mercatoria* es el ideal para abordar la contratación electrónica segura en el Derecho Internacional Privado Mexicano aunando la *Lex Informática*, lo que da como resultado una propuesta de *Lex Electro-Mercatoria* o *Lex Info-Mercatoria.*

58. La CNUCCIM señala que no es necesaria la forma escrita para los contratos de compraventa internacional que regula, pero realizando una interpretación conjunta con la CNUUCECI, se puede hacer uso de métodos electrónicos de comunicación en los contratos internacionales, la formación del contrato por medios automatizados de comunicación, el momento y el lugar en que las comunicaciones electrónicas se consideran emitidas y recibidas, la determinación de ubicación de las partes que utilizan comunicaciones electrónicas y los criterios para establecer una equivalencia funcional entre la comunicación y la autenticación en formato electrónico e impreso.

59. La CNUUCECI menciona en su texto de manera general a los contratos internacionales sin dirigirse a algún tipo de operación particular, no obstante, sí incluyó normas jurídicas para las transacciones electrónicas internacionales de bienes materiales.

60. El artículo 9 de la CNUUCECI, reproduce el artículo 7º de la LMCE, fundamento de nuestra regulación en el CCo y de la LFEA.

61. En cuanto a los principios de la contratación electrónica, la Convención reconoce expresamente: la equivalencia funcional, la neutralidad tecnológica, la libertad de forma y de prueba.

62. Los *ICC eTerms 2004* están diseñados para mejorar la seguridad jurídica de los contratos celebrados por medios electrónicos, para proporcionar dos cláusulas cortas, fáciles de incorporar en los contratos, que dejan claro que ambas partes tienen la intención de vincularse en un contrato electrónico.

63. Cuando los contratantes hacen referencia específica a uno de los INCONTERMS (*International Commerce Terms* de la CCI) prácticamente no existen interpretaciones equivocas relativas a los términos usados, y por ende, evita la generación de conflictos entre las partes; lo que aúna más certeza a las contrataciones electrónicas internacionales.

Capítulo VI. Alternativas y consideraciones para la consagración de la Firma Electrónica Avanzada en el comercio electrónico.

64. Es absolutamente necesario poner mayor énfasis en la perspectiva del usuario de las Firma Electrónicas, ciertamente sólo se oye de la visión técnica y de negocios, pero su ausencia ha derivado en un conjunto de soluciones técnicas y legales que frecuentemente se alejan de las necesidades comunes de los usuarios de tales firmas.

65. Para el almacenamiento, conservación y preservación digital de los MD y documentos electrónicos a los que se adjunta la FEA, se ofrecieron tres soluciones técnicas de archivo digital: a) los Servicios de Archivos de Confianza, b) la actualización de los sellos de tiempo de la firma o *resignature* y c) la canonización. El común denominador de las tres alternativas es que aseguran como mejor forma de garantizar la autenticidad del MD, la preservación de la integridad de la cadena de bits subyacente en ellos. Solución ofrecida y examinada por la archivología, rama que casi no se toma en cuenta por el derecho y que durante años se ha preocupado por preservar la integridad y la inteligibilidad de la prueba documental.

66. La brecha entre las respuestas ofrecidas por la comunidad jurídica, técnica y de archivología sobre la conservación a largo plazo de documentos firmados digitalmente se entiende mejor como un enfrentamiento entre dos concepciones diferentes de autenticidad electrónica.

67. Existen dos concepciones de autenticidad electrónica: la técnica y la contextual.

68. La concepción de autenticidad electrónica técnica es adoptada por algunos sectores de la comunidad jurídica, se basa en la medición de una propiedad física del documento: integridad de la cadena de bits (bit a bit) de los que se advierte que si los datos fueron alterados sin autorización -mediante la inserción, reordenación, inversión, sustitución o eliminación de bits- desde el momento de su creación, transmisión o archivo por una fuente autorizada.

69. El reclamo de la archivología a la autenticidad electrónica técnica consiste en que la integridad de la cadena de bits radica en la esperanza de que la autenticidad pueda ser susceptible a cuantificación precisa; pues desde el punto de vista de la archivología, si bien tal medida física de autenticidad es muy útil en puntos específicos en el ciclo de vida del documento (por ejemplo, cuando la transmisión de documentos a través del espacio), el método para establecer la autenticidad, agrava y altera la efectividad de la preservación.

70. La concepción de autenticidad electrónica contextual es defendida por los archivistas porque documenta todos los controles y procedimientos, independientemente si lo realiza un ser humano o una computadora, pero que aseguran la identidad e integridad de un registro electrónico en toda la totalidad de su ciclo de vida.

71. Con el fin de ser una prueba adecuada del contrato mercantil, un MD debe ir acompañado de los rastros y señales de todas las operaciones de las que es susceptible de incurrir en: la creación, modificación, anotaciones, firma, conversión, transmisión, etc.

72. Las FEA´s no son capaces de dar testimonio en sí mismas de la identidad y la integridad de un documento, y para ser eficaz, por ello debe ser acompañada de las diversas huellas digitales que den testimonio de su propia identidad e integridad como evidencia (certificados de clave públicos, listas de revocación, cadenas de certificados, registros de auditoría, las huellas digitales de patata, etc.).

73. En un futuro no lejano, los criterios de autenticidad electrónicos no serán establecidas de inmediato, sino que se irán formando de acuerdo a las prácticas comerciales graduales en los medios técnicos de apoyo a la autenticidad.
74. Si bien la legislación mercantil relativa a la FEA proporciona un vasto apoyo, se requieren mayores esfuerzos para dictar sus reglas precisas en materia de preservación y autenticidad de los MD, documentos eléctricos y firmas digitales.
75. La firma digital representa un problema de confianza entre sus usuarios, por lo que la CNUDMI/UNCITRAL expidió un documento explicativo de las operaciones mediante la utilización del comercio electrónico, y así emitió en 2009 *Fomento de la Confianza en el Comercio Electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónicas.*
76. La configuración de las leyes ante las tecnologías muestran una relación particular, la de que no todo es materia legal, ni todo es materia tecnológica, ello lo evidencia el hecho de que la criptografía asimétrica necesita de una entidad, una tercera parte de confianza, en este caso, la autoridad certificadora, PSC y proveedores relacionados con servicios relacionados con la FEA, tales como el proveedor de servicios de confianza que asegure el vínculo entre la clave pública y el titular de la clave privada, además de tener un rol relevante en cuestiones de certificación de fechas, horas, identidades, publicar digitalmente las claves privadas que han sido revocadas o suspendidas, etc.
77. Los sellos digitales de tiempo son esenciales para el funcionamiento del esquema de certificados, sobre todo para garantizar la fecha de creación de un MD o documentos electrónicos dentro del periodo de validez de un certificado.
78. El esquema de Autoridades de Certificación (AC) tiene que organizarse de acuerdo a la naturaleza del comercio electrónico, nacional e internacional, considerando la interoperabilidad y los esquemas cruzados de certificación por medio de una jerarquización y conexión de las AC.
79. Existen varias zonas de incertidumbre, tanto tecnológicas como legales, que requieren alternativas y propuestas de solución basadas en una adecuada infraestructura técnica, legal e institucional, a fin de consagrar el uso extensivo de la FEA en el comercio electrónico.
80. No existe una absoluta seguridad en criptografía asimétrica porque en el área de *seguridad informática* existen riesgo o probabilidades de que un evento nocivo ocurra, tan es así que a esta materia de seguridad se le prefiere llamar *administración calculada del riesgo,* que evidencia que para alcanzar dicha seguridad informática se requiere un proceso constante y evolutivo a cada momento que se presenten amenazas, riesgos y vulnerabilidades nuevas; por tal razón hay un empeño constante en actualizar las prácticas y políticas de seguridad a la par que la legislación lo hace.
81. Se visualiza que en la materia de preservación de documentos electrónicos y/o MD a largo plazo, se crearán prestadores de servicios de certificaciones en materia de archivos, los cuales trabajaran en un sistema de diseño y construcción de ambientes de preservación de documento electrónico y MD a largo plazo siempre contemplando el nivel de necesidad y riesgo que requiere la empresa que realiza prácticas comerciales electrónicas.
82. Es importante asegurar que los métodos de criptografía utilizados para la generación de la FEA sean lo suficientemente complejos para que no puedan descifrarse y permitir que un Tercero Legalmente Autorizado (TLA) pueda migrar información que no cumpla con los

estándares de seguridad internacionales.

83. Existen diferentes formas de signar un documento digital con la FEA, sin embargo cada mecanismo tiene ventajas y desventajas. Últimamente se usa el *SHA-2 (Secure Hash Algorithm* o Algoritmo de Hash Seguro) de 256 bits para generar el valor resumen de la firma digital. No obstante, nuestra propuesta es fomentar el la *Elliptic Curve Digital Signature Algorithm (ECDSA).*

84. Las *Elliptic Curve Digital Signature Algorithm (ECDSA)* cumplen con el reclamo de brindar un esquema donde la firma con la clave privada de un comerciante emplee su criptografía y, por ende, la utilización de certificados digitales *Elliptic Curve Cryptography* (ECC); desafortunadamente aún no existe un estándar para una ICP con certificados que utilicen Curvas Elípticas.

85. La gran ventaja de las economías emergentes como la Mexicana es que pueden aprovechar los avances tecnológicos sin necesidad de hacer las grandes inversiones en investigación y desarrollo en estándares y esquemas de FEA que otros países ya hicieron; por lo que no hay motivos para esperar en la integración de avances como lo son la FEA; para ello, es preciso que el gobierno y las legislaturas estimulen la formulación de la normatividad técnica adecuada.

86. Para la interoperabilidad de los trámites gubernamentales digitales se requiere que los documentos digitales se codifiquen en un lenguaje universal, no propietario (de uso libre), con estandarización de su estructura y que sean accesibles a todos los actores, como lo es el lenguaje XML descrito en archivos XSD así como contar con elementos de seguridad que garanticen su confiabilidad y veracidad.

87. Los elementos de seguridad que garantizan la integridad y autoría de documentos digitales son: la FEA, el sello digital y el timbre electrónico, este último estampado por un certificador autorizado. Todos estos elementos de seguridad son generados mediante unan infraestructura de llave pública (PKI) la cual está basada en la generación y administración de certificados digitales expedidos a todos los actores firmantes de documentos digitales.

88. Entre los beneficios que el país recibe como resultado de la implementación gubernamental de la LFEA están: reducir el impacto ambiental; lograr ahorros relacionados con los procesos en papel; disminuir el combustible; optimizar espacios físicos; reducir costos por arrendamiento de archivo muerto; mejorar el aprovechamiento de las horas-hombre de trabajo; y reducir los riesgos e inconvenientes relacionados con el envío por correspondencia.

89. Existe desconocimiento o desdén por la figura jurídica de los servicios de la sociedad de la información en el comercio electrónico, se debería considerar dicha figura como lo hace la *Directiva 2000/31/CE sobre Comercio Electrónico. relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información* de la Unión Europea, donde la concepción de estos servicios incluyen los aspectos impositivos de la ocupación y registro de nombres de dominio, rigidez en la regulación sobre el spam y protección de datos personales en los sitios web, ofrecimiento de productos y su pago con efectos fiscales vía Internet.

90. La consagración de la FEA mercantil no ha sido lograda a plenitud, una de sus causas es no homogeneizar a través de una Ley general su objeto, alcance y figuras participantes.

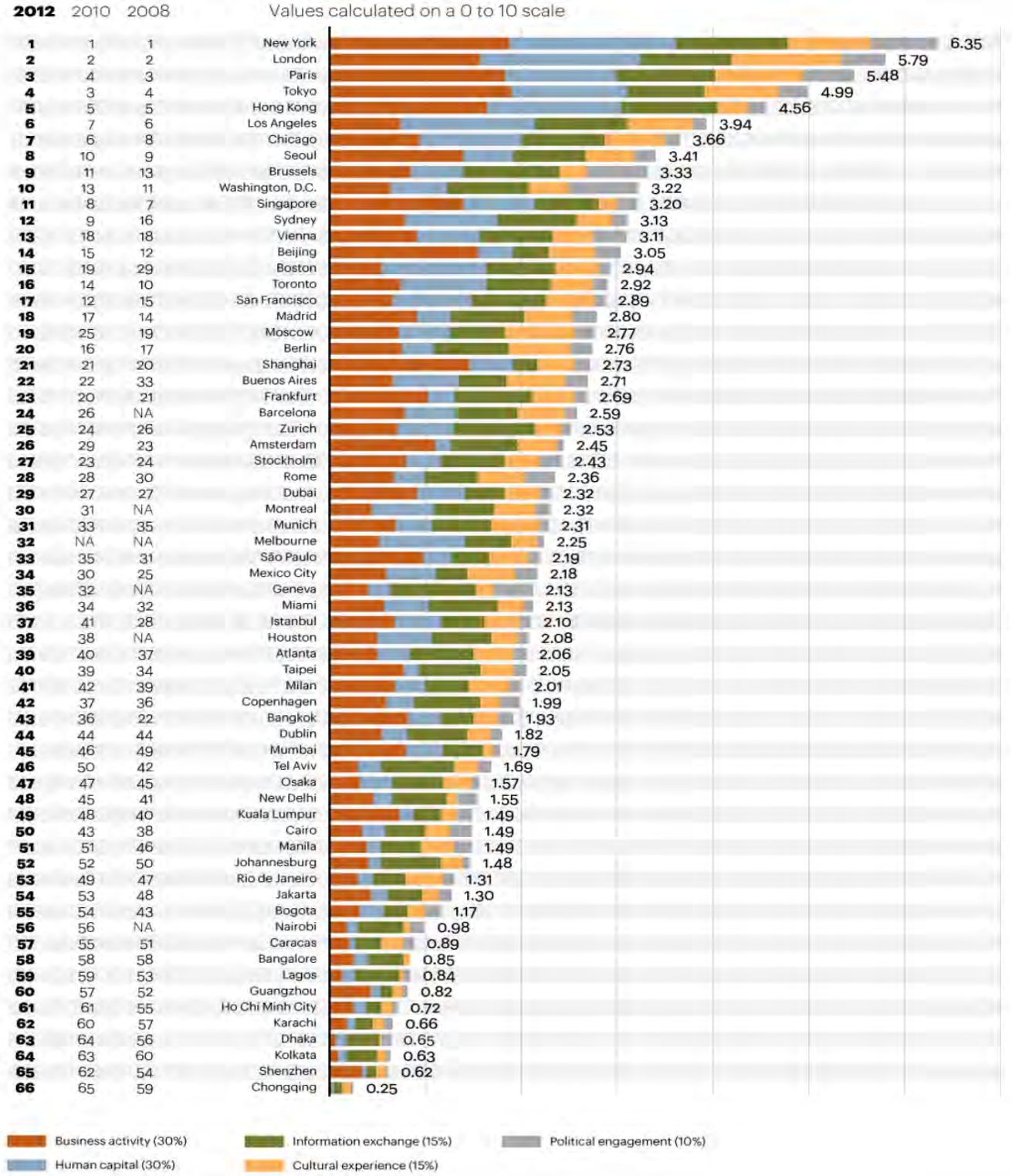
91. El avance de la consagración de la FEA mercantil no puede cuantificarse porque no se cuenta con la expresión de indicadores cualitativos ni cuantitativos susceptibles de medición

a través de indicadores objetivamente verificables, los cuales servirían como herramienta de desagregación específica de los elementos que evalúan y constituyen la naturaleza de la FEA.
92. Los indicadores de evaluación del grado de consolidación e implantación de la FEA mercantil así como de su administración electrónica por la SE, SAT y SFP deben por lo menos abarcar los siguientes indicadores:

a) No. de PSC acreditados
b) No. de Certificados digitales expedidos en el país
c) No. de documentos electrónicos y no electrónicos signados con la FEA
d) No. de comerciantes que han firmado electrónicamente las actas
e) No. de sesiones informativas y de capacitación impartidas por la SE
f) No. de Asistentes a sesiones informativas y de capacitación impartidas
g) No. de Procedimientos que se pueden realizar a través de la Sede electrónica
h) No. de Personas registradas como usuarios de la FEA
i) No. de Solicitudes de registro de autoridades certificadoras ante la SE.

APÉNDICES

Apéndice I. Índice de Ciudades Globales en 2012.



A.T. Kearney and The Chicago Council on Global Affairs, 2012 Global Cities Index and Emerging Market Outlook study 9 p., accesible en http://www.atkearney.com.au/research-studies/global-cities-index/2012, consultada el 3 de Abril de 2015.

Apéndice II. Ejemplo de Conocimiento de firma bancaria.

Empresa S.A. de C.V.
Atención Cuentas por Pagar:

Por medio de la presente, les informamos los datos bancarios para efectuar transferencias electrónicas a nuestro favor, en pago de las facturas a su cargo.

Razón Social:
(De acuerdo a la Cédula de Identificación Fiscal)
Domicilio Fiscal:
Teléfono:
Nombre del Banco:
Número de Cuenta Cheques: *(18 dígitos)*
Número de Sucursal:
Nombre de Sucursal:
Localidad de Cuenta:
Población y Estado
Número de Plaza:
Correo Electrónico[475]**:**
Contacto **Nombre**
Teléfono
Correo Electrónico[476]
Anexamos:

- ❑ Copia de la Cédula de Identificación Fiscal.
- ❑ Copia de Estado de Cuenta donde aparezca el código CLABE para transferencias interbancarias.

Nos responsabilizamos a la destrucción de los contra-recibos, una vez recibido el depósito en nuestra cuenta de cheques.

ATTE. CONOCIMIENTO DE FIRMA BANCARIO

Firma de funcionarios autorizados de empresa

[475] e-mail, donde desea recibir la integración de facturas que le serán pagadas vía transferencia bancaria.
[476] e-mail, sólo que sea diferente al anterior (1)

Apéndice III-A: Declaración de Prácticas de Certificación de la AC-DGNM y AC-SIGER de la Secretaría de Economía.

SE SECRETARÍA DE ECONOMÍA	**DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AC-DGNM Y AC-SIGER**	2.0
		27/AGO/2008

Control de Versiones

Versión	Sustituye	Entra en	Elaboró	Fecha Revisión	Revisó	Autorización	Próxima	Observacion
2.0		27/08/2008	CSI-DGNM	01/07/2008	CSI-DGNM	CSI-DGNM	14/07/2009	
1.0		24/09/2007	CSI-DGNM	24/09/2007	CSI-DGNM	CSI-DGNM	26/02/2008	Primera

Declaración de Intensión

En este documento se describe la Declaración de Prácticas de Certificación (DPC) para las Autoridades Certificadoras del SIGER (AC-SIGER) y de la DGNM (AC-DGNM), que son parte de la Infraestructura de Clave Pública de la Secretaría de Economía.

Audiencias y Alcances

Agentes certificadores, auxiliares de agente, administradores y usuarios de la AC-SIGER y la AC-DGNM.

Objetivos

Definir los procedimientos aplicables a la solicitud, validación, emisión, aceptación y revocación de certificados digitales emitidos por la AC-SIGER y la AC-DGNM.

Definiciones y Acrónimos

AC: Autoridad Certificadora.
Agente certificador: Personal de la DGNM designada para realizar el procedimiento de generación y revocación de certificados digitales.
Auxiliar de agente: Personal autorizado, que apoya al agente certificador en el proceso de generación de certificados digitales, a excepción de la generación del certificado digital.
DPC: Declaración de Prácticas de Certificación de la AC-DGNM y AC-SIGER.
AC-SIGER: Autoridad Certificadora del SIGER. AC-DGNM Autoridad Certificadora de la DGNM.
CD: Certificado Digital.
Centro de Datos del SIGER: Centro encargado de la operación y servicios del SIGER.
Claves: Clave Pública y Clave Privada.
Comunidad de la AC-SIGER: Aquella integrada por agentes certificadores, responsables de oficina, fedatarios públicos, sistemas o equipos a quienes se les ha emitido un certificado digital de la AC-SIGER.
Comunidad de la AC- DGNM: Aquella integrada por agentes certificadores y personal de Unidades Administrativas y organismos descentralizados y desconcentrados de la SE, a quienes se les ha emitido un certificado digital de la AC-DGNM.
CRL: Lista de Certificados Revocados, por sus siglas en inglés (Certificate Revocation List)
DSA: Digital Signature Algorithm. Algoritmo de Firma Digital
DGNM: Dirección General de Normatividad Mercantil
DSIGER: Dirección del Sistema Integral de Gestión Registral.
e- mail: Dirección de correo electrónico.

FEA (Firma Electrónica Avanzada): Firma Electrónica que cumple con los requisitos contemplados en el artículo 97 del Código de Comercio.
Firmante: La persona que posee los datos de creación de la firma electrónica y que actúa en nombre propio o de la persona a la que representa.
FIPS 140- 1: Acrónimo de Federal Information Processing Standard (Estándares Federales de Procesamiento de la Información), publicación 140-1, es un estándar de seguridad de ordenadores del gobierno de Estados Unidos para la acreditación de módulos criptográficos.
HSM: Dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas y suele aportar aceleración hardware para operaciones criptográficas
OCSP: Protocolo de Estatus de Certificados en Línea (por sus siglas en inglés).Online Certificate Status Protocol.)
PC (Política de Certificación): Conjunto de reglas establecidas y difundidas por la DGNM, para garantizar un nivel alto de operación y seguridad en la emisión y en la revocación de los certificados de la AC-SIGER y AC-DGNM.
PKI (Public Key Infrastructure): Infraestructura de Clave Pública.
PSC: Prestadores de Servicios de Certificación.
SE: Secretaría de Economía.
SIGER: Sistema Integral de Gestión Registral.
RPC: Registro Público de Comercio.
RSA: Algoritmo criptográfico de clave pública que adopta su nombre de las iniciales de sus creadores: Rivest, Shamir y Adleman.
SSH: Secure Shell, protocolo y programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red.
SSL: Secure Socket Layer, protocolo que proporciona autenticación y privacidad de la información a través de Internet mediante el uso de criptografía
Titular: Persona a cuyo favor fue expedido el certificado digital.
Página del SIGER: http://www.siger.gob.mx
UPS: Sistema de Alimentación Ininterrumpida (Uninterruptible Power Supply), es un dispositivo que, gracias a su batería, puede proporcionar energía eléctrica tras un apagón a todos los dispositivos existentes en la red eléctrica.

Introducción

Este documento se desarrolló tomando como base el ETSI 102 042 y el RFC 3647 [1].
Las Autoridades Certificadoras de la DGNM y del SIGER (AC-DGNM y AC-SIGER), emiten certificados digitales del tipo que se especifican en el punto 5.1 del presente documento.

Identificación

A este documento se le denomina “Declaración de Prácticas de Certificación de las Autoridades Certificadoras de la DGNM y del SIGER” (DPC). La versión actual está disponible en la página del SIGER (http://www.siger.gob.mx).
El Object Identifier, identificador de objeto (OID) ASN.1 de esta DPC es el siguiente: 2.16.484.101.10.316.1.10.2. Se compone de las siguientes partes:

JOINT - ISO - ITU-T	2
PAÍS	16

MÉXICO	484
GOBIERNO FEDERAL	101
SECRETARÍA DE ECONOMÍA	10
DGNM	316
AUTORIDAD CERTIFICADORA DE LA SECRETARÍA DE ECONOMÍA	1
AUTORIDAD CERTIFICADORA DEL SIGER	10
DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AC-DGNM y AC-SIGER	**2**

1. INTERPRETACIÓN Y APLICACIÓN

1.1 ÁMBITO LEGAL

Esta DPC se desarrolla considerando la Política de Certificación de la AC-DGNM y AC-SIGER, Código de Comercio, Reglamento del RPC, Lineamientos para la Operación del RPC y Acuerdo Interinstitucional por el que se establecen los lineamientos para la homologación, implantación y uso de la Firma Electrónica Avanzada en la APF, publicado en el Diario Oficial de la Federación el 24 de agosto de 2006.

1.2. VIGENCIA Y NOTIFICACIÓN

La DGNM garantiza la continuidad de las actividades de las AC por un periodo de 1 año tras el vencimiento del último certificado firmado por las AC.

Si por alguna razón, la entidad responsable de la operación de las AC cambiara, la DGNM se compromete a publicar en la página del SIGER, si es posible, como mínimo 2 meses antes de que se produzca dicho cambio.

La organización que a partir de ese momento se haga cargo de las AC debe apegarse al presente documento.

Una vez terminada la operación de los servicios proporcionados por las AC, éstas no firman CRL ni certificado digital alguno.

Cualquier certificado digital firmado antes de la terminación de los servicios, y una vez anunciada ésta, no puede tener un periodo de validez superior a la fecha fijada como cese de actividad. Una semana después del cese de la actividad, son revocados los certificados que continúen siendo válidos.

1.3. RESOLUCIÓN DE DISCREPANCIAS

En caso de existir dudas o discrepancias en la interpretación de esta DPC, el personal del Comité de Seguridad de la Información de la DGNM es quien las resuelve, emitiendo criterios definitivos para su aplicación.

2. PUBLICACIÓN Y ACTUALIZACIÓN DE LA DPC

La última versión autorizada de este documento de DPC de las AC está en todo momento disponible al público en la página del SIGER.

2.1. REPOSITORIOS

La DGNM, a través de la DSIGER, es responsable de administrar el repositorio de certificados digitales y CRL de las AC. Las AC no mantienen copias de las claves privadas asociadas con los certificados digitales emitidos por ellas.

2.2. FRECUENCIA DE FIRMADO DE CRL Y OCSP

Cada AC debe generar una CRL cada 24 horas, y tienen el compromiso de mantenerla actualizada, incluyendo

todos los certificados digitales revocados desde la última actualización.
El servicio de OCSP es en línea, por lo que comprueba directamente del repositorio de claves públicas.

2.3. COMPROBACIÓN DE CRL Y OCSP.

Cualquier parte involucrada en una transacción electrónica que haga uso de certificados digitales emitidos por alguna AC, debe verificar el estado de los mismos contra la última CRL publicada por las AC en el camino de certificación o contra el OCSP, desde el certificado digital en sí hasta la raíz de la jerarquía.

2.4. DISPONIBILIDAD DEL CRL Y OCSP.

Las AC ofrecen un servicio de consulta en línea de CRL disponible en:

- AC-DGNM: https://ac.siger.gob.mx/crls/dgnm
- AC-SIGER: https://ac.siger.gob.mx/crls/siger

Las AC ofrecen el servicio de OCSP en la siguiente URL:

- https://ac.siger.gob.mx/ocsp

2.5. CONTROL DE ACCESO

La información publicada sobre DPC, PC, OCSP y CRL es de dominio público. Este acceso es de sólo lectura.

3. POLÍTICA DE CONFIDENCIALIDAD

3.1 TIPO DE INFORMACIÓN CONSIDERADA CONFIDENCIAL Y RESERVADA

Las AC, de acuerdo con la Política de Identificación y Clasificación de la Información de la DGNM, consideran como información confidencial la siguiente:

- Toda información de los usuarios que no aparezca en el certificado digital emitido a favor de los mismos.

Y como reservada:

- Material criptográfico privado asociado con las AC.
- Información técnica de la infraestructura de las AC.

La información de carácter confidencial y reservada es tratada de acuerdo a lo dispuesto en la Política de Identificación y Clasificación de la Información de la DGNM, basada en la Ley Federal de Transparencia y Acceso a la Información Gubernamental, Criterios específicos para la administración de documentos, organización de archivos y clasificación de información, Lineamientos Generales para la clasificación y desclasificación de la información de las dependencias y entidades de la APF; Lineamientos Generales para la organización y conservación de los archivos de las dependencias y entidades de la APF; Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental; Lineamientos de Protección de Datos Personales; Ley Federal de Responsabilidades Administrativas de los Servidores Públicos; Lineamientos para la Elaboración de Versiones Públicas, por parte de las Dependencias y Entidades de la Administración Pública; Ley Federal de Procedimiento Administrativo.

4. REGISTRO INICIAL

4.1. TIPOS DE NOMBRES

Cada entidad perteneciente a esta infraestructura debe tener un DN (Distinguished Name o Nombre Distinguido) único y claro.

El campo “Subject” o “Asunto” del certificado digital de identificación personal, firmado por las AC, debe proporcionar los siguientes atributos.

O	OrganizationName	Razón Social

OU	OrganizationalUnitName	Área
CN	CommonName	Nombre
T	Title	Cargo
STREET	StreetAddress	Dirección
PostalCode	PostalCode	Código Postal
L	LocalityName	Ciudad
S	State	Entidad Federativa
C	CountryName	País
E	EmailAddress	Correo Electrónico
Phone	Phone	Teléfono
2.5.4.23	Fax	Fax

Adicionalmente se puede incorporar los siguientes atributos:
El DN de los certificados digitales para equipo de cómputo a firmar por las AC deben proporcionar los siguientes atributos:

SN	SerialNumber	CURP Titular del Certificado Digital
2.5.4.45	X500uniqueIdentifier	RFC del Titular del Certificado

El DN de los certificados digitales para equipo de cómputo a firmar por las AC deben proporcionar los siguientes atributos:

O	OrganizationName	Razón Social
OU	OrganizationalUnitName	Área
CN	CommonName	Nombre
STREET	StreetAddress	Dirección
PostalCode	PostalCode	Código Postal
L	LocalityName	Ciudad
S	State	Entidad Federativa
C	CountryName	País
E	EmailAddress	Correo Electrónico

4.2. PROCEDIMIENTOS DE GENERACIÓN DE CLAVES DE LAS AC
Los únicos casos en los que se realiza generación de claves para Autoridad Certificadora son:
a) Fin de vida de la AC (al cubrir el 80%)
b) Claves privadas comprometidas.
c) Avance tecnológico.
En cualquiera de los casos anteriores, se generará un nuevo par de claves de la longitud y tecnología adecuada.

5. EMISIÓN DE CERTIFICADOS
5.1. TIPOS DE CERTIFICADOS.

La AC-SIGER emite exclusivamente:

1. Certificados Digitales para Agentes Certificadores del SIGER (CD-AGS);
2. Certificados Digitales para Responsables de Oficina (CD-RO);
3. Certificados Digitales para Fedatarios Públicos (notarios y corredores públicos) (CD- FP);
4. Certificados Digitales para Identidad de equipo de cómputo y telecomunicaciones del SIGER (CD-SSL)
5. Certificados Digitales para Código de Programas Fuente y Objeto de los Sistemas y Subsistemas del SIGER (CD-CSSS)
6. Certificados de Dispositivos de Firma Electrónica (CD-DFE)

La AC-DGNM emite exclusivamente:

7. Certificados Digitales para Agentes Certificadores de la DGNM (CD-AGNM);
8. Certificados Digitales para personas de Unidades Administrativas y organismos descentralizados y desconcentrados de la SE (CD-SE);
9. Personas de Organismos del Sector Público autorizados por la DGNM.(CD-SP)

Para fines de los procedimientos descritos en esta DPC, los certificados de Identidad personal (CD-IP) serán los siguientes:

- CD-AGS
- CD-RO
- CD-FP
- CD-AGNM
- CD-SE
- CD-SP

Los certificados que emiten las AC-SIGER y AC-DGNM almacenan la llave privada en un token o tarjeta biométrica.
Los únicos certificados con almacenamiento de llave privada en archivo son los que se emitirán para los Agentes Certificadores, para personas de Unidades Administrativas y organismos descentralizados y desconcentrados de la SE (CD-SE) y Personas de Organismos del Sector Público autorizados por la DGNM. (CD-SP).

5.2. PERÍODO DE VALIDEZ DE LOS CERTIFICADOS DIGITALES

- Para la Autoridad Certificadora es de veinte años, a partir de su fecha de emisión.
- Para los Agentes Certificadores es de dos años, a partir de su fecha de emisión.
- Para servidor y código fuente y objeto de los sistemas y subsistemas del SIGER, es de cinco años a partir de su fecha de emisión.
- Para el resto de la **comunidad** es máximo de dos años, a partir de su fecha de emisión.
- Se puede emitir certificados de menor duración, siempre y cuando así lo exprese el solicitante en el formato de solicitud firmado, o bien en el caso establecido en el punto 5.3.1. de esta DPC.

5.3. PROCEDIMIENTO DE IDENTIFICACION Y PERSONALIDAD JURÍDICA

5.3.1. Documentos de Identificación y Personalidad Jurídica para certificados de identidad personal:

La identificación del solicitante de un certificado digital se hace tomando en cuenta los documentos de identidad señalados en el formato de solicitud DGNM-IT-5-CG-SOL

Asimismo, debe acreditar su personalidad jurídica:

- Notarios Públicos: con su patente, FIAT, nombramiento o credencial de notario.
- Corredores Públicos: con su credencial o habilitación de corredor.
- Responsables de oficina: Habilitación expedida por la SE o Nombramiento de Gobierno del Estado, cédula profesional o título profesional de licenciado en Derecho o carta de pasante y carta compromiso del titular del RPC en la entidad para la entrega del título en un plazo no mayor a un año, por una sola vez.
- Personal de Unidades Administrativas y organismos descentralizados y desconcentrados de la SE y Personal de organismos del Sector Público autorizados por la DGNM: Credencial del IFE y credencial de empleado de la unidad administrativa, en caso de no contar con esta última, deberán presentar el talón de pago de la última quincena, así mismo, deberá aparecer su nombre en la lista de Solicitud de Certificado Digital para Servidor Público autorizado por la DGNM.

5.3.2. El procedimiento de identificación comprende los siguientes pasos:

1. El solicitante de un certificado digital se presenta personalmente ante el Agente Certificador o Auxiliar de Agente, con el original y copia de cualquiera de los documentos de identidad, así como de personalidad jurídica, establecidas en el punto 5.3.1, para cotejar la información con la copia simple de éste, la cual se integra a su expediente.
2. Para el caso de certificados CD-SE y CD-SP el Agente o Auxiliar de Agente deberá cotejar de que su nombre aparezca en la lista de Solicitud de Certificado Digital para Servidor Público autorizado por la DGNM, de la cual pedirá copia simple al solicitante o confirmará con el archivo del Departamento de Control de Certificados Digitales de la DGNM.
3. Confirmada la validez de las identificaciones, el agente certificador o el auxiliar del agente, verifica la coincidencia entre la fotografía contenida en aquellas y la filiación del solicitante.
4. El solicitante debe llenar el formato de solicitud correspondiente.
5. Realizado lo anterior, el agente certificador o el auxiliar, procede a solicitar que firme de forma autógrafa la solicitud del certificado y coteja la firma autógrafa de la solicitud contra el documento de identidad.

5.4. PROCEDIMIENTO DE EMISIÓN DE CERTIFICADOS DE IDENTIDAD PERSONAL:

1. El agente certificador o el auxiliar del agente, verifica si el solicitante cuenta con un certificado anterior, conectándose a:
   https://ac.siger.gob.mx para certificados de la AC-SIGER.
   https://ac.siger.gob.mx/DGNM para certificados de la AC-DGNM
   En el módulo de consulta, introduce el nombre o apellido del solicitante, para buscar si tiene certificados a su nombre y si están vigentes.
   De ser así, si la actividad la hizo el auxiliar de agente, procede a notificar al agente certificador para que realice el procedimiento de revocación señalado en el punto 6.2.3 de esta DPC. Si el agente certificador no puede realizar la revocación del certificado existente, deberá realizar la petición al Administrador de la AC correspondiente.
2. El agente certificador o el auxiliar del agente, prepara la tarjeta o token biométrico del solicitante y captura la huella dactilar en la misma.
3. En caso de que, el solicitante presente ilegibilidad en sus huellas dactilares, el agente certificador o auxiliar de agente deberá llenar la Constancia de I legibilidad de Huellas Dactilares, en donde certifica que se realizaron varios intentos con sus diferentes dedos y no se encontraron huellas

dactilares, y se procederá a preparar el token para que utilice contraseña. Es responsabilidad del Auxiliar de Agente comunicarle al Agente que se trata de un certificado de esta naturaleza y asentar la leyenda que se señala en los criterios de llenado del punto 5.4.1. de este documento

4. Solo la AC-DGNM podrá emitir certificados de identidad personal con protección de las claves en archivos y para lo cual se seguirá el procedimiento descrito en el punto 5.6 de esta DPC
5. A continuación el agente certificador o el auxiliar del agente, de acuerdo a la comunidad a la que pertenezca el solicitante, se conecta a una de las siguientes páginas:
   https://ac.siger.gob.mx para solicitudes de certificados de la AC-SIGER.
   https://ac.siger.gob.mx/DGNM para solicitudes de certificados de la AC-DGN
6. Se procede a llenar el requerimiento, sujetándose a los criterios de llenado, que se detallan en el numeral 5.4.1. de este documento. El agente certificador o auxiliar del agente, así como el solicitante, deben cerciorarse que se haya capturado correctamente la información y que esté conforme a la solicitud. A continuación, el solicitante genera el requerimiento y graba la clave privada en la tarjeta o token, autentificándose con su huella dactilar o con su contraseña para los casos señalados en el punto 3 de este procedimiento. El requerimiento se envía a la autoridad certificadora.
7. En caso de que todos los pasos anteriores los haya realizado un auxiliar de agente, éste se debe comunicar con el agente certificador, para notificar que se envió el requerimiento. El agente certificador se conecta a la AC, según corresponda la comunidad del solicitante, revisa el requerimiento, y emite el certificado con la vigencia autorizada.
8. Si el requerimiento no cumple con los criterios señalados en el punto 5.4.1, se debe repetir el proceso para generar otro requerimiento.
9. Si el auxiliar de agente ha realizado correctamente las actividades señaladas del punto 1 al 4 de este procedimiento, el agente certificador se comunica con el auxiliar y le proporciona el número de serie del certificado generado.
10. El agente certificador ó el auxiliar del agente entra a la página de la AC correspondiente, y apoya al usuario en la instalación del certificado en la tarjeta o token. Para el caso de las tarjetas, comprueba que realmente se haya grabado, para lo cual quita y agrega el certificado del Contenedor de Windows. Y para eltoken se elimina el certificado del contenedor de Windows, se expulsa el token, se vuelve a conectar y se observa que se agregue automáticamente al contenedor de Windows.
11. El titular del certificado debe firmar la carta de confidencialidad de acuerdo a la comunidad que pertenezca, así como el comprobante de emisión de certificado digital de FEA.
12. El agente certificador y el auxiliar del agente debe recopilar la documentación establecida en el formato de Solicitud de Certificado Digital DGNM-IT-5-CG-SOL, Carta de Confidencialidad y Comprobante de Emisión del Certificado.
13. El agente certificador y el auxiliar del agente son responsables de enviar la documentación derivada del procedimiento de generación al Departamento de Control de Certificados Digitales de la DGNM.

5.4.1. CRITERIOS DE LLENADO DEL REQUERIMIENTO DE CD DE IDENTIDAD PERSONAL:

1. Se utilizan mayúsculas y minúsculas.
2. No se utilizan acentos.
3. Sólo se utilizan abreviaturas en los campos de Razón Social y Dirección cuando la información exceda el límite, conforme a las reglas ortográficas.
4. Razón Social:

- Para AC-DGNM: se captura “Secretaria de Economía”.
- Para Responsables de Oficina: se captura “Registro Público de la Propiedad y de Comercio”,

seguido del municipio y estado al que pertenezca.

- Para el Registro Inmediato de Empresas (RIE) es “Registro Público de la Propiedad y del Comercio del Estado de” seguido del nombre del estado correspondiente.
- Para Fedatarios Públicos: se captura “Correduria” o “Notaria Publica” seguido del número, municipio o delegación política (en el caso del Distrito Federal) y entidad correspondiente.
- En caso de que el titular del certicado tenga la personalidad jurídica de Corredor y Notario se asentará “Correduria No. nn y Notaria Publica No.nn” seguido de municipio o delegación política y entidad correspondiente. (En donde nn es el número de correduría o notaría correspondiente).

5. Área:
   - Para AC-DGNM: Dirección de Área, Delegación o Subdelegación Federal de la SE a la que pertenezcan: ejemplo “Delegación Federal en Guanajuato”.
   - Para AC-SIGER: se deja en blanco, excepto para el RIE que se coloca la leyenda “ Registro Inmediato de Empresas” y para el caso de los certificado que se emite por ilegibilidad de huellas dactilares, se pondrá “ Clave Privada en Token”
6. Tanto el RFC y CURP son necesarios cuando el titular del certificado desee que su certificado sea aceptado por las dependencias integrantes de la Subcomisión de la FEA. En cuyo caso se debe aplicar el “Procedimiento para la Validación de CURP y RFC” que se encuentra en la dirección electrónica http://www.cidge.gob.mx.
7. Nombre, se captura primero el nombre de pila y en seguida los apellidos del solicitante.
8. Profesión:
   - Para AC-DGNM: cargo o puesto correspondiente.
   - Para fedatario público se anota “Notario Publico” Titular, Suplente, Adscrito o como señale su patente o FIAT y “Corredor Publico”.
   - Para Responsable de Oficina: se anota “Responsable de Oficina” o “Registrador Publico”.
9. Dirección: Se anota el domicilio en que se ubique la oficina del solicitante; utilizando el signo # , en lugar de cualquier otra forma de abreviatura para el número del inmueble en el que se ubiquen.
10. Código postal: (5 dígitos),
11. Ciudad y entidad federativa: los que corresponden al domicilio.
12. Nivel de seguridad: al menos de High Grade (1024 bits).
13. País: México.
14. Correo electrónico: se captura el e-mail del solicitante, todo en minúsculas.
15. Teléfono y fax: se anota la clave lada entre paréntesis y después el número de teléfono correspondiente si tiene extensión, especificar. Ejemplo: (33)51433121 Ext. 33544
16. Clave de anulación: se anota en letras mayúsculas o minúsculas, o números, o las combinaciones de ambos con un máximo de 20 caracteres.
17. Confirmación, se repite la clave de anulación, con el mismo formato.
18. CryptProvider (Proveedor criptográfico): el que corresponda a la tecnología utilizada en los dispositivos biométricos, ejemplos:

- Para tarjetas criptográficas Cyberflex y Miotec: SeguriCSP-Criptographic Service Provider v 1.0
- Para lector Biotoken: SafeSign Standard Cryptographic Service Provider

5.5. EMISIÓN DE CERTIFICADOS DIGITALES PARA EQUIPOS DE CÓMPUTO.

Se emiten certificados para equipo de los siguientes tipos:

- Certificados Digitales para Identidad de Equipo de Cómputo y Telecomunicaciones del SIGER (CD-SSL), se activa el atributo de SSL.
- Certificados Digitales para Código de Programas Fuente y Objeto de los Sistemas y Subsistemas del SIGER (CD-CSSS), se activa el atributo de firma de código.

- Certificados de Dispositivos para Servicios de Firma Electrónica (CD-DSFE), se activa el atributo de firma.

La emisión de dichos certificados se realiza de la siguiente manera:

1. El solicitante debe llenar y firmar formato de Solicitud de Certificado para Equipo de Cómputo, el cual debe entregar para su autorización a la DGNM.
2. Una vez autorizado, la solicitud se debe hacer llegar al agente certificador.
3. El solicitante debe llenar el requerimiento de acuerdo a lo señalado en el apartado 5.5.1.
4. El archivo del requerimiento se debe enviar por medios electrónicos al agente certificador autorizado por la DGNM para su emisión.
5. El agente certificador recibe el formato de solicitud y el requerimiento, debe comprobar que estén debidamente llenados según lo descrito en esta DPC y que todos los datos que aparecen en los mismos son correctos, con lo que procede a la generación del certificado activando el atributo de acuerdo al tipo de certificado que se autorizó.
6. El agente certificador debe cerciorarse de recibir debidamente firmada la carta de confidencialidad y uso del certificado de equipo antes de hacer entrega del certificado al solicitante.
7. Si la solicitud o el requerimiento no cumplen con lo establecido, se debe hacer del conocimiento del solicitante, para que haga las correcciones correspondientes.

5.5.1. CRITERIOS DE LLENADO DEL REQUERIMIENTO PARA CERTIFICADOS DE EQUIPO.

1. Se utilizan mayúsculas y minúsculas.
2. No se utilizan acentos.
3. Sólo se utilizan abreviaturas en los campos de Razón Social y Dirección cuando la información exceda el límite, conforme a las reglas ortográficas.
4. Razón Social: Se captura el nombre de la organización correspondiente, por ejemplo: “Secretaria de Economía”.
5. Área: Se captura el área a la que pertenezca.
6. Nombre: Nombre del equipo, dominio o IP pública del servidor o equipo correspondiente
7. Dirección: Se anota el domicilio en donde se ubique el equipo; utilizando el signo #, en lugar de cualquier otra forma de abreviatura para el número del inmueble en el que se ubiquen.
8. Código postal: (5 dígitos)
9. Ciudad y entidad federativa, los que corresponden al domicilio.
10. Nivel de seguridad: es al menos High Grade (1024 bits).
11. País: México.
12. Correo electrónico: se captura el e-mail del solicitante, todo en minúsculas.
13. Clave de Acceso: Capturar una contraseña de al menos 8 caracteres, con combinación de letras y números (opcional).
14. CryptProvider (Proveedor criptográfico): el que corresponda al dispositivo o mecanismo de protección de la clave privada (opcional).

5.6. EMISIÓN DE CERTIFICADOS DIGITALES CON PROTECCIÓN DE CLAVES EN ARCHIVOS.

1. Solo se emitirán en los casos señalados en esta DPC.
2. Se utilizará una herramienta informática para la generación del archivo .req y .key.
3. El Archivo .req se generará utilizando los criterios de llenado de requerimiento.
4. El Archivo .key solo debe quedar en posesión del titular y no se guardarán copias.
5. El archivo .req se enviará al agente certificador para la generación del certificado digital y se

enviará el archivo .cer al titular.

6. El titular o responsable del certificado deberá firmar los documentos señalados en los apartados correspondientes para el tipo de certificado digital que se le emitió.

6. REVOCACIÓN DE CERTIFICADOS DIGITALES

6.1 CAUSAS ADMISIBLES DE REVOCACIÓN

Cuando la clave privada de las AC estuviera comprometida, se revocan todos los certificados digitales de la comunidad correspondiente. No se puede solicitar ni generar certificados digitales hasta que no se restaure la identidad de la AC.

Cualquier certificado digital puede ser revocado si:

- Por extinción del periodo de validez del propio certificado digital
- Ha existido pérdida, robo, modificación, divulgación no autorizada u otro compromiso de la clave privada asociada al certificado digital.
- Por incumplimiento del titular en alguna de las obligaciones descritas en la Política de Certificación y en esta DPC.
- Falsedad, inexactitud o errores en los datos presentados en el certificado digital.
- Cuando alguno de los requisitos de emisión del certificado digital no se cumplió.
- El sistema de certificación se vio comprometido de modo tal que afecta a la fiabilidad del certificado digital.
- Fallecimiento del titular o incapacidad jurídica declarada por una autoridad competente.
- Cambio de información relativa al titular.
- Resolución administrativa o judicial que lo ordene.
- A solicitud del titular del certificado.
- Imposibilidad de lectura de la tarjeta o token en que se resguardó la clave privada.
- Conclusión de las funciones para las que le fue otorgado el certificado.

6.2. PROCEDIMIENTO DE REVOCACIÓN DE CERTIFICADOS

6.2.1. Por petición del titular del certificado:

- El titular del certificado, deberá acudir a las oficinas de la Dirección General de Normatividad Mercantil o a las Delegaciones Federales de la Secretaría de Economía
- Presentar un escrito libre con firma autógrafa del titular.
- Presentar algún documento de identidad de los señalados en el formato de solicitud DGNM-IT-5-CG-SOL.
- Si el procedimiento se realiza ante el Auxiliar de Agente, deberá ponerse en contacto con el Agente Certificador que emitió el certificado o con el Administrador de la AC y esperar la confirmación de revocación.
- Se deberá emitir el comprobante de revocación del certificado y entregarlo al solicitante, de acuerdo con los Lineamientos para la homologación, implantación y uso de la FEA en la APF, capítulo VI párrafo noveno.

6.2.2. Revocación en Línea:

Se brinda el servicio de revocación en línea para que el titular revoque su certificado digital, proporcionando para ello únicamente su clave de revocación que indicó en el requerimiento de certificación:

Para la AC-SIGER: https://ac.siger.gob.mx

Para la AC-DGNM: https://ac.siger.gob.mx/DGNM

6.2.3. Otras Revocaciones:
Si se produjo algún error durante la emisión de un certificado y es necesario generar otro, el agente certificador, debe revocar de inmediato el anterior, para poder generar otro al mismo titular. Si el titular, cuenta con certificado previamente y no puede usarlo, se le revocará previo a la generación de un nuevo certificado.

7. AUDITORÍA DE SEGURIDAD I NFORMÁTICA
Se recomienda la auditoría del Programa para Autoridades Certificadoras WebTrust.

7.1. TIPOS DE EVENTOS REGISTRADOS
- Los registros de accesos al servidor que contiene al sistema de las AC.
- Los registros que genera el sistema de las AC.
- Las solicitudes de emisión de certificados y de revocación (documental).
- La generación de los CD y las CRL.

7.2. PROCEDIMIENTOS DE RESPALDO DE REGISTROS DE AUDITORÍA
Para los registros electrónicos, se aplica la Política de Respaldos de la Información de la DGNM y sus procedimientos.

7.3. NOTIFICACIÓN DE VULNERABILIDADES
El administrador de la AC notifica cualquier vulnerabilidad en el sistema de AC al personal del área de Seguridad. El área de Seguridad deberá revisar el análisis de riesgos del sistema de AC al menos una vez al año.

8. ARCHIVOS
8.1. ARCHIVO DOCUMENTAL
El Departamento de Control de Certificados Digitales de la DGNM. Almacena los siguientes registros en papel: Para los Certificados de Identidad Personal:
- Formato de solicitud DGNM-IT-5-CG-SOL
- Copia simple de los documentos de identidad señalados en el formato DGNM-IT-5- CG-SOL.
- Copia simple de los documentos de personalidad jurídica señalados en el formato
- DGNM-IT-5-CG-SOL.
- Carta de Confidencialidad
- Comprobante de Emisión del Certificado.
- Copia de la Solicitud de Certificado Digital para Servidor Público

Para los Certificados de Equipo:
- Formato de solicitud DGNM-IT-5-CG-SOL.
- Carta de Confidencialidad y Uso
- Copia de la Identificación del Responsable del Equipo.

En caso de Revocaciones a petición del titular:
- Comprobante de Solicitud y Revocación de Certificado de FEA de Identidad Personal.

Otros:
- Copia de Nombramiento de Agentes.

- Copia de Nombramiento de Auxiliar de Agentes

PROTECCION DE ARCHIVOS

Los archivos electrónicos de auditoría son almacenados digitalmente de forma segura para evitar lectura, modificación o destrucción no autorizada. Para hacer esto, las copias de seguridad están protegidas criptográficamente y almacenadas en lugares de acceso sólo a personal autorizado.

La contraseña utilizada en las copias, sigue la Política de Contraseñas para el SIGER, y es sólo conocida por el personal que administra las AC.

La información almacenada en papel está bajo llave. Esta llave está bajo la responsabilidad del personal autorizado.

8.2. PERIODO DE ALMACENAMIENTO

Los archivos de auditoría y documental, se almacenan por un tiempo máximo de doce años.

9. RESPALDO Y RECUPERACIÓN

9.1. RESPALDOS

Se respalda la información del servidor que opere la AC-DGNM y AC-SIGER de acuerdo a la Política de Respaldo de la Información de la DGNM.

En cuanto a la clave privada de las AC está en todo momento cifrada cuando se almacene de modo permanente (FIPS 140-1 nivel 3). Este almacenaje se realiza en un lugar seguro que permita su recuperación si se produce algún tipo de contingencia.

9.2. RECUPERACION

9.2.1. POR COMPROMISO DE LA CLAVE PRIVADA

Si la clave privada de la AC-DGNM o AC-SIGER estuviera comprometida, se procedería a la revocación de la misma, siendo solamente válidos aquellos certificados digitales emitidos por la AC-DGNM o AC-SIGER cuya fecha de emisión fuera anterior a la fecha de revocación de la misma. El Comité de Seguridad de la Información de la DGNM decidirá si se toman medidas adicionales.

La generación de CRL se suspende hasta que se restaure la identidad de la AC comprometida.

El mismo procedimiento se lleva a cabo en las organizaciones con las que se hayan establecido reconocimiento de certificados digitales.

9.2.2. POR CONTINGENCIAS

En caso de contingencia, el personal a cargo de las AC-SIGER seguirá el procedimiento establecido en Plan de Contingencias del SIGER y PKI-SE.

10. SEGURIDAD

10.1. SEGURIDAD FÍSICA

El servidor que contiene las AC debe estar ubicado en la bóveda de seguridad del Centro de Datos de la DGNM.

El área está protegida por esclusas y un mecanismo de seguridad que evita la captación externa de las emanaciones de ondas electromagnéticas de los equipos.

10.1.1. ACCESO FÍSICO

El acceso a la bóveda de seguridad del centro de datos, está restringido a personal del SIGER autorizado, mediante un sistema de control de accesos, quedando registrado y grabado en CCTV (Circuito Cerrado de Televisión) cualquier acceso a la misma.

10.1.2. CONDICIONES FÍSICAS DE LA BÓVEDA DE SEGURIDAD.

La bóveda de seguridad del centro de datos tiene unidades de aire acondicionado de precisión. Tanto la humedad como la temperatura se controlan automáticamente.

Tiene módulos UPS instalados, una planta de emergencia generadora de energía eléctrica, supresores de transitorios que garantizan un fluido eléctrico constante sin interrupciones ni picos, y tierra física.
El centro de datos tiene medidas de seguridad contra inundaciones. Así mismo, tiene sistemas de detección temprana de humo y extinción de incendios.

10.1.3. MEDIOS DE ALMACENAMIENTO

Los sistemas del SIGER cuentan con software para respaldos (en el equipo HP). Se realizan copias de seguridad de acuerdo a la Política de Respaldos de la Información de la DGNM. Las copias de seguridad se resguardan en sitios determinados.

10.1.4. RESPALDO DE INFORMACIÓN FUERA DEL CENTRO DE DATOS DE LA DGNM

El respaldo de información se localiza en un sitio alterno.

10.2. SEGURIDAD EN LOS PROCEDIMIENTOS DE OPERACIÓN

10.2.1. ACTORES DE CONFIANZA INVOLUCRADOS

Se puede distinguir los siguientes actores en la operación de las AC:

- La DSIGER.
- Administrador del sistema de AC.
- Personal de seguridad del SIGER.
- Los agentes certificadores.
- Auxiliares de agente.

Las responsabilidades de estos actores, se delimitan en la sección de Responsabilidades de este documento.

10.2.2. NÚMERO DE PERSONAS REQUERI DO POR TAREA

- Un administrador del servidor de AC, del servidor de publicación de certificados digitales, CRL y del servicio OCSP.
- Un administrador de la infraestructura de emisión de Sellos de Tiempo.
- Agentes certificadores.
- Al menos un auxiliar de agente en cada representación federal.

10.2.3. IDENTIFICACIÓN Y AUTENTICACIÓN DE CADA ACTOR

No existe ningún tipo de identificación y autenticación para los actores. Los actores de confianza involucrados se conocen unos a otros y forman parte del personal de la DGNM, a excepción de los auxiliares de agente de las delegaciones estatales, quienes se autenticarán previamente a la emisión de cada certificado, con el envío de su nombramiento firmado por el titular de la dependencia y se podrá consultar en el archivo del Departamento de Control de Certificados Digitales de la DGNM.

10.3. SEGURIDAD EN EL PERSONAL

10.3.1. REQUERIMIENTOS DE FORMACIÓN DEL PERSONAL DE SEGURIDAD

El personal debe ser licenciado o ingeniero en Informática o área afín. Comprobar al menos dos años de experiencia en el campo de seguridad informática y acreditar conocimientos en seguridad informática.

Cumplir con el requisito de no haber sido condenado por delito contra el patrimonio de las personas o que haya merecido pena privativa de la libertad, ni que por cualquier motivo haya sido inhabilitado para el ejercicio de su profesión, para desempeñar un puesto en el servicio público, en el sistema financiero o para ejercer el comercio.

10.3.1.1. DOCUMENTACIÓN PROPORCIONADA AL PERSONAL QUE OPERA LAS AC

Al personal que se encarga de la operación de las AC se le entrega la siguiente documentación:

1) Política de Certificación de las AC-DGNM y AC-SIGER.
2) Declaración de Prácticas de Certificación de las AC-DGNM y AC-SI GER.
3) Manuales de Operación de las AC-DGNM y AC-SIGER.
4) Plan de Administración de Claves de las AC-DGNM y AC-SI GER.
5) Política General de Seguridad de la Información de la DGNM.
6) Política de Seguridad Física del SIGER.
7) Plan de Contingencias del SIGER y PKI-SE.

10.3. 2. DESIGNACIÓN DE UN AGENTE CERTIFICADOR

1. El candidato a agente certificador, debe ajustarse al Procedimiento de Nombramiento de Agente Certificador, procedimiento interno de la DGNM.
2. Una vez concluido el mismo, recibe un oficio de Nombramiento de Agente Certificador, emitido por el Director General de Normatividad Mercantil, con copia para el Director del SIGER para que se le genere su certificado de agente.
3. Con la recepción de su certificado de agente, debe firmar su carta de Confidencialidad y de Reconocimiento de la Política de Certificación.

10.3.3. DESIGNACIÓN DE UN AUXILIAR DE AGENTE CERTIFICADOR

1. El auxiliar de agente certificador, debe ser nombrado por el delegado o subdelegado federal de la entidad correspondiente mediante el oficio de Nombramiento de Auxiliar de Agente, con copia al Director General de Normatividad Mercantil.
2. Por la naturaleza de sus funciones, se recomienda que cuente con licenciatura o carrera técnica en el área de informática.
3. Debe obtener los conocimientos sobre las actividades que realiza el auxiliar de agente, auto-capacitándose con los manuales que le proporcionará la DGNM.
4. Debe firmar su carta de Confidencialidad y de Reconocimiento de la Política de Certificación y enviarla a la Dirección General de Normatividad Mercantil.

10.4. SEGURIDAD LÓGICA

10.4.1. INSTALACIÓN Y GENERACIÓN DEL PAR DE CLAVES

El par de claves de cada AC, son generadas utilizando el módulo criptográfico de almacenamiento seguro de claves (HSM).

La contraseña para la protección de la clave privada, almacenada en el módulo criptográfico (HSM), debe cumplir con lo estipulado en la Política de Contraseñas del SIGER y PSC. La clave privada, una vez que se almacene en el módulo criptográfico, debe estar cifrada.

10.4.2. SISTEMA DE CUSTODIOS PARA LA OPERACIÓN DE LA AC.

El arranque de la operación de la AC está protegido por el módulo criptográfico, el cual está configurado con un sistema de operadores o custodios en el que se requieren n de m tarjetas presentes, que están bajo resguardo de personal de la DGNM.

Las contraseñas utilizadas para el arranque de las AC deben cumplir con la Política de Contraseñas del SIGER. La contraseña de cada persona que gestiona la actividad de las AC es conocida sólo por ésta. Cualquier cambio de dicho personal implica la modificación de dicha contraseña.

Mantenimiento

Todos los cambios realizados sobre estas Prácticas de Certificación son anunciados en la página WEB del SIGER.
Si los cambios son de envergadura se deja abierto un periodo de quince días para la recepción de comentarios. Si no es posible conseguir una aprobación de los cambios estos no son realizados.

Responsabilidades

RESPONSABILIDADES DE LA DSIGER

1. Ofrecer y mantener la infraestructura necesaria para el establecimiento de una PKI, según lo descrito en este documento.
2. Implantar y mantener los requerimientos de seguridad impuestos a las claves criptográficas de la AC-SI GER y AC-DGNM, según lo descrito en este documento.
3. Poner a disposición de quien desee verificar una FEA, las copias de los certificados digitales y de cualquier información de revocación con referencia a dichos certificados digitales. Para ello cumplirá con lo establecido en el apartado de Disponibilidad de CRL y OCSP.
4. Proteger los datos de carácter personal que sean suministrados por la comunidad,
5. de acuerdo con la Ley Federal de Transparencia y de Acceso a la Información Pública Gubernamental.
6. Comunicar inmediatamente a la comunidad, el compromiso, pérdida, divulgación, modificación o uso no autorizado de la clave privada de las AC, con el fin de restaurar la PKI lo antes posible según lo establecido en este documento.
7. Cualquier anomalía o incidente producidos entre el momento de la revocación del certificado digital y de la clave privada de las AC y el momento de la notificación a la comunidad y posterior revocación de los certificados digitales emitidos, es responsabilidad única y exclusiva de la DSIGER.
8. Cualquier incidente o responsabilidad generada de la clave privada de las AC que se encuentre comprometida, es responsabilidad única y exclusiva de la DSIGER.

RESPONSABILIDADES DEL ADMINISTRADOR DEL SISTEMA DE AC:

1. Dar mantenimiento y manejar los servidores que opera la AC.
2. Respaldar información (software, base de datos, etc.)
3. Seguir los procedimientos y dictámenes de esta DPC para la generación y revocación de certificados digitales.
4. Monitorear los registros generados por el sistema de AC, del S.O. del servidor y de los accesos a la bóveda de seguridad del centro de datos que alberga el servidor dedicado a la operación de la AC.

RESPONSABILIDADES DEL PERSONAL DE SEGURIDAD DEL SIGER:

1. Mantener la seguridad física de la PKI.
2. Revisar los registros generados por el sistema de AC, del S.O. del servidor de AC y de los accesos

a la bóveda de seguridad del centro de datos donde se localiza el servidor de AC.

DE LOS AGENTES CERTIFICADORES

1. Conocer la Política de Certificación y la Declaración de Prácticas de Certificación y seguir todas las reglas en ellas descritas.
2. Vigilar la vigencia de su certificado de Agente Certificador y gestionar su renovación previo a su vencimiento.
3. Llevar a cabo el procedimiento para la emisión de CD, establecido en esta DPC.
4. Emitir certificados digitales de la duración y tipo establecidos en esta DPC.
5. No emitirán certificados de prueba.
6. Cuando el CD es solicitado ante un Auxiliar de Agente, es responsabilidad del agente certificador cerciorarse de que el titular de un CD haya acreditado su personalidad jurídica y comprobado su identidad.
7. Cuando el CD es solicitado ante un agente, debe llevar a cabo la identificación y acreditación jurídica del titular, conforme a lo establecido en la DPC.
8. Realizarán la revocación de certificados digitales, de acuerdo a lo establecido en esta DPC.
9. Cuando el CD es solicitado ante el Agente, deberá recabar la documentación que se indica en la presente DPC y hacerla llegar al Departamento de Control de Certificados Digitales de la DGNM para su archivo.
10. Cualquier incidente o responsabilidad generada por el compromiso de la clave privada de los agentes certificadores será responsabilidad única y exclusiva de ellos

DE LOS AUXILIARES DE AGENTES CERTIFICADORES

1. Conocer la Política de Certificación y la Declaración de Prácticas de Certificación y seguir todas las reglas en ellas descritas
2. Llevar a cabo la identificación y acreditación jurídica del titular, de acuerdo con los procedimientos establecidos en esta DPC.
3. Realizar los pasos que los involucran y que están descritos en los Procedimientos de Emisión de Certificados Digitales de la presente DPC
4. Recabar la documentación que se indica en la presente DPC y hacerla llegar al Departamento de Control de Certificados Digitales de la DGNM para su archivo.

RESPONSABILIDADES DE LOS USUARIOS

1. En el caso de compromiso de la clave privada (o de sospecha de compromiso) del certificado digital de un usuario, éste se compromete a notificarlo a AC-DGNM o AC- SIGER y a las partes implicadas.
2. Cualquier anomalía o incidente producidos entre el momento de la revocación de un certificado digital emitido por la AC-DGNM y AC-SIGER, y el momento de la notificación de tal evento a la Autoridad Certificadora, es responsabilidad única y exclusiva del usuario propietario de dicho certificado digital.
3. Cualquier incidente o responsabilidad originados del compromiso de la clave privada de un usuario será responsabilidad única y exclusiva de éste.
4. El titular del CD es el responsable único y final de mantener la confidencialidad de la clave privada de FEA, por tanto la información que firme utilizando su CD le será atribuible exclusivamente a él.

SANCIONES

Los agentes certificadores y sus auxiliares, para salvaguardar la legalidad, honradez, lealtad, imparcialidad y eficiencia que deben ser observadas en el desempeño de su función y cuyo

incumplimiento dará lugar al procedimiento y a las sanciones que correspondan, en términos de la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos, y tendrán las siguientes obligaciones:

I. Cumplir con la máxima diligencia el servicio que le sea encomendado y abstenerse de cualquier acto u omisión que cause la suspensión o deficiencia del servicio que implique abuso o ejercicio indebido de su cargo o comisión;
II. Utilizar los recursos que tengan asignados para el desempeño de su cargo o comisión, las facultades que le sean atribuidas o la información reservada a que tenga acceso por su función exclusivamente para los fines establecidos es esta política;
III. Custodiar y cuidar la documentación e información que por razón de su cargo o comisión conserve bajo su cuidado o a la cual tenga acceso, impidiendo o evitando el uso, la sustracción, destrucción, ocultamiento o inutilización indebidas de aquéllas;
IV. Observar buena conducta en su cargo o comisión, tratando con respeto, diligencia, imparcialidad y rectitud a las personas con las que tenga relación con motivo de éste.

Sí llegare a detectarse alguna anomalía que presuma el incumplimiento de la política de certificación, la misma será puesta a consideración del Comité de Seguridad de la Información de la DGNM a fin de evaluar la gravedad del caso y de considerarlo necesario se hará del conocimiento del Director General de Normatividad Mercantil a fin a que proceda a instrumentar las acciones necesarias para evitar reincidencias e independientemente, de hacerlo del conocimiento del órgano de control interno para los efectos correspondientes.

Registro de Cambios			
Versión Anterior	**Descripción del Cambio**	**Fecha del Cambio**	**Participantes en la Revisión del Cambio**
1.0	• Se eliminan secciones y procedimientos considerados como internos de la DGNM. • Se modifica la redacción de la DPC, en todas sus secciones, para que quede más clara, precisa y sobre todo previendo los cambios tecnológicos. • Se agrega el procedimiento para tipo de certificado para el Sector Público. (CD-SP). • Se agrega el procedimiento para la Emisión de Certificados Digitales con Protección de Claves en Archivos. Se agregan especificaciones para los certificados que se emiten con motivo de huellas ilegibles. Se realizaron modificaciones a los formatos. Se agrega el cuadro de registro de cambios.	Del 01/ May/ 2008 al 07/ Ago/ 2008/	Silvia Elena Hernández Martínez Karina Romo Maldonado Ernesto del Castillo Hernández Mario Guerrero Barrera

REFERENCIAS

[1] RFC 2527 “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework” Marzo 1999, ftp://ftp.isi.edu/in-notes/rfc2527.txt
[2] Ley Orgánica 15/ 1999, de 13 de Diciembre, de Protección de protección de datos de carácter personal y sus normas de desarrollo, https://www.agenciaprot ecciondatos.org/datd1.htm
[3] RFC 2459 “Internet X.509 Public Key Infrastructure: Certificate and CRL Profile” Enero 1999, ftp://ftp.isi.edu/in-notes/rfc2459.txt

ANEXOS

SOLICITUD DE CERTIFICADO DIGITAL DE FEA

<table>
<tr><td colspan="3">Nombre del Solicitante:_____
R.F.C: .:_____CURP _____</td></tr>
<tr><td colspan="2">Razón Social: Area:</td><td>Estado/plaza: Municipio:</td></tr>
<tr><td colspan="3">Domicilio de la oficina del Solicitante: (Incluir: calle, número, colonia, Del. o Mun. y Código Postal)</td></tr>
<tr><td colspan="2">Correo electrónico:</td><td>Tel.(s):</td></tr>
<tr><td>DOCUMENTO DE IDENTIDAD</td><td>DOCUMENTO PROBATORIO DE IDENTIDAD</td><td>DOCUMENTO DE PERSONALIDAD JURÍDICA</td></tr>
<tr><td>Cédula Profesional
Pasaporte
Credencial de Elector
Cartilla del Servicio Militar Nacional.
Identificación con fotografía expedida por Gobierno Federal, Estatal o Municipal</td><td>Copia Certificada de Acta de Nacimiento
Documento Migratorio
Carta de Naturalización
Certificado de Nacionalidad Mexicana</td><td>FIAT
Nombramiento
Patente
credencial de notario
Credencial de corredor
Habilitación de corredor.
Habilitación de Responsables de oficina.</td></tr>
<tr><td colspan="3">Observaciones:
Fecha y Firma del Solicitante
Datos del Agente Certificador o Auxiliar del Agente:</td></tr>
<tr><td colspan="3">Nombre:</td></tr>
<tr><td colspan="2">Cargo:</td><td>Firma:</td></tr>
</table>

TERMINOS:

• El suscrito, cuyos datos generales aparecen al anverso de la presente solicitud, y a quien en lo sucesivo se le denominará como "El Solicitante" para todos los efectos legales que deriven del presente documento a que haya lugar, manifiesta ante ***La Secretaría de Economía*** a quien en lo sucesivo se le denominará como "La Agencia o Autoridad Certificadora" (AC), que es su libre voluntad contar con un Certificado Digital de Firma Electrónica Avanzada en el que conste la clave pública que se encuentra asociada a la clave privada y frase de seguridad de revocación que manifiesta haber generado previamente y en absoluto secreto, sin que persona alguna lo haya asistido durante dicho proceso.

• Asimismo, "El Solicitante", manifiesta su conformidad en que "La AC" utilice el procedimiento de certificación de identidad que estime conveniente.

• "El Solicitante" reconoce que para la emisión del referido Certificado Digital de Firma Electrónica Avanzada, "La AC" revisó la documentación que se indica en el anverso de esta solicitud, con la cual el propio usuario se identificó, constatando a simple vista que los documentos corresponden a "El Solicitante", por lo que este último asume la responsabilidad exclusiva respecto de la autenticidad de los datos y documentación por él proporcionada a "La AC". De la misma forma "El Solicitante" asume la responsabilidad exclusiva del debido uso del Certificado Digital de Firma Electrónica Avanzada.

• "El Solicitante" en este acto acepta el certificado digital mencionado, sirviendo este documento como el acuse de recibo más amplio que en derecho proceda.

• Adicionalmente, "El Solicitante", acepta que el uso de la clave privada y frase de seguridad de revocación, con base en las cuales dicho certificado fue elaborado, quedarán bajo su estricta y absoluta responsabilidad, la cual incluye en forma enunciativa, los daños y perjuicios, incluso aquéllos de carácter financiero, que pudieran causarse por su uso indebido, no pudiendo alegar que tal uso se realizó por persona no autorizada.

• "El Solicitante" conoce y acepta que la clave pública proporcionada por él y contenida en el Certificado Digital de Firma Electrónica Avanzada, así como en cualquier otro certificado digital que con posterioridad se obtenga, será de carácter público y podrá ser consultada libremente por cualquier interesado a través de los medios y formas que disponga "La AC".

• Por lo anterior, "El Solicitante" se obliga a mantener absoluta confidencialidad de la clave privada y frase de seguridad de revocación, así como a realizar los trámites necesarios para la revocación de dicho certificado ante "La AC", mediante los mecanismos y procedimientos que el mismo establezca, en el caso de que por cualquier causa dicha información sea divulgada o se

realice cualquier supuesto por el que "El Solicitante" deba solicitar su revocación en los términos de las disposiciones legales vigentes.

• Por otra parte "El Solicitante" manifiesta conocer el contenido y alcance de las disposiciones legales y reglamentarias relativas a la celebración de actos jurídicos mediante el uso de medios electrónicos, digitales o de cualquier otra tecnología, por lo que asume plena responsabilidad respecto de la información y contenido de todo documento electrónico o digital elaborado y enviado en el que se haga uso de la citada clave privada, toda vez que por ese solo hecho se considerara que el documento electrónico o digital le es atribuible.

• "El Solicitante" reconoce y acepta que "La AC" únicamente es responsable de los errores que, en su caso, llegaren a cometer con motivo de culpa grave en el proceso de generación, registro, entrega y revocación del certificado digital, según corresponda, así como que no será responsable por los daños y perjuicios que se pudieran causar a "El Solicitante" o a terceros, cuando por caso fortuito o fuerza mayor no puedan realizarse registros, verificaciones, revocaciones o tramitar documentos electrónicos cifrados con las claves públicas y privadas relacionadas con dicho certificado. Por caso fortuito o fuerza mayor se entenderá todo acontecimiento o circunstancia inevitable, más allá del control razonable de "La AC", que le impida el cumplimiento de sus funciones con el carácter que le corresponde y reconoce a través de su firma autógrafa asentada en el espacio designado para ello en el anverso y reverso de este formato, como prueba fehaciente de la aceptación de todo lo especificado en el mismo.

CONDICIONES:

• El Certificado Digital que se genera, derivado de la realización de este trámite, estará disponible en https://***ac.siger.gob.mx*****;** para que "El Solicitante" realice la descarga del mismo.

• La Firma Electrónica Avanzada asignada es personal e intransferible y el uso de la misma es responsabilidad de la persona que la solicite.

• La Firma Electrónica Avanzada tendrá los mismos alcances y efectos que la firma autógrafa.

• Con esta firma podrá hacer uso de servicios y trámites electrónicos disponibles en las Dependencias, Entidades, Organizaciones e Instituciones.

• "El Solicitante" será responsable de las obligaciones derivadas del uso no autorizado de su firma.

• "El Solicitante" acepta que deberá notificar oportunamente a "La AC", la invalidación, pérdida o cualquier otra situación que pudiera implicar la reproducción o uso indebido de su clave privada.

• "El Solicitante" acepta las condiciones de operación y límites de responsabilidad de la ***Secretaria de Economía*** en su calidad de "La AC".

Firma del Solicitante:

_____

COMPROBANTE DE EMISIÓN DE CERTIFICADO DE IDENTIDAD PERSONAL DE FIRMA ELECTRONICA AVANZADA

< Lugar y fecha aquí>

La Autoridad Certificadora < del Sistema Integral de Gestión Registral o de la Dirección General de Normatividad Mercantil> de la Secretaría de Economía, certifica que el Solicitante: < poner aquí nombre del Solicitante> , entregó un requerimiento de certificación que contiene la solicitud para la generación de su Certificado Digital de Firma Electrónica Avanzada.

Estando presente el Solicitante se llevó a cabo el procedimiento de emisión y registro de certificados digitales de conformidad con lo establecido en el "Acuerdo Interinstitucional por el que se establecen los lineamientos para la homologación, implantación y uso de la Firma Electrónica Avanzada en la Administración Pública Federal" publicado en el Diario Oficial de la Federación el 24 de agosto de 2006.

Asimismo, que como resultado del proceso se generó su Certificado Digital con número de serie: < poner aquí número de serie> y clave pública: < poner clave pública en cadena de caracteres>

Previo a la emisión del presente certificado, el titular reconoce haber leído y aceptado los términos y condiciones de uso establecidos en el anverso del formato "Solicitud de Certificado Digital de Firma Electrónica Avanzada".

El resguardo de la clave privada relacionada con el certificado amparado por el presente Acuse, así como su medio de almacenamiento, es responsabilidad del titular del Certificado Digital.

Titular: < poner nombre del Solicitante aquí>
CURP: < poner CURP aquí>
RFC: < poner RFC aquí>

_____
Firma de conformidad

COMPROBANTE DE SOLICITUD Y REVOCACION DE CERTIFICADO DIGITAL DE FIRMA ELECTRONICA AVANZADA DE IDENTIDAD PERSONAL.

La Autoridad Certificadora < del Sistema Integral de Gestión Registral o de la Dirección General de Normatividad Mercantil> de la Secretaría de Economía, certifica que el Titular: < poner aquí nombre del Titular>, solicitó la revocación de su Certificado Digital con número de serie: < poner aquí número de serie> y clave pública: < poner clave pública en cadena de caracteres>, en virtud de < poner el motivo de la revocación>, de conformidad con lo establecido en el Acuerdo Interinstitucional por el que se establecen los lineamientos para la homologación, implantación y uso de la Firma Electrónica Avanzada en la Administración Pública Federal" publicado en el Diario Oficial de la Federación el 24 de agosto del 2006.

Por consiguiente, se llevó a cabo la revocación del referido Certificado Digital, siendo las < poner hora aquí> del < poner fecha aquí>.

Nombre y Firma del solicitante:	Nombre y Firma del Agente:

CARTA DE CONFIDENCIALIDAD Y RESPONSABILIDAD DE FEDATARIO PÚBLICO

Secretaría de Economía
P r e s e n t e.

El que suscribe (nombre del fedatario público), titular de la (señalar: 1) si se trata de notaría o correduría, 2) el número que le corresponde, 3) estado o plaza y 4) en caso de notarios el municipio o distrito) cuyos datos de certificado se anexan a la presente carta, advertido por (el agente certificador o auxiliar de agente)(nombre del agente certificador ó del auxiliar de agente que actúa) de la (Dirección General de Normatividad Mercantil o Delegación Federal de la Secretaría de Economía del Estado de) de los delitos en que incurren los que se conducen con falsedad ante una autoridad distinta a la judicial, manifiesto que:

I. Reconozco desde el día de hoy como propia y auténtica la información que en lo sucesivo envíe por medios electrónicos, que sea distinguida a través de la firma electrónica que se produzca a partir de la utilización de mis datos de creación de firma y del certificado que me ha generado la Secretaría de Economía por conducto de la Dirección General de Normatividad Mercantil, con número de serie y la vigencia del _____al _____.
II. Que el agente certificador de la Secretaría de Economía puso a mi disposición los elementos técnicos necesarios para elaborar mi requerimiento, y posteriormente generar mis datos de creación de firma, estos últimos han sido de mi exclusivo conocimiento en todo momento.
III. Acepto que el uso de mis datos de creación de firma quedará bajo mi exclusiva responsabilidad y que no debo de revelar mis datos de creación de firma. le corresponda.
IV. Notificaré a la Secretaría de Economía, para su invalidación, la pérdida o cualquier otra situación que pudiera implicar el uso indebido de mis datos de creación de firma en los términos a que se refiere el artículo 14 del Reglamento del Registro Público de Comercio.
V. Estoy de acuerdo en proporcionar a la Dirección General de Normatividad Mercantil de la Secretaría de Economía, la información adicional que respecto del proceso de generación de mi certificado me sea requerida.
VI. Manifiesto que el agente certificador de la Secretaría de Economía dio lectura y explicó el alcance de los artículos 11 y 12 del Reglamento del Registro Público de Comercio.
VII. Que el certificado y mis datos de creación de firma los utilizaré para los efectos que marcan los artículos 30 Bis y 30 Bis 1 del Código de Comercio los cuales me fueron leídos y explicados en su alcance por el agente certificador de la Secretaría de Economía.
VIII. En caso de incumplir con lo estipulado en la presente carta acepto que la Secretaría de Economía revoque en cualquier momento mi certificado, sin perjuicio de las demás responsabilidades en las que pueda incurrir o que me correspondan.

(Nombre y firma del fedatario público al calce y al margen)

CONSTANCIA DE ILEGIBILIDAD DE HUELLAS DACTILARES

< Lugar y fecha aquí>

El Agente Certificador o Auxiliar del Agente Certificador< poner aquí nombre del Agente o Auxiliar > adscrito a la < poner aquí nombre de la unidad a la que pertenece> de la Secretaría de Economía, **HACE CONSTAR** que el fedatario < poner aquí nombre del Solicitante y número de la Notaria o Correduría Pública> se presentó de forma personal para solicitar la generación de su Certificado de Digital de Firma Electrónica Avanzada y se hace constar lo siguiente:

Se llevó a cabo el procedimiento de captura de su huella dactilar, para el procedimiento de generación de Certificado Digital con el uso de dispositivo biométrico, y una vez que se probó el procedimiento con todos sus dedos sin que se haya conseguido capturar su huella dactilar por ser ilegible, por lo que se procede, dada esta circunstancia, a generar un certificado digital con uso de contraseña, almacenando en el dispositivo biométrico sus llaves pública y privada.

_____

Nombre y Firma del Agente Certificador o Auxiliar del Agente Certificador.

CARTA DE CONFIDENCIALIDAD Y RESPONSABILIDAD DE FEDATARIO PÚBLICO
(Para huellas ilegibles)

Secretaría de Economía
P r e s e n t e.

El que suscribe (nombre del fedatario), titular de la (señalar: 1) si se trata de notaría o correduría, 2) el número que le corresponde, 3) estado o plaza y 4) en caso de notarios el municipio o distrito) cuyos datos de certificado se anexan a la presente carta, advertido por (el agente certificador o auxiliar de agente)(nombre del agente certificador o del auxiliar de agente que actúa) de la (Dirección General de Normatividad Mercantil o Delegación Federal de la Secretaría de Economía del Estado de) de los delitos en que incurren los que se conducen con falsedad ante una autoridad distinta a la judicial, manifiesto que:

Debido a que durante el procedimiento de captura de la huella dactilar en el dispositivo biométrico, no fue posible realizarlo para ninguno de mis dedos por ser ilegibles los rasgos, ante esta imposibilidad y a mi solicitud, la Dirección General de Normatividad Mercantil por conducto del Agente Certificados antes señalado, procedió a generar mi certificado digital con el uso de contraseña que solo yo conozco, asimismo, que en el dispositivo biométrico queda almacenada mi llave pública y privada, por lo que a partir de este momento me hago responsable único del uso que se le de a mi llave privada, adicionalmente:

I. Reconozco desde el día de hoy como propia y auténtica la información que en lo sucesivo envíe por medios electrónicos, y que sea distinguida a través de la firma electrónica que se produzca a partir de la utilización de mis datos de creación de firma y del certificado que me ha generado la Secretaría de Economía por conducto de la Dirección General de Normatividad Mercantil, con número de serie y la vigencia del al _____.
II. Que el agente certificador de la Secretaría de Economía puso a mi disposición los elementos técnicos necesarios para elaborar mi requerimiento, y posteriormente generar mis datos de creación de firma, estos últimos han sido de mi exclusivo conocimiento en todo momento.
III. Acepto que el uso de mis datos de creación de firma quedará bajo mi exclusiva responsabilidad y que no debo de revelar mi contraseña ni mis datos de creación de firma a ningún tercero, ya que son de mi exclusivo uso y responsabilidad.
IV. Notificaré a la Secretaría de Economía, la pérdida o cualquier otra situación que pudiera implicar el uso indebido de mi contraseña, así como de mis datos de creación de firma en los términos a que se refiere el artículo 14 del Reglamento del Registro Público de Comercio, para su invalidación.
V. Estoy de acuerdo en proporcionar a la Dirección General de Normatividad Mercantil de la Secretaría de Economía, la información adicional que respecto del proceso de generación de mi certificado me sea requerida.
VI. Manifiesto que el agente certificador de la Secretaría de Economía dio lectura y explicó el alcance de los artículos 11 y 12 del Reglamento del Registro Público de Comercio.
VII. Que el certificado, mi contraseña y mis datos de creación de firma los utilizaré para los efectos que marcan los artículos 30 Bis y 30 Bis 1 del Código de Comercio los cuales me fueron leídos y explicados en su alcance por el agente certificador de la Secretaría de Economía.
VIII. En caso de incumplir con lo estipulado en la presente carta acepto que la Secretaría de Economía revoque en cualquier momento mi certificado, sin perjuicio de las demás responsabilidades de carácter civil y/o penal en las que pueda incurrir o que me correspondan.

_____
(Nombre y firma del fedatario público)

CARTA DE CONFIDENCIALIDAD Y RESPONSABILIDAD DE RESPONSABLE DE OFICINA

Secretaría de Economía
P r e s e n t e.

El que suscribe (nombre del responsable de oficina), habilitado por la Secretaría de Economía como Responsable de la Oficina en (señalar la oficina según su habilitación) cuyos datos de certificado se anexan a la presente carta, advertido por (el agente certificador o auxiliar de agente) (nombre del agente certificador o del auxiliar de agente que actúa) de la (Dirección General de Normatividad Mercantil o Delegación Federal de la Secretaría de Economía del Estado de) de los delitos en que incurren los que se conducen con falsedad ante una autoridad distinta a la judicial, manifiesto que:

I. Reconozco desde el día de hoy como propia y auténtica la información que en lo sucesivo envíe por medios electrónicos, que sea distinguida a través de la firma electrónica que se produzca a partir de mis datos de creación de firma y de la utilización del certificado que me ha generado la Secretaría de Economía por conducto de la Dirección General de Normatividad Mercantil, con número de serie_____ y la vigencia del_____ al_____.
II. Que el agente certificador de la Secretaría de Economía puso a mi disposición los elementos técnicos necesarios para elaborar mi requerimiento, y posteriormente generar mis datos de creación de firma, estos últimos han sido de mi exclusivo conocimiento en todo momento.
III. Acepto que el uso de mis datos de creación de firma quedará bajo mi exclusiva responsabilidad y que no debo de revelar mis datos de creación de firma.
IV. Notificaré a la Secretaría de Economía, para su invalidación, la pérdida o cualquier otra situación que pudiera implicar el uso indebido de mis datos de creación de firma en los términos a que se refiere el artículo 11 del Reglamento del Registro Público de Comercio.
V. Estoy de acuerdo en proporcionar a la Dirección General de Normatividad Mercantil de la Secretaría de Economía, la información adicional que respecto del proceso de generación de mi certificado me sea requerida.
VI. Manifiesto que el agente certificador de la Secretaría de Economía dio lectura y explicó el alcance del artículo 11 del Reglamento del Registro Público de Comercio.
VII. Que el certificado y mis datos de creación de firma sólo los utilizaré para los efectos que marcan los artículos 20 Bis y 21 Bis inciso c) del Código de Comercio y 11 del Reglamento del Registro Público de Comercio, los cuales me fueron leídos y explicados en su alcance por el agente certificador de la Secretaría de Economía.
VIII. En caso de incumplir con lo estipulado en la presente carta acepto que la Secretaría de Economía revoque en cualquier momento mi certificado y habilitación, sin perjuicio de las demás responsabilidades en las que pueda incurrir o que me correspondan.

_____

(Nombre y firma del responsable de oficina al calce y al margen)

CARTA DE CONFIDENCIALIDAD Y RESPONSABILIDAD DE RESPONSABLE DE OFICINA (PARA EL REGISTRO INMEDIATO DE EMPRESAS)

Secretaría de Economía
P r e s e n t e.

El que suscribe (Nombre del Res. de Oficina), habilitado por la Secretaría de Economía como Responsable de la Oficina del Registro Público de Comercio en el Estado de _____, cuyos datos de identificación se anexan a la presente carta, advertido por (el agente certificador o auxiliar de agente)(Nombre del agente autorizado por la DGNM), de los delitos en que incurren los que se conducen con falsedad ante una autoridad distinta a la autoridad judicial, manifiesto que:

I. Reconozco a partir del día de hoy como propia y auténtica la información que en lo sucesivo certifique o firme, a través de la firma electrónica, utilizando el Certificado Digital que me fue expedido por la Secretaría de Economía, por conducto de la Dirección General de Normatividad Mercantil, con número de serie___y la vigencia del_____ al_____

II. Asimismo, que el agente certificador de la DGNM, puso a mi disposición los elementos técnicos necesarios para elaborar mi requerimiento, y posteriormente generar mi Certificado Digital, datos de creación que han sido de mi exclusivo conocimiento.

III. Acepto que el uso de mis datos de creación de firma quedan bajo mi exclusiva responsabilidad y que no debo de revelar mi contraseña ni mis datos de creación de firma.

IV. Debo notificar a la DGNM, para que invalide mi certificado en caso de presentarse alguna situación que pudiera implicar el uso indebido de mis datos de creación de firma en los términos a que se refiere el artículo 11 del Reglamento del Registro Público de Comercio.

V. Estoy de acuerdo en proporcionar a la DGNM de la Secretaría de Economía, la información adicional que respecto del proceso de generación de mi certificado me sea requerida.

VI. Manifiesto que el agente certificador de la DGNM, una vez concluido el procedimiento de generación de mi certificado digital dio lectura y explicó el alcance del artículo 11 del Reglamento del Registro Público de Comercio.

VII. Que el certificado digital y mis datos de creación de firma electrónica se utilizarán para los efectos de inscribir en el Registro Público de Comercio de esta entidad federativa los actos a constitución de Sociedades Mercantiles y Sociedades Microindustriales utilizando las Formas Precodificadas M-4 y M-5 y siempre y cuando sean enviadas por Fedatarios Públicos autorizados utilizando el SIGER-Fed@net.

VIII. En caso de incumplir con lo estipulado en la presente carta acepto que la DGNM revoque en cualquier momento mi certificado y habilitación, sin perjuicio de las demás responsabilidades en las que pueda incurrir o que me correspondan.

_____

Nombre y firma del Responsable de Oficina

CARTA DE CONFIDENCIALIDAD Y RESPONSABILIDAD DEL SERVIDOR PÚBLICO

Secretaría de Economía
Presente

El que suscribe <nombre del servidor público>, en mi carácter de titular de < señalar puesto y unidad administrativa, estado, > en términos del acuerdo <poner términos> mediante el cual < poner términos >, manifiesto, bajo protesta de decir verdad lo siguiente:

I. Reconozco desde el día de hoy como propia y auténtica la información que en lo sucesivo envíe por medios electrónicos, que sea distinguida a través de la firma electrónica que se produzca a partir de mis datos de creación de firma y de la utilización del certificado que me ha generado la Secretaría de Economía por conducto de la Dirección General de Normatividad Mercantil, con número de serie _____y la vigencia del _____al_____.

II. Notificaré a la Dirección General de Normatividad Mercantil, como Unidad Certificadora de la Secretaría de Economía para la revocación del certificado a que se refiere la presente carta; la pérdida o cualquier otra situación que pudiera implicar la reproducción o uso indebido de mis datos de creación de firma electrónica y del certificado en un plazo que no mayor a 12 horas por medios electrónicos con acuse de recibo o por escrito al día hábil siguiente.

III. Acepto que el uso de datos de creación de mi firma electrónica y de mi certificado por persona distinta quedará bajo mi exclusiva responsabilidad, que por lo tanto soy responsable de su resguardo, asimismo, que en el caso de revelarlos en cualquier forma acepto como propia la información que sea enviada.

IV. Asumo cualquier tipo de responsabilidad derivada del mal uso que haga de mi certificado digital.

V. Que mi certificado y mis datos de creación de firma sólo los utilizaré para los efectos que marca el capítulo VI del Reglamento Interior de la Secretaría de Economía, publicado en el Diario Oficial de la Federación el 22 de noviembre de 2002.

VI. Estoy de acuerdo en ser requerido para el envío de cualquier información adicional respecto de mi certificado.

VII. Acepto que en caso de incumplir con lo estipulado en la presente carta la Unidad Certificadora de la Secretaría Economía podrá revocar en cualquier momento mi certificado, sin perjuicio de las demás responsabilidades en las que puedan incurrir o que correspondan.

_____
<Nombre, cargo y firma del servidor público>.

SOLICITUD DE CERTIFICADO DIGITAL PARA SERVIDOR PÚBLICO

TITULAR DE LA UNIDAD SOLICITANTE	
Nombre:	
Cargo:	
Organización:	
Correo Electrónico:	**Tel/Fax.**
Firma:	**Fecha.**

Por este conducto solicito la generación de certificado digital para las siguientes personas:	
Nombre:	**Cargo**

AUTORIZACIÓN DGNM		
Nombre:		
Cargo:		
Firma:	**Fecha.**	**Tipo de Certificado Autorizado**

AGENTE CERTIFICADOR	
Nombre:	
Cargo:	
Firma:	**Fecha.**

Ver términos y condiciones al reverse.

TERMINOS:

• Los suscritos, cuyos datos generales aparecen al anverso de la presente solicitud, y a quienes en lo sucesivo se le denominará como "El Solicitante" para todos los efectos legales que deriven del presente documento a que haya lugar, manifiestan ante ***La Secretaría de Economía*** a quien en lo sucesivo se le denominará "La Autoridad Certificadora" (AC), que es su voluntad contar con un Certificado Digital para Firma del Equipo de cómputo descrito en el anverso de la presente.

• "El Solicitante", manifiesta su conformidad en que "La AC" para que utilice el procedimiento de certificación de identidad que estime conveniente.

• "El Solicitante" reconoce que para la emisión del referido Certificado Digital, "La AC" acredito la personalidad de los solicitantes, por lo que el responsable del equipo aquí descrito, asume la responsabilidad exclusiva respecto de la autenticidad de los datos y documentación por él proporcionada a "La AC". De la misma forma el titular de la unidad solicitante, asume la responsabilidad de supervisar el correcto uso del Certificado Digital del equipo de cómputo.

• "El Solicitante" en este acto acepta el certificado digital mencionado, sirviendo este documento como el acuse de recibo más amplio que en derecho proceda.

• Adicionalmente, "El solicitante", acepta que el uso de la clave privada y frase de seguridad de revocación, con base en las cuales dicho certificado fue elaborado, quedarán bajo su estricta y absoluta responsabilidad, la cual incluye en forma enunciativa, los daños y perjuicios, incluso aquéllos de carácter financiero, que pudieran causarse por su uso indebido, no pudiendo alegar que tal uso se realizó por persona no autorizada.

• "El Solicitante" conoce y acepta que la clave pública proporcionada y contenida en el Certificado Digital para firma de equipo, así como en cualquier otro certificado digital que con posterioridad se obtenga, será de carácter público y podrá ser consultado libremente por cualquier interesado a través de los medios y formas que disponga "La AC".

• Por lo anterior, "El Solicitante" se obliga a mantener absoluta confidencialidad de la clave privada y frase de seguridad de revocación, así como a realizar los trámites necesarios para la revocación de dicho certificado ante "La AC", mediante los mecanismos y procedimientos que el mismo establezca, en el caso de que por cualquier causa dicha información sea divulgada o se realice cualquier supuesto por el que "El Solicitante" deba solicitar su revocación en los términos de las disposiciones legales vigentes.

• Por otra parte "El Solicitante" manifiesta conocer el contenido y alcance de las disposiciones legales y reglamentarias relativas a la celebración de actos jurídicos mediante el uso de medios electrónicos, digitales o de cualquier otra tecnología, por lo que asume plena responsabilidad respecto de la información y contenido de todo documento electrónico o digital elaborado y enviado en el que se haga uso de la citada clave privada, toda vez que por ese solo hecho se considerara que el documento electrónico o digital le es atribuible.

• "EL Solicitante" reconoce y acepta que "La AC" únicamente es responsable de los errores que, en su caso, llegaren a cometer con motivo de culpa grave en el proceso de generación, registro, entrega y revocación del certificado digital, según corresponda, así como que no será responsable por los daños y perjuicios que se pudieran causar a "El Solicitante" o a terceros, cuando por caso fortuito o fuerza mayor no puedan realizarse registros, verificaciones, revocaciones o tramitar documentos electrónicos cifrados con las claves públicas y privadas relacionadas con dicho certificado. Por caso fortuito o fuerza mayor se entenderá todo acontecimiento o circunstancia inevitable, más allá del control razonable de "La AC", que le impida el cumplimiento de sus funciones con el carácter que le corresponde y reconocen a través de sus firmas autógrafas asentada en el espacio designado para ello en el anverso y reverso de este formato, como prueba fehaciente de la aceptación de todo lo especificado en la presente Solicitud.

CONDICIONES:

• El Certificado Digital para Servidor Público que se genera, derivado de la realización de este trámite, estará disponible en https://***ac.siger.gob.m/DGNMx*****;** para que "La Unidad Solicitante" realice la descarga del mismo.

• El Certificado Digital para Firma de Servidor Público asignada es exclusiva para el Servidor Público especificado en la presente e intransferible y el uso de la misma es responsabilidad de la persona señalada y que tiene a su cargo el Servidor Público.

• Con este certificado podrá realizar las actividades asignadas estrictamente al Servidor Público dentro de la organización.

• "El Solicitante" será responsable de las obligaciones derivadas del uso no autorizado del Servidor Público.

• "El Solicitante" y el Servidor Público aceptan que deberán notificar oportunamente a "La AC", la invalidación, pérdida o cualquier otra situación que pudiera implicar la reproducción o uso indebido del certificado Digital para Firma de Servidor Público y aceptan las condiciones de operación y límites de responsabilidad de la **Secretaria de Economía** en su calidad de "La AC".

Firma el titular de la Unidad solicitante:

SOLICITUD DE CERTIFICADO DIGITAL PARA EQUIPO DE CÓMPUTO

DATOS DEL EQUIPO		
No. de serie:	IP:	
No. Inventario:	MAC Address:	
Nombre y dominio:		
Ubicación:		
Del. o Mpio.:	Estado:	C.P.
Breve descripción del uso que se le dará al certificado		
TITULAR DE LA UNIDAD SOLICITANTE		
Nombre:		
Cargo:		
Correo Electrónico:	Tel/Fax.	
Firma:	Fecha.	
RESPONSABLE TÉCNICO DEL EQUIPO		
Nombre:		
Quien se identificó con:		
Cargo:		
Organización:		
Correo Electrónico:	Tel/Fax.	
Firma:	Fecha.	
AUTORIZACIÓN DGNM		
Nombre:		
Cargo:		
Firma:	Fecha.	Tipo de Certificado Autorizado
AGENTE CERTIFICADOR		
Nombre:		
Cargo:		
Firma:	Fecha.	

TERMINOS Y CONDICIONES

Términos:

- Los suscritos, cuyos datos generales aparecen al anverso de la presente solicitud, y a quienes en lo sucesivo se le denominará como “El Solicitante” para todos los efectos legales que deriven del presente documento a que haya lugar, manifiestan ante La Secretaría de Economía a quien en lo sucesivo se le denominará “La Autoridad Certificadora” (AC), que es su voluntad contar con un Certificado Digital para Firma del Equipo de cómputo descrito en el anverso de la presente.
- “El Solicitante”, manifiesta su conformidad en que “La AC” para que utilice el procedimiento de certificación de identidad que estime conveniente.
- “El Solicitante” reconoce que para la emisión del referido Certificado Digital, “La AC” acredito la personalidad de los solicitantes, por lo que el responsable del equipo aquí descrito, asume la responsabilidad exclusiva respecto de la autenticidad de los datos y documentación por él proporcionada a “La AC”. De la misma forma el titular de la unidad solicitante, asume la responsabilidad de supervisar el correcto uso del Certificado Digital del equipo de cómputo.

- El Solicitante" en este acto acepta el certificado digital mencionado, sirviendo este documento como el acuse de recibo más amplio que en derecho proceda.
- Adicionalmente, "El solicitante", acepta que el uso de la clave privada y frase de seguridad de revocación, con base en las cuales dicho certificado fue elaborado, quedarán bajo su estricta y absoluta responsabilidad, la cual incluye en forma enunciativa, los daños y perjuicios, incluso aquéllos de carácter financiero, que pudieran causarse por su uso indebido, no pudiendo alegar que tal uso se realizó por persona no autorizada.
- "El Solicitante" conoce y acepta que la clave pública proporcionada y contenida en el Certificado Digital para firma de equipo, así como en cualquier otro certificado digital que con posterioridad se obtenga, será de carácter público y podrá ser consultado libremente por cualquier interesado a través de los medios y formas que disponga "La AC".
- Por lo anterior, "El Solicitante" se obliga a mantener absoluta confidencialidad de la clave privada y frase de seguridad de revocación, así como a realizar los trámites necesarios para la revocación de dicho certificado ante "La AC", mediante los mecanismos y procedimientos que el mismo establezca, en el caso de que por cualquier causa dicha información sea divulgada o se realice cualquier supuesto por el que "El Solicitante" deba solicitar su revocación en los términos de las disposiciones legales vigentes.
- Por otra parte "El Solicitante" manifiesta conocer el contenido y alcance de las disposiciones legales y reglamentarias relativas a la celebración de actos jurídicos mediante el uso de medios electrónicos, digitales o de cualquier otra tecnología, por lo que asume plena responsabilidad respecto de la información y contenido de todo documento electrónico o digital elaborado y enviado en el que se haga uso de la citada clave privada, toda vez que por ese solo hecho se considerara que el documento electrónico o digital le es atribuible.
- "EL Solicitante" reconoce y acepta que "La AC" únicamente es responsable de los errores que, en su caso, llegaren a cometer con motivo de culpa grave en el proceso de generación, registro, entrega y revocación del certificado digital, según corresponda, así como que no será responsable por los daños y perjuicios que se pudieran causar a "El Solicitante" o a terceros, cuando por caso fortuito o fuerza mayor no puedan realizarse registros, verificaciones, revocaciones o tramitar documentos electrónicos cifrados con las claves públicas y privadas relacionadas con dicho certificado. Por caso fortuito o fuerza mayor se entenderá todo acontecimiento o circunstancia inevitable, más allá del control razonable de "La AC", que le impida el cumplimiento de sus funciones con el carácter que le corresponde y reconocen a través de sus firmas autógrafas asentada en el espacio designado para ello en el anverso y reverso de este formato, como prueba fehaciente de la aceptación de todo lo especificado en la presente Solicitud.

Condiciones:

- El Certificado Digital para Firma de Equipo que se genera, derivado de la realización de este trámite, estará disponible en https://ac.siger.gob.mx; para que "La Unidad Solicitante" realice la descarga del mismo.
- El Certificado Digital para Firma de Equipo asignada es exclusiva para el equipo especificado en la presente e intransferible y el uso de la misma es responsabilidad de la persona señalada y que tiene a su cargo el equipo.
- Con este certificado podrá realizar las actividades asignadas estrictamente al equipo de cómputo dentro de la organización.
- "El Solicitante" será responsable de las obligaciones derivadas del uso no autorizado del equipo.
- "El Solicitante" y el responsable del equipo aceptan que deberán notificar oportunamente a "La AC", la invalidación, pérdida o cualquier otra situación que pudiera implicar la reproducción o uso indebido del certificado Digital para Firma de Equipo y aceptan las condiciones de operación y límites de responsabilidad de la Secretaría de Economía en su calidad de "La AC"

.

CARTA DE CONFIDENCIALIDAD Y USO DE CERTIFICADO DIGITAL DE EQUIPO DE CÓMPUTO

Secretaría de Economía
P r e s e n t e.

El que suscribe , en mi carácter de____, adscrito a la unidad de _____ de la Secretaría de Economía, advertido por (el agente certificador o auxiliar de agente)(Nombre del Agente Certificador) de la Dirección General de Normatividad Mercantil, de los delitos en que incurren los que se conducen con falsedad ante una autoridad distinta a la autoridad judicial, manifiesto que:

I. Que a partir de este día, acepto bajo mi responsabilidad el uso del certificado digital con número de serie y con vigencia del al emitido por la Dirección General de Normatividad Mercantil para el uso del equipo de cómputo con número de serie; modelo, marca, con número de inventario.

II. Acepto que el uso de los datos de creación del certificado digital señalado con anterioridad, queda bajo mi responsabilidad, en virtud de que el agente certificador de la Dirección General de Normatividad Mercantil puso a mi disposición los elementos técnicos necesarios para elaborar el requerimiento, y generación del certificado digital, datos que han sido de mi exclusivo conocimiento en todo momento, por lo que me obligo a no revelar los datos de creación del certificado, ya que en el caso de hacerlo, me serán atribuibles las responsabilidades administrativas, civiles y penales que se pudieran derivar por el mal uso que se le pudiera dar.

III. Que alinearé todas mis actividades y procesos para cumplir con la Política de Certificación y con la Declaratoria de Prácticas de Certificación de la DGNM y me aseguraré que sea ejecutada por las personas bajo mi supervisión, a fin de mantener la integridad, confidencialidad y disponibilidad la información del equipo de cómputo señalado en la fracción I de esta Carta.

IV. Que me aseguraré de informar a mi superior jerárquico y al Comité de Seguridad de la Información de la DGN, sobre cualquier conducta violatoria de que tenga conocimiento que pudiera incidir en la correcta operación del equipo de cómputo antes descrito, así como de la confidencialidad o disponibilidad de la información en éste contenida.

V. En caso de incumplir con lo estipulado en la presente carta, acepto que la DGNM revoque el certificado Digital del equipo de cómputo a mi cargo y que ha quedado descrito en la presente carta, sin perjuicio de que me puedan ser aplicables las responsabilidades administrativas, civiles o penales, por las acciones u omisión en que pudiera haber incurrido.

Oficio No. 316.08.
Asunto: Nombramiento de Agente Certificador
México, D.F.

(Nombre del Agente y Cargo)

Por este conducto le comunico que a sido designado Agente Certificador de la Secretaría de Economía, para los efectos que disponen los artículos 30 bis del Código de Comercio, 20 fracción X del Reglamento Interior de la Secretaría de Economía y 11 del Reglamento del Registro Público de Comercio.

Por lo que, a partir de esta fecha está facultado para generar y revocar los Certificados Digitales de las Autoridades Certificadoras de la DGNM y del SIGER, conforme a lo establecido en la Política de Certificación y Declaración de Prácticas de Certificación emitidas por esta Dirección General.

A t e n t a m e n t e
El Director General

Oscar A. Margain Pitman

C.c.p.- Act. Gustavo de la Colina Flores, Director del SIGER.- Para la Generación del certificado de Agente correspondiente.

DELEGACIÓN O SUBDELEGACIÓN FEDERAL DE LA SECRETARIA DE ECONOMIA EN EL ESTADO DE _____

Oficio No.

Asunto: Nombramiento de Auxiliar de Agente Certificador.
México, D.F.

(Nombre del Auxiliar de Agente Certificador y Cargo)

Por este conducto le comunico que a sido designado Auxiliar de Agente Certificador de la Secretaría de Economía, para los efectos que disponen los artículos 30 bis del Código de Comercio, 20 fracción X del Reglamento Interior de la Secretaría de Economía y 11 del Reglamento del Registro Público de Comercio.

Por lo que, a partir de esta fecha deberá brindarle apoyo a los Agentes Certificadores nombrados por la Dirección General de Normatividad Mercantil de esta Secretaría, en la generación de los Certificados Digitales de las Autoridades Certificadoras de la DGNM y del SIGER, conforme a lo establecido en la Política de Certificación y Declaración de Prácticas de Certificación emitidas por la Dirección General de Normatividad Mercantil.

A t e n t a m e n t e
El Delegado o Subdelegado

Nombre y Firma

C.c.p.- Lic. Oscar A. Margain Pitman.- Director General de Normatividad Mercantil.

CARTA DE CONFIDENCIALIDAD DE AUXILIAR DE AGENTE

Secretaría de Economía
Presente

El que suscribe <nombre del Auxiliar de Agente>, habilitado por < Delegado o subdelegado, de la ciudad y estado > como Auxiliar de Agente Certificador, con pleno conocimiento de causa y advertido por la Dirección General de Normatividad Mercantil de los delitos en los que incurren los que se conducen con falsedad ante una autoridad distinta a la judicial, manifiesto que:

I. Declaro bajo protesta de decir verdad que es de mi conocimiento la Política de Certificación y Declaración de Prácticas de Certificación, misma que entiendo y en consecuencia estoy de acuerdo en aplicarlas y cumplirlas cabalmente.

II. Que es de mi conocimiento que toda la información derivada del procedimiento de Generación de Certificados Digitales de la Secretaría de Economía es estrictamente confidencial, por lo que me obligo a respetar dicha condición de la información y abstenerme de divulgarla o distribuirla a terceras personas.

III. Igualmente, que me abstendré de conservar copias o respaldos totales o parciales, sean físicos o electrónicos, salvo aquellos realizados en el ejerció de mis funciones laborales, y no utilizaré en provecho propio la información que obtuve en el proceso de generación de certificados digitales.

IV. Que realizaré de manera cuidadosa, imparcial y gratuita el apoyo para la generación certificados digitales y en especial el procedimiento de identificación y personalidad jurídica de los solicitantes y el envío de la documentación recopilada en el procedimiento.

V. Estoy de acuerdo en proporcionar a la Dirección General de Normatividad Mercantil de la Secretaría de Economía la información adicional que respecto del proceso de generación de certificados me sea requerida.

_____

<Nombre, cargo y firma del Auxiliar de agente>

APÉNDICE III-B: Política de Certificados de la Autoridad Certificadora Raíz de la Secretaría de Economía

Noviembre 2005

1. INTRODUCCIÓN

La Política de Certificados, es un conjunto de reglas que indican la aplicabilidad de un certificado a una comunidad y clase de aplicaciones con requerimientos comunes de seguridad.

En este documento se describe la Política de Certificados para la Autoridad Certificadora Raíz de la Secretaría de Economía (ACR-SE). La Política de Certificados se aplica a la solicitud, validación, aceptación, emisión o revocación de los certificados digitales dentro de una Infraestructura de Clave Pública (PKI por sus siglas en inglés).

La ACR-SE, a través de la Dirección General de Normatividad Mercantil (DGNM), certificará las claves públicas de las Autoridades Certificadoras que hallan sido acreditados por la DGNM.

2. ALCANCE

De acuerdo a la estructura jerárquica de certificación descrita en el apartado COMUNIDAD Y APLICABILIDAD DE LA ACR-SE, la ACR-SE podrá certificar la clave pública de autoridad certificador a:

a) La Dirección General de Normatividad Mercantil (CD-ACDGNM). Ésta a su vez podrá certificar las clave públicas de autoridades certificadoras para Instituciones Públicas Gubernamentales; para entidades de la SE; de identidad personal (CD-IP) para funcionarios públicos de la SE y para los particulares que realicen trámites ante esta Secretaría.
b) SIGER (CD-ACSIGER). Ésta a su vez podrá certificar las clave públicas de los RPC y fedatarios públicos.
c) Prestadores de Servicios de Certificación (CD-ACPSC), que hayan sido acreditadas por la DGNM y cuya Política de Certificados sea tan restrictiva como lo descrito en este documento. Éstos podrán certificar las claves públicas de personas físicas o morales para efectos comerciales, entre otros.
La Autoridad Certificadora Raíz de la SE, se establece para crear y desarrollar una PKI a nivel nacional para el desarrollo del comercio electrónico.

3. REFERENCIAS

- RFC 3647 -Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, noviembre 2003. http://www.faqs.org/rfcs/rfc3647.html
- *RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile abril 2002*, http://www.faqs.org/rfcs/rfc3280.html
- ISO/IEC 9594-8:2001 Information technology: Open Systems Interconnection-The Directory: Public-key and attribute certificate frameworks.
- Código de Comercio, publicado el 29 de agosto de 2003, en el Diario Oficial de la Fedración.
- REGLAMENTO del Código de Comercio en Materia de Prestadores de Servicios de Certificación, Publicado el 19 de julio de 2004 en el Diario Oficial de la Federación
- REGLAS generales a las que deberán sujetarse los prestadores de servicios de certificación. Publicadas el 10 de agosto de 2004, en el Diario Oficial de la Federación.

4. DEFINICIONES

- **Certificado:** Todo Mensaje de Datos u otro registro que confirme el vínculo entre un Firmante y los datos de creación de Firma Electrónica.
- **Comunidad:** Estará integrada por los Prestadores de Servicios de Certificación, acreditados por la DGNM, Instituciones Públicas Gubernamentales y áreas que integran la Secretaría de Economía.
- **Emisor:** Toda persona que, al tenor del Mensaje de Datos, haya actuado a nombre propio o en cuyo nombre se haya enviado o generado ese mensaje antes de ser archivado, si éste es el

caso, pero que no haya actuado a título de Intermediario.

- **Firma Electrónica:** Los datos en forma electrónica consignados en un Mensaje de Datos, o adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al Firmante en relación con el Mensaje de Datos e indicar que el Firmante aprueba la información contenida en el Mensaje de Datos, y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio.
- **Firma Electrónica Avanzada o Fiable:** Aquella Firma Electrónica que cumpla con los requisitos contemplados en las fracciones I a IV del artículo 97, del CoCo. En aquellas disposiciones que se refieran a Firma Digital, se considerará a ésta como una especie de la Firma Electrónica.
- **Prestador de Servicios de Certificación:** La persona o institución pública que preste servicios relacionados con Firmas Electrónicas y que expide los Certificados, en su caso.
- **Secretaría:** Se entenderá la Secretaría de Economía.
- **Titular del Certificado:** Se entenderá a la persona a cuyo favor fue expedido el certificado.

5. ABREVIACIONES:

- **ACR-SE** Autoridad Certificadora Raíz de la Secretaría de Economía.
- **CoCo** Código de Comercio.
- **RGPSC** Reglas Generales de Prestadores de Servicios de Certificación.
- **CD-IPAC** Certificados Digitales de Identidad Personal para sus Agentes Certificadores de la Secretaría de Economía.
- **CD-IP** Certificados Digitales de Identidad Personal.
- **CD-ACPSC** Certificados Digitales de Autoridad Certificadora de Prestadores de Servicios de Certificación.
- **CD-ACSIGER** Certificado Digitales de Autoridad Certificadora de Sistema Integral de Gestión Registral.
- **CD-ACDGNM** Certificado Digitales de Autoridad Certificadora de la Dirección General de Normatividad Mercantil.
- **CD-ACIPG** Certificados Digitales de Autoridad Certificadora de Instituciones Publicas Gubernamentales.
- **DGNM** Dirección General de Normatividad Mercantil.
- **RPSC:** Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación.
- **LCR** Lista de Certificados Revocados.
- **OCSP** Protocolo de Estatus de Certificados en Línea (por sus siglas en inglés).
- **CLAVES** Clave Pública y Clave Privada.
- **RA-SE** Autoridad Registradora de la Secretaría de Economía
- **PSC** Prestadores de Servicios de Certificación
- **URL** "Uniform Resource Locator": Localizador uniforme de recurso.

6. IDENTIDAD DE LA ACR-SE

Distinguished Name (DN): C=MX, O=Secretaría de Economía, OU=Dirección General de Normatividad Mercantil, CN=ACR-SE/

Ubicación: Insurgentes Sur #1940, 1er. Piso, Del. Álvaro Obregón
C.P. 01030, México, D.F. Correo electrónico de la ACR-SE: acrse@economia.gob.mx Teléfono (+52) (55) 52.29.61.00 ext. 33533, Fax : 52.29.91.00 ext. 33599

Información sobre la Infraestructura de Clave Pública de la ACR-SE:
http://ac.economia.gob.mx.gob.mx

7. COMUNIDAD Y APLICABILIDAD DE LA ACR-SE

La comunidad y aplicabilidad de la ACR-SE están determinadas en esta Política de Certificados. La ACR-SE emitirá certificados de identidad personal (CD-IPAC) para sus agentes certificadores; certificados digitales de autoridad certificadora (CD-ACPSC) a las autoridades certificadoras de las

personas físicas y morales de carácter privado o público que hayan sido acreditados como Prestadores de Servicios de Certificación por la DGNM; a la Autoridad Certificadora (CD-ACSIGER) a del SIGER para el ámbito del Registro Público de Comercio y a las autoridades certificadoras de las áreas que integran a la Secretaría de Economía.

Solo emitirá otro tipo de certificado digital, en caso de ser necesario para la operación de alguna necesidad de la Secretaría de Economía. Éste deberá ser autorizado por el Comité de Seguridad de la DGNM.

8. ESTRUCTURA JERÁRQUICA

La estructura jerárquica de certificación se compone de los siguientes elementos:

1. **Autoridad Certificadora Raíz de la Secretaría de Economía**-. Ofrece servicios de certificación de clave pública de las autoridades certificadoras subordinadas a la ACR-SE de la SE. La SE es una institución pública gubernamental establecida para el desarrollo del ámbito comercial, tanto en el Registro Público de Comercio como para el comercio electrónico, entre otros.
2. **Autoridades Certificadoras Subordinadas** de la **ACR-SE** de la Secretaría de Economía.- Serán las personas físicas o morales acreditadas como PSC, instituciones públicas gubernamentales, direcciones generales de la SE, de acuerdo al CoCo, RPSC, RGPSC y a esta Política de Certificados.
3. **Agentes Certificadores** de la Autoridad Certificadora Raíz de la Secretaría de Economía.- Serán los encargados de emitir los certificados digitales, a las entidades subordinadas de la ACR-SE.
4. **Autoridad Registradora** de la Autoridad Certificadora Raíz de la
5. Secretaría de Economía.- Será la encargada de la autenticación de documentos e identificación de los solicitantes y titulares del certificado digital de la autoridad certificadora y de completar el procedimiento definido para la emisión de los certificados Anexo I.

9. PRIVACIDAD Y SEGURIDAD

9.1. REQUERIMIENTOS DE SEGURIDAD PARA LA ACR-SE Y SUS CLAVES.

- La ACR-SE operará en un servidor de misión crítica redundante desconectado de la red, el intercambio de información con sus entidades subordinadas será mediante dispositivos de almacenamiento removible, únicamente para efectos de certificación de las mismas.
- El intercambio de información entre el servidor WEB de la ACR-SE con los Autoridades Certificadoras Subordinadas, será en los términos establecidos en las reglas de la 5 a la 5.3 de las RGPSC.
- La clave privada de la ACR-SE estará en todo momento cifrada, en un dispositivo de alta seguridad que cumpla con la norma FIPS 140-2 nivel 3.
- Tanto el *hardware* como el *software* que opera la ACR-SE se mantendrá en todo momento físicamente seguro.
- El par de claves RSA de la ACR-SE tendrá una longitud de 2048 bits.
- Se establecerá un procedimiento periódico de respaldo de los servidores que opere la ACR-SE. Las copias se guardarán en un lugar seguro, protegido de accesos no autorizados.
- Si la clave privada de la ACR-SE estuviera comprometida, se procedería a la revocación de la misma y del certificado de la ACR-SE, así como todos los certificados emitidos por ella, no importando la fecha de emisión. A partir de ese momento, deberán revocarse todos los certificados emitidos por las Autoridades Certificadoras Subordinadas ala ACR-SE y no deberán emitir certificados válidos hasta que no se restaure la identidad de la ACR-SE y se vuelvan a generar certificados respectivos a las Autoridades Certificadoras Subordinadas.

10. REQUERIMIENTOS DE SEGURIDAD IMPUESTOS A LAS AUTORIDADES CERTIFICADORAS 10.1. SUBORDINADAS Y SUS CLAVES.

- Las Autoridades Certificadoras operarán en un servidor de misión crítica redundante.
- Éste servidor podrá estar conectado a la red, en tal caso, el intercambio de información se hará entre el servidor y sus usuarios por lo menos vía SSL o la tecnología que ofrezca mayor seguridad, asimismo, deberá deshabilitar todos los servicios de red que no se requieran para el buen funcionamiento del servicio, manteniendo
- seguros y monitoreados aquellos que sean necesarios.
- La clave privada de la Autoridad Certificadora estará cifrada en un dispositivo que cumpla con el estándar FIPS 140 nivel 3.
- Tanto el hardware como el software del servidor de misión crítica que opera la Autoridad Certificadora se mantendrá en todo momento físicamente seguro.
- El par de claves RSA de una Autoridad Certificadora tendrá como mínimo una longitud de 2048 bits.
- El par de claves RSA de los certificados emitidos por las Autoridades Certificadora Subordinadas tendrá como mínimo una longitud de 1024 bits.

11. LA AUTORIDAD CERTIFICADORA ACR-SE:

La ACR-SE es la instancia de la Secretaría de Economía, encargada de certificar la clave pública de las Autoridades Certificadoras Subordinadas, de acuerdo al Código de Comercio, Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación y sus Reglas Generales. Así como de emitir o revocar los certificados de las autoridades referidas como se menciona en el apartado "ALCANCE", para más información consultar: http://ac.economia.gob.mx. http://www.economia.gob.mx.

12. POLITICA DE CERTIFICACIÓN

12.1. POLÍTICA DE SEGURIDAD

El objetivo de la ACR-SE será únicamente la emisión y revocación de certificados citados en el apartado "ALCANCE" y Certificados Digitales de Servidores, Certificados Digitales de Autoridad Certificadora de Estampas de Tiempo.

Se emitirán CD-IPAC para sus Agentes Certificadores.

Se emitirán CD-ACPSC para aquellos PSC que hayan sido acreditados por la DGNM, en términos del CoCo, RPSC y RGPSC, y que hayan presentado su solicitud de certificado. Se emitirán también CD-ACSIGER, CD-ACDGNM y CD-ACIPG para las Autoridades correspondientes.

La revocación de cualquier certificado se realizará de acuerdo a lo establecido en el apartado "REVOCACIONES".

Las Autoridades Certificadoras subordinadas de la ACR-SE, emitirán Certificados Digitales de Identidad Personal, Certificados Digitales de Servidores, Certificados Digitales de Autoridad Certificadora de Estampas de Tiempo, y Certificados Digitales para Agentes Certificadores dentro de la misma Autoridad Certificadora Subordinada.

Sólo se emitirán Certificados Digitales de Servidores a para los equipos que pertenezcan a las ACR-SE.

13. PERÍODO DE VALIDEZ DE LOS CERTIFICADOS DIGITALES

El período de validez del Certificado Digital de la ACR-SE no será menor a 10 años a partir de su fecha de emisión.

El período de validez de los Certificados Digitales de Autoridad Certificadora subordinada no será menor de 10 años a partir de su fecha de emisión, igualmente para los certificados de servidor. Cuando se haya superado cuatro quintos del tiempo de vida de la ACRSE, se generará un nuevo certificado digital y en su caso una nueva identidad. A partir de ese momento, las nuevas inscripciones se harán firmando certificados con esa nueva identidad. De este modo las Autoridades Certificadoras Subordinadas dispondrán de una quinta parte del tiempo para solicitar nuevos certificados a la nueva identidad.

14. CONVENCIONES DE NOMBRES

Cada Autoridad Certificadora deberá asegurar que su DN (*Distinguished Names*) sea único, en función de que será el DN que tendrán los certificados que emita.
El *CountryName* deberá ser "mx".
Cada Autoridad Certificadora Subordinada, tiene que establecer mecanismos que aseguren la unicidad de los DN (*Distinguished Names*) de los certificados digitales que emita.
C=<CountryName>
O= <OrganizationName> CN= <CommonName>

15. DISPOSICIÓN DE CERTIFICADOS

Cada Autoridad Certificadora debe mantener un repositorio o base de datos con los certificados que emita, de manera que estén disponibles al público a través de un servicio de distribución de certificados.
Así mismo, la ACR-SE mantendrá constancia, en las páginas Web habilitadas para tal fin, de los certificados emitidos o revocados por ésta.

15.1. LISTA DE CERTIFICADOS REVOCADOS (LCR)

Las LCRs (Listas de Certificados Revocados) deben ser firmadas por lo menos con la periodicidad establecida en la regla 2.4.8.1.5 de las RGPSC, por las Autoridades Certificadoras Subordinadas a ésta. Las Autoridades Certificadoras subordinadas serán responsables de indicar en los certificados que emita, la dirección en Internet (URL siglas en inglés) de su página en donde se localizará la Lista de Certificados Revocados y el Protocolo de Estatus de Certificados en Línea (OCSPs), para que de esta manera sea fácilmente accesible por los usuarios.
Toda Autoridad Certificadora se comprometerá a mantener actualizada la LCR y la OCSP, incluyendo todos los certificados revocados desde la última actualización.

16. OBLIGACIONES

16.1. OBLIGACIONES DE LA DGNM COMO GESTOR DE LA ACR-SE:

- Ofrecer y mantener la infraestructura necesaria para el establecimiento de una estructura jerárquica de certificación de Autoridades Certificadoras, según la Política de Certificados descrita en este documento.
- Implementar y mantener los requerimientos de seguridad impuestos a las claves de la ACR-SE, según lo descrito en este documento en el apartado "PRIVACIDAD Y SEGURIDAD".
- Aprobar o denegar las solicitudes de de acreditación así como de certificados y, en el primer caso, emitir los certificados de acuerdo con lo establecido en el apartado "POLÍTICA DE SEGURIDAD" de este documento.
- Poner copias de sus propios certificados y de cualquier información de revocación a disposición de quien desee verificar una firma electrónica avanzada con referencia a dichos certificados. Para ello, se publicará y se mantendrá actualizada dicha información en las páginas Web destinadas a la infraestructura de certificación (Ver apartado “IDENTIDAD DE LA ACR-SE”)
- Revocar los certificados según el procedimiento establecido en el apartado "REVOCACIONES" de este documento.
- Mantener actualizada la LCR, incluyendo todos los certificados revocados desde la última actualización.
- Proteger los datos de carácter personal que sean suministrados por los solicitantes a acreditación de PSC, de acuerdo con la Ley de Transparencia y de Acceso a la Información Pública Gubernamental.
- Comunicar inmediatamente, a los profesionales informáticos y responsables directos de las Autoridades Certificadoras, el compromiso, pérdida, divulgación, modificación, uso no autorizado de la clave privada de la ACR-SE, con el fin de restaurar la jerarquía lo antes posible según lo establecido en el apartado "PRIVACIDAD Y SEGURIDAD" de este documento.

16.2. OBLIGACIONES DE LA RA-SE DE LA ACR-SE

La Autoridad Registradora de la ACR-SE:

- Llevará a cabo cada uno de los pasos descritos en el procedimiento de emisión de certificados

digitales por parte de la ACR-SE para las Autoridades Certificadoras, según lo descrito en el **anexo I** de este documento.

- Llevará a término la identificación y autenticación para la revocación de certificados, de acuerdo con los procedimientos de validación establecidos en el apartado "REVOCACIONES" de este documento.
- Protegerá los datos personales de los solicitantes de certificados digitales, que no podrán ser cedidos a terceros bajo ningún concepto de acuerdo a la Ley Federal de Transparencia y Acceso a la información Pública Gubernamental.

16.3. OBLIGACIONES DE LAS AUTORIDADES CERTIFICADORAS SUBORDINADAS.

- Toda Autoridad Certificadora y sus correspondientes Autoridades Registradoras deben conocer la Política de Certificados de la ACR-SE, comprometiéndose a seguir las siguientes normas:
- Una Autoridad Certificadora en ningún caso emitirá certificados con una duración superior a la vigencia del vínculo administrativo existente entre el solicitante y la misma Autoridad Certificadora.
- Toda Autoridad Certificadora se compromete y obliga a enviar una copia a la ACR-SE, de los certificados emitidos de acuerdo a lo establecido en la regla 5 de las RGPSC, asimismo copia de su última LCR firmada.
- Toda Autoridad Certificadora se compromete y obliga a proteger sus claves secretas utilizadas en la emisión de certificados con el nivel de seguridad que se especifica en este documento en el apartado "REQUERIMIENTOS DE SEGURIDAD IMPUESTOS A LA ACR-SE Y SUS CLAVES".
- La Política de Certificados de las Autoridades Certificadoras registradas bajo la ACR-SE, será tan restrictiva o más que la especificada en este documento.
- Comunicar inmediatamente, a los titulares de los certificados emitidos por ésta, el compromiso de su clave privada, pérdida, divulgación, modificación, uso no autorizado, con el fin de revocar y volver a generales el par de claves a cada usuario .

14. RESPONSABILIDADES

14.1. RESPONSABILIDADES DE LA ACR-SE

- La DGNM, como administrador de la ACR-SE, garantiza el cumplimiento de las obligaciones descritas en este documento.
- Cualquier anomalía o incidente producidos entre el momento de la revocación de la clave privada de la ACR-SE y el momento de la notificación de tal acto a las Autoridades Certificadoras subordinadas y posterior revocación de los certificados emitidos es responsabilidad única y exclusiva de ACR-SE.
- Cualquier incidente o responsabilidad nacidos de la clave privada de la ACR-SE que se encuentra comprometida, es responsabilidad única y exclusiva de DGNM.

14.2.RESPONSABILIDADES DE LA RA-SE.

- Es responsabilidad de la AR-SE la correcta identificación de los solicitantes, para la emisión de certificados ó para la revocación de los mismos.

14.3. RESPONSABILIDADES DE LAS AUTORIDADES CERTIFICADORAS ACREDITADAS POR LA ACR-SE

- Cualquier anomalía o incidente producidos entre el momento de la revocación, de un certificado emitido por la ACR-SE, y el momento de la notificación de tal evento a la Autoridad de Certificadora, es responsabilidad de ésta última.
- Cualquier incidente o responsabilidad derivados del compromiso de la clave privada de la Autoridad Certificadora subordinada es responsabilidad de ésta.
- Los PSC deberán cumplir con el marco jurídico en lo referente a las responsabilidades de PSC conformado por el CoCo, RPSC y RGPSC.

15. REVOCACIONES

15.1.CAUSAS DE REVOCACIÓN

Cualquier certificado podrá ser revocado si:

- Ha existido pérdida, robo, modificación, divulgación no autorizada u otro compromiso de la clave privada asociada al certificado.
- Se han incumplido alguna de las obligaciones descritas en la Política de Certificados.
- Se conoce o se tienen motivos para creer razonablemente que uno de los hechos representados en el certificado es falso.
- Se conoce que alguno de los requisitos de emisión del certificado no fue cumplido.
- El sistema de certificación se vio comprometido de modo tal que afecta a la fiabilidad del certificado.
- Fallecimiento del titular del certificado.
- Cambio de información relativa al suscriptor.
- Se sospecha que la información contenida en el certificado es inexacta.
- Resolución administrativa o judicial que lo ordene.
- Se produce un error en la emisión de un certificado.
- Cese voluntario, en el caso de los PSC deberán cumplir con lo establecido en la regla 10 de la RGPSC.
- La clave privada de la ACR-SE fuese comprometida, en cuyo caso, serían revocados todos los certificados de las Autoridades Certificadoras y éstas no podrían emitir certificados válidos hasta que no se restaure la identidad de la ACR-SE y se vuelvan a generar los certificados de las Autoridades Certificadoras registradas por la ACRSE.
- Además de cualquiera de las causas que se señalan en el CoCo, RPSC y RGPSC, que le sean aplicables.

15.2. REVOCACIÓN DE UN CERTIFICADO DIGITAL.

- La revocación de un certificado digital firmado por la ACR-SE, se realizará siguiendo el procedimiento descrito a continuación:
- En caso de ser un PSC, será el representante legal del PSC y el profesional informático de la Autoridad Certificadora Subordinada, quienes solicitarán a la ACR-SE la revocación de su certificado.
- Para que dicha revocación se lleve a cabo, los responsables deberán cumplir con lo establecido en el artículo 16 del RPSC, anexando los documentos que fundamenten dicha solicitud.
- En su caso deberá entregar la documentación que recibieron de los titulares de cada certificado que emitieron.
- En caso de ser una institución pública gubernamental será mediante oficio firmado por el titular y el representante de la institución.
- En caso de un certificado de identidad personal emitidos al personal de la SE o a los particulares que realizan trámites ante la SE, serán éstos los que soliciten la revocación mediante escrito dirigido al Director General de Normatividad Mercantil.

ANEXO I. Procedimiento de emisión de Certificados Digitales de Autoridad Certificadora.

La emisión de un certificado digital firmado por la ACR-SE se hará bajo el procedimiento descrito a continuación:

1 El PSC, deberá designar al profesional informático y responsable directo de la Autoridad Certificadora; Las Instituciones Públicas Gubernamentales designarán al titular del área responsable que emitirá sus certificados; el cual deberá mantener una relación permanente con la ACR-SE.

2 El PSC deberá presentar su documento mediante el cual fue acreditado por la DGNM de conformidad con lo requerido en el trámite SE-09-026-B. Para la identificación fehaciente del titular del certificado, se requerirá su presencia física y deberá presentar una identificación oficial vigente como el pasaporte, credencial del IFE o cedula profesional.

3 La DGNM remitirá dicha información a la ACR-SE, la cual analizará la información requerida en el punto anterior, para determinar si procede o no la emisión del certificado.

4 Estas solicitudes quedarán en poder del ACR-SE. Es responsabilidad de la ACR-SE comprobar que dichas solicitudes están debidamente requisitado y que todos los datos que aparecen en las mismas son correctos.

5 Confirmada la autenticidad y validez del o los documentos presentados por el PSC, la ACR-SE verificará la razonable coincidencia entre la fotografía contenida en aquellas y la apariencia física del solicitante.

6 La ACR-SE requerirá a las Autoridades Certificadoras subordinadas que firme original y copia del documento de solicitud para verificar la firma autógrafa del documento de solicitud con la que aparece en las credenciales oficiales presentadas, después de lo cual procederá también a la firma autógrafa de la solicitud, considerada a partir de ese momento como aceptada.

7. La ACR-SE, emitirá el certificado correspondiente con el precertificado que presentarán las Autoridades Certificadoras Subordinadas de las siguientes formas:

a. Las Autoridades Certificadoras Subordinadas se autocertificarán su AC, en el nivel más seguro de sus instalaciones, dicho certificado será presentado en un medio de almacenamiento removible, el cual será certificado por la ACR-SE.
b. Las Autoridades Certificadoras Subordinadas emitirán su precertificado en PKCS#10 en su AC, en el nivel más seguro de sus instalaciones, dicho certificado será presentado en un medio de almacenamiento removible, el cual será certificado por la ACR-SE.

Nota: En la **Declaración de Prácticas de Certificación** se detallan los procedimientos correspondientes.

Apéndice IV: Anteproyecto de NOM-151-SCFI-2015: Requisitos que deben Observarse para la Conservación de Mensajes de Datos y Digitalización de Documentos

PREFACIO

En la elaboración de la presente Norma Oficial Mexicana participaron las siguientes empresas e instituciones:

INDICE

0. Introducción

De conformidad con lo dispuesto por los artículos 40 de la Ley Federal sobre Metrología y Normalización y, en relación con los artículos 34, 38, 46 Bis y 49 del Código de Comercio, la Secretaría de Economía deberá emitir una Norma Oficial Mexicana que permita el cumplimiento de la obligación a cargo de los comerciantes que utilicen mensajes de datos para realizar actos de comercio, de conservar por el plazo establecido en dicho Código, y cuyo contenido debe mantenerse integro e inalterado a partir del momento en que se generó por primera vez en su forma definitiva, debiendo ser accesible para su ulterior consulta, así como la digitalización de documentos.

1. Objetivo

La presente Norma Oficial Mexicana establece los requisitos que deben observarse para la conservación de mensajes de datos y la digitalización de documentos en términos de lo dispuesto en los artículos 34, 38, 46 Bis y 49 del Código de Comercio.

2. Campo de aplicación

La presente Norma Oficial Mexicana es de observancia general para los comerciantes que conforme a lo establecido en los artículos 34, 38, 46 Bis y 49 del Código de Comercio conserven mensajes de datos conforme a su definición en el artículo 89 del mismo Código, así como los requisitos a cumplir en la digitalización de toda o parte de la documentación relacionada con sus negocios en soporte papel a un mensaje de datos.

3. Definiciones

- ASN.1: A la versión 1 de Abstracts Sintax Notation (Notación Abstracta de Sintaxis).
- Constancia del prestador de servicios de certificación: Mensaje de datos emitido por un prestador de servicios de certificación, conforme a lo establecido en el Apéndice 7 de la presente Norma.
- Criptografía: Al conjunto de técnicas matemáticas para cifrar información.
- Digitalización: Proceso que permite la generación de archivos electrónicos a partir de documentos soportados en medios físicos, de una manera íntegra, precisa y fiable.
- Formato: A la secuencia claramente definida de caracteres, usada en el intercambio o generación de información.
- Objetos: A las definiciones del lenguaje ASN.1
- Secretaría: A la Secretaría de Economía.
- Para efectos de lo dispuesto en la presente Norma Oficial Mexicana aplicarán las definiciones contenidas en el Título Segundo del Código de Comercio.

4. Disposiciones generales

4.1 Los comerciantes deberán observar los métodos que se describen en los Apéndices 7 y 8 de la presente Norma Oficial Mexicana para conservar los mensajes de datos, así como para la digitalización de toda o parte de la documentación en papel relacionada con sus negocios.

4.2 La información que se desee conservar se podrá almacenar en uno o varios archivos diferentes y/o en una o varias computadoras.

4.3 Sin perjuicio de lo que dispongan otros ordenamientos jurídicos aplicables, cuando se pretenda almacenar en un medio electrónico, óptico o de cualquier otra tecnología, información derivada de un acto de comercio, que se encuentre soportada en un medio físico, los comerciantes podrán optar por migrar dicha información a una forma digital y, observar para su conservación en forma digital, las disposiciones a que se refiere la presente Norma Oficial Mexicana.

Los requisitos mínimos de los mensajes de datos resultantes de las digitalizaciones, procedimiento de migración de soporte físico a un medio electrónico, incluyendo el formato, niveles de calidad, condiciones técnicas y estándares aplicables, se determinan en el Apéndice 8 de la presente Norma Oficial Mexicana.

El proceso de digitalización deberá ser controlado por un tercero legalmente autorizado, que constatará que dicha migración se realice íntegra e inalterablemente tal y como se generó por primera vez en su forma definitiva. El tercero legalmente autorizado deberá ser un Prestador de Servicios de Certificación acreditado para tales efectos.

4.4 Los programas informáticos para la conservación de los mensajes de datos así como los equipos para digitalización, deberán cumplir con los métodos que se describen en los Apéndices 7 y 8 de la presente Norma Oficial Mexicana.

5. Elementos que intervienen en la conservación de mensajes de datos y digitalización.

5.1 Para la emisión de la firma electrónica avanzada, el Prestador de Servicios de Certificación o la Autoridad Certificadora, deberá observar los requisitos que la normatividad aplicable señale para su operación.

5.2 La constancia emitida por el Prestador de Servicios de Certificación, acreditado para tales efectos, deberá observar los términos establecidos en el Apéndice 7 de la presente Norma Oficial Mexicana.

5.3 El almacenamiento de las constancias de conservación así como los documentos digitalizados a los que se refiere la presente Norma Oficial Mexicana, quedarán en control del usuario pudiendo contratar para su administración a terceros.

6. Vigilancia

La vigilancia de la Norma Oficial Mexicana estará a cargo de la Secretaría conforme a sus atribuciones y la legislación aplicable.

7. Apéndice Constancia Conservación de Mensajes de Datos
Introducción

En este Apéndice se presentan los elementos necesarios que describen los procesos involucrados en la conservación de mensajes de datos.

Formación de solicitud de la constancia de conservación de mensajes de datos

La formación de la solicitud de la constancia de conservación de mensajes de datos se efectúa conforme a la especificación descrita en el RFC 3161. La solicitud de la constancia sigue el formato ASN.1 con al menos el siguiente contenido:

(i) Huella digital electrónica del mensaje de datos, y
(ii) Identificador de objeto cuyo contenido corresponderá con la versión del documento de las políticas de emisión de estampas de tiempo del Prestador de Servicios de Certificación.

La huella digital electrónica se obtiene mediante el empleo de alguna de las funciones de digestión que le haya notificado la Secretaría al momento de la acreditación del Prestador de Servicios de Certificación para emitir constancias de conservación de mensajes de datos conforme a la presente Norma.

En todo momento, el interesado deberá mantener el control sobre el mensaje de datos por lo que el Prestador de Servicios de Certificación únicamente recibirá la huella digital electrónica del mensaje de datos.

Obtención de la constancia de conservación de mensajes de datos del Prestador de Servicios de Certificación

La obtención de la constancia de conservación de mensajes de datos se efectuará a través de los mecanismos establecidos entre el interesado y el Prestador de Servicios de Certificación. El interesado enviará la solicitud al Prestador de Servicios de Certificación y este último le devolverá la constancia de conservación de mensajes de datos por el mismo medio.

El Prestador de Servicios de Certificación implementará un sistema que permita al comerciante identificar la constancia de conservación de mensajes de datos, pudiendo tomar como referencia el nombre del mensaje de datos o la fecha, entre otros.

Formación de la constancia de conservación de mensajes de datos

El Prestador de Servicios de Certificación formará una constancia siguiendo el formato ASN.1 del RFC 3161 que se conformará de una estampa de tiempo electrónica.

Cada estampa de tiempo constará de:
(i) Versión de la Estampa,
(ii) Identificador de Objeto cuyo contenido corresponderá con la versión del documento de las políticas de emisión de estampas de tiempo,
(iii) Huella digital electrónica que se obtiene de la solicitud,
(iv) Número serial único que identifica a la estampa,
(v) Fecha y hora en que se está generando la estampa, y
(vi) Extensiones para aquellos casos en que se trate de refrendos de una constancia.

Método de verificación de autenticidad de la constancia de conservación de mensajes de datos

La verificación de la autenticidad de una constancia de conservación de mensajes de datos se realizará por medio de los siguientes pasos, para cada estampa de tiempo electrónica que conforma la constancia:

1. Obtención de forma confiable del certificado del Prestador de Servicios de Certificación que firmó la estampa.
2. Verificación de la firma electrónica avanzada del Prestador de Servicios de Certificación en la estampa.
3. Obtención de la huella digital del mensaje de datos original empleando la función de digestión indicada en la estampa.
4. Verificación que el resultado obtenido en el punto anterior, es idéntico al valor asentado en la estampa.

La fecha de inicio de vigencia asentada en cada estampa de tiempo electrónica, indica desde cuándo el mensaje de datos se considera existente para efectos de conservación de acuerdo a esta Norma

Definiciones de los objetos ASN.1 involucrados en la constancia.

En la presente sección se detallan los procesos y los formatos asociados a la emisión de estampas de tiempo.

Especificación de la estampa

Conforme al RFC 3161, el elemento que trae la información de la estampa de tiempo es la estructura TSTInfo, la cual se define de la siguiente forma:

Definición del elemento TSTInfo

```
TSTInfo ::= SEQUENCE {
 version  INTEGER { v1(1) },
 policy  TSAPolicyId,
 messageImprint MessageImprint,
 -- MUST have the same value as the similar field in
 -- TimeStampReq
 serialNumber  INTEGER,
 -- Time-Stamping users MUST be ready to accommodate integers
 -- up to 160 bits.
 genTime  GeneralizedTime,
 accuracy Accuracy  OPTIONAL,
 ordering BOOLEAN DEFAULT FALSE,
 nonce INTEGER OPTIONAL,
 -- MUST be present if the similar field was present
 -- in TimeStampReq. In that case it MUST have the same value.
 tsa  [0] GeneralName OPTIONAL,
 extensions  [1] IMPLICIT Extensions OPTIONAL }
```

Extensiones

Una de las extensiones a usar en la presente norma se encuentra especificada en el RFC 5280.
En la siguiente definición, MAX indica que la cota superior no está especificada. Cada implementación queda con la libertad de escoger la cota superior.

```
Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension
Extension ::= SEQUENCE {
 extnID OBJECT IDENTIFIER,
 critical BOOLEAN DEFAULT FALSE,
 extnValue OCTET STRING }

id-at OBJECT IDENTIFIER ::= { joint-iso-ccitt(2) ds(5) 4 }

-- Upper Bounds
ub-serial-number INTEGER ::= 64

-- Naming attributes of type X520SerialNumber
id-at-serialNumber OBJECT IDENTIFIER ::= { id-at 5 }
X520SerialNumber ::= PrintableString (SIZE (1..ub-serial-number))

-- en el objeto ASN.1 X520SerialNumber se almacenará la
```

-- expresión hexadecimal del campo serialNumber del elemento TSTInfo.

Con la finalidad de identificar el inicio de vigencia de la constancia, se incorporan los dos siguientes elementos, cuya definición se expresa en la notación ASN.1

id-nom-ini-time OBJECT IDENTIFIER ::= {2 37 1117 1973 9719 5}
NOM151IniTime ::= GeneralizedTime

Detalle de los procesos de obtención y verificación
A continuación se describen los procedimientos para la generación y verificación de las constancias de acuerdo a esta norma.

Obtención por primera vez de una estampa de tiempo electrónica como constancia NOM:

1. El interesado genera una solicitud de estampa de tiempo de acuerdo al RFC 3161, empleando alguna función hash avalada por la Secretaría y el identificador de objeto referente a la política de la Secretaría a la que se apegará la emisión de la estampa.
2. El interesado envía la solicitud al PSC a través del mecanismo previamente establecido entre el PSC y el interesado.
3. El PSC valida que la longitud de la huella corresponda al algoritmo de digestión empleado en su generación y genera la estampa de tiempo de acuerdo al RFC 3161.
4. El PSC envía la estampa de tiempo a través del mismo mecanismo por el cual recibió la solicitud.

La estampa de tiempo electrónica obtenida es la evidencia de que el documento existe desde la *fecha asentada en la estampa.*

Verificación de la constancia con una estampa de tiempo contra un mensaje de datos:

1. Se obtiene de la estampa de tiempo electrónica la huella digital del documento generada con la función hash indicada en la estampa.
2. Se obtiene en línea el certificado del PSC que firmó la estampa de tiempo desde una fuente confiable.
3. Se verifica la firma digital contenida en la estampa.
4. Si la verificación fue exitosa, entonces el mensaje de datos existe, al menos, desde la fecha asentada en la estampa. Además, el mensaje de datos es íntegro.

Extensión de vigencia

La vigencia de la constancia de conservación de mensajes de datos será de por lo menos diez años a partir de su emisión, y el comerciante podrá decidir si requiere la extensión de dicha vigencia según la naturaleza de la información de acuerdo con los ordenamientos legales aplicables.
Obtención de Extensión de vigencia

1. El interesado genera una solicitud de estampa de tiempo de acuerdo al RFC 3161, empleando la función hash notificada por la Secretaría.
2. El interesado envía la solicitud y la estampa de tiempo vigente del mensaje de datos en cuestión al Prestador de Servicios de Certificación a través de los mecanismos previamente establecidos entre el Prestador de Servicios de Certificación y el interesado.
3. El Prestador de Servicios de Certificación valida que la longitud de la huella digital electrónica corresponda con la longitud que se obtiene con la función hash empleada; obtiene de la estampa de tiempo electrónica recibida la fecha de inicio de vigencia y el número serial de esa estampa, con esta información genera la nueva estampa de tiempo electrónica de acuerdo al RFC 3161, agregando en la sección de extensiones la

información relativa al inicio de vigencia y al número serial de la estampa anterior a la que se está generando.

4. El Prestador de Servicios de Certificación envía la estampa de tiempo a través del mismo mecanismo por el cual recibió la solicitud.

A partir de la segunda estampa de tiempo electrónica, ésta contendrá dos fechas: una es la fecha de la propia estampa y la otra, dentro de una de sus extensiones, indicará la fecha en que la primera estampa fue creada para el correspondiente mensaje de datos.

El Prestador de Servicios de Certificación implementará un sistema que permita al comerciante identificar la constancia de conservación de mensajes de datos así como las extensiones que se generen, pudiendo tomar como referencia el nombre del mensaje de datos o la fecha de la constancia.

La estampa de tiempo electrónica obtenida junto con las estampas anteriores conforma la evidencia de que el documento existe, al menos, desde la fecha asentada en la estampa inicial.

Verificación de la constancia conformada por más de una Estampas de Tiempo.

1. Se realizan las verificaciones del mensaje de datos contra cada una de las estampas de tiempo electrónicas que conforman la constancia (proceso similar al caso de una sola estampa).
2. Se verifica que todas y cada una de las fechas de inicio de vigencia sean la misma.
3. Se verifica que el valor en la extensión respectiva para el serial coincida con el de la estampa de tiempo previa.
4. Si el certificado del Prestador de Servicios de Certificación que firmó la más reciente estampa es vigente y las verificaciones fueron exitosas, entonces el mensaje de datos existe, al menos, desde la fecha asentada en la estampa de tiempo y es íntegro.

8. Apéndice Digitalización de documentos en soporte físico

Introducción

En este Apéndice se presentan los elementos necesarios que describen los procesos involucrados en la digitalización de documentos en soporte físico a mensajes de datos con el fin de su conservación.

Requisitos mínimos de los mensajes de datos resultantes de la digitalización

Los componentes de un mensaje de datos resultante de la digitalización serán:

(i) Representación en medios electrónicos de documentos en soporte físico conforme al método de migración contenido en el presente Apéndice.
(ii) Solicitud de constancia de conservación de mensajes de datos.

Procedimiento de migración de documentos en soporte físico a un medio electrónico, óptico o de cualquier tecnología.

a. Formato

El formato del mensaje de datos resultante de la migración se definirá por el interesado siempre que se trate de un formato estándar, diseñado para contener el tipo de documento y con posibilidad de visualizar su contenido mediante algún programas de cómputo (*software)* disponible en el mercado.

En caso que el documento en soporte físico contenga texto impreso, se deberá ejecutar un proceso de reconocimiento óptico de caracteres, llamado OCR por sus siglas en inglés (Optical Character Recognition), el cual extrae el texto de una imagen digitalizada, permitiendo indexar el documento y hacer búsquedas sobre éste.

b. Niveles de calidad

El mensaje de datos resultante de la migración debe ser fiel al contenido original y garantizar su integridad.

El nivel de calidad mínimo para los mensajes de datos resultantes será:

Representaciones gráficas: 300 píxeles por pulgada o superior para representaciones en blanco y negro, color o escala de grises.
Audio: Frecuencia de muestreo de 44.1kHz y 16 bits o superior.
Video: Resolución de 352 píxeles de ancho por 288 píxeles de alto o superior de acuerdo al formato CIF definido en la H.261 de la ITU (International Telecommunication Union)

La calidad de una imagen se puede definir a partir de los siguientes factores:

- Resolución: se determina por el número de pixeles utilizados para representar la imagen. Los pixeles se expresan en puntos por pulgada (ppp o dpi: dots per inch). Incrementar el número de pixeles da como resultado una imagen de mayor resolución y una mejor delineación de los detalles finos, pero llega un punto en el que seguir aumentándolo no va a mejorar la calidad de la imagen, sólo aumentará el tamaño del archivo resultante. La clave es determinar el punto en el cual se utilice la suficiente resolución para capturar los detalles significativos del documento fuente.
- Profundidad de bits: es la medida del número de bits utilizado para definir cada pixel. Mientras mayor sea, más tonos de grises y colores se van a poder representar. La elección de este valor afecta la posibilidad de capturar tanto la apariencia física como el contenido del documento fuente. Se debe tomar en cuenta si la apariencia física, o partes de ésta, proporcionan un valor agregado, de ser así, es necesario aumentar la profundidad de bits.
- Procesos de mejora: estos procesos pueden ser utilizados para modificar o mejorar la imagen capturada, transformando su tamaño, color, contraste, brillo e incluso analizándola en busca de características que el ojo humano no percibe. En éstos se incluye, por ejemplo, el uso de filtros, curvas de reproducción tonal y herramientas de manejo de colores. Estos procesos se deben utilizar con mucho cuidado, ya que pueden hacer que desaparezcan elementos importantes en una imagen.
- Compresión: la compresión generalmente es utilizada para reducir el tamaño necesario en el procesamiento, almacenamiento o envío de imágenes. Los métodos para lograrla varían; por ejemplo, se puede lograr abreviando información repetida o eliminando aquella que el ojo humano difícilmente ve. Las técnicas de compresión pueden ser “sin pérdidas” —al ser reducida la imagen no se descarta información—, o “con pérdidas” —la información menos relevante es promediada o descartada—. Se recomienda aplicar una compresión “con pérdidas”, pero lo suficientemente buena para las necesidades, y obtener así una imagen “visualmente sin pérdidas”.
- Dispositivo utilizado: el equipo utilizado y su rendimiento tienen un impacto importante en la calidad de la imagen. Equipos de diferentes fabricantes pueden desempeñarse de distintas maneras, aun cuando cuenten con las mismas capacidades técnicas.
- Juicio y cuidado del operador: este aspecto siempre va a tener un considerable impacto en la calidad.

Se deberá generar un mensaje de datos que permita asegurar la fidelidad e integridad conforme a los documentos amparados en soportes físicos; el mensaje de datos generada debe ser de alta calidad y debe tratarse con un intenso control de calidad, de manera que si existe algún error en el proceso de captura, ésta deberá efectuarse una vez más.

En todo caso se podrán aplicar requisitos adicionales de acuerdo con las circunstancias específicas del documento en soporte físico, para asegurar su fidelidad e integridad, como el cotejo realizado por un fedatario público.

El mensaje de datos será fiel al documento en soporte físico, para lo cual:

(i) Respetará la geometría o aspecto del origen en tamaños y proporciones;

(ii) Respetará codificación y cantidad de imágenes por segundo cuando el origen sea video,

(iii) No contendrá caracteres o gráficos que no figurasen en el soporte físico, y

(iv) Su generación atenderá a lo establecido en esta norma.

c. Condiciones técnicas

El proceso de migración se realizará a través de un procedimiento en el que, garantizando la integridad de cada uno de los pasos, se efectúen las acciones siguientes:

(i) Por un medio de conversión de señales se obtendrá un archivo electrónico en la memoria del sistema asociado al dispositivo;

(ii) Si procede, la aplicación de un proceso de optimización automática de archivo electrónico para garantizar su legibilidad, de modo que todo contenido del documento origen pueda apreciarse y sea válido para su gestión (valor umbral, reorientación, eliminación de bordes negros, eliminación de ruido, u otros de naturaleza analógica).

(iii) Generación automática de una solicitud de constancia a partir del archivo electrónico resultante del proceso

El mensaje de datos debe ser una representación visual del objeto original lo más exacta posible que sirva para las necesidades de la institución; en este sentido, se debe entender que la solución no es capturar una imagen con la más alta calidad posible, sino evaluar el contenido del documento original y decidir la calidad de la imagen a utilizar al realizar la digitalización.

Como un primer paso en este proceso, se analizan los atributos de los documentos originales; éstos pueden diferir en cuanto a dimensiones, rango de colores o la forma en la que fueron producidos: a mano, con una imprenta, por medio de una cámara fotográfica, medios electrónicos, etcétera.
El estado de conservación de los documentos puede afectar el proceso de conversión, por eso es importante identificar si existe la necesidad de realizar una estabilización o restauración previa, idealmente con el apoyo de un especialista en conservación de documentos.

d. Metadatos

Por medio de metadatos se deberán incluir los principios descriptivos de catalogación en archivos digitales, así como información necesaria para obtención, acceso y gestión de esos archivos.

Se debe generar un conjunto de metadatos personalizado para satisfacer completamente los requerimientos específicos de una institución, definiendo el nombre del metadato y el tipo de dato que contiene. Se pueden extraer elementos de esquemas de metadatos ya definidos; existen diversos estándares internacionales (Dublin Core, PREMIS, METIS, MARC, OAIS, entre otros) que pueden servir como base, los cuales se pueden combinar y personalizar para adecuarse a las necesidades específicas. En el conjunto de metadatos que se defina, se debe especificar si el dato es obligatorio u opcional.

A continuación se muestran, de manera enunciativa más no limitativa, algunos tipos de metadatos:

- Descriptivos: Sirven para ayudar a encontrar y obtener documentos, distinguir entre unos y otros, así como para descubrir su tema o contenido (Ejemplos: título, fecha, descripción).
- Técnicos: sirven para ayudar a que se tenga consistencia en un gran número de archivos, imponiendo estándares para su creación (Ejemplos: escáner utilizado, formato de archivo, resolución).
- Estructurales: Contemplan las relaciones entre múltiples archivos digitales, permitiendo a los usuarios recorrer objetos complejos como pueden ser las páginas y capítulos de un libro (Ejemplos: tabla de contenidos, página, capítulo, volumen).
- Administrativos: En general, contemplan las necesidades locales administrativas de un proyecto o institución (Ejemplos: fecha de captura, proveniencia (historia), revisiones de integridad del archivo).
- Para preservación: Están conformados por toda la información necesaria para gestionar y preservar archivos digitales a lo largo del tiempo. Deben contener la información que va a asistir a la toma de

decisiones relacionada con el valor a largo plazo de un recurso digital (Ejemplos: secuencia de cambios de formato, respaldos
Realizados).

e. Preservación Digital

Cuando se elabora un proyecto de digitalización con fines de preservación, es necesario definir una estrategia y políticas específicas para la preservación digital. Ambas son esenciales para asegurar que existen medios confiables y verificables que permitan preservar la integridad de los archivos digitales.

f. Estándares aplicables

El Prestador de Servicios de Certificación contemplará la aplicación de un conjunto de operaciones de mantenimiento preventivo y comprobaciones rutinarias que permitirán garantizar mediante su cumplimiento que, en todo momento, el estado de la aplicación de digitalización y los dispositivos asociados producirán archivos electrónicos fieles al documento en soporte físico, que deberá reflejar en un Plan de Gestión de Calidad.

En el Plan de Gestión de Calidad se describirá el mantenimiento de los procedimientos y dispositivos asociados, en su caso, la aplicación de digitalización, así como otros aspectos que puedan afectar al propio software tales como, el seguimiento de la vigencia de las normas y algoritmos empleados, o aspectos de mantenimiento de los sistemas operativos que pudieran afectar al rendimiento de la aplicación de digitalización, u otros de naturaleza analógica.

g. Cotejo de la digitalización

El usuario será responsable de cotejar la digitalización que haya hecho de sus documentos físicos y el Prestador de Servicios de Certificación usará alguna técnica de muestreo estadístico para obtener un tamaño de muestra razonable y altamente representativa de documentos físicos para auditar el cotejo de documentos.

h. Destrucción del documento físico

El usuario decidirá si destruye el documento físico o no.

i. Empresas digitalizadoras y prestadores de servicios de certificación

Para ser Prestador de Servicios de Certificación de digitalización de documentos se tendrá que Acreditar de acuerdo al Código de Comercio, el Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación y a las Reglas generales a las que deberán sujetarse los de Prestadores de Servicios de Certificación.

Las empresas digitalizadoras desarrollarán o comprarán el software y los dispositivos necesarios para la digitalización, mientras que el Prestador de Servicios de Certificación verificará y autorizará el software y hará las auditorías necesarias a las empresas digitalizadoras que quieran trabajar con ellos.
La empresa digitalizadora podrá enviar al Prestador de Servicios de Certificación un requerimiento de conservación de mensaje de datos del documento digitalizado.

Apéndice V: Convenio *tipo* de colaboración entre el SAT y Entidades/Dependencias, su Anexo único y el Formato de Volumetría.

CONVENIO DE COLABORACIÓN QUE CELEBRAN _____, EN LO SUCESIVO _____, REPRESENTADO EN ESTE ACTO POR _____, EN SU CARÁCTER DE _____ Y EL SERVICIO DE ADMINISTRACIÓN TRIBUTARIA, EN LO SUCESIVO "SAT", REPRESENTADO EN ESTE ACTO POR _____, EN SU CARÁCTER DE _____, A QUIENES DE FORMA CONJUNTA SE LES DENOMINARÁ "LAS PARTES", AL TENOR DE LOS SIGUIENTES ANTECEDENTES, DECLARACIONES Y CLÁUSULAS:

ANTECEDENTES

Dentro de los objetivos del "Plan Nacional de Desarrollo 2013-2018", publicado en el Diario Oficial de la Federación el 20 de mayo de 2013, se encuentra el maximizar la calidad de los bienes y servicios que presta la Administración Pública Federal ("APF"), mejorando la entrega de los servicios públicos mediante el uso y aprovechamiento de las tecnologías de información y comunicación, así como que las políticas y los programas de la Administración Pública, se encuentren enmarcadas en un Gobierno Cercano y Moderno orientado a resultados, que optimice el uso de los recursos públicos, utilice las nuevas tecnologías de la información y comunicación e impulse la transparencia.

Por su parte, la Ley Federal de Procedimiento Administrativo establece en su artículo 69-C que los particulares pueden realizar promociones o solicitudes a través de medios de comunicación electrónica en las etapas de los procedimientos administrativos que las propias dependencias y organismos descentralizados así lo determinen mediante reglas de carácter general publicadas en el Diario Oficial de la Federación, utilizando medios de identificación electrónica en sustitución y con el mismo valor probatorio que la firma autógrafa, así como que dichas dependencias y organismos puedan hacer uso de esos medios para realizar diversas actuaciones en determinados supuestos.

Ahora bien, la Firma Electrónica Avanzada ("FIEL") es un instrumento tecnológico con validez jurídica, con el que se puede verificar la procedencia e integridad de los mensajes de datos firmados y transmitidos durante el intercambio electrónico, por medio de las distintas redes de telecomunicaciones, lo que permite evitar la suplantación de identidad y el repudio de la autoría de los mismos, cuando se toman las medidas necesarias para ello.

En este sentido, el Gobierno Federal a través del **SAT**, órgano desconcentrado de la Secretaría de Hacienda y Crédito Público, ha venido instrumentando el uso de la FIEL con diferentes dependencias y entidades de la APF.

El 11 de enero de 2012 se publicó en el Diario Oficial de la Federación el *"Decreto por el que se expide la Ley de Firma Electrónica Avanzada*", misma que en su artículo 2, fracción IV, define como autoridad certificadora a las dependencias y entidades de la APF y a los prestadores de servicios de certificación que conforme a las disposiciones jurídicas, tengan reconocida esa calidad y cuenten con la infraestructura tecnológica para la emisión, administración y registro de certificados digitales, así como para proporcionar servicios relacionados con los mismos.

Asimismo, de conformidad con lo dispuesto por los artículos 23 y 28 de la Ley de Firma Electrónica Avanzada, el **SAT** es considerado como autoridad certificadora para emitir certificados digitales en los términos de la citada Ley, por lo cual podrá celebrar bases o convenios de colaboración para la prestación de servicios relacionados con la FIEL.

Por otra parte, el 21 de marzo de 2014, se publicó en el Diario Oficial de la Federación el "Reglamento de la Ley de Firma Electrónica Avanzada, misma que en su artículo 23 señala que el SAT, deberá remitir a la Secretaría de la Función Pública, una copia de los Convenios de Colaboración que suscriba para la prestación de servicios relacionados con la Firma Electrónica Avanzada.

Al respecto, el **_____**busca implementar el uso de la FIEL con el fin de impulsar el desarrollo y los estándares de calidad en los trámites o servicios que proporciona, lo anterior, basado en el establecimiento de un marco jurídico para la utilización de una herramienta que aporte seguridad y confianza en la realización de operaciones electrónicas en redes abiertas, como es el caso de Internet. 2

Con lo anterior, se pretende minimizar el tiempo de atención en los trámites y los servicios, reduciendo considerablemente costos, además de incorporar las nuevas tecnologías de seguridad de las comunicaciones electrónicas entre los usuarios del _____.

D E C L A R A C I O N E S

I.DEL _____:

I.1. Que de acuerdo con los artículos (señalar naturaleza jurídica)
I.2. Que el _____, en su carácter de _____**,** cuenta con las facultad es suficientes para celebrar el presente Convenio, de conformidad con lo dispuesto en los artículos_____.
I.3 Que para los fines y efectos legales del presente Convenio, señala como domicilio el ubicado en_____.

II.DEL SAT:
II.1. Que es un órgano desconcentrado de la Secretaría de Hacienda y Crédito Público, con el carácter de autoridad fiscal, que tiene a su cargo el ejercicio de las facultades y el despacho de los asuntos que le encomiendan la Ley del Servicio de Administración Tributaria y las distintas disposiciones jurídicas aplicables, de acuerdo con lo dispuesto por los artículos 2, fracción I, 17 y 26 de la Ley Orgánica de la Administración Pública Federal; 1 y 7 de la Ley del Servicio de Administración Tributaria, y 2, rubro D, fracción I y 98-B del Reglamento Interior de la Secretaría de Hacienda y Crédito Público.
II.2. Que el _____, en su carácter de _____ Jefe del Servicio de Administración Tributaria cuenta con las facultades suficientes para celebrar el presente Convenio de conformidad con lo previsto en los artículos _____.
II.3. Que para los fines y efectos legales del presente Convenio, señala como domicilio el ubicado en Av. Hidalgo número 77, Colonia Guerrero, Delegación Cuauhtémoc, Código Postal 06300, en la Ciudad de México, Distrito Federal.

III.DE LAS PARTES:
III.1 Que se reconocen en forma recíproca la personalidad jurídica y capacidad legal que ostentan, misma que al momento de suscribir el presente Convenio, no les ha sido revocada, modificada, ni limitada en forma alguna.
III.2 Que están en la mejor disposición de apoyarse, sumar esfuerzos, recursos para cumplir cabalmente con el objeto del presente instrumento jurídico.
III.3 Que es su deseo celebrar el presente Convenio de colaboración, de conformidad con las siguientes:

C L Á U S U L A S

PRIMERA.- El objeto del presente Convenio es establecer las acciones necesarias y los mecanismos de colaboración para el uso gratuito de la FIEL de personas físicas que expide el **SAT**, en los procesos, trámites o servicios que el **_____** defina en el ámbito de su competencia y que dichas personas físicas lleven a cabo ante el mismo.

SEGUNDA.- El **_____** reconocerá los certificados digitales de FIEL que emita el **SAT**, los cuales se utilizarán en los procesos, trámites o servicios electrónicos que el **_____** lleve a cabo conforme a las normas que permitan su actuación mediante el uso de la FIEL. 3

Para efectos de lo anterior, el _____ cuenta con la infraestructura tecnológica que se requiere para llevar a cabo el procedimiento completo de dichos trámites o servicios, ello, sin perjuicio de que en el supuesto de adicionar con posterioridad nuevos procesos, trámites o servicios, implementará los ajustes que se requieran, apegados a las disposiciones jurídicas y administrativas correspondientes.
Asimismo y de conformidad con el plan de trabajo que el **_____** tenga definido, podrá solicitar al **SAT** la colaboración y asesoría técnica necesarias, notificándole por escrito y con un mínimo de un mes de anticipación, las fechas en que éstas se requieran.

TERCERA.- Para la correcta implementación de la FIEL en los trámites señalados en la cláusula primera que antecede, el **_____** recibirá las solicitudes o promociones que formulen los usuarios o particulares de sus servicios vía electrónica a través de Internet, siempre que **LAS PARTES** manifiesten la suficiencia operativa en sus tecnologías de información correspondientes, para lo cual, el **_____** consultará ante el **SAT** la validez y vigencia de los certificados digitales de la FIEL, conforme al procedimiento establecido en los lineamientos que al respecto se diseñen, mismos que debidamente suscritos por **LAS PARTES**, formarán parte integrante del presente Convenio como **ANEXO ÚNICO**.
Por lo anterior, el **_____** verificará el certificado digital de la FIEL que conste en la solicitud electrónica que formulen los promoventes o usuarios conforme a su normatividad, a fin de estar en posibilidad de aceptar, autorizar o rechazar la firma electrónica plasmada en el trámite o servicio solicitado a través de medios electrónicos.
Asimismo, el **_____** verificará ante el **SAT** la autenticidad, validez y vigencia de los certificados digitales de la FIEL de sus funcionarios o servidores públicos, facultados para llevar a cabo los trámites solicitados por los promoventes o usuarios.

CUARTA.- El **SAT** establecerá con el **_____** un mecanismo ágil que le permita a esta última recibir un mensaje con la información oportuna referente al estado de revocación de los certificados digitales de FIEL. Este mecanismo se desarrollará mediante la asistencia del Protocolo de Verificación del Estado de Certificados en Línea, "*Online Certificate Status Protocol*" (OCSP por sus siglas en idioma inglés) del **SAT**, en donde el **_____** podrá verificar en línea el estado de los certificados digitales de la FIEL en las transacciones relacionadas con su gestión.

QUINTA.- El **_____,** en el marco de sus atribuciones, promoverá entre sus áreas administrativas la difusión, adopción y uso de la FIEL que los usuarios hayan tramitado previamente ante el **SAT**, para lo cual, este último podrá prestar la asesoría técnica necesaria que el **_____** requiera.

SEXTA.- El **_____** se compromete a no utilizar el nombre e imagen de la FIEL en actividades de publicidad, promoción o similares sin contar con el consentimiento previo y por escrito del **SAT**.

SÉPTIMA.- LAS PARTES se obligan a guardar confidencialidad respecto de las actividades materia de este Convenio, así como de la información que en su caso se intercambie, en los términos de la legislación aplicable a cada una de ellas en materia de protección de datos y de conformidad con la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

OCTAVA.- LAS PARTES manifiestan que realizarán todas las acciones posibles para el cumplimiento del presente Convenio, y en caso de presentarse alguna discrepancia sobre su interpretación, la resolverán de mutuo acuerdo y por escrito.

NOVENA.- Ninguna de **LAS PARTES** será responsable de cualquier retraso o incumplimiento de este Convenio, que resulte de caso fortuito o fuerza mayor. Asimismo, el **SAT** no será responsable por los daños y perjuicios que se puedan ocasionar como resultado de la implementación y operación de la FIEL que lleve a cabo el **_____** para su uso en sus trámites o servicios. En tal supuesto el **_____** libera de responsabilidad al **SAT** y asume las cargas que se llegasen a imponer por tal motivo.4

DÉCIMA.- LAS PARTES convienen en asumir cada una cualquier responsabilidad en relación con el personal designado para dar cumplimiento al objeto del presente Convenio, reconociendo expresamente que no existirá sustitución ni solidaridad patronal entre las mismas.

DÉCIMA PRIMERA.- El presente instrumento podrá ser modificado o adicionado por acuerdo de **LAS PARTES**; dichas modificaciones deberán constar por escrito y entrarán en vigor a partir de la fecha en que sean acordadas.

DÉCIMA SEGUNDA.- El presente Convenio entrará en vigor a partir de la fecha de su firma y tendrá una vigencia indefinida, pudiendo darse por terminado por cualquiera de ellas, previa notificación por escrito a la otra parte con tres meses de anticipación.

El presente Convenio fue leído y, manifestándose conocedoras LAS PARTES de su contenido y alcances legales, se firma por cuadruplicado en México, Distrito Federal a ____ de _____ de 2014.

Por _____	**Por el SAT**
(señalar nombre y cargo del funcionario que firmará por parte de la entidad federativa)	**(señalar nombre y cargo del funcionario del SAT que firmará el Convenio)**

Anexo Único del Convenio de Colaboración Convenio de Colaboración *nombre del convenio* **celebrado entre el Servicio de Administración Tributaria (SAT) y** *nombre de la dependencia o entidad*

REQUERIMIENTOS TÉCNICOS PARA EL USO DEL *"ONLINE CERTIFICATE STATUS PROTOCOL"* (OCSP) DEL SAT

El servicio de consulta basado en protocolo de comunicación OCSP permite a los usuarios consultar el estado que guarda un Certificado Digital emitido por el SAT.
El procedimiento y requisitos que deberá cumplir la Dependencia, para estar en condiciones de utilizar el protocolo de comunicación OCSP se enlista a continuación:

1. Contar con su propia infraestructura de comunicación que permita consultar el estado que guarda dicho certificado a efecto de lograr su reconocimiento.
2. Proporcionar la dirección IP y la URL desde la cual se realizaran las consultas al servicio(considerando la dirección IP del firewall).
3. Se deberá considerar el documento RFC 2560 - X.509 Internet *Public Key Infrastructure Online Certificate Status Protocol – OCSP*, configuración de los servicios.
4. Tener la capacidad de leer las respuestas firmadas de las consultas al servicio OCSP utilizando el certificado de la Agencia Certificadora (AC) del SAT.

La AC del SAT proporcionará a *nombre de la dependencia o entidad* la dirección electrónica para llevar a cabo la consulta correspondiente de los certificados de la Agencia Registradora Central (ARC), Infraestructura Extendida de Seguridad (IES), a través, del protocolo OCSP.
Dicho servicio de consulta mantendrá una disponibilidad de 24 x 7.

Esquema de comunicación. Las consultas o coordinación con el SAT para brindar el apoyo o asesoría técnica será través de la Administración de Manejo de Identidades y FEA de la Administración Central de Seguridad, Monitoreo y Control de la Administración General de Comunicaciones y Tecnologías de la Información.

Área Tecnológica:	
Nombre:	Act. Andrés Medina Aguilar
Cargo:	Administrador de Manejo de Identidades y FEA
Correo electrónico:	andres.medina@sat.gob.mx
Teléfono	Tel: 58090200 Ext: 44634

Área Tecnológica:	
Nombre:	José Manuel González Salas
Cargo:	Subadministrador de Seguridad de la Información
Correo electrónico:	manuel.gonzalez@sat.gob.mx
Teléfono	58 02 00 00 Ext. 50361 y 22316 Dir. 58 09 03 61

Por parte de *nombre de la dependencia o entidad* serán las siguientes áreas:

Área Tecnológica:	
Nombre:	Act. Andrés Medina Aguilar
Cargo:	Administrador de Manejo de Identidades y FEA
Correo electrónico:	andres.medina@sat.gob.mx
Teléfono	Tel: 58090200 Ext: 44634

Área Tecnológica:	
Nombre:	José Manuel González Salas
Cargo:	Subadministrador de Seguridad de la Información
Correo electrónico:	manuel.gonzalez@sat.gob.mx
Teléfono	58 02 00 00 Ext. 50361 y 22316 Dir. 58 09 03 61

Nota: Con el objetivo de garantizar la estabilidad de los servicios, los cambios a los datos asentados en el presente documento deberán ser notificados por escrito en un término no mayor a 30 días naturales.

ANEXO Convenio de Colaboración nombre del convenio celebrado entre el Servicio de Administración Tributaria (SAT) y nombre de la dependencia o entidad Volumetría

VOLUMETRÍA DE LOS SERVICIOS DE NOMBRE DE LA
DEPENDENCIA Y/O ENTIDAD FEDERATIVA:
NOMBRE DEL SERVICIO:
ÁREA QUE OPERA EL SERVICIO:
NOMBRE Y CARGO DE LA PERSONA RESPONSABLE DEL REPORTE:

VOLUMETRÍA: Es la consulta que realiza la Dependencia y/o Entidad Federativa con la finalidad de corroborar si un certificado digital de firma electrónica "e.firma" emitido por el SAT es o no válido y con esto estar en posibilidad de realizar el servicio o trámite que la Dependencia y/o Entidad Federativa tenga implementado.

RANGO DE IP's:

AÑO	MESES											
	ENERO	FEB	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOST.	SEP	OCT	NOV	DIC
*2015												
*2016												
*2017												
*2018												
*2019												

* Estas cifras se reportarán con cantidades estimadas o proyectadas

PERIODO PICO DE LA DEMANDA DEL SERVICIO

En este rubro se indicarán los días y horas en que el o los servicios o trámites estarían teniendo un alta demanda.

Fecha de actualización.

Nota: La información del presente formato deberá ser remitido por la nombre de la dependencia o entidad de manera anual

Apéndice VI: Lineamientos para la Implementación de la Firma Electrónica Avanzada en el Instituto Federal Electoral

DISPOSICIONES GENERALES[477]

Primero.- Los presentes Lineamientos tienen por objeto establecer las bases para la operación de la Firma Electrónica Avanzada, en los siguientes supuestos:
a) Cuando el certificado digital sea emitido por el Instituto Federal Electoral en los términos del Reglamento para el uso y Operación de la Firma Electrónica Avanzada en el Instituto Federal Electoral; y
b) Cuando se reconozca el uso de la firma electrónica avanzada emitida por la autoridad certificadora en los términos de la Ley de Firma Electrónica Avanzada con quien se tenga celebrado convenio de colaboración respectivo.
Para los efectos del inciso b) se reconoce la firma electrónica avanzada emitida por el Sistema de Administración Tributaria previa firma del convenio correspondiente.
La Firma Electrónica Avanzada podrá ser utilizada en documentos electrónicos y, en su caso, en mensajes de datos, en aquellos actos o actuaciones electrónicas que se realicen a través de los sistemas y servicios informáticos, sujetos al uso de la Firma Electrónica Avanzada conforme a los lineamientos específicos que se emitan para cada caso.

Segundo.- Los presentes lineamientos serán de observancia obligatoria y general para todos los funcionarios del Instituto, de la Rama Administrativa o miembros del Servicio Profesional Electoral.

Tercero.- Son sujetos de aplicación de los presentes Lineamientos los servidores públicos del Instituto que de conformidad a las atribuciones conferidas en la normatividad vigente tengan la facultad de suscribir documentos, así como los usuarios externos que hagan uso de los sistemas y servicios informáticos sujetos al uso de la Firma Electrónica Avanzada en el Instituto Federal Electoral.

Cuarto.- Para los efectos de los presentes Lineamientos, serán aplicables las definiciones establecidas en el artículo 2 del Reglamento para el Uso y Operación de la Firma Electrónica Avanzada en el Instituto Federal Electoral.

Quinto.- La Firma Electrónica Avanzada tiene la misma validez jurídica que la firma autógrafa, por lo cual todos los actos, documentos electrónicos que se firmen con los datos de generación de la Firma Electrónica Avanzada asociados al certificado digital, serán imputables a su titular, por lo que es de exclusiva responsabilidad de éste el resguardo del certificado digital y la confidencialidad de la llave privada que conforma la Firma Electrónica Avanzada, con el fin de evitar la utilización no autorizada de la misma.

Sexto.- La utilización de los Sistemas en el Instituto, así como de la información registrada en ellos, será de uso restringido y solamente los usuarios responsables y autorizados podrán hacer uso de los mismos para los fines establecidos en las leyes y normatividad vigente dentro del marco de las atribuciones o derechos que su cargo, función o actividad les otorguen.

Séptimo.- El uso de la Firma Electrónica Avanzada implica:
I. La vinculación indubitable entre el Firmante y el Documento Electrónico en el que se contenga la Firma Electrónica Avanzada, que se asocia con los datos que se encuentran bajo el control exclusivo del Firmante y que expresan en medio digital su identidad;
II. La responsabilidad de prevenir cualquier modificación o alteración en el contenido de los Documentos Electrónicos que se presentan en el Sistema, al existir un control exclusivo de los medios para insertar la referida firma, y
III. La integridad y autenticidad del contenido del documento firmado electrónicamente.

[477] Publicado en el DOF el 7 mayo 2014.

Octavo.- Los titulares de una Firma Electrónica Avanzada tendrán las siguientes obligaciones:
I. Resguardar la confidencialidad de la llave privada que se requiere para signar electrónicamente los documentos;
II. Mantener el control físico, personal y exclusivo de su Firma Electrónica Avanzada;
III. Actualizar los datos proporcionados para su tramitación, e
IV. Informar de manera inmediata al prestador de servicios de certificación, de cualquier circunstancia que ponga en riesgo su privacidad o confidencialidad en su uso, a fin de que, de ser necesario, se revoque.

DE LA FIRMA ELECTRÓNICA AVANZADA INSTITUCIONAL

Noveno.- La Firma Electrónica Avanzada Institucional es un medio de identificación electrónica que otorga el Instituto a través de la Dirección Ejecutiva de Administración a aquellos funcionarios públicos con atribuciones legales y normativas para suscribir documentos al interior de la Institución, en aquellos Sistemas y Servicios Informáticos que al efecto determine el Consejo General y la Junta General Ejecutiva.
Los funcionarios públicos del Instituto legalmente autorizados podrán solicitar ante la Dirección Ejecutiva de Administración el otorgamiento de la Firma Electrónica Avanzada Institucional o bien hacer uso de la Firma Electrónica Avanzada emitida por el Servicio de Administración Tributaria (SAT).

Décimo.- Los funcionarios públicos del Instituto deberán cumplir con los requisitos previstos en el Reglamento, en estos Lineamientos; además de requisitar la solicitud correspondiente y firmar la Carta de Términos y Condiciones que forman parte de los presentes Lineamientos, mediante la cual se manifestará que se convalidan todos aquellos actos que se celebren con la Firma Electrónica Avanzada Institucional, como si hubieran sido firmados autógrafamente por su suscriptor.

SISTEMA DE REGISTRO Y CERTIFICACIÓN

Décimo Primero.- Los Firmantes serán responsables del buen uso de los Sistemas y Servicios Informáticos en que utilicen la Firma Electrónica Avanzada Institucional, en los términos de estos Lineamientos y demás disposiciones aplicables.
Los Firmantes deberán informar por escrito a la Dirección Ejecutiva de Administración del Instituto acerca de cualquier modificación en sus datos personales o laborales, a efecto de realizar la actualización correspondiente.

Décimo Segundo.- La Dirección Ejecutiva de Administración por conducto de la Dirección de Personal será la Autoridad Registradora responsable de:
I. Verificar que se cuenta con la documentación a que se refiere el Lineamiento Décimo Cuarto para sustentar la pertenencia e identidad del solicitante;
II. Registrar a los funcionarios públicos autorizados para el uso de la firma electrónica avanzada institucional;
III. En coordinación con la Unidad Técnica de Servicios de Informática y la Coordinación de Tecnología de Información Administrativa de la Dirección Ejecutiva de Administración proporcionar los elementos tecnológicos necesarios con el propósito de que los Firmantes estén en condiciones de generar su Certificado Digital;
IV. En aquellos supuestos a que se refiere el Lineamiento Décimo Séptimo y Décimo Octavo dará aviso a la Coordinación de Tecnología de Información Administrativa de la Dirección Ejecutiva de Administración como autoridad certificadora para que lleve a cabo los procedimientos necesarios para la cancelación o modificación del certificado digital, y
V. Las demás que se deriven de las disposiciones de los presentes Lineamientos y demás normatividad aplicable.

Décimo Tercero.- Para efectos de registro para la obtención del certificado digital, se considerará como identificación oficial cualquiera de los siguientes documentos:
I. Pasaporte vigente expedido por la Secretaría de Relaciones Exteriores;
II. Credencial para votar vigente expedida por el Instituto Federal Electoral;
III. Cédula profesional expedida por la Secretaría de Educación Pública;
IV. Cartilla del Servicio Militar Nacional, expedida por la Secretaría de la Defensa Nacional;

V. Tratándose de extranjeros, el documento migratorio vigente que corresponda, emitido por la autoridad competente;
VI. Visa emitida por el consulado o embajada, y
VII. Certificado de Matricula Consular, expedido por la Secretaría de Relaciones Exteriores o en su caso por la Oficina Consular de la circunscripción donde se encuentre el connacional.

Décimo Cuarto.- Con la finalidad de dar certeza y seguridad para el otorgamiento del certificado digital, los funcionarios se apersonarán en el domicilio ubicado en las instalaciones de la Dirección Ejecutiva de Administración en el que deberán cumplir con los siguientes requisitos:
I. Llenar la solicitud para obtener el certificado digital;
II. Proporcionar su nombre completo;
III. Precisar su domicilio (calle, número exterior e interior, calles que lo circundan, colonia, ciudad, código postal, delegación o municipio, entidad federativa y país);
IV. Proporcionar su correo institucional;
V. Indicar su Clave Única de Registro de Población (CURP) siempre que se trate de personas físicas de nacionalidad mexicana;
VI. Precisar su nacionalidad;
VII. Exhibir su identificación oficial, y
VIII. Nombramiento del funcionario público solicitante.
Los documentos mencionados en las fracciones VII y VIII deberán presentarse en original o copia certificada y copia simple para su cotejo. El documento mencionado en la fracción I deberá presentarse en original. Cuando el solicitante sea un extranjero, tratándose del dato señalado en la fracción VI, deberá exhibir el documento con el que acredite su nacionalidad en el formato expedido por la Secretaría de Gobernación o impreso desde el portal de la misma y en copia simple.
Cumplidos los requisitos señalados, el solicitante obtendrá su certificado digital, el cual contendrá los parámetros de seguridad determinados por la Unidad Técnica de Servicios de Informática además de la constancia de registro.

Décimo Quinto.- La Autoridad Registradora otorgará los certificados digitales a los Firmantes respectivos.
Los Firmantes de los Sistemas y Servicios Informáticos sólo podrán contar con un certificado digital. Éstos se asignarán de manera personalizada, por lo que la Llave Privada y su contraseña sólo deberán ser de su conocimiento y no deberá difundirla.
A la Autoridad Registradora le corresponde informar a la Autoridad Certificadora acerca de las altas, bajas o modificaciones de las llaves de acceso de los Firmantes.
La Autoridad Registradora remitirá las referidas solicitudes a la Autoridad Certificadora, misma que en su caso, llevará a cabo los procedimientos necesarios para los registros de alta, modificación o baja de los certificados digitales de los usuarios.
La Autoridad Certificadora comunicará las respuestas de las referidas solicitudes a la Autoridad Registradora para que, por su conducto, se comunique al Titular del área de adscripción del funcionario Firmante.

Décimo Sexto.- Los titulares del certificado digital serán responsables de su uso por lo que suscribirán una carta de conocimiento de dicha responsabilidad al obtener estos elementos electrónicos.

Décimo Séptimo.- Los funcionarios públicos que requieran revocar o modificar los datos de su certificado digital, deberán apersonarse en el domicilio ubicado en las instalaciones de la Dirección Ejecutiva de Administración y cumplir con los siguientes requisitos:
I. Llenar la solicitud de baja o modificación de información proporcionada para la obtención de la Llave Pública y de la Llave Privada. En este último caso, precisando la información objeto de actualización.
II. Proporcionar su nombre completo, y
III. Presentar identificación oficial.
El documento referido en la fracción III deberá presentarse en original o copia certificada y copia simple para su cotejo y copia simple. El documento mencionado en la fracción I deberá presentarse en original.
Una vez cumplidos estos requisitos se otorgará al solicitante una constancia impresa que indicará, además de la información antes precisada, la fecha de revocación o modificación de su certificado digital según sea el caso.

Décimo Octavo.- La Autoridad Registradora tendrá la responsabilidad de hacer del conocimiento de la Autoridad Certificadora los ascensos, cambios de adscripción, renuncias y modificaciones que ameriten una revisión o revocación de los certificados digitales asignados a Usuarios Internos, para proceder a su cancelación en los casos en que estos causen baja.
Asimismo, deberá de revocar los Certificados Digitales cuando se detecte o acredite su uso indebido, comunicándolo a la Autoridad Registradora, a efecto de que proceda en los términos de las medidas aplicables.

Décimo Noveno.- A la Dirección Ejecutiva de Administración por conducto de la Coordinación de Tecnología de Información Administrativa como Autoridad Certificadora le corresponde:
I. En coordinación con la Unidad Técnica de Servicios de Informática Tecnología habilitar la utilización de la Firma Electrónica Avanzada con todas sus características, emitiendo los certificados digitales correspondientes;
II. Asesorar, con la colaboración de la Unidad Técnica de Servicios de Informática, a los funcionarios públicos del Instituto así como a los usuarios externos, para el uso del Sistema de Registro y Certificación;
III. Llevar un registro de los certificados digitales que emitan y de los que revoquen;
IV. Revocar los certificados de Firma Electrónica Avanzada, cuando se actualice alguno de los supuestos de revocación señalados en el artículo 19 del Reglamento para el Uso y Operación de la Firma Electrónica Avanzada en el Instituto Federal Electoral.
V. Autentificar que la información que se incorpora a la solicitud de certificado digital, corresponda efectivamente a la identidad del solicitante;
VI. Informar al solicitante las razones por las cuales, en su caso, no fue posible emitirle el certificado correspondiente, y
VII. Las demás que se deriven de las disposiciones del presente Reglamento y demás normatividad aplicable.

Vigésimo.- Una vez completada la solicitud y validada la información del solicitante la Autoridad Certificadora del Instituto emitirá el Certificado Digital correspondiente.
El Certificado Digital se almacenará en un Medio electrónico que proporcionará y estará bajo el resguardo del Firmante. Este Certificado tendrá una vigencia de tres años, contados a partir de su alta en el sistema.
Los Firmantes de los Sistemas y Servicios Informáticos sólo podrán contar con un Certificado Digital vigente.

DE LA FIRMA ELECTRÓNICA AVANZADA, EMITIDA POR EL SERVICIO DE ADMINISTRACIÓN TRIBUTARIA (SAT) O CUALQUIER OTRA AUTORIDAD CERTIFICADORA LEGALMENTE RECONOCIDA

Vigésimo Primero.- Los usuarios externos que hagan uso de los sistemas y servicios informáticos sujetos al uso de la Firma Electrónica Avanzada en el Instituto Federal Electoral, lo harán a través de un certificado digital emitido por el Servicio de Administración Tributaria (SAT) o cualquier otra autoridad certificadora legalmente reconocida, con la que el Instituto tenga celebrado el convenio de colaboración respectivo.
Los funcionarios del Instituto, en los actos jurídicos que lleven a cabo conforme a las atribuciones legalmente otorgadas, podrán optar por el uso de la Firma Electrónica Avanzada (FIEL) emitida por el Servicio de Administración Tributaria, para la cual deberán hacerlo del conocimiento por escrito de la Dirección Ejecutiva de Administración.
En términos de lo dispuesto por el punto de Acuerdo Cuarto del Acuerdo CG314/2013, los actos y actuaciones electrónicas en la que se llevará a cabo la implementación de la Firma Electrónica Avanzada estará sujeta a la emisión de los Lineamientos correspondientes a cada materia, en la que se determine el uso de la misma, por parte de la Junta General Ejecutiva.

Vigésimo Segundo.- Los usuarios externos que hagan uso de la Firma Electrónica Avanzada en el Instituto Federal Electoral, podrán hacer uso a través de un certificado digital vigente emitido por el Servicio de Administración Tributaria (SAT) y la llave pública y privada que conforman la Firma Electrónica Avanzada.

Vigésimo Tercero.- La Firma Electrónica Avanzada contenida en los documentos electrónicos garantizará y dará certeza de lo siguiente:

I. Que el documento electrónico ha sido emitido por el firmante de manera tal que su contenido le es atribuible al igual que las consecuencias jurídicas que de él se deriven;
II. Que el documento electrónico ha permanecido completo e inalterado desde su firma, con independencia de los cambios que hubiere podido sufrir el medio que lo contiene como resultado del proceso de comunicación, archivo o presentación;
III. Que dicha firma corresponde exclusivamente al firmante, por lo que todos los documentos electrónicos o mensajes de datos presentados con la misma serán imputables a su titular y no serán susceptibles de repudio, con lo que se garantiza la autoría e integridad del documento, y
IV. Que el documento sólo puede ser cifrado por el firmante y el receptor.

Vigésimo Cuarto.- La autenticación de los usuarios externos, así como los documentos electrónicos firmados con la Firma Electrónica Avanzada (FIEL), serán considerados hechos legítima y auténticamente por el firmante y, en caso de personas morales, por la persona que acredite tener legal representación de la persona moral de que se trate, en el momento en que se realizó el acto correspondiente. Lo anterior, no admitirá prueba en contrario ante el IFE, y el titular del certificado digital será responsable de las consecuencias jurídicas que deriven de los actos que realicen ante el Instituto utilizando la FIEL.
Vigésimo Quinto.- En caso de pérdida, robo o destrucción de la Firma Electrónica Avanzada (FIEL), o cualquier otro evento que ponga en riesgo la confidencialidad de los certificados electrónicos o las llaves que conforman la Firma Electrónica Avanzada (FIEL), el usuario externo, persona física o moral, bajo su absoluta responsabilidad, deberá proceder con su inmediata revocación o reposición ante el Servicio de Administración Tributaria (SAT), sujetándose a los procesos y lineamientos que este último determine.

Vigésimo Sexto.- El uso de la Firma Electrónica Avanzada (FIEL) para la realización de actos ante el Instituto mediante medios electrónicos, estará sujeto a que el Instituto ponga a disposición de los usuarios las herramientas tecnológicas necesarias en los trámites y procesos de que se trate, así como para la firma de documentos electrónicos mediante la Firma Electrónica Avanzada (FIEL) y por ende, la autenticación del usuario. Para tal efecto, el Instituto emitirá y pondrá a disposición de los particulares los manuales de usuario respectivos, en los cuales se detallarán los pasos y procedimientos a seguir para la realización de actos mediante el uso de la Firma Electrónica Avanzada (FIEL).

Vigésimo Séptimo.- Una vez autenticado el firmante, se tendrá por válido y sin que se admita prueba en contrario, el vínculo entre el firmante y los datos que fueron utilizados para la creación de la respectiva Firma Electrónica Avanzada (FIEL), generándose el acceso y registro de la persona de que se trate como usuario de los sistemas y servicios informáticos establecidos con el uso de la Firma Electrónica Avanzada Firma Electrónica Avanzada (FIEL) en el Instituto. Sólo los usuarios externos debidamente registrados podrán acceder a dichos sistemas y servicios.

Vigésimo Octavo.- Los usuarios externos podrán hacer uso de los sistemas y servicios informáticos establecidos con el uso de la Firma Electrónica Avanzada (FIEL) en el Instituto, personalmente o a través de su representante legal, quien debe acreditar esa representación y contar con poder suficiente, debidamente otorgado conforme a la legislación civil vigente, para poder registrarse y realizar actos ante el Instituto.

Vigésimo Noveno.- El usuario externo personalmente o a través de su representante legal se autenticará mediante el uso de su Firma Electrónica Avanzada (FIEL) y podrá presentar actos ante el Instituto mediante el uso de la misma.

Trigésimo.- Conforme lo dispuesto en el artículo anterior, los actos que firme el usuario externo personalmente o a través de su representante legal con su Firma Electrónica Avanzada (FIEL), serán considerados hechos legítima y auténticamente por el firmante, siendo responsable ante el Instituto de las consecuencias jurídicas que deriven de los actos realizados. Lo anterior no admitirá prueba en contrario ante el Instituto, sin perjuicio de las acciones civiles o penales que puedan derivarse.

Trigésimo Primero.- La consulta respecto al estado de los certificados expedidos por el Servicio de Administración Tributaria (SAT) se desarrollará mediante la asistencia del Protocolo de Verificación del Estado de Certificados en

Línea (OCSP por sus siglas en idioma inglés), en donde el Instituto podrá verificar en línea y tiempo real el estado de los certificados digitales de la Firma Electrónica Avanzada (FIEL), en las transacciones relacionadas con su gestión.

DISPOSICIONES FINALES

Trigésimo Segundo.- Corresponde a la Dirección Ejecutiva de Administración y a la Unidad Técnica de Servicios de Informática además de las facultades y obligaciones previstas en los artículos 14 y 15 del Reglamento para el uso y operación de la Firma Electrónica Avanzada en el Instituto Federal Electoral, atender los requerimientos relacionados con las solicitudes de emisión de certificados digitales en sus respectivos ámbitos de competencia.

Trigésimo Tercero.- Corresponderá a la Dirección Ejecutiva de Administración la interpretación de los presentes Lineamientos.

Transitorios

PRIMERO.- Para efectos del inciso b) del artículo 1 de los presentes lineamientos, la Dirección Ejecutiva de Administración gestionó la firma del convenio con el Sistema de Administración Tributaria mismo que ha sido suscrito con 11 de febrero del 2014.
SEGUNDO.- Para la operación de la firma electrónica avanzada institucional, se someterá a Acuerdo de la Junta General Ejecutiva los actos y procedimientos que serán objeto de la misma conforme a la normatividad vigente, así como la planeación institucional para su implementación.
TERCERO.- La Carta de Términos y Condiciones para utilizar la Firma Electrónica Avanzada en los actos que se realicen en el Instituto Federal Electoral, que se anexa forma parte integrante de los Lineamientos.

CARTA DE TÉRMINOS Y CONDICIONES PARA UTILIZAR LA FIRMA ELECTRÓNICA AVANZADA EN LOS ACTOS QUE SE REALICEN EN EL INSTITUTO FEDERAL ELECTORAL.

El suscrito para todos los efectos legales a que haya lugar, y cuyos datos generales aparecen en ella presente documento, manifiesto haber solicitado la emisión de un Certificado Digital en el que consten los Datos de Verificación de Firma Electrónica Avanzada (Llave Pública) asociados a los Datos de Creación de Firma Electrónica Avanzada (Llave Privada) y Contraseña de Llave Privada, que se generaron previamente y en absoluto secreto, sin que persona alguna me haya asistido durante dicho proceso.

Con fundamento en los Lineamientos para la Implementación de la Firma Electrónica Avanzada en el Instituto Federal Electoral, aprobados por la Junta General Ejecutiva mediante Acuerdo JGE26/2014, de fecha 18 de marzo de 2014, como servidor público del Instituto, que conforme a mis atribuciones legalmente establecidas, podre realizar los actos previstos en los procedimientos determinados por el Consejo General y/o la Junta General Ejecutiva del Instituto Federal Electoral de manera electrónica a través de mi Firma Electrónica Avanzada Institucional, cuyo certificado Digital esté vigente y haya sido emitido por el Instituto Federal Electoral.

La Firma Electrónica Avanzada institucional sustituye la firma autógrafa del firmante y producirá los mismos efectos que las leyes otorgan a los documentos con firma autógrafa, teniendo el mismo valor probatorio. Asimismo, con el uso de la Firma Electrónica Avanzada institucional se tiene por reconocida la garantía de la autoría del Firmante y de la integridad de los documentos electrónicos que firmen con ella y, por ende, el contenido de los mismos no podrá desconocerse ni admitirá prueba en contrario.

Asimismo manifiesta su conformidad en que se utilice un procedimiento de certificación de identidad que conste del registro electrónico de huellas dactilares, fotografía, firma autógrafa y documentos, con el fin de confirmar el vínculo que debe existir entre el Certificado Digital y su titular.

Adjunto a la presente la documentación solicitada con el fin de identificarme, por lo que la Autoridad Registradora sólo podrá constatar a simple vista que los documentos correspondan a los rasgos fisonómicos y caligráficos en mi carácter de servidor público, por lo que este último asume responsabilidad exclusiva respecto de la autenticidad

de tales documentos, así como de la veracidad de los demás datos que proporcione en el proceso de su identificación.

La Autoridad Certificadora manifiesta que los datos personales recabados del Servidor Público durante su comparecencia serán incorporados y protegidos en los sistemas del Instituto Federal Electoral, de conformidad con los Lineamientos de Protección de Datos Personales y con las diversas disposiciones legales sobre la confidencialidad y protección de datos.

La Certificadora manifiesta que el servidor público podrá corregir sus datos personales acudiendo directamente a la Dirección Ejecutiva de Administración.
Al finalizar el trámite el servidor público recibirá y aceptará el Certificado Digital emitido por el Instituto Federal Electoral, sirviendo este documento como el acuse de recibo más amplio que en derecho proceda.

Adicionalmente, el servidor público reconoce y acepta que el uso de la Llave Privada y Contraseña de Llave Privada con base en las cuales dicho Certificado Digital será elaborado, quedarán bajo su exclusiva responsabilidad, y que los documentos electrónicos que tengan asociada una firma electrónica avanzada generada con las referidas Llave Privada y Contraseña de Llave Privada que pueda ser verificada con la Llave Pública contenida en el Certificado Digital, le serán atribuibles, por lo que asume la responsabilidad de su información y contenido. Por lo anterior, se obliga a mantener absoluta confidencialidad respecto de las aludidas Llave Privada y Contraseña de Llave Privada, así como a realizar los trámites necesarios para solicitar la revocación de dicho Certificado Digital ante la Dirección Ejecutiva de Administración, mediante los mecanismos que la misma establezca, en el evento de que por cualquier causa dicha información haya sido divulgada y, por tanto, la integridad y/o confidencialidad de dicha información haya sido comprometida.

Por otra parte el servidor público manifiesta conocer el contenido y alcance de las disposiciones legales y reglamentarias relativas a la celebración de actos jurídicos mediante el uso de medios electrónicos, digitales o de cualquier otra tecnología, por lo que asume plena responsabilidad respecto de la información y contenido de todo documento electrónico o digital elaborado y enviado en el que se haga uso de la citada Llave Privada y Contraseña de Llave Privada, toda vez que por ese sólo hecho se considerará que el documento electrónico o digital le es atribuible.

El servidor público reconoce y acepta que la Llave Pública proporcionada por él y contenida en el Certificado Digital, así como en cualquier otro que con posterioridad se obtenga para efectos de acceder a diversos servicios que implemente el Instituto Federal Electoral, será de carácter público y podrá ser consultada libremente por cualquier interesado a través de los medios y formas que disponga.

Por otra parte, el servidor público reconoce y acepta que el Instituto Federal Electoral en su carácter de Certificadora y Registradora únicamente será responsable por los errores que, en su caso, llegare a cometer con motivo de culpa grave en el proceso de generación, registro, entrega y revocación del Certificado Digital, según corresponda, así como que no serán responsables por los daños y perjuicios que se pudieran causar al servidor público o a terceros, cuando por caso fortuito o fuerza mayor no puedan realizarse registros, verificaciones, revocaciones o tramitar documentos electrónicos cifrados con las Llaves Públicas y Privadas relacionadas con dicho Certificado Digital.

Por caso fortuito o fuerza mayor se entenderá todo acontecimiento o circunstancia inevitable, más allá del control razonable de la Certificadora, que le impida el cumplimiento de sus funciones con el carácter que le corresponde, por lo que el servidor público reconoce a través de su firma autógrafa asentada en el espacio designado para ello en el anverso y reverso de este formato, al presente como prueba fehaciente de la aceptación de todo lo especificado en el mismo.

Apéndice VII. Formato de solicitud de la Firma Electrónica para el Seguimiento de Expedientes (FESE)

Nombre (del solicitante, si actúa en representación de alguna persona moral) con **domicilio** en (_____), *en términos del Acuerdo General 21/2007 del Pleno del Consejo de la Judicatura Federal, aprobado en sesión de veintitrés de mayo de dos mil siete y publicado en el Diario Oficial de la Federación el siete de junio del mismo año, y del Acuerdo de la Comisión de Administración del propio Consejo en sesión de catorce de junio de la misma anualidad, por el que se dan a conocer las modalidades de los trámites jurisdiccionales a través de medios de comunicación electrónica, sistema de información; manifiesto, bajo protesta de decir verdad:*

I. Que reconozco como propia, veraz y auténtica la información que en lo sucesivo enviaré por medios electrónicos, avalada por mi FESE y acepto como válido el acuse de recibo electrónico generado por el órgano jurisdiccional.
II. Que la clave electrónica que utilizaré como mi FESE en la documentación que envíe por medios de comunicación electrónica, los reconozco como propios y auténticos.
III. Que acepto que el uso de mi FESE quedará bajo mi exclusiva responsabilidad.
IV. Que para el caso de que alguien me represente utilizando la citada clave, me comprometo a comunicar al órgano de la clave a que se refiere el presente escrito; la pérdida o cualquier otra situación que pudiera implicar la reproducción o uso indebido de mis datos de creación de firma electrónica y de la clave electrónica, en un plazo no mayor a 12 horas por medios electrónicos con acuse de recibo o por escrito al día hábil siguiente.
V. Que estoy de acuerdo en ser requerido para el envío de cualquier información adicional respecto de mi clave electrónica.
VI. Que bajo protesta de decir verdad manifiesto, que los datos asentados en mi solicitud son ciertos y que pueden verificarse, bajo la pena de incurrir en el delito de falsedad de declaraciones dadas a una autoridad judicial en caso de ser falsos, que acepto que la FESE otorgada a mi favor es intransferible y por ello debe equipararse como si fuera mi firma estampada en original.
VII. Que es mi voluntad que en la fecha y hora que ingrese al sistema de información electrónica y consultar los archivos que contengan acuerdos o resoluciones usando mi FESE me hago sabedor de éstos, de conformidad con lo dispuesto por el artículo 320, del Código Federal de Procedimientos Civiles, independientemente del día en que se fijen las listas con las publicaciones en los estrados o los rotulones en las puertas de los Tribunales de Circuito y Juzgados de Distrito, según corresponda. Que acepto que el sistema de información electrónica es el medio de comunicación ordinario que utilizaré con los órganos jurisdiccionales del PJF a excepción de la SCJN y del Tribunal Electoral, y que me obligo a consultar todos los días y será la vía por la que enviaré cualquier promoción o documento, obligándome a presentar los originales, de requerirlo el órgano jurisdiccional, independientemente del valor que tienen las pruebas generadas o comunicadas que consten en el medio electrónico, óptico o en cualquier otra tecnología, en términos del artículo 210-A del Código Federal de Procedimientos Civiles.
VIII. XIII. Que acepto que en caso de incumplir con lo estipulado en el presente escrito, el órgano jurisdiccional o la Unidad de Control de Certificación de Firmas Electrónicas, podrán revocar mi firma electrónica.

Apéndice VIII: Políticas de Operación del Uso de la Firma Electrónica Avanzada emitida por el CJF

- *Las firmas electrónicas avanzadas emitidas por el Consejo de la Judicatura Federal tendrán una vigencia de un año contando a partir de su expedición.*
- *La Unidad para el Control de Certificación Firmas (UNCOCEFI), dependiente de la Dirección General de Estadística Judicial, será el área del Consejo de la Judicatura Federal encargada de la expedición, renovación, revocación y administración de las firmas electrónicas avanzadas emitidas por el propio Consejo.*
- *La firma electrónica avanzada que emita la UNCOCEFI únicamente podrá ser solicitada por personas físicas, cuya solicitud se realizará exclusivamente por la persona interesada, sin que otra pueda hacerlo a su nombre y representación.*
- *La firma electrónica avanzada emitida por la UNCOCEFI garantizará la autenticidad, integridad, no repudio y confidencialidad de los documentos (y de su contenido) firmados electrónicamente.*
- *La firma electrónica avanzada hará las veces de firma autógrafa, por lo que toda documentación firmada electrónicamente se tendrá como signada autógrafamente.*
- *El uso adecuado y resguardo del certificado digital y de la llave privada que componen la firma electrónica avanzada será responsabilidad del solicitante.*
- *La solicitud de una firma electrónica avanzada emitida por la UNCOCEFI deberá hacerse en línea desde la liga correspondiente de la página de Internet de la Dirección General de Estadística Judicial.*
- *El solicitante deberá llenar el formulario respectivo e ingresar los archivos electrónicos que contengan la digitalización de su identificación oficial, así como de su acta de nacimiento, carta de naturalización o documento migratorio vigente, así como su comprobante de domicilio, el cual no podrá ser mayor a 3 meses.*
- *Una vez que la solicitud es recibida por el sistema, este emitirá un acuse de recibo con número de folio, con el cual el interesado deberá acudir ante un agente registrador a fin de que coteje los documentos originales con los previamente digitalizados y verifique que la información capturada en el formulario concuerda completamente con la información que se desprende de la documentación presentada.*
- *El agente registrador, si así procediere, certificará en el propio sistema los archivos electrónicos acompañados a la solicitud y emitirá la firma electrónica avanzada. El solicitante recibirá un mensaje en la cuenta de correo electrónico que capturó en la solicitud, con la liga correspondiente para la descarga del certificado.*
- *La descarga de la firma electrónica avanzada deberá hacer necesariamente en el equipo de cómputo desde donde se realizó la solicitud, en virtud de que es ahí en donde se generó y almacenó la llave privada, con independencia de que posteriormente se desee exportar e importar dicha firma.*
- *En caso de que durante el procedimiento previo a la emisión de las firmas electrónicas avanzadas se detecten inconsistencias en la información capturada en el formulario o en la documentación digitalizada, o así lo solicitase el interesado, el agente registrador cancelará la solicitud de la firma electrónica avanzada.*
- *En caso de extravío de la firma electrónica avanzada o del dispositivo en donde se encuentra almacenada, esta deberá revocarse y solicitarse una nueva.*
- *El titular de una firma electrónica avanzada emitida por la UNCOCEFI, si así lo desea, podrá auto-revocarla. La auto-revocación deberá hacerse a través de la liga correspondiente de la página de Internet de la Dirección General de Estadística Judicial.*

- *Las firmas electrónicas avanzadas emitidas por la UNCOCEFI serán revocadas por el fallecimiento de su titular o por resolución del Pleno del Consejo de la Judicatura, de la Comisión de Administración o por la UNCOCEFI.*
- *Las firmas electrónicas avanzadas que emita la UNCOCEFI, podrán renovarse dentro de los últimos treinta días de vigencia de la misma. La solicitud de renovación será en línea desde la liga correspondiente de la página de Internet de la Dirección General de Estadística Judicial.*
- *Si el titular de una firma electrónica avanzada emitida por la UNCOCEFI no la renovó en los treinta días previos a su vencimiento, tendrá que realizar una nueva solicitud y volver a proporcionar la documentación requerida.*
- *La UNCOCEFI cancelará las solicitudes de firmas electrónicas avanzadas de las cuales los interesados no hayan acudido ante un agente registrador a finalizar su trámite. Dichas cancelaciones se harán el primer día hábil de cada mes.*
- *La UNCOCEFI diseñará los mecanismos necesarios para la emisión de las firmas electrónicas avanzadas de las áreas administrativas del CJF, así como de las personas físicas que ostentan un cargo de autoridad.*

Apéndice IX. “Anexos I.A y I.B de la Directiva 2011/83/UE del parlamento europeo y del consejo de 25 de octubre de 2011 sobre los derechos de los consumidores, por la que se modifican la Directiva 93/13/CEE del Consejo y la Directiva 1999/44/CE del Parlamento Europeo y del Consejo y se derogan la Directiva 85/577/CEE del Consejo y la Directiva 97/7/CE del Parlamento Europeo y del Consejo.”

Anexo I.A. Derecho de Desistimiento

Tiene usted derecho a desistir del presente contrato en un plazo de 14 días sin necesidad de justificación. El plazo de desistimiento expirará a los 14 días del día (1).

Para ejercer el derecho de desistimiento, deberá usted notificarnos (2) su decisión de desistir del contrato a través de una declaración inequívoca (por ejemplo, una carta enviada por correo postal, fax o correo electrónico). Podrá utilizar el modelo de formulario de desistimiento que figura a continuación, aunque su uso no es obligatorio. (3) Para cumplir el plazo de desistimiento, basta con que la comunicación relativa al ejercicio por su parte del derecho de desistimiento sea enviada antes de que venza el plazo de desistimiento.

- Consecuencias del desistimiento:
En caso de desistimiento por su parte, le devolveremos todos los pagos recibidos de usted, incluidos los gastos de entrega (con la excepción de los gastos adicionales resultantes de la elección por su parte de una modalidad de entrega diferente a la modalidad menos costosa de entrega ordinaria que ofrezcamos) sin ninguna demora indebida y, en todo caso, a más tardar 14 días a partir de la fecha en la que se nos informe de su decisión de desistir del presente contrato. Procederemos a efectuar dicho reembolso utilizando el mismo medio de pago empleado por usted para la transacción inicial, a no ser que haya usted dispuesto expresamente lo contrario; en todo caso, no incurrirá en ningún gasto como consecuencia del reembolso. (4), (5), (6).

- Instrucciones para su cumplimentación:
(1) Insértese una de las expresiones que aparecen entre comillas a continuación:
a) en caso de un contrato de servicios o de un contrato para el suministro de agua, gas o electricidad —cuando no estén envasados para la venta en un volumen delimitado o en cantidades determinadas—, de calefacción mediante sistemas urbanos o de contenido digital que no se preste en un soporte material: «de la celebración del contrato.»;
b) en caso de un contrato de venta: «que usted o un tercero por usted indicado, distinto del transportista, adquiera la posesión material de los bienes.»;
c) en caso de un contrato de entrega de múltiples bienes encargados por el consumidor en el mismo pedido y entregados por separado: «que usted o un tercero por usted indicado, distinto del transportista, adquiera la posesión material del último de esos bienes.»;
d) en caso de entrega de un bien compuesto por múltiples componentes o piezas: «que usted o un tercero por usted indicado, distinto del transportista, adquiera la posesión material del último componente o pieza.»;
e) en caso de un contrato para la entrega periódica de bienes durante un plazo determinado: «que usted o un tercero por usted indicado, distinto del transportista, adquiera la posesión material del primero de esos bienes.».
(2) Insértese su nombre, su dirección geográfica y, si dispone de ellos, su número de teléfono, su número de fax y su dirección de correo electrónico.
(3). Si usted ofrece al consumidor en su sitio web la opción de cumplimentar y enviar electrónicamente información relativa a su desistimiento del contrato, insértese el texto siguiente: «Tiene usted asimismo la opción de cumplimentar y enviar electrónicamente el modelo de formulario de desistimiento o cualquier otra declaración inequívoca a través de nuestro sitio web [insértese la dirección electrónica]. Si recurre a esa opción, le comunicaremos sin demora en un soporte duradero (por ejemplo, por correo electrónico) la recepción de dicho desistimiento.».
(4). En caso de un contrato de venta en el que usted no se haya ofrecido a recoger los bienes en caso de desistimiento, insértese la siguiente información: «Podremos retener el reembolso hasta haber recibido los bienes,

o hasta que usted haya presentado una prueba de la devolución de los bienes, según qué condición se cumpla primero.».
(5). Si el consumidor ha recibido bienes objeto del contrato insértese el texto siguiente:
(a) insértese:
— «Recogeremos los bienes.», o bien
— «Deberá usted devolver o entregar los bienes a nosotros mismos o a… [Insértese el nombre y la dirección geográfica, si procede, de la persona autorizada por usted a recibir los bienes], sin ninguna demora indebida y, en cualquier caso, a más tardar en el plazo de 14 días a partir de la fecha en que nos comunique su decisión de desistimiento del contrato. Se considerará cumplido el plazo si efectúa la devolución de los bienes antes de que haya concluido el plazo de 14 días.»;
(b) insértese:
— «Nos haremos cargo de los costes de devolución de los bienes.»;
— «Deberá usted asumir el coste directo de devolución de los bienes.»;
— En caso de que, en un contrato a distancia, usted no se ofrezca a hacerse cargo de los costes de devolución de los bienes y estos últimos, por su naturaleza, no puedan devolverse normalmente por correo: «Deberá usted asumir el coste directo de devolución de los bienes,… EUR [insértese el importe].»; o, si no se puede realizar por adelantado un cálculo razonable del coste de devolución de los bienes: «Deberá usted asumir el coste directo de devolución de los bienes. Se calcula que dicho coste se eleva a aproximadamente… EUR [insértese el importe]. como máximo.», o bien
— En caso de que, en un contrato celebrado fuera del establecimiento, los bienes, por su naturaleza, no puedan devolverse normalmente por correo y se hayan entregado ya en el domicilio del consumidor en el momento de celebrarse el contrato: «Recogeremos a cargo nuestro los bienes.»;
(c) «Solo será usted responsable de la disminución de valor de los bienes resultante de una manipulación distinta a la necesaria para establecer la naturaleza, las características y el funcionamiento de los bienes».
(6). En caso de un contrato para la prestación de servicios o para el suministro de agua, gas, electricidad —cuando no estén envasados para la venta en un volumen delimitado o en cantidades determinadas— o calefacción mediante sistemas urbanos, insértese lo siguiente: «Si usted ha solicitado que la prestación de servicios o el suministro de agua/gas/electricidad/calefacción mediante sistemas urbanos [suprímase lo que no proceda] dé comienzo durante el período de desistimiento, nos abonará un importe proporcional a la parte ya prestada del servicio.

Anexo I.B. Modelo de formulario de desistimiento propuesto por el Parlamento Europeo
(Solo debe cumplimentar y enviar el presente formulario si desea desistir del contrato)[478]

— A la atención de [aquí el comerciante deberá insertar el nombre del comerciante, su dirección geográfica y, si dispone de ellos, su número de fax y su dirección de correo electrónico]:
— Por la presente le comunico/comunicamos (*) que desisto de mi/desistimos de nuestro (*) contrato de venta del siguiente bien/prestación del siguiente servicio (*)
— Pedido el/recibido el (*)
— Nombre del consumidor o de los consumidores
— Dirección del consumidor o de los consumidores
— Firma del consumidor o de los consumidores (solo si el presente formulario se presenta en papel)
__ Fecha

(*) Táchese lo que no proceda.

[478] Anexo I.B de la Directiva 2011/83/UE del parlamento europeo y del consejo de 25 de octubre de 2011 sobre los derechos de los consumidores, por la que se modifican la Directiva 93/13/CEE del Consejo y la Directiva 1999/44/CE del Parlamento Europeo y del Consejo y se derogan la Directiva 85/577/CEE del Consejo y la Directiva 97/7/CE del Parlamento Europeo y del Consejo.

REFERENCIAS

A) BIBLIOGRAFÍA Y HEMEROGRAFÍA

ABA, Digital Signature Guidelines, Washington, American Bar Association, 1996, 136 pp., accesible en http://www.americanbar.org/content/dam/aba/events/science_technology/2013/dsg_tutorial.authcheckdam.pdf, consultada 3 de enero de 2015.

ACOTA ROCA, Felipe. INCOTERMS: Términos de Compra-Venta Internacional, 1ª ed., 1989, México, D.F., Ed. Ediciones Fiscales ISEF, 136 p.

ACOSTA ROMERO, Miguel y Lara Luna, Julieta Arelí. Nuevo derecho mercantil, 1. ed., 2000, México, Porrúa, 576 p.

AGUILA-REAL, Jesús Alfaro. Las condiciones generales de la contratación, 1. ed., 1991, Madrid, Ed. Civitas, 509 p.

ÁLVAREZ-CIENFUEGOS Suárez, José María: La firma y el comercio electrónico en España: Cometarios a la legislación vigente, 2000., Elcano: Aranzadi, 258 p.

ARIAS POU, María. Manual práctico de comercio electrónico, 2006, Madrid, Ed. La Ley, 1061 p.

ASOCIACIÓN Nacional de Tiendas de Autoservicio y Departamentales (ANTAD), *Comercio electrónico pone a prueba logística de empresas*, accesible en http://www.antad.net/index.php/publicaciones/antad-informa/antad-informa/item/20421-comercio-electr%C3%B3nico-pone-a-prueba-log%C3%ADstica-de-empresas, publicado el 28 Abril 2014, consultada 15 mayo 2015.

ASOCIACIÓN Nacional de Tiendas de Autoservicio y Departamentales (ANTAD), *Pagos Móviles Aumentan 46%, el doble que el Comercio Electrónico*, accesible en: http://www.antad.net/proyectoantad/index.php/publicaciones/antad-informa/antad-informa/item/25993-pagos-moviles-aumentan-46-el-doble-que-el-comercio-eectronico, 12 Diciembre 2014, consultada el 13 de febrero 2015.

ASOCIACIÓN Nacional de Tiendas de Autoservicio y Departamentales (ANTAD), *Comercio electrónico pone a prueba logística de empresas,* accesible en: http://www.antad.net/index.php/publicaciones/antad-informa/antad-informa/item/20421-comercio-electr%C3%B3nico-pone-a-prueba-log%C3%ADstica-de-empresas, publicación del 28 Abril 2014, consultada 15 mayo 2015.

ASOCIACIÓN Nacional de Tiendas de Autoservicio y Departamentales (ANTAD), Pagos Móviles Aumentan 46%, el doble que el Comercio Electrónico", accesible en: http://www.antad.net/proyectoantad/index.php/publicaciones/antad-informa/antad-informa/item/25993-pagos-moviles-aumentan-46-el-doble-que-el-comercio-eectronico, publicación del 12 Diciembre 2014, consultada el 13 de febrero 2015.

A.T. KEARNEY and The Chicago Council on Global Affairs, *2012 Global Cities Index and Emerging Market Outlook Study*, accesible en http://www.atkearney.com.au/research-studies/global-cities-index/2012, consultada el 3 de Abril de 2015, p. 12.

ATREYA, PAINE, BURNETT, HAMMOND, STARRETT y WU, Digital Signatures. 2002, McGraw-Hill, Osborne, p. 368.

BAKER y Hurst. *The limits of trust: Cryptography, Governments and Electrónic Commerce,* 1998, The Hague, Kluwer Law International, p. 621.

BALTIERRA GUERRERO, Alfredo. *La firma autógrafa en el derecho bancario*, Revista de la Facultad de Derecho de México, UNAM, Núm. 121-122-123, Enero - Junio, 1982, p. 17 - 48.

BANTIN, Philip C. *Developing a strategy for managing electronic records*, in The American Archivist, Vol. 61, No. 2 (Fall, 1998), pp. 328-364.

BASTIDAS, Ma. Teresa; Novoa, Jorge y Pérez, Alfonso (c*oord.). La firma y la factura electrónicas: Entorno jurídico, fiscal e informático,* Ed. Instituto Mexicano de Contadores Públicos (IMCP), 2004, México D.F., 295 p.

BAYER, Dave HABER Stuart, STORNETTA, W. Scott. *Improving the Efficiency and Reliability of Digital Time-Stamping,* en CAPOCELLI, Renato, DE SANTIS, Alfredo y VACCARO, Ugo, Sequences II: Methods in Communication, Security, and Computer Science, 1993, Springer New York, pp 329-334

BEARMAN, David. *Archival Principles and the Electronic Office, Information Handling in Offices and Archives,* 1993, New York, Ed. K.G.Saur, p. 177-193; reprinted in #92 http://www.archimuse.com/publishing/electronic_evidence/ElectronicEvidence.Ch5.pdf.

BECERRA, Ricardo, *Internet llega a la Constitución: el derecho de acceso a la información y los sistemas electrónicos,* en Pedro Salazar Ugarte (coord.) El derecho de acceso a la información en la Constitución mexicana: razones, significados y consecuencias, México, UNAM / IFAI, 2008, pp. 71-88.

BERGER, Klaus Peter. *The Concept of the "Creeping Codification" of Transnational Commercial Law,* 2009, Center for Transnational Law (CENTRAL), University of Cologne, Germany, accesible en http://www.trans-lex.org/000004#Footnote-Inline-931c95115ba531dd2c3b935c6c262159, consultado el 25 de enero de 2015.

BLACK'S LAW DICTIONARY, 9. ed., St. Paul, Minnesota West, 2009, XXXI, 1920 p.

BLANCHETTE Jean-François. *The digital signature dilemma,* Annales Des Télécommunications, August 2006, Volume 61, Issue 7-8, pp 908-923

BORJA SORIANO, Manuel. Teoría general de las obligaciones, 2001, México, Porrúa, p. 732 p.

BOURDIEU, Pierre. La fuerza del Derecho, 2005, Bogotá, Colombia, Ed. Universidad de los Andes, 220 p.

BRAID, Matthew. Collecting Electronic Evidence After a System Compromise, Computer Emergency Response Team (CERT) in Australia (AusCERT) 2001, accesible en http://www.auscert.org.au/Information/Auscert_info/Papers/Collecting_Evidence_After_A_System_Compromise.html, 13 p., consultada 1 de noviembre de 2014.

CALLOWAY, Jim. What is electronic evidence, in Family Advocate, Vol. 28, No. 3, winter 2006, pp. 8-9.

CARBONELL, Miguel. *Notas sobre la Regulación Constitucional de los Medios Electrónicos de Comunicación,* en *Boletín Mexicano de Derecho Comparado,* número 104, Mayo - Agosto 2002, Nueva Serie Año XXXV, conferencia impartida en la ciudad de Morelia, Michoacán, dentro del Seminario Nacional de Responsabilidad, Autorregulación y Legislación en Radio y Televisión, el 17 de julio de 2001; accesible en http://biblio.juridicas.unam.mx/revista/DerechoComparado/numero/104/abs/abs1.htm, consultada 1 mayo de 2015.

CARRASCOSA, Valentín, Pozo; Ma. A., Rodríguez, E.P. 1999. La Contratación Informática: el Nuevo Horizonte Contractual. Los Contratos Electrónicos e Informáticos. Granada: Segunda Edición, Editorial Comares, p. 15.

CASADOS BORDE, Alfonso Jesús. El Derecho Comercial y la Búsqueda de una Teoría Jurídica Global, en Revista del Posgrado en Derecho de la UNAM, Nueva época, núm. 2, julio-diciembre 2015, 30 p.

CASADOS BORDE, Alfonso Jesús. La jurisdicción mercantil y la globalización comercial. Derecho y Ciencias Sociales, Octubre 2015, No. 13, pp. 40-70, Instituto de Cultura Jurídica y Maestría en Sociología Jurídica. FCJ y S. UNLP.

CASADOS BORDE, Alfonso Jesús. El Contractualismo Mercantil como fuente de la Globalización, en Godínez Méndez, Wendy A. y García Peña, José Heriberto. *Derecho Económico y Comercio*

Exterior. 40 Años de Vida Académica: Homensaje al Doctor Jorge Witker. 1ª ed., 2015, Serie Doctrina Jurídica núm. 732, Ed. Instituto de Investigación Jurídicas de la UNAM, p. 231-259.

CASEY, Eoghan. Digital evidence and computer crime, 2a ed., 2004, Londres, Inglaterra, Academic Press, 690 p.

CASTRILLÓN Y LUNA, Víctor M. Contratos mercantiles, 2011,México, Porrúa, 603 p.

CONSTANTINESCO, Leontin-Jean. Tratado de Derecho Comparado, Introducción al Derecho Comparado, vol. I, 1981, Madrid, Ed. Tecnos., trad. de E. Freitas da Costa, 360 p.

COWEN, David. Computer Forensics InfoSec Pro Guide, 2013, McGraw-Hill, 512 p.

CUADRADO Pérez, Carlos. Oferta, aceptación y conclusión del contrato. Bolonia, Publicaciones del Real Colegio de España, 2003, 395 p.

DAVARA RODRÍGUEZ, Miguel Ángel: Manual de derecho informático, 2008, 10. ed., Cizur Menor (Navarra) : Thomson Aranzadi, 528 p.

DE BUEN LOZANO, Néstor. La decadencia del contrato, 1965, México, 309 p.

DE MIGUEL ASENSIO, Pedro Alberto. Derecho Privado de Internet, 2ª ed., 2001, Civitas, Madrid, 583 p.

DEVOTO, Mauricio. Comercio Electrónico y Firma Digital: La Regulación del Ciberespacio y las Estrategias Globales, 1ª Ed., 2001, Ed. La Ley-Fondo Editorial de Derecho y Economía, Buenos Aires-Argentina, 503 p.

DÍAZ BRAVO, Arturo. Contratos mercantiles, 2012, México, De Iure, p. 253.

DIFFIE, Whitfield y HELLMAN, Martin E. "New Directions in Cryptography," IEEE Trans. on Info. Theory, Vol. IT-22, Nov. 1976, pp. 644-654 (Invited Paper).

DUMORTIER, J., KELM, S., NILSSON, H., SKOUMA, G., VAN EECKE, P., "The Legal and Market Aspects of Electronic Signatures", Datenschutz und Datensichering, 2004, n° 3, p. 141-146.

DUMORTIER, Jos, VAN DEN EYNDE, Sofie, *Electronic signatures and trusted archival services,* in *Proceedings of the DLMForum 2002, Barcelona 6-8 May 2002*, Luxembourg, Office for Official Publications of the European Communities, 2002, p. 520-524, accesible en http://www.law.kuleuven.ac.be/icri, consultada 1 de noviembre de 2014.

DURANTI, L., et al., *Strategy Task Force Report, in The Long-term Preservation of Authentic Electronic Records*, Vancouver, InterPARES, 2002, accesible en http://www.interpares.org/ip2/display_file.cfm?doc=ip2_book_bibliography.pdf, consultada 1 de noviembre de 2014.

EASTERBROOK, Frank H. *Cyberspace and the Law of the Horse,* 1996 University of Chicago Legal Forum 207, p. 207- 216

ELECTRONIC Exchange of Social Security Information (EESSI) European Electronic Signature Standardisation Initiative, accessible en http://ec.europa.eu/idabc/en/document/7189/5637.html, consultada el 3 de mayo de 2014.

ELECTRONIC Signature in Global and National Commerce Act (E-Sign), enacted by President Clinton in 2000, accesible en https://www.fdic.gov/regulations/compliance/manual/pdf/X-3.1.pdf, consultada 1 de noviembre de 2014.

EUROPEAN Electronic Signature Standardisation Initiative (EESSI) Expert Team Final report, June 2003, accesible en http://www.ict.etsi.org/Working_Groups/EESSI/Index.htm, consultada 13 de noviembre de 2014.

FEDERAL JUDICIAL CENTER. The manual for complex litigation, USA, 4ª ed., 2004, 798 p.

FERNÁNDEZ GÓMEZ, Eva. Comercio electrónico. Madrid: McGraw-Hill/Interamericana de España, S.A.U, 2006.

FLECHTNER, Harry M., Convención de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías, 2010, United Nations Audiovisual Library of International Law, pp. 1-4, accesible en: www.un.org/law/avl, consultada el 14 de diciembre de 2014.

FORD, WARWICK AND BAUM, Michael S.: Secure Electronic Commerce: Building the infrastructure for digital signatures and encryption, 1997, Upper Saddle River, NJ: Prentice Hall PTR, 470 p.

GAMBOA Montejano, Claudia. Derecho Financiero Mexicano: Estudio teórico conceptual, antecedentes, derecho comparado y opiniones especializadas (1ª parte), 2009, México, Centro de Documentación, Información y Análisis de la Cámara de Diputados, LXI Legislatura, 133 p.

GARCÍA MÁS, Francisco Javier. Comercio y firma electrónicos. Análisis sociedad de la información. 2. ª ed. Valladolid: Edit. Lex Nova, 2004, 580 p.

GARCÍA SAIS, Fernando, Derecho de los consumidores a la información. Una aproximación a la publicidad engañosa en México, Ed. Porrúa-ITAM, México, 2007, 138 p.

GARTNER Group Inc. *Research Methodologies: Gartner Hype Cycle*, accesible en http://www.gartner.com/technology/research/methodologies/hype-cycle.jsp, consultada 6 mayo de 2015

GARTNER Publications. Hype Cycle for E-Commerce 2013, 31 de julio 2013, Stamford, descarga accesible con membresía: https://www.gartner.com/doc/2571916/hype-cycle-ecommerce-f.

GARZÓN VALDÉS, Ernesto. Entre lo íntimo, lo privado y lo público, Cuadernillo no. 06 de la Colección de Transparencia, 2015, México, Ed. IFAI, 45 p., accesible en http://inicio.ifai.org.mx/Publicaciones/Cuadernillo%2006%20B.pdf, consultado el 3 de mayo de 2015.

GÓMEZ DÍEZ, José Luis. El título valor electrónico: especial referencia a la letra de cambio electrónica y la actuación notarial, 2009, Mallorca, en Títulos valores electrónicos, Dirección General de Investigación del Ministerio de Educación y Ciencia Española, p. 101-107.

GÓMEZ VIEITES, Álvaro y VELOSO ESPIÑEIRA, Manuel. Economía digital y comercio electrónico. Santiago de Compostela; Ed. Escuela de Negocios Caixa Nova-Tórculo, 280 p.

GONZÁLEZ DE COSSIO, Francisco,(2004) Arbitraje, edit. Porrúa, México, p 3-4.

GONZÁLEZ OROPEZA, Manuel. Conceptualización Histórica de la terminológica legislativa, Soberanes Fernández, José Luis (coord.), en Memoria del III Congreso de Historia del Derecho Mexicano (1983), 1984, México, Ed. UNAM, 319-348 p.

GUISADO MORENO, Ángela. Formación y perfección del contrato en Internet. Madrid: Marcial Pons, Ediciones jurídicas y Sociales, S. A., 2004, p. 223 p.

GUTIÉRREZ Y GONZÁLEZ, Ernesto. Derecho de las obligaciones, 14ª ed., 2002, México, Ed. Porrúa, 1284 p.

HART, Jonathan D.: *Internet law: A field guide,* 5a ed., Washington, D.C., BNA Books, 2007. - XXVII, 831 p.

HERNÁNDEZ GIL, Antonio. Metodología de la ciencia del Derecho, Tomo V, 1987, Madrid, España, Ed. Espasa-Calpe, 700 p.

HESS Araya, Christian. 2001. "Inteligencia artificial y Derecho", Revista Electrónica de Derecho Informático. N° 39. Ed. Vlex, accesible en http://vlex.com/redi, consultada 6 mayo de 2015

IETF, S/MIME Version 3 Message Specification, Network Working Group , B. Ramsdell, Editor, Request for Comments: RFC 3851, Obsoletes: RFC 2633, Category: Standards Track , Internet Engineering Task Force, July 2004, 36 p.

ILLESCAS ORTÍZ, Rafael: *Derecho de la contratación electrónica*, 2009, 2. ed., Madrid, Civitas Thomson Reuters (Estudios y comentarios), 367 p.

INTERNET Law & Policy Forum (ILPF), An Analysis of International Electronic and Digital Signature Implementation Initiatives, September 2000, 48 p., accesible en: http://www.ilpf.org/groups/index.htm#jurisdiction, consultada 1 de noviembre de 2014.

IPSEN, Nils Christian. Private Normenordnungen als Transnationales Recht? Ed. Duncker & Humblot, 2009, Berlín, 269 p.

JIMÉNEZ GÓMEZ, Juan Ricardo. El principio de la buena fe en la teoría general del contrato, en Un Siglo de Derecho Civil Mexicano. Memoria del II Coloquio Nacional de Derecho Civil Serie C, Estudios Históricos, Instituto de Investigaciones Jurídicas –UNAM, Núm. 20, 1985. 189-197.

JIMÉNEZ Paz, Aarón. Criterios y evaluación de la publicidad engañosa en la labor de la PROFECO, Seminario el derecho a la información de los consumidores y la publicidad responsable, IIJ-UNAM-PROFECO, 16 y 17 de mayo de 2012, accesible en: http://www.consumidor.gob.mx/wordpress/wp-content/uploads/2012/05/presentacionAaronJimenez.pdf, consultada 3 enero de 2015.

LABARIEGA VILLANUEVA, Pedro Alfonso. "La moderna *Lex Mercatoria* y el comercio internacional" en Revista de Derecho Privado Núm. 26, 1998, Instituto de Investigaciones Jurídicas de la UNAM, p.43-56.

LABORDE, Carolina M.: Electronic signatures in International Contracts, 2010, Frankfurt, Ed. Lang, European University Studies: Series II, law, 247 p.

LESSIG, Lawrence. el código y otras leyes del ciberespacio, 1ª ed., 2001, Madrid-España, ed. Taurus-digital, trad. del inglés por Ernesto Alberola, 1ª ed., 1999), 540 p.

LIBRARY and Archives Canada (LAC), Guidelines For Records Created Under a Public Key Infrastructure Using Encryption and Digital Signatures, Ottawa, Library and Archives Canada, 2001, accesible en: http://www.collectionscanada.ca, consultada 1 de noviembre de 2014.

LÓPEZ-AYLLÓN, Sergio (coord.). Democracia, Transparencia y Constitución: Propuestas para un debate necesario, 1ª ed., 2006, México, Ed. UNAM-IFAI, 262 p.

LORENZETTI, Ricardo L. Comercio electrónico: documento, firma digital, contratos, daños, defensa del consumidor, 1ª ed., 2001, ed. Abeledo-Perrot, Buenos Aires-Argentina, 330 p.

LYNCH, C., Canonicalization: A Fundamental Tool to Facilitate Preservation and Management of Digital Information. D-Lib Magazine, 5(9), 1999, Corporation for National Research Initiatives (CNRI), USA, accesible en http://www.dlib.org/dlib/september99/09lynch.html, consultada el 3 de diciembre de 2014.

LLANEZA GONZÁLEZ, PALOMA: E-contratos: Modelos de contratos, clausulas y condiciones generales comentadas, 2004, 1ª ed., Barcelona, Ed. Bosch, 582 p.

MALAGARRIGA, Carlos C. Tratado elemental de derecho comercial, 3ª ed., 1963, Buenos Aires, 1010 p.

MARTIN, Paul-Edouard e Instituto Español de Estudios Estratégicos, Inseguridad Cibernética en América Latina: Líneas de Reflexión para la Evaluación de riesgos, Documento de Opinión 79/2015, 24 de julio de 2015, p. 4, accesible en: http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO79-2015_InseguridadCibernetica_AmericaLatina_PaulE.Martin.pdf, consultado el 1 de agosto de 2015.

MARCUS, Richard L. Confronting the future: Coping with discovery of electronic material, Law and Contemporary Problems, Vol. 64, No. 2/3, Complex Litigation at the Millennium (Spring - Summer, 2001), Duke University School of Law pp. 253-281

MARCUS, Richard L. Confronting the future: Coping with discovery of electronic material, Law and Contemporary Problems, Vol. 64, No. 2/3, Complex Litigation at the Millennium (Spring - Summer, 2001), Duke University School of Law pp. 253-281

MARTÍN-CASALLO LÓPEZ, Juan José (Dir.). Problemática jurídica en torno al fenómeno de Internet, 1ª ed., 2000, Madrid-España, ed. consejo general del poder judicial, 205 p.

MARTÍNEZ NADAL, Apol·lònia: *Comercio electrónico, firma digital y autoridades de certificación*, 2001, 3ª ed., Madrid, Civitas, 327 p.

MARTÍNEZ, Luciana Paula y Menicocci, Alejandro Aldo, "Jurisdicción y ley aplicable en las relaciones jurídicas concluidas por Internet". Investigación y Docencia, N° 40, 67-79 pp., accesible en: http://www.centrodefilosofia.org.ar/IyD/iyd40_6.pdf, consultada el 20 octubre de 2015.

MEEHAN, S. C., BEARD, D.B. What Hath Congress Wrought: E-Sign, The UETA, and the Question of Preemption. Idaho L. Rev., 37, pp. 389-414, 2001.

MINC, Alain. www.capitalismo.net., 2001, Buenos Aires, Ed. Paidós, Colección Espacios del Saber, 231 p.

MUSITANI, Alfredo, Desmaterialización de títulos valores, 2006, Revista Argentina de Derecho Empresario, No. 5, accesible en : http://www.ijeditores.com.ar/articulos.php?idarticulo=42143&print=2, consulado el 2 de febrero de 2015.

NICOLESCU, Basarab. La transdisciplinarité. Manifeste, 1996, Ed. Du Rocher, Mónaco, Francia. (trad. del francés, Consuelo Falla Garmilla, Escuela Nacional de Trabajo Social de la UNAM). También visible en la página oficial de "International Center for Transdisciplinary Research" (CIRET), http://ciret-transdisciplinarity.org/transdisciplinarity.php

NUÑEZ, Adriana S. Comercio Electrónico: Aspectos Impositivos, Contables y Tecnológicos, 1ª Ed., 2001, Ed. La Ley-Fondo Editorial de Derecho y Economía, Buenos Aires-Argentina, 268 p.

OECD. Gateways to the Global Market: Consumers and Electronic Commerce, que es un reporte del Foro "Caminos al Mercado Global: los consumidores y el comercio electrónico" celebrado en Marzo de 1997 por el Comité de Política del Consumidor, Paris, 136 p.

OECD, Recommendation of the council concerning guidelines for cryptography Policy, de fecha 27 March 1997 - C(97)62/FINAL, accesible http://acts.oecd.org/Instruments/ShowInstrumentView.aspx?InstrumentID=115&InstrumentPID=111&Lang=en&Book= , OECD. consultado en 15 Junio de 2015.

OMINSKY, Harris .Oops! I Just Clicked My Life Away, The Legal Intelligencer, July 26, 2000.

ORGAZ, Alfredo. "Valor de la impresión digital en los documentos no firmados", en Estudios de Derecho Civil, 1948, Topográfica Editora Argentina, Buenos Aires, 352 p.

OVIEDO ALBÁN, Jorge, Convención de las Naciones Unidas sobre la utilización de comunicaciones electrónicas en contratos internacionales, en Int. Law: Rev. Colomb. Derecho Int. Bogotá, Colombia, N° 7, p. 11-59, enero-mayo de 2006.

PÉREZ CHÁVEZ, José, et al. Firma Electrónica Avanzada, Documentos Digitales y Comprobantes Electrónicos, 1a ed., 2005, Tax, México, 93 p.

PHILIP Kotler, Kevin Lane Keller (2006). Marketing Management, 14 ed., 2012, New Jersey, Prentice Hall, 812 p.

PHILLIPS, Jeremy: Butterworths e-commerce and IT law handbook / consultant ed. Jeremy Phillips, 4a ed., London: Lexis Nexis Butterworths, 2007 - XIV, 2030 p.

PINKAS, D., Electronic Signature Formats, European Electronic Signature Standardization Initiative, ETSI TS 101 733 V1.2.2.

PINOCHET Olave, Ruperto. Los sistemas informáticos expertos de toma de decisiones y la voluntad como elemento de validez del contrato electrónico, Revista Ius et Praxis v.9 n.2, p 161-184, Talca (Chile), 2003, accesible en: http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-00122003000200005&lng=es&nrm=iso, consultada el 20 enero 2015.

PINOCHET Olave, Ruperto. Los sistemas informáticos expertos de toma de decisiones y la voluntad como elemento de validez del contrato electrónico, Revista Ius et Praxis v.9 n.2, p 161-184, Talca (Chile), 2003, accesible en: http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-00122003000200005&lng=es&nrm=iso, consultada el 20 enero 2015

RADIN, Margaret J., Rothchild, John A., Reese, R. Anthony & Silverman, Gregory M.: Internet commerce: The emerging legal framework, 2006, 2ª ed., New York Foundation Press, 1266 p.

REAMS, Bernard D. (comp.) The law of E-SIGN: A legislative history of the Electronic Signature in Global and National Commerce Act, Public Law No. 106-229, 2002, volúmenes del 1 al 7, Buffalo, N.Y., William S. Hein Editorial.

REIDENBERG, Joel R. "Governing Networks and Cyberspace Rule-Makin", Emory L.J.911.928. 1996. 912-930 pp., consultada el 13 de febrero 2015.

REMOLINA ANGARITA, Nelson y PEÑA NOSSA, Lisandro. De los títulos valores y de los valores en el contexto digital. Ediciones Uniandes y editorial Temis, 2011, 377 p.

REYES KRAFFT, Alfredo Alejandro. La Firma Electrónica y Las Entidades de Certificación, 2003, 1ª ed., Porrúa, México, 259 p.

RIBAS ALEJANDRO, Javier. "Riesgo legales en Internet. Especial referencia a la protección de datos personales", en MATEU DE ROS, Rafael. y CENDOYA MÉNENDEZ DE VIGO, Juan Manuel (coords). Derecho de internet. Contratación electrónica y firma digital. Navarra: Aranzadi, S.A., 2000, 1094 p.

RIBAS ALEJANDRO, Javier. Aspectos Jurídicos Del Comercio Electrónico en Internet, 2ª Ed., 2003, Ed. Aranzadi, Navarra-España, 490 p.

ROCHA VARGAS, Marcelo Emilio, Castello, Ricardo J. y Bollo, Daniel E., Criptografía y Firma Electrónica/Digital en el Aula, Universidad Nacional de Catamarca – Secretaría de Ciencia y Tecnología, Ed. Científica Universitaria, 19 p. accesible en: http://www.editorial.unca.edu.ar/Publicacione%20on%20line/CD%20INTERACTIVOS/DUTI/PDF/EJE2/ROCHA%20VARGAS.pdf, consultado el 12 de enero de 2015.

RICO CARRILLO, M. Comercio electrónico. Internet y Derecho, 2. ª ed. Venezuela: LEGIS, 2005.

RODRÍGUEZ de las Heras Ballell, Teresa, "El régimen jurídico de los mercados electrónicos cerrados (e-Marketplaces): Contrato de Acceso (desde la perspectiva de los participantes)", en E-business de eMarket Services España, Agosto 2006, pp. 4, accesible en http://www.emarketservices.es/FicherosEstaticos/auto/0806/Libro%20Teresa-rev1-participantes_22051_.pdf, consultada el enero de 2015.

RODRÍGUEZ DE LAS HERAS BALLELL, Teresa. El régimen jurídico de mercados electrónicos cerrados (e-Marketplaces. Marcial Pons, 2006., 728 p.

ROGERS, Everett M., Diffusion of Innovations, 1983, USA, 3a ed., Ed. Macmillan Publishing, 453 p.

ROJAS SORIANO, Raúl. Guía para realizar investigaciones sociales, 2005, México, Ed. Plaza y Valdes Editores, 437 p.

ROJINA VILLEGAS, Rafael. Derecho Civil Mexicano, 4ª ed,1981, México, Porrúa.

ROJAS ULLOA, Milushka Felícitas. "La Importancia del Derecho Comparado en el Siglo XXI", en Revista On Line del Instituto de Investigación Jurídica de la Universidad de San Martín de Porres, 2009, Perú, accesible en: http://www.derecho.usmp.edu.pe/instituto/revista/articulos/Articulo_de_Investigacion_Juridica.pdf, consultada el 22 de marzo 2015, 12 p.

ROTHENBERG, J., Ensuring the Longevity of Digital Documents, 1995, Ed. Scientific American, 272, p.

SALAZAR UGARTE, Pedro y Paula S. Vásquez Sánchez, "La reforma al artículo 6o. De la Constitución mexicana: contexto normativo y alcance interpretativo", en Pedro Salazar Ugarte, coordinador, El derecho de acceso a la información en la Constitución mexicana: razones, significados y consecuencias, México, UNAM / IFAI, 2008, 200 p.

SALAZAR UGARTE, Pedro. El Derecho de acceso a la información en la Constitución Mexicana, 2008, México, Ed. UNAM-IFAI, 200 p.

SASSEN, Saskia. 2006. "The Global City: Strategic Site, New Frontier", in Managing Urban Frontiers: Sustainability and Urban Growth in Developing Countries, 2005, Ed. Marco Kainer, Martina Koll-Schretzenmayr & Willy A. Schmind. Burlington, VT, Ashgate (trad. al español: "La ciudad global: Emplazamiento estratégico, nueva frontera"), p 35-45.

SÁNCHEZ del Castillo, Vilma. La Publicidad en Internet: régimen jurídico de las comunicaciones electrónicas, 2006, Ed. La ley, España, 400 p.

SÁNCHEZ SODI, Horacio. Código de Comercio concordado y con jurisprudencias de la 7a, 8a y 9a épocas, 2006, México, Porrúa, 962 p.

SCHELLEKENS, Maurice H. M.: Electronic signatures: Authentication technology from a legal perspective, The Hague : Asser Press, 2004(Information technology & law series ; 5) 150 p.

SILVA SILVA, Jorge Alberto. Arbitraje comercial internacional en México, 2ª ed., 2001, Oxford, México D.F., 167 p.

SMEDINGHOFF, Thomas J (ed.): Online law: The SPA's legal guide to doing business on the Internet, 1996, 2ª impresión, Reading, Mass: Addison-Wesley, 544 p.

SUÁREZ Dávila, Francisco y Díaz, Juan Luis. Reestructuración del sistema financiero, 1988, 1ª ed., México, Ed. FCE-Secretaria de Hacienda y Crédito Público, 176 p.

TEUBNER, Gunther y BOURDIEU, Pierre. La fuerza del Derecho, 2005, Bogotá, Colombia, Ed. Universidad de los Andes, 220 p.

TEUBNER, Gunther. Societal Constitutionalism: Alternatives to State-Centred Constitutional Theory? Oxford, 2004, Ed. Hart Publishing, 24 p., accesible: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=876941, consultado el 2 de noviembre de 2015, consultada el 13 de febrero 2015.

THIBODEAU, K. Overview of Technological Approaches to Digital Preservation and Challenges in Coming Years, in The State of Digital Preservation: An International Perspective, Washington D.C.: Council on Library and Information Resources, 2002.

UNIFORM Electronic Transaction Act (UETA), National Conference of Commissioners for Uniform State Law (NCCUSL), 1999, accesible en http://www.ncsl.org/research/telecommunications-and-information-technology/uniform-electronic-transactions-acts.aspx, consultada el 1 de noviembre de 2014.

UNITED NATIONS Public Administration Network (UNPAN). UN e-Government Survey 2008: from e-Government to Connected Governance, December 2007, New York, 225 p., accesible en http://unpan1.un.org/intradoc/groups/public/documents/un/unpan028607.pdf, consultada el 2 de noviembre de 2014.

VAN DER VEER, Hans y WILES, Anthony. Achieving Technical Interoperability the European Telecommunications Standards Institute (ETSI) Approach, 3rd edition, Abril 2008, France, 30 p., accesible en http://www.etsi.org/WebSite/document/whitepapers/IOP%20whitepaper%20Edition%203%20final.pdf, consultada el 1 de noviembre de 2014.

VARA, Pina. Derecho Mercantil Mexicano, 2005, 30ª ed., Porrúa, México, 585 p.

VASQUEZ CALLAO, Enrique; BERROCAL COMENAREJO, Julio. Comercio electrónico. Material para Análisis. Madrid: Centro de publicaciones, Técnica, Ministerio de Fomento, 2000, 727 p.

VÁSQUEZ DEL MERCADO Cordero, Óscar. Contratos mercantiles, 14. ed., 2006, México, Porrúa, 601 p.

VILLANUEVA, Ernesto. Régimen Jurídico de las Libertades de Expresión e Información en México, IIJ-UNAM, 1998, 247 p.

VOUTSSAS M., Juan. Preservación documental digital y seguridad informática. Investing. Biblioteca online, 2010, vol.24, n.50, pp. 127-155. ISSN 0187-358X.

WANG, Faye Fangfei, Internet Jurisdiction and choice of Law, 2010, United Kingdom, Ed. Cambridge University Press, Cambridge, 13 p.

WARREN, Samuel y Brandeis, Louis. *The right to privacy*, en Harvard Law Review, Vol. 4, No. 5, Dec. 15, 1890, pp. 193-220.

WEBOPEDIA. Online dictionary and Internet search engine for information technology and computing definitions: accessible en http://www.webopedia.com, consultada 1 de noviembre de 2014.

WELLS, Thomas O. Electronic and Digital Signatures: In Search of a Standard. IT Professional, IEEE Educational Activities Department, (May-June 2000), 24-30 p.

WRIGHT, Timothy E. "An Introduction to the Field Guide for Investigating Computer Crime (Part 1)" 17 April 2000, accesible en: http://www.symantec.com/connect/articles/field-guide-part-one, consultado el 3 de octubre de 2015.

WRIGHT, Timothy E. "The Field Guide for Investigating Computer Crime: Overview of a Methodology for the Application of Computer Forensics (Part 2)" 26 May 2000, accesible en: http://www.symantec.com/connect/articles/field-guide-part-two, consultado el 3 de octubre de 2015.

WRIGHT, Timothy E. "The Field Guide for Investigating Computer Crime: Search and Seizure Basics (Part 3)" 28 July 2000, accesible en: http://www.symantec.com/connect/articles/field-guide-part-three, consultado el 3 de octubre de 2015.

WRIGHT, Timothy E. "The Field Guide for Investigating Computer Crime : Search and Seizure Planning (Part 4)" 1 September 2000, accesible en: http://www.symantec.com/connect/articles/field-guide-part-four, consultado el 3 de octubre de 2015.

WRIGHT, Timothy E. "The Field Guide for Investigating Computer Crime: Search and Seizure Approach, Documentation, and Location (Part 5)" 10 November 2000, accesible en: http://www.symantec.com/connect/articles/field-guide-part-five, consultado el 3 de octubre de 2015.

WRIGHT, Timothy E. "The Field Guide for Investigating Computer Crime, Part 6: Search and Seizure - Evidence Retrieval and Processing" 8 January 2000, accesible en: http://www.symantec.com/connect/articles/field-guide-part-six, consultado el 3 de octubre de 2015.

WRIGHT, Timothy E. "The Field Guide for Investigating Computer Crime, Part 7: Information Discovery Basics and Planning" 26 February 2001, accesible en: http://www.symantec.com/connect/articles/field-guide-part-seven, consultado el 3 de octubre de 2015.

WRIGHT, Timothy E. "The Field Guide for Investigating Computer Crime, Part 8: Information Discovery - Searching and Processing" 21 March 2001, accesible en: http://www.symantec.com/connect/articles/field-guide-part-eight, consultado el 3 de octubre de 2015.

B) LEGISGRAFÍA E INFORMES

ACUERDO de la Comisión de Administración del Consejo de la Judicatura Federal, que establece el procedimiento de asignación, certificación y uso de la Firma Electrónica para el Seguimiento de Expedientes (FESE), publicado en el DOF el 3 de julio de 2007.

ACUERDO General 34/2014 del Pleno del Consejo de la Judicatura Federal, que regula la firma electrónica certificada del Poder Judicial de la Federación (FIREL) emitida por el propio Consejo, publicado en el DOF el 13 de octubre de 2014.

ACUERDO General conjunto número 1/2013, de la Suprema Corte de Justicia de la Nación, del Tribunal Electoral del Poder Judicial de la Federación y del Consejo de la Judicatura Federal, relativo a la Firma Electrónica Certificada del Poder Judicial de la Federación (FIREL) y al expediente electrónico, emitido el 4 de julio de 2014.

ACUERDO por el que se establece el Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal del 6 de septiembre de 2011, 6 p.

AGENCIA de los Derechos Fundamentales de la Unión Europea, Manual de legislación europea de la protección de datos, Consejo de Europa, 2014, Bélgica, 222 p., accesible en

http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-es.pdfhttp://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-es.pdf

AMIPCI. Estudio de Comercio Electrónico en México 2015, 10ª versión, México, D.F., 46 diapositivas, accesible en: https://amipci.org.mx/estudios/comercio_electronico/Estudio_de_Comercio_Electronico_AMIPCI_2015_version_publica.pdf, consultada el 2 de diciembre de 2015.

ANTEPROYECTO NORMA OFICIAL MEXICANA NOM-151-SCFI-2002, Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos, accesible en: http://www.cofemersimir.gob.mx/expedientes/18066, consultado el 2 de enero de 2016.

CIRCULAR ÚNICA DE BANCOS, Disposiciones de carácter general aplicables a las instituciones de crédito, publicada en el DOF el 02 de diciembre de 2005, accesible en: http://www.cnbv.gob.mx/Paginas/NORMATIVIDAD.aspx, consultado el 2 de marzo de 2015.

CIRCULAR ÚNICA DE SEGUROS Y FIANZAS, publicada en el DOF, el 19 de diciembre de 2014, SHCP y CNSF, accesible a partir de la segunda sección en: http://www.dof.gob.mx/index.php?year=2014&month=12&day=19

CIRCULAR MODIFICATORIA 3/15 de la Única de Seguros y Fianzas, publicada en el DOF el 03/07/2015, SHCP y CNSF, accesible en: http://www.cnsf.gob.mx/Normativa/CUSF_2014/CIRCULAR%20%C3%9Anica%20de%20Seguros%20y%20Fianzas.pdf

CNUDMI, Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónicas, Naciones Unidas, Viena, Marzo 2009, 120 p.

CNUDMI, Ley Modelo de la CNUDMI sobre Comercio Electrónico 1996 y su Guía para la incorporación de la Ley al derecho interno, Naciones Unidas, Nueva York, 1997, 91 p.

CNUDMI, Ley Modelo de la CNUDMI sobre Firma Electrónica 2001 y su Guía para la incorporación de la Ley al derecho interno, Naciones Unidas, Nueva York, 2002, 91 p.

CNUDMI, Guía de la CNUDMI: Datos básicos y funciones de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, Naciones Unidas, Viena, 2013, 63

COMISIÓN Intersecretarial para el Desarrollo del Gobierno Electrónico (CIDGE), "Instrumentación de la Ley de Firma Electrónica Avanzada", Junio 2015, accesible en: http://cidge.gob.mx/menu/ejes-de-trabajo/digitalizacion-del-gobierno/gobierno-sin-papel/firma-electronica-avanzada/instrumentacion-ley-de-firma-electronica-avanzada/, consultada el 4 julio de 2015.

CONVENCIÓN de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales (CNUUCECI), Nueva York, 2005, 111 p.

CONVENCIÓN de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías de 11 de abril de 1980, más habitualmente conocida como Convención de Viena de 1980 o por sus acrónimos español (CNUCCIM) o inglés (CISG), 45 p.

DECRETO del 29 de mayo de 2000 por el que se reforman y adicionan los siguientes instrumentos jurídicos nacionales: CCiF, Código Federal de Procedimientos Civiles, Código de Comercio y la Ley Federal de Protección al Consumidor, SECOFI, 7 p.

DECRETO 3960 del 25 de octubre 2010 del Ministerio de Hacienda y Crédito Público, por el cual se establece el "Libro 14: Normas aplicables a los depósitos centralizados de valores", 11 p.

DECRETO por el que se reforman y adicionan diversas disposiciones del Código de Comercio y del Código Penal Federal, documento de la Comisión de Comercio y Fomento Industrial de la Cámara de Senadores, publicado el 4 de noviembre de 2015, accesible en: http://sil.gobernacion.gob.mx/Archivos/Documentos/2016/03/asun_3342045_20160303_1456849421.pdf, fecha de consulta: 31 de noviembre de 2015.

DECRETO por el que se reforman y adicionan diversas disposiciones de la Ley General de Sociedades Mercantiles, publicado en el DOF el 14 de marzo de 2016, accesible en:http://dof.gob.mx/nota_detalle.php?codigo=5429707&fecha=14/03/2016, consultado el 14 de marzo de 2016.

DIRECTIVA 1999/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999 por la que se establece un marco comunitario para la firma electrónica, Diario Oficial de las Comunidades Europeas 19. 1. 2000.

DIRECTIVA 2000/31/CE del Parlamento Europeo y del Consejo de 8 de junio de 2000 relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico), Diario Oficial n° L 178 de 17-VII-2000, 16 p.

DIRECTIVA 2011/83/UE del parlamento europeo y del consejo de 25 de octubre de 2011 sobre los derechos de los consumidores, por la que se modifican la Directiva 93/13/CEE del Consejo y la Directiva 1999/44/CE del Parlamento Europeo y del Consejo y se derogan la Directiva 85/577/CEE del Consejo y la Directiva 97/7/CE del Parlamento Europeo y del Consejo, 25 p.

DIRECTRICES de la OCDE para la Protección de los Consumidores de Prácticas Comerciales Transfronterizas Fraudulentas y Engañosas, edición en Español © 2004 por la Procuraduría Federal del Consumidor (Profeco), México, 22 p.

DIRECTRICES de la OCDE para la Seguridad de Sistemas y Redes de Información: hacia una cultura de Seguridad se adoptaron como Recomendación del Consejo de la OCDE en su sesión 1037 de 25 de julio de 2002), 12 p.

GOBIERNO Federal de la República Mexicana, Estrategia Digital Nacional, Coordinación de Estrategia Digital Nacional, noviembre de 2013, 43 p.

INICIATIVA CON PROYECTO de decreto por el que se reforman y adicionan diversas disposiciones de la Ley Federal de Protección al Consumidor, JUEVES 15 DE OCTUBRE DE 2015, GACETA: LXIII/1PPO-31/58463, accesible en http://www.senado.gob.mx/sgsp/gaceta/63/1/2015-10-15-1/assets/documentos/Iniciativa_PRI_PROFECO.pdf , consultada el 8 de diciembre de 2015.

ICC GUIDE FOR ECONTRACTING, Cámara de Comercio Internacional (CCI), accesible en http://iccwbo.org/, consultado el 3 de mayo de 2015.

ICC eTERMS 2004, Cámara de Comercio Internacional (CCI), accesible en http://iccwbo.org/, consultado el 3 de mayo de 2015.

LEY del Estado de Utah sobre Firma Digital (Utah Digital Signature Act), de 27 de febrero de 1995 modificada en 1996, publicada en octubre de 1995 por The American Bar Association's Information Security Committee (Comité de la ABA Science and Technology).

LINEAMIENTOS para la creación y uso de Sistemas Automatizados de Gestión y Control de Documentos, expedido por la Archivo General de la Nación y publicado en el DOF el 3 de julio de 2015.

LINEAMIENTOS para el Uso de los Medios de Identificación Electrónica-Anexo 39.1.4, SHCP y CNSF, accesible en: http://www.cnsf.gob.mx/Normativa/CUSF/ANEXOS%20T%C3%8DTULO%2039/ANEXO%2039.1.4.pdf

LINEAMIENTOS para la operación, funcionalidad, comunicación y seguridad de los sistemas automatizados de control de gestión, expedido por la SFP y la SHCP, publicado en el DOF el 24 abril de 2006.

NACIONES UNIDAS, Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales de 2005, Naciones Unidas, Nueva York, 2007, 124 p.

NORMA MEXICANA: NMX-I-289-NYCE-2013: Tecnologías de la Información – Metodología de Análisis

Forense de Datos y Guías de Ejecución Information Technology- Forensic Methodology Data Analysis and Implementation Guidelines

NORMA MEXICANA: NMX-I-291–NYCE-2013: Tecnologías de la Información – Digitalización Documental con Valor Agregado Information Technology- Added Value Document Digitizing

NORMA OFICIAL MEXICANA NOM-151-SCFI-2002: "Prácticas comerciales: Requisitos que deben observarse para la conservación de mensajes de datos".

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS y SYMANTEC. Tendencias en la seguridad cibernética en América Latina y el Caribe (Latin American and Caribbean Cybersecurity Trends), informe de la XLIV Asamblea General del organismo, Washington, D.C., accesible en: https://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf, consultado el 1 de diciembre de 2014, 96 p.

RESOLUCIÓN de fecha 13 de julio de 2011 suscrita por la Cuarta Sala Regional Metropolitana del Tribunal Federal de Justicia Fiscal y Administrativa en el expediente número: 12598/06-17-04-6 promovido por Banco Santander Serfin, S.A., Institución de Banca Múltiple, Grupo Financiero Santander Serfin, que demanda la nulidad de la Norma Oficial Mexicana NOM-151-SCFI-2002: "Prácticas comerciales: Requisitos que deben observarse para la conservación de mensajes de datos", expedida por la Secretaría de Economía

RECOMENDACIÓN de la Unión Internacional de Telecomunicaciones UIT-T.X.810 (1995 s).

RECOMENDACIÓN del Consejo de la OCDE relativa a los lineamientos para la protección al consumidor en el contexto del comercio electrónico, 9 December 1999, *trad.* al español del inglés: OECD Guidelines for Consumer Protection in the Context of Electronic Commerce, Secretaría de Comercio y Fomento Industrial-Procuraduría Federal del Consumidor, México, 10 p.

RECOMENDATION of the OECD Council Concerning Guidelines for Consumer Protection in the context of Electronic Commerce (Recomendación del Consejo de la OCDE relativa a los Lineamientos para la Protección al Consumidor en el contexto del Comercio Electrónico), 9 de diciembre de 1999, traducción al español de la Secretaría de Comercio y Fomento Industrial y la Procuraduría Federal del Consumidor, 10 p.

RESUMEN de las Directrices de la OECD sobre protección de la privacidad y flujos transfronterizos de datos personales de1980 ("directrices de privacidad"), © OCDE, 2002, 12 p.

SAT, La Evolución de la Firma Electrónica, en Nuevos servicios digitales del SAT, Diapositivas de la Expo feria 2015, 16 de Diciembre de 2015, World Trade Center, Ciudad de México, accesible en: http://www.sat.gob.mx/innovacionestecnologicas/Paginas/a/documentos/EvolucionFirmaElectronica.pptx, consultado el 17 de diciembre de 2015.

SECRETARÍA DE ECONOMÍA, Documento informativo relativo a APEC, México, 4 p., accesible en: http://www.economia.gob.mx/files/Documento_Informativo_APEC.pdf, consultado el 1 de enero de 2015.

SECRETARIADO DE APEC, Marco de Privacidad del Foro de Cooperación Económica Asia-Pacífico, 2005, Singapur, traducción al español por la Secretaría de Economía, 39 p., accesible en https://www.sellosdeconfianza.org.mx/docs/marco_de_privacidad_APEC.pdf, consultado el 1 de febrero de 2015.

UTAH Digital Signature Act, Utah Code Ann. 46-3-101 to 602 (2004).