



**UNIVERSIDAD NACIONAL
AUTÓNOMA DE MÉXICO**



**FACULTAD DE ESTUDIOS SUPERIORES
ACATLAN**

NATURALEZA JURÍDICA DE LA ENTIDAD CERTIFICADORA

TESIS

QUE PARA OBTENER EL TITULO DE

LICENCIADO EN DERECHO

PRESENTA

PERLA IVONNE MORENO RUIZ



**ASESOR: LIC. MARIA DEL CARMEN GUADALUPE MELESIO
GONZALEZ**

OCTUBRE 2005

m348918

A mi Abuelita
Concepción Estrada López
*Sigues viva, en mis recuerdos y
en ese lugar en que nos esperas y desde donde cuidas
de nosotros, sé que hubieras deseado ver concluido
este trabajo. A ti más que a nadie dedico esta tesis
Te extraño*

A mi papá
Ramón Moreno Cano
*Por su inmenso cariño y apoyo, por creer en
mi y hacer posibles mis sueños, por inculcarme
el amor a la vida, el respeto a mis semejantes,
y el aprecio por el trabajo honesto y dedicado.
Con todo mi cariño,*

A mi mamá
Teresa Ruiz Estrada
*Por quererme a pesar de todo, por aguantar
mis malos genios y caras, por darme el
maravilloso regalo de la vida, por enseñarme
a no dejarme vencer por la adversidad, a pesar de
lo granda que parezca, por todo tu amor
incondicional y desmedido.
Te quiero mucho*

A mi Lulú
María de Lourdes Moreno Ruiz
*Las palabras no alcanzan para expresar
mi inmenso amor por ti y mi profundo
agradecimiento; mucho de lo que soy, te lo debo a ti.
A uno de los seres mas nobles y buenos de mi vida*

A mi Normita
Norma Moreno Ruiz
*Por todo tu sacrificio constante, tú profundo
amor y constante preocupación por nuestro bienestar
y felicidad, por enseñarme a tener fe.
Un pequeño homenaje a ese gran ser humano que eres*

A mi Tere
Ana Teresa Moreno Ruiz
*Flaquita, gracias por quererme tanto,
Por tantas horas de tu vida dedicadas a hacer de
mi un ser humano bueno y feliz, eres una luz en
mi vida.
Te quiero mucho*

A Monchito
Ramón Moreno Ruiz
*Gracias hermano por quererme tanto,
por hacerme reír tantas veces, por todos
los buenos ratos
Te quiero mon*

A mi sensei
Jesús Moreno Ruiz
*Hermano, se que las palabras no son
necesarias para que sepas todo lo que te quiero
y admiro, gracias por todo tu cariño y apoyo y
por enseñarme a creer en mi misma
Con cariño a mi sensei*

Al señor Spook
José Manuel Moreno Ruiz
*Gracias por todos los buenos ratos y
tiempo compartido a mi lado, por tu
apoyo y cariño Por ser tú.
Te quiero mucho pepe*

A mis sobrinitos.
Braulio (*mi mejor amigo y compañero*)
Abril (*mi princesa y mi orgullo*)
Anita (*la alegría de todas partes*)
Manuel (*mi niño precisos*)
Diego (*el hombre araña*)
Anuar (*con cariño*)
Carlitos (*mi chino del alma*)
y Tere (*niña de mis ojos*)
*Siempre desee tener hermanos pequeños,
Dios me los concedió en unos seres maravillosos
que vinieron a alegrar y llenar de esperanza mi vida.
Los quiero mucho enanos*

A mis abuelitos
Porfirio Cano Raya
Jesús Moreno Zapien
*Por darme un papá maravilloso
por su gran esfuerzo y ejemplo
Con respeto y carino*

A mis cuñados y cuñadas.
Alex, Fabián, Marcela, Beti y Laura
*A los que he llegado a querer como mi
familia, con mucho cariño*

A mis amigos y seres queridos:

**Alex, Eiko, Eric, Fabiola, Flor, Giselle,
Hugo Roberto, Isaac, Ismene, Israel, Itzel,
Juan Guillermo, Laura, Lizet, Luis,
Manta (Griselda), Maribel, Miriam (Sarmiento y Necha),
Pascual (Eduardo), Pati, Pilar, Rafael, Tokko y Victor.**

Y todos los demás...

*Un pequeño homenaje por todo su apoyo
y cariño en las buenas y en las malas, por hacer
de esta vida un mejor lugar para recorrer,
a todos ustedes mi mas grande amor y gratitud.
Gracias por estar ahí, los quiero mucho.*

A mi asesora

Lic. Maria del Carmen Guadalupe Melesio González

Como profesora y ser humano un ser excepcional.

Sin Usted esto no hubiera sido posible,

*Gracias! Mil gracias! mi eterno agradecimiento
y cariño hacia Usted*

**A mi honorable Sínodo
Lic. Gerardo Goyenechea Godinez
Lic. Javier Sifuentes Solis
Lic. Jorge Morales Camacho
Lic. Juan José López Tapia
Con respeto y admiración**

INDICE

NATURALEZA JURÍDICA DE LA ENTIDAD DE CERTIFICADORA

INTRODUCCIÓN.....	6
-------------------	---

CAPITULO PRIMERO. COMERCIO ELECTRONICO

1.1. Comercio Tradicional.....	8
1.1.1. El Comercio y el nacimiento del Derecho Mercantil Moderno.....	8
1.1.2. Los Actos de Comercio.....	23
1.1.2.1. Sistemas Legales.....	23
1.1.2.2. El Acto de Comercio.....	24
1.1.2.3. Concepto.....	27
1.1.2.4. Clasificación.....	32
1.1.2.4.1. Doctrinaria.....	32
1.1.2.4.2. Legal.....	35
1.2. Comercio Electrónico.....	37
1.2.1. La Cibernetica.....	37
1.2.2. La Informática.....	39
1.2.2.1. La Computadora.....	40
1.2.2.1.1. Antecedentes Históricos.....	40
1.2.2.1.2. Las Generaciones.....	44
1.2.2.1.3. Concepto.....	52
1.2.2.1.4. Clasificación.....	53
1.2.2.1.5. Componentes.....	55
1.2.2.2. Redes.....	58
1.2.2.2.1. Antecedentes.....	58
1.2.2.2.2. Estructura de la red.....	59
1.2.2.2.3. Arquitectura de redes.....	60
1.2.2.2.4. Ejemplos de redes.....	61
1.2.2.2.4.1. Red de la Agencia de Proyectos de Investigación Avanzada (ARPANET).....	62
1.2.2.2.4.2. Computer Science Network (CSNET) Y Because It's Time Network (BITNET).....	64
1.2.2.2.4.3. USENET.....	64
1.2.2.3. El Comercio Electrónico.....	65
1.2.2.3.1. Concepto.....	66
1.2.2.3.2. Clasificación.....	67
1.2.2.3.2.1. Dependiendo de los Agentes Implicados.....	68
1.2.2.3.2.2. Por la forma de relacionarse.....	68
1.3. Derecho Informático.....	69
1.3.1. Informática Jurídica.....	72
1.3.2. Derecho de la Informática.....	74
1.3.2.1. Contratos Electrónicos.....	74

1.3.2.1.1.	El Contrato en General.....	74
1.3.2.1.2.	Requisitos de Existencia.....	77
1.3.2.1.3.	Requisitos de Validez.....	83
1.3.2.1.4.	Contratación Electrónica en Diversos Códigos Mexicanos.....	86

CAPITULO SEGUNDO. LA FIRMA ELECTRÓNICA

2.1	Los mensajes de datos o documentos electrónicos.....	90
2.2.	La Firma Autógrafa.....	95
2.2.1.	Concepto.....	98
2.2.2.	La firma en el Derecho Bancario Mexicano.....	102
2.2.3.	La firma en los títulos de crédito.....	105
2.2.4.	La firma en materia de fianzas.....	109
2.2.5.	La firma en pólizas de seguros.....	110
2.2.6.	Características de la firma.....	110
2.2.7.	Elementos de la firma.....	111
2.3.	La Firma Electrónica. Recuento Histórico.....	112
2.3.1.	La Firma Electrónica.....	117
2.3.1.1.	La Firma Electrónica Avanzada.....	119
2.3.1.1.1.	Criptografía.....	121
2.3.1.1.1.1.	Simétrica.....	123
2.3.1.1.1.2.	Asimétrica.....	124
2.3.1.1.1.2.1.	La Infraestructura de Clave Pública.....	127
2.4.	La firma Electrónica Mundialmente.....	128
2.4.1.	Estados Unidos Americanos.....	128
2.4.2.	Argentina.....	129
2.4.3.	Colombia.....	131
2.4.4.	Chile.....	132
2.4.5.	Ecuador.....	133
2.4.6.	Panamá.....	133
2.4.7.	Perú.....	135
2.4.8.	Venezuela.....	136
2.4.9.	Brasil.....	136
2.4.10.	Canadá.....	136
2.4.11.	Europa.....	137
2.4.11.1.	España.....	138
2.4.11.2.	Alemania.....	140
2.4.11.3.	Bélgica.....	141
2.4.11.4.	Dinamarca.....	141
2.4.11.5.	Finlandia.....	141
2.4.11.6.	Francia.....	142
2.4.11.7.	Irlanda.....	142
2.4.11.8.	Italia.....	142
2.4.11.9.	Luxemburgo.....	143
2.4.11.10.	Portugal.....	143
2.4.11.11.	Reino Unido.....	143

2.4.11.12. Suecia.....	144
2.4.12. Otros países.....	144
2.4.12.1. Australia.....	144
2.4.12.2. Japón.....	144
2.4.12.3. Malasia.....	144
2.4.13. Organismos Internacionales.....	144
2.4.13.1. Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNDUMI).....	144
2.4.13.2. Organización para la Cooperación y Desarrollo Económico (OCD).....	147
2.4.13.3. Organización Internacional de Normas (ISO).....	147
2.5. Aplicaciones Mercantiles de la Firma Electrónica Avanzada.....	148

CAPITULO TERCERO. FE PÚBLICA Y CERTIFICACIÓN

3.1. Fe Pública.....	150
3.1.1. Aspecto filosófico.....	150
3.1.2. Concepto Fe Pública.....	151
3.1.3. Requisitos de Fe pública.....	152
3.1.3.1. Evidencia.....	152
3.1.3.2. Objetivación.....	152
3.1.3.3. Coetaneidad o simultaneidad.....	153
3.1.4. Notas o accidentes de la Fe Pública.....	153
3.1.4.1. Exactitud.....	153
3.1.4.1.1. Natural.....	153
3.1.4.1.2. Funcional.....	154
3.1.4.2. Integridad.....	154
3.1.5. Tipos de Fe Pública.....	154
3.1.5.1. Originaria.....	154
3.1.5.2. Derivada.....	154
3.1.6. Clases de Fe Pública.....	154
3.1.6.1. Notarial.....	155
3.1.6.2. Judicial.....	155
3.1.6.3. Mercantil.....	156
3.1.6.4. Registral.....	157
3.1.6.5. Consular.....	157
3.1.6.6. Administrativa.....	158
3.1.6.7. Marítima.....	159
3.1.6.8. Registro Civil.....	159
3.1.6.9. Agraria.....	159
3.1.6.10. Legislativa.....	160
3.1.6.11. De los archivos notariales.....	160
3.2. Certificación.....	161
3.2.1. Concepto.....	161
3.2.2. Características.....	162
3.2.3. Organismos de Certificación.....	163

3.2.3.1. Ejemplos de Organismos de Certificación.....	167
3.2.3.1.1. A nivel nacional.....	167
3.2.3.1.1.1. Instituto mexicano de Normalización y Certificación.....	167
3.2.3.1.1.2. Organismo Nacional de Normalización y Certificación de la Construcción y Edificación.....	168
3.2.3.1.1.3. Asociación Nacional de Normalización y Certificación del Sector Eléctrico.....	168
3.2.3.1.1.4. Consejo para el Fomento de la Calidad de la Leche y sus derivados.....	168
3.2.3.1.2. A nivel internacional.....	169
3.2.3.1.2.1. La Comisión del CODEX Alimentarius (CAC).....	170
3.2.3.1.2.2. Organización Internacional de Normas (ISO).....	171
3.2.3.1.2.3. Comisión Electrónica Internacional.....	172
3.2.3.1.2.4. Comisión Panamericana de Normas Técnicas.....	172
3.2.4. Beneficios de la Certificación.....	173
3.3. Diferencias entre fe pública y certificación.....	174
3.4. La Existencia de la entidad certificadora en el marco del comercio electrónico como un tercero confiable, más no un dador de fe pública.....	176

CAPITULO CUARTO. ENTIDADES DE CERTIFICACIÓN

4.1. Entidades de Certificación.....	179
4.1.1. Concepto.....	179
4.1.2. Protocolos.....	180
4.1.2.1. Arbitrarios.....	181
4.1.2.2. Notariales.....	181
4.1.2.3. Autoverificables.....	181
4.1.3. El documento A/CN.9/WG.IV/WP.71 Documento de la Sesión 31ª del Grupo de Trabajo IV, en Materia de Comercio Electrónico.....	181
4.1.4. Tipos de Certificación.....	182
4.1.4.1. Identidad.....	182
4.1.4.2. Autorización o Potestad.....	183
4.1.4.3. Transaccionales.....	183
4.1.4.4. Tiempo.....	183
4.1.5. Requisitos legales para la prestación de servicios de certificación.....	183
4.1.5.1. Código de Comercio.....	184
4.1.5.2. Norma Oficial Mexicana NOM –151-SCFI-2002, Prácticas comerciales – Requisitos que deben observarse para la conservación de mensajes de datos.....	186
4.1.5.3. Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación.....	187
4.1.5.4. Reglas generales a las que deberán sujetarse los prestadores de servicios de certificación.....	189
4.1.6. Autoridades Públicas de Certificación.....	196
4.1.7. Autoridades Privadas de Certificación.....	200
4.1.8. Certificados.....	203

4.1.8.1.	Concepto.....	203
4.1.8.2.	Obligaciones de las partes.....	205
4.1.8.2.1	Obligaciones de los prestadores de servicios de certificación	206
4.1.8.2.2.	Obligaciones del Firmante	207
4.1.8.2.3.	Obligaciones de quien confía.....	208
4.1.8.3.	Administración de Certificados.....	208
4.1.8.4.	Registro de Certificados.....	209
4.1.8.5.	Declaración de Prácticas de Certificación.....	211
4.1.8.6.	Lista de Revocación de Certificados	211
4.1.8.7.	Dispositivos de Almacenamiento Digitales.....	212
4.1.8.8.	Vigencia de certificados.....	214
4.1.8.9.	Los Certificados Extranjeros.....	215
4.1.13.	La Naturaleza Jurídica de la Entidad Certificadora	216
4.1.14.	La necesidad de la prestadora de servicios de certificación basándose en el criterio de que la confianza es la variable crítica para incentivar el desarrollo del comercio electrónico.....	224
CONCLUSIONES.....		226
GLOSARIO.....		229
BIBLIOGRAFIA.....		234

**TESIS CON
FALLA DE ORIGEN**

NATURALEZA JURÍDICA DE LA ENTIDAD CERTIFICADORA

INTRODUCCIÓN

La presente tesis tiene como título “Naturaleza Jurídica de la Entidad Certificadora”, porque se plantea como objetivo desentrañar la esencia jurídica de la Entidad Certificadora de la Firma Electrónica.

La elección del dicho tema obedece a que en los últimos tiempos el desarrollo de nuevas tecnologías ha afectado a muchos campos de la vida humana, entre ellos el comercio y por proyección al Derecho Mercantil. En Agosto del 2003 se publicaron una serie de reformas al Código de Comercio Vigente en Materia de Comercio Electrónico; dichas reformas introducen nuevas instituciones y conceptos, con el propósito de que el comercio electrónico alcance un mejor y mayor desarrollo en nuestro país. Una de estas nuevas instituciones es la Entidad Certificadora (o Prestador de Servicios de Certificación), que es abordada por numerosos artículos del Código de Comercio y dada su importancia dentro del comercio electrónico, se hace necesario un estudio que desentrañe la naturaleza jurídica de esta institución auxiliar del comercio electrónico.

Para la consecución de dicho objetivo emprendemos la siguiente investigación que se conforma de cuatro capítulos; en ellos partimos desde nociones históricas y generales de comercio hasta llegar a la figura del prestador de servicios de certificación (entidad certificadora). A grandes rasgos los temas a tratar por cada capítulo son los siguientes; el primero titulado Comercio Electrónico se dedica al estudio del comercio electrónico, redes y Derecho aplicable a este nuevo medio, entre otros temas; parte de nociones generales de comercio hasta llegar al objetivo específico que es el comercio electrónico; es decir sienta las bases y los antecedentes necesarios para emprender el estudio del Prestador de Servicios de Certificación.

El segundo es más específico, se titula firma electrónica, en él se agotan los temas más relevantes relativos a la firma electrónica, y cuestiones relacionadas a éstas (mensaje de datos), que son de medular importancia para comprender a la entidad certificadora.

En tanto que el tercer capítulo lleva el título de Fe Pública y Certificación; esto con el fin de analizar las diferencias entre la actividad de certificación (a la que se enfocan los prestadores de servicios de certificación) en comparación con otro tipo de actividades con las que podría llegar a confundirse dicha función, entendiendo también con esto la estructura y el tipo de funciones que debe realizar una entidad certificadora.

Finalmente, el cuarto y último capítulo, se dedica al estudio de la Entidad Certificadora; Toca puntos técnicos y jurídicos, se tratan las funciones del prestador de servicios de certificación, su composición, los tipos de certificación, el certificado digital, entre otros temas; para finalmente llegar a desentrañar la naturaleza jurídica la entidad certificadora.

Uno de los mayores obstáculos y limitantes (pero paradójicamente un gran aliciente) de la presente tesis, es el rápido avance tecnológico de los mecanismos de seguridad electrónica y por lo tanto de los temas relativos al prestador de servicios de certificación. Ya que este factor podría hacer que durante el tiempo de tramitación, presentación y antes de su llegada ante el sínodo esta tesis; pudieran surgir nuevas teorías o reformas en materia de Entidades de Certificación que no fueran contempladas por este estudio. Por lo que esperamos la consideración del lector en dicho punto para con el presente trabajo.

CAPITULO I. COMERCIO ELECTRÓNICO

1.1 Comercio Tradicional

1.1.1. El Comercio y el nacimiento del Derecho Mercantil Moderno

¿Qué nos hace distintos de los demás animales que pueblan la tierra? Es una pregunta infinitamente antigua; una de tantas dudas que la filosofía ha tratado de resolver a lo largo de la historia humana. Algunos filósofos místicos hablan del alma y del libre albedrío; otras opiniones más científicas apelan a nuestra superioridad mental.

Pero desde el particular punto de vista de la autora, para que la verdadera naturaleza del ser humano sea comprendida, debemos de observarlo en grupo. Ya que una de las características del ser humano, al igual que otras especies animales, es tender a la sociabilidad. Somos una especie con un innegable carácter gregario; tendemos a estar juntos; ya sea por necesidad o comodidad. Es esta sociabilidad inherente a muchos seres vivos y sus consecuencias, como lo son las agrupaciones ya sean animales o humanas, las que paradójicamente nos pueden dar una pista para entender lo que nos diferencia de los animales.

La historia humana va de la mano con la evolución (para bien o para mal) en organización de los grupos humanos. Si hojeamos un libro de historia podemos concluir que los seres humanos parten de simples grupos tribales hasta llegar a las complejas naciones o comunidades de naciones de nuestros días. En este transcurrir de siglos, los seres humanos además de formar complejas estructuras sociales, crean refinados productos intelectuales; para su placer o para una mejor organización, como son: el derecho, la literatura, el arte, la ciencia y una de medular importancia para nuestro estudio: "el comercio"

Como dice el profesor Cervantes Ahumada: "el comercio es una actividad esencial y exclusivamente humana"¹. Coincidimos con él, porque hasta el día de hoy no se conoce algún animal que trafique con los restos del producto de su trabajo. Tal vez los animales compartan con los demás miembros de su grupo los resultados de la cacería o recolección, pero en ellos la idea del lucro o intercambio nunca está presente, ya que no son capaces de efectuar las abstracciones intelectuales necesarios para otorgarle valor a los bienes.

Como primer punto, para que exista el comercio deben existir los bienes, que posteriormente se convertirán en mercancías susceptibles de tráfico. Por que

¹ Cervantes Ahumada, Raúl. Derecho Mercantil, 1er curso. 2ª ed. Porrúa. 2002, México. p. 1

es precisamente de la palabra mercancía de donde surge la raíz etimológica latina de la palabra comercio de "commercium", que a su vez deriva de las voces cum, que quiere decir "con" y merx, que equivale a mercancía.

Estos bienes necesarios para el comercio; en principio son los excedentes de lo producido por las primitivas comunidades sedentarias, puesto que las nómadas no conocen la agricultura (base de estos primitivos intercambios). Siendo así que el comercio comienza con un primitivo trueque de excedentes, que con la evolución de las sociedades y de sus formas de organización, hará que en medio de este intercambio surja un intermediario; ya sea para buscar que el precio de dicho intercambio sea justo; o para evitar a ambas partes la engorrosa labor de buscar a alguien que necesite el excedente de su trabajo; que cuente y esté dispuesto a cambiarlo por lo que en ese momento desea o necesita la otra parte.

Surge el comerciante, este intermediario casi omnipresente en las sociedades humanas desde entonces, quien se convierte en la primera piedra de esa pirámide que es el comercio moderno, en su acepción económica. Es preciso señalar que el comercio en su acepción económica es un concepto difícil de precisar, en gran medida por su constante expansión ya sea por los procesos de globalización a nivel mundial o por la introducción de nuevas tecnologías, etc. Factores que directa o indirectamente afectan al comercio.

Aun así existen intentos por definirlo. Tenemos: el hecho por el Profesor Pedro Astudillo Ursúa que lo considera como "los procesos necesarios para mover los bienes necesarios en espacio y tiempo del productor al consumidor"²

Otros consideran al comercio como "la intermediación entra la oferta y la demanda de mercancías con el objetivo de obtener lucro"³

Mientras que algunos más consideran que el comercio es un "Proceso cuyo objetivo es hacer llegar los bienes desde el productor al consumidor. Involucra actividades como compraventas al por mayor y al por menor, publicidad, pruebas de ventas, información de mercado, transporte, almacenaje y financiamiento."⁴

Para entender esta definición es preciso explicar estos elementos unidos al concepto de comercio: lucro, especulación comercial y la intermediación. El lucro tiene una connotación eminentemente económica. Su concepto técnico proviene del latín "lucrum" que es el fin que se persigue en una relación o negocio, que envuelve la intención de obtener una ganancia o provecho, por alguna de las partes o las dos partes, el marco normativo puede calificarla de lícita o ilícita,

² Astudillo Ursúa, Pedro. Elementos de Teoría Económica. 4ª ed. Porrúa. México. 1997. p 191

³ <http://www.eumed.net/cursecon/dic/C.htm>

⁴ <http://www.businesscol.com/economia/glosaeco/glecon-abc.htm#C>

según su demasía o armonía, para poderle señalar determinadas consecuencias jurídicas.

La realización regular y usual de la búsqueda del lucro, es lo que consideramos como especulación. En tanto que la intermediación procede del latín *intermedius* que significa "está en medio". Para fines mercantiles es la forma por medio de la que se enlaza la circulación de satisfactores entre productores y consumidores al unir a dos o más personas para efectuar una operación sin ser agente, subordinado o delegado de ninguna de éstas.

Podemos decir que en general todos estos conceptos se refieren a "una actividad de mediación o interposición entre productores y consumidores"; con algunas variantes como el hecho de tomar al lucro como una finalidad preponderante, así como también añadir más actividades a la de interposición, como son el transporte, financiamiento y almacenaje, etc. De la que no podemos dejar fuera al productor y al consumidor.

Retomando al comerciante, será la figura de éste y sus agrupaciones; las que dan origen a los primeros ordenamientos jurídicos codificados; que son el más directo antecedente de nuestros modernos Códigos Mercantiles. En principio a dichas colecciones jurídicas se les considera como un derecho especial de esta clase social (comerciantes) pero posteriormente, con la llegada de la corriente codificadora bonapartista francesa, sería desplazada por la figura del acto de comercio como pieza fundamental de la noción jurídica de comercio de ese entonces. Y mientras más pasa el tiempo la separación entre comercio, comerciante y derecho mercantil se hace cada vez más y más amplia.

Actualmente no es posible definir al Derecho Mercantil tomando como referencia el Comercio en su acepción económica. Las normas que se aplican en la rama mercantil van más allá que simples actos de intermediación comercial, llegando incluso al punto en que existen algunos que no tiene ningún tipo de relación o finalidad comercial, pero se les otorga el carácter de mercantiles por el simple hecho de ser considerados mercantiles por lo establecido en los ordenamientos. Por lo que sería un absurdo tratar de tomar como base al comercio para definir al Derecho Mercantil de nuestros días.

A pesar de que el contenido actual del Derecho Mercantil no es el comercio. Sus antecedentes históricos si tienen origen en él; muchas instituciones jurídicas tienen origen en actividades de comercio; además de que el comercio tiene un significado profundamente económico y funcional, que se amplía con el paso del tiempo, no es una institución perenne, o inmune a los cambios históricos humanos, por el contrario, sigue nutriendo de nuevos campos de aplicación al Derecho Mercantil. No obstante "Comercio y Derecho Mercantil no son lo mismo".

Por lo que antes de aventurarnos a dar un concepto de Derecho Mercantil, así como de otros que se harán necesarios a lo largo de la exposición del presente trabajo. Haremos una revisión histórica, en un intento de aclararnos el cómo y

porqué de nuestros conceptos y figuras jurídico - mercantiles modernas; que al mismo tiempo nos ubicará en el momento histórico en que actualmente vivimos, que hace necesaria la regulación y estudio del comercio electrónico y de todas las nuevas figuras jurídicas de él emanadas, como lo es **la entidad certificadora**.

La revisión histórica emprendida nos recordará que una de las tareas del Derecho Mercantil es ser auxiliar del tráfico comercial (cualquiera que sea la modalidad que asuma) así como, cristalizar dentro de sus ordenamientos y codificaciones de derecho, instituciones que la costumbre comercial de hecho utiliza.

Los primeros antecedentes de lo que podríamos llamar comercio los encontramos en los pueblos del norte de África (antropológicamente considerada como la cuna de la humanidad), que según cuenta el historiador griego Herodoto en su obra los Nueve Libros de la Historia: a pesar de encontrarse en guerra establecían periodos de armisticio para comerciar, en los que una de las partes colocaba sus mercancías cerca de la playa y se marchaban; enseguida llegaban los posibles compradores y colocaban a un costado lo que proponían dar a cambio, hecho esto se retiraban. Si los primeros consideraban que el intercambio era justo, levantaban la mercancía y se retiraban; permitiendo a la otra parte recogerla lo que le correspondía.

Otro manuscrito antiguo que nos habla del comercio es el llamado "Código de Hamurabi" (2000 a. C. aproximadamente) Que regula figuras mercantiles tales como el depósito, el préstamo a interés, el contrato de sociedad y el contrato de comisión.

Contemporáneo del anterior, es el Código de Manú, de origen hindú, que considera al comercio como una ocupación estimable. Esto es muy importante; si tomamos en cuenta que para algunos pensadores antiguos como Demóstenes y Cicerón la figura del comerciante era objeto de calumnias y acusaciones. Dicho ordenamiento regula la compraventa de mercancías ultramarinas.

Empero los pueblos de mayor desarrollo comercial, son los que más influyeron en la creación de ordenamientos jurídicos. Tal es el caso de los fenicios, caldeos, asirios, persas, indios, hebreos, Árabes, etc.

Los persas contribuyeron al desarrollo del comercio en Asia al establecer mercados frecuentes y protección en comunicaciones. Mientras que los fenicios, históricamente reconocidos como notables marinos y negociantes, regularon el comercio marítimo a través de tratados (antiguos antecedentes de los tratados de reciprocidad internacional actuales); además establecieron los primeros puertos y factorías. Se sabe habitaron la isla de Rodas; de la que son originarias las famosas Leyes Rodias (a las que algunos autores atribuyen origen griego), las cuales versan sobre la avería común y la avería gruesa. Estas leyes posteriormente serían compiladas dentro de Digesto Romano bajo el nombre de "Lex Rodia de lactu.

Del mismo modo es importante citar a los pueblos griego y egipcio; quienes contaban con comerciantes especializados en banca (trapezitas), así como la figura de préstamo a la gruesa, a la que los griegos llamaron "nauticum foenus", que es uno de los antecedentes del moderno contrato de seguro. El desarrollo del pueblo griego en cuestiones monetarias es de subrayarse, porque entre ellos el uso de la moneda acuñada es generalizado. La muestra más clara de cómo el comercio debió ser una actividad redituable entre estos pueblos, es el inmortal filósofo Platón, a quien su actividad como comerciante permitió la riqueza y "ocio" necesarios para el desarrollo de su pensamiento⁵.

Y siguiendo lo expuesto por el profesor Raúl Cervantes Ahumada en su libro Derecho Mercantil, sabemos que entre el pueblo chino la profesión de comerciante también era considerada honrosa⁶.

Para los romanos (como para la mayoría de los pueblos de la antigüedad) no había un ordenamiento mercantil especial; todas las leyes formaban parte del "corpus iuris" general. Los primeros preceptos de derecho comercial romano, pertenecían al "ius gentium", es decir a su derecho internacional, debido a que no sólo se les permitía practicarlo a los romanos, sino también a los extranjeros; de los problemas relativos a éste conocía el "praetor peregrinus". Esta figura pretoriana que hace del derecho un instrumento bastante flexible, capaz de encontrar la solución correcta para cada caso, lo que hace innecesaria una desarrollada codificación mercantil.

En general existieron tres tipos de formaciones comerciales romanas. Las que no se limitaban a una determinada profesión (como la "actio institoria" que permite la representación); Las instituciones especiales para el comercio marítimo ("Lex Rodia de jactu o hechazón, "nauticum foenus" o préstamo a la gruesa y la "actio exercitoria", que permite ejercitar acción directamente contra el armador a pesar de haber contratado con el capitán del barco) y las de Derecho Bancario (los cambistas eran los llamados "argentarii", los "numularii" eran los banqueros propiamente dichos; la "receptum argentariorum" por medio de la cual el banquero se obliga por su cliente frente a un tercero; la "actio institoria" por la que se podía reclamar al dueño de una negociación mercantil el cumplimiento de las obligaciones contraídas por su administrador o representante –institor–⁷ y la "liberti accepti et depensi", es decir la contabilidad mercantil).

A grandes rasgos éste es el panorama del mundo occidental antiguo, desde el 4000 a. C. hasta la caída del Imperio Romano de Occidente, en el año 476 a.C. a causa de todas las invasiones barbaras sufridas y otros factores. A partir de este momento comienza lo que conocemos como edad media, que sería un periodo

⁵ Cfr. Cervantes Ahumada, Raúl, Ob. cit.

⁶ Ibidem

⁷ Quevedo Coronado, Ignacio. Compendio de Derecho Mercantil. Addison Wesley Longman de México. 1998, México, p 13

histórico germen de muchos ordenamientos jurídicos de gran importancia para la historia del Derecho Mercantil.

Formalmente se considera como Edad Media el milenio entre la caída del imperio Romano de Oriente y el Imperio Romano de Occidente. Ésta denominación la debe a los pensadores renacentistas que ven a éste milenio como una etapa intermedia entre los dos grandes periodos de la humanidad: la antigüedad y el propio renacimiento. Comienza con las invasiones bárbaras de los pueblos germánicos tales como: los suevos, visigodos, anglos, vascones, borgoñones, sajones, bretones, ostrogodos, eslavos, bizantinos, vándalos, hunos, etc. Que disuelven a la Europa alguna vez unida bajo el imperio romano. A partir de entonces recuperar la cultura, organización y cohesión europea será una de las metas a alcanzar por los regímenes más importantes de dicha etapa.

El estado de desorganización y falta de seguridad de las poblaciones; provocado por el fraccionamiento del imperio occidental y las invasiones barbarás, afectaría directamente a la actividad comercial que disminuiría considerablemente. Estos fenómenos se proyectarían claramente en los escasos ordenamientos mercantiles surgidos antes de la caída del imperio (su "corpus juris"), que virtualmente perecerá a manos de las tribus bárbaras y sus sistemas jurídicos basados en las costumbres.

De esta suerte que, el clima de inseguridad y los cambios en el pensamiento de los pueblos tras la introducción de la filosofía cristiana, dan como resultado dos de las instituciones más características de la edad media: el feudalismo y la servidumbre. El primero como una necesidad de protección y seguridad para los pobladores de una determinada región, y la segunda en contra posición al régimen esclavista de la antigüedad.

El Feudo, esa "unidad autosuficiente de producción", que muchas veces ataba a los individuos a su tierra (caso de la servidumbre de gleba), hizo que la idea de comercio o tráfico prácticamente desapareciera del vocabulario de aquel entonces. Había algo de trueque pero éste se limitaba a los productores y entre los siervos del propio feudo.

De este modo el comercio en los primeros cinco siglos del periodo se vería estancado. Los peligros y dificultades existentes para cualquiera que quisiera dedicarse a comerciar como lo eran: el pillaje, el mal estado de los caminos, el derecho de peaje que imponían muchos señores feudales, la escasez de dinero (derivado de la autosuficiencia feudal que lo hacía innecesario), la falta de uniformidad monetaria, la variación de los pesos y medidas de un territorio a otro, la piratería, etc., fulminarían con cualquier idea de tráfico internacional. Es éste el paisaje general de Europa durante los primeros siglos de la Edad Media: fraccionamientos, inseguridad y reposo social.

A pesar de todo, la idea de un Imperio de Occidente subsiste en la figura del Papa o en el Emperador, luchando por la maltrecha herencia romana.

Tomando como base esta idea de unión, se dan varios intentos de cohesión europea: los ostrogodos en el reinado de Teodorico en Italia, a principios del siglo VI; los visigodos (también en el siglo VI) en España y Francia. Siendo el intento más palpable el de Carlomagno, a quien incluso el Papa entrega la Corona imperial de Occidente. Pero todas quedan en tentativas.

Sería una serie de guerras lo que paradójicamente vendría a culminar ésta etapa de inseguridad y adormecimiento de la sociedad, estas guerras impulsarían las artes, los descubrimientos y por supuesto el comercio: "las cruzadas". El llamado del Papa a la población de Europa para recuperar la Tierra Santa de manos musulmanas hizo gran eco entre los súbditos europeos que a mares atravesaron el continente para emprender esta difícil empresa.

Las guerras fueron un fracaso militar, pero no comercial. Nuevas rutas de tráfico entre Oriente y Occidente fueron abiertas, se restableció el comercio entre los diferentes territorios europeos; resultado de esto ciudades geográficamente claves para los nuevos intercambios internacionales y transcontinentales experimentaron un despertar de su letargo medioeval y un renacimiento de las artes, ciencias y economía como nunca antes se había visto.

Entre las primeras ciudades que experimentaron dicho desarrollo están las ciudades italianas de Amalfi, Florencia, Pisa, Milán, Bolonia, Venecia y Génova. Pero fue también ahí donde se dieron cuenta de que a pesar de ser receptoras directas de la antigua herencia legislativa romana, ésta no respondía a las necesidades que el tráfico comercial de aquella época imponía. Recurrieron entonces al Derecho implantado por las tribus germánicas, pero lo encontraron también insuficiente. Por lo que un nuevo derecho surgido de las costumbres comerciales de cada comunidad, cristalizado después a leyes escritas comenzaría a gestarse.

Entre los primeros que emprendieron esta labor de organización tenemos a los mercaderes marítimos (como siglos antes lo hicieran los fenicios). Quienes crearon sus propios tribunales y jueces, a quienes nombraron respectivamente "consulados y cónsules". Para algunos casos que por su importancia admitían la apelación existían los "sopraconsoli"; llegando incluso a poderse recurrir a una tercera instancia que constituía la decisión pronunciada por el consejo general de mercaderes. Los primeros documentos de los que se auxilian dichas instituciones para dirimir controversias "son recopilaciones de costumbres, y sentencias, hechas por juristas, jueces y comerciantes."⁸

Estas compilaciones retomadas por los italianos fueron llamadas "estatutos", y cuyo conjunto conforma al "Derecho Estatutario". Algunos de ellos fueron: los "Ordinamenta et consuetudo maris, de 1063, de la ciudad de Trani, los Capitula et ordinationes curiae maritimae, nobilis civitatis Amalfae o Tablas Amalfitanas, del siglo XI, los Curiae maris de Pisa, etc. Entre las ciudades

⁸ Cervantes Ahumada, Raúl. Ob.cit. p.6

mediterráneas encontramos: los estatutos de Marsella, Barcelona, Hamburgo y Lubeck.

Uno de los más famosos serían el Consulat de la Mar promulgado por Pedro IV en Barcelona, en 1340, compilación de los Consuetudinis et usus maris, que reglan en Barcelona desde el siglo XII. Es una reproducción de las costumbres reinantes en los países a la ribera del mediterráneo; compuesto por 297 capítulos, es la legislación marítima más extensa y completa de la edad media. Sería ampliamente difundido en Europa gracias a la versión italiana.

Igual de famosos son los llamados "Roles de Olerón" del siglo XII, que reciben este nombre de la isla francesa donde se encontraba el tribunal que dicto las sentencias que dieron cuerpo a esta recopilación. Su importancia e influencia sería tal que se verían reproducidos en documentos tales como las leyes de Westcapelle, en Zelandia, las sentencias de la ciudad flamenca de Damne y las Leyes de Wisby, que regularan a los puertos de la Liga Hanseática (de la que hablaremos más adelante) en el mar del Norte, en especial Suecia y Dinamarca. También francés, es el "guión del mar" del siglo XV. Que contenía diversas reglas sobre el contrato de seguro.

Además del Consulado del Mar, habría otras importantes contribuciones españolas a las codificaciones europeas de esta época como: las Siete Partidas o Leyes de Partida que comienzan a prepararse durante el reinado de Alfonso X "el Sabio" en 1256, pero regirán hasta 1348, en el reinado de Alfonso XI, quien las decreta vigentes mediante el Ordenamiento de Alcalá, que también instituye el orden de prelación siendo que la Orden de Alcalá está en primero, los fueros municipales en segundo y por último las Siete Partidas. Así como también tenemos al Fuero Real de Castilla, ambos del siglo XIII. Las primeras contienen el primer antecedente legislativo del convenio preventivo de la quiebra y el segundo trata de instituciones comerciales tales como averías, mercancías naufragadas y el préstamo.

A la par de las ciudades italianas del mediterráneo, en el Norte otras importantes ciudades costeras buscan la unión con el fin de adquirir cierto poderío frente al orden feudal, además de protección contra peligros de la piratería y el pillaje. Su influjo sobre el comercio, y las instituciones jurídico mercantiles es considerable.

Las ciudades del Norte se alían bajo la "Liga Hanseática o de Hansa Teutónica"; las ciudades que inicialmente se concretan son Lubek y Hamburgo. Pero poco a poco crece, para fines del siglo XIII, ésta es dueña de importantes ciudades de Alemania, entre al Vístula y el Escalda. Para el siglo XIV se conformaba por setenta y siete ciudades; cien años después alcanzaría su máximo apogeo al llegar a ochenta y cinco ciudades miembro. Otras importantes ligas en el Mar Báltico serían la Liga del Rin y la Liga Suavia.

Su desenvolvimiento, es análogo a las ciudades italianas (con las que tuvieron contacto). Pero además de los estatutos de las ciudades de Hamburgo, Lubeck y Brema; surge una legislación general de la liga Hanseática, originada en la Dieta de la Confederación en forma de actas registradas; la más antigua de éstas es de 1312.

Los ingleses harán su contribución a las legislaciones de este periodo con dos documentos importantes: "La carta magna de Juan sin Tierra, en 1215 y la Carta Mercatoria, de 1285.

Entre las instituciones generales a todas las ciudades en este período están las corporaciones. Son uniones de trabajadores libres que se dedican a una misma actividad, las formadas por comerciantes llegarían a ser las más importantes, sus comunidades que reciben el nombre de universidades de mercaderes. Organizan sus propios ordenamientos, tribunales y crean sus propias leyes. El espíritu de unión viene de la necesidad de unir fuerzas contra todas las arbitrariedades de los señores feudales.

Estas comunidades dan origen así a un derecho especial, que atendía al individuo, más que al objeto de la controversia. Con base en esta subjetividad, emergen dos importantes instituciones jurídicas que influenciarían enormemente a la ciencia del Derecho Mercantil desde entonces: la matriculación, antecedente directo del registro de comercio y el régimen de publicidad mercantil; y la jurisdicción consular, que hace que se creen tribunales especializados en comercio y la atribución de una competencias en cuestión de materias, que hicieron de los procedimientos mercantiles algo rápido, sencillo y sin tantas formalidades como otros derechos.

Otro punto importante de comercio en esta era son las ferias. Los mercados semanales locales eran diminutos y negociaban sólo con artículos locales, primordialmente agrícolas. Las ferias "(...) eran enormes, traficándose en ellas con productos al por mayor, que procedían de todo el mundo. La feria era el centro de distribución donde grandes comerciantes, que se distinguían de los buhoneros errantes y de los artesanos de la localidad, compraban y vendían los artículos extranjeros que venían del Este y el Oeste, del Norte y del Sur".⁹

Entre las ferias más famosas tenemos a las de Nápoles y Florencia en Italia, Champaña en Francia, Medina de Campo en España y Ninji-Nogvorov en Rusia.

Las ferias contribuyeron al Derecho mercantil aportando persistentes instituciones como: la quiebra, la bancarrota y sobre todo a estructurar un derecho mercantil uniforme para todos los países, que recibió el nombre de jus nundinarum, que se caracterizó por el impulso al desarrollo del crédito y la rapidez de sus operaciones.

⁹ Huberman, Leo. Los bienes terrenales del hombre. 27ª ed. Nuestro Tiempo. México, 1987. p.36

La Iglesia católica (trascendental para este periodo histórico), se vio afectada por instituciones de origen puramente mercantil. La idea de la personalidad jurídica, que es una creación mercantil; es adoptada por el Papa Inocencio IV, para distinguirla a la Iglesia de los fieles que la conformaban. Y en contrasentido, la Iglesia influye a la actividad comercial al prohibir el préstamo con interés, dejando a los no creyentes (principalmente judíos) las vías abiertas para el comercio bancario.

Pero el comercio es algo en constante evolución, y nuevas condiciones históricas se aproximan. La caída de Constantinopla, y por consiguiente del Imperio Romano de Oriente; la era de los grandes descubrimientos geográficos (que hace de España una potencia comercial con grandes ordenamientos mercantiles) y el inicio del renacimiento marca el fin de lo que conocemos como Edad Media y el principio de lo que llamamos Edad Moderna (que terminará con el fin del imperio absolutista francés a manos de los revolucionarios en 1789). El sello distintivo de esta etapa será la codificación del derecho mercantil, que surgiera en la Edad Media. Podríamos decir que es la época de las grandes codificaciones.

El nacimiento de los primeros Estados Nacionales, hace que figuras de poder locales como los señores feudales y los gremios se vean debilitados. Es interesante que los comerciantes agremiados que fueron una de las fuerzas que ayudaron a derribar el poder feudal, se vieran afectados por éste nuevo cambio de fuerzas.

Ante este cambio de poderes de local a Estatal, el Derecho Mercantil, como alguna vez lo fuera en la época de los imperios antiguos volverá a ser materia regulada por el poder estatal. Y que mejor manera hacerlo que a través de ordenamientos emanados del monarca. Siendo claros ejemplos de esto las Ordenanzas de Colbert u Ordenanzas de Luis XIV, de marzo 1673 y agosto de 1681, que comprenden al comercio terrestre y marítimo. Ninguno de los ordenamientos anteriores tiene el poder público coercible. Pero los franceses se preocuparían por darles poder coercitivo a estas compilaciones.

Estos ordenamientos además de tener como novedad la codificación y la coercitividad, son relevantes por dejar la perspectiva subjetiva que hasta ese entonces tenía el Derecho Mercantil para acudir a la objetividad del acto de comercio. Esto marcará un gran hito, ampliará la noción jurídica de lo que es el derecho y dará para miles discusiones sobre la naturaleza del Derecho Mercantil que continúan hasta la actualidad.

Siguen su ejemplo varios monarcas europeos. En Dinamarca el rey Cristian V expide una codificación en 1683 y en Suecia para 1667 el rey Carlos IX expide una codificación mercantil.

En España, hubo diversas ordenanzas, edictos, bandos y fueros, entre los más importantes tenemos a la Nueva y Novísima Recopilación del derecho castellano de Felipe II, dictada en 1567; las Ordenanzas de Burgos 1495; las de Sevilla de 1554 y las de Bilbao (la primera versión de estas data de 1560, que es adicionada en 1665, pero la versión final es de 1737, confirmada por Felipe V). Las de Bilbao son fundamentales por que fueron "el Código de Comercio" para la mayoría de las colonias Americanas, entre ellas el Virreinato de la Nueva España, y que serían de medular importancia en nuestro país por que seguirían rigiendo aun después de la consumación de la Independencia.

Un siglo después de su publicación las ordenanzas de Colbert, éstas ya no respondían a las necesidades del tráfico comercial, por lo que para 1787 se nombra una comisión para revisar y actualizar, pero los acontecimientos históricos hacen caer en el olvido el proyecto.

El 14 de julio de 1789, el pueblo francés toma por asalto la cárcel de la Bastilla, acontecimiento que se toma como fecha de inicio de la revolución francesa, el fin de la época moderna y el inicio de la contemporánea. Estamos en una nueva época de revoluciones y cambios sociales. La inestabilidad en Francia provocada por la revolución y las diferentes experiencias de gobierno abre el camino para que se eleve la figura de Napoleón, quien difundirá la filosofía revolucionaria francesa y todas sus creaciones (como sus códigos) a lo largo del continente mediante sus campañas militares. Inicia una nueva era de nuevas ideologías políticas, económicas y sociales. El Derecho Mercantil crecerá y crecerá, a partir de este momento los ordenamientos de cada nación trataran de cristalizar en papel la mutante realidad diaria del Derecho Mercantil.

La situación de Francia tras la revolución es de inestabilidad, por lo que será hasta el 3 de abril de 1801 que el gobierno revolucionario retoma la idea de modificar las ordenanzas de Colbert y nombra una nueva comisión para elaborar un Código de Comercio, resultado de esto se crea un proyecto que tras ser discutido en la asamblea queda en el olvido.

A la llegada de Napoleón al poder la crisis del Estado francés (sobre todo la hacendaría, es terrible, y como todo nuevo régimen trae a costas nuevos ordenamientos jurídicos, surgen los famosos cinco Códigos de Napoleón. El de Comercio se basa en el proyecto de 1801, que es renovado y discutido, siendo aprobado un proyecto definitivo que comienza a regir el 1º de enero de 1808.

Algunos consideran a éste como un Código de exportación, por la gran influencia que ejerció en otras naciones Europeas, debido a la poderosa figura de Napoleón tras de él o del prestigio de la Revolución francesa. Este Código abarcaría a toda la materia comercial hasta entonces existente: regula a los principales contratos mercantiles, a los tipos de sociedades, la quiebra, el derecho marítimo, y algunas disposiciones aplicables al proceso mercantil; también verá al comercio como algo objetivo, más que algo subjetivo y clasista.

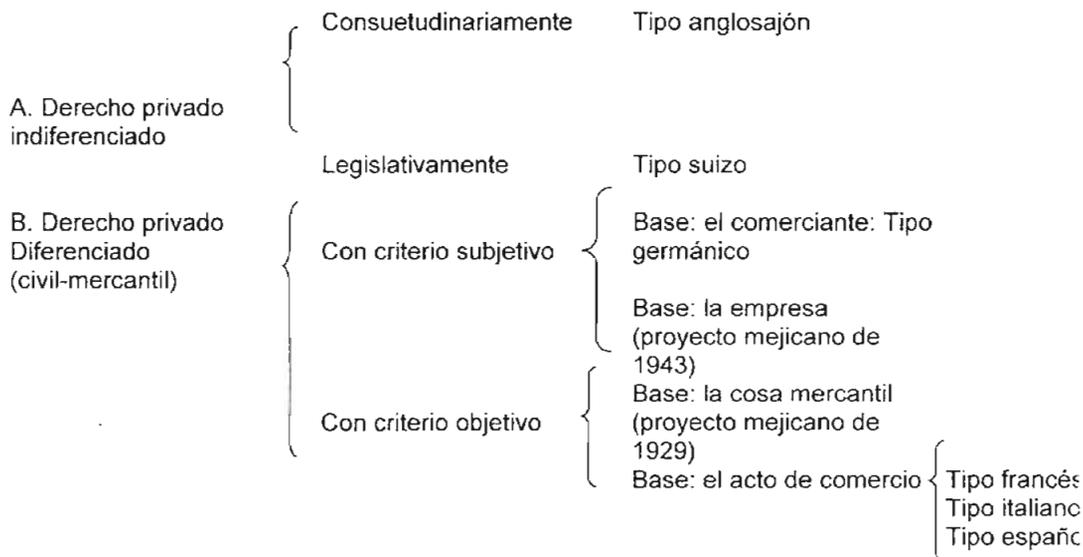
Algunas codificaciones claramente influenciadas por el Código francés serían el Código Albertino de 1829 en Italia, sustituido dos veces: una en 1865 y 1882, hasta su derogación por el de 1942 que consagra la unificación del derecho privado romano; el código de comercio de las dos Sicilias. El de España de 1829; el de Portugal de 1833; el Código de las obligaciones de Suiza de 1881 y de 1911, que regula conjuntamente las materias civiles y mercantiles y el de Alemania, el Código de Comercio de 1861, seguido por el de 1900. También es de resaltarse el influjo de la codificación francesa en los ordenamientos jurídicos mercantiles de las jóvenes naciones americanas, ejemplo de ello son Haití 1847, Argentina 1859, Brasil 1850 y Chile 1865.

Para esta época en España el régimen monárquico está en crisis tras la invasión Napoleónica a sus territorios. Hay un gobierno liberal reunido en Cádiz con el propósito de elaborar una Constitución que de fundamento a este nuevo orden. ¿Qué sucede con la materia comercial?

A pesar de la importancia de las anteriores recopilaciones españolas en materia comercial, en las Cortes de Cádiz de 1810 se nombra una comisión para la creación de un Código de Comercio Español. Pero al retorno de los monarcas al poder, se deja algo en el olvido el proyecto, sin embargo ante la imperiosa necesidad, finalmente se acepta el proyecto redactado por Pedro Sainz de Andino que retoma las antiguas codificaciones españolas y el moderno Código francés. El proyecto es sancionado y promulgado por Cédula Real del 30 de mayo de 1829. No obstante éste es sustituido por un nuevo proyecto sancionado el 22 de agosto de 1885.

El panorama europeo a partir de las revoluciones seguiría en constante transformación, a la par de los cambios históricos. Llega el comunismo, la influencia del sistema de common law de los países del norte, entre otros fenómenos. El Derecho Mercantil sigue creciendo, el comercio internacional es notable. En lo subsecuente las argumentaciones mercantiles versaran sobre que sistema de los existentes (ver cuadro) es aplicable para dirimir las controversias mercantiles; la implicación de las nuevas tecnologías y otros puntos. El maestro Mantilla Molina resume los sistemas de codificación mercantil existentes en nuestros días mediante el siguiente cuadro¹⁰.

¹⁰ Mantilla Molina, Roberto L. Derecho Mercantil. 29ª ed. Porrúa. México. 2001 p.22



¿Qué sucede en nuestro país en todo este tiempo? En la época de los antiguos imperios precolombinos, el comerciante tenía un papel respetado dentro de la organización social. Entre los mayas hay muchas referencias antropológicas sobre comerciantes, incluso contaban con un Dios consagrado a la protección de los mercaderes llamado Ek Chuah.

Entre los nahuas (aztecas) los comerciantes o potchecas eran una figura de gran poder político y económico, su Dios protector era el Yacatecutli. Contaban con una figura parecida a las corporaciones, un jefe de la misma y tribunales especiales para dirimir las controversias surgidas en su seno. Sus grandes centros de tráfico comercial eran los Tianguis, que como el de Tlatelolco, llegaron a albergar hasta cincuenta mil personas. Pero hasta el momento no se han encontrado datos de que haya existido alguna reglamentación específica en cuanto a comercio.

Tras la caída del imperio azteca la cultura, ordenamientos jurídicos y religiosos fueron impuestos a las poblaciones indígenas por los conquistadores. Desde entonces el territorio fue conocido como el Virreinato de la Nueva España y las costumbres comerciales españolas se implantaron. Entre ellas la idea de las corporaciones y universidades; se estableció así la Universidad de mercaderes de la Nueva España en 1581, que recibió autorización real a manos de Felipe II mediante Cédulas Reales del 15 de junio 1592 y 8 de noviembre de 1594. A esta Institución también se le conocía como Consulado de México, tenía atribuciones de Tribunal Comercial. Su jurisdicción abarcaba los territorios de Nueva Vizcaya, Nueva Galicia, Guatemala, Yucatán y Soconusco.

Inicialmente rigieron en la Nueva España las ordenanzas de Burgos y Sevilla; según una Recopilación de Indias sancionada por Carlos II en 1680, se ordenó que éstas se aplicaran de manera subsidiaria, a las que la Universidad de mercaderes de la Nueva España o Consulado Mexicano, promulgó unas bajo el título de "Ordenanzas del Consulado de México, Universidad de Mercaderes de Nueva España, aprobadas por Felipe II en 1604.

Pero con la llegada de las ordenanzas de Bilbao todas las anteriores cayeron en desuso. Carlos II crearía mediante Cédulas Reales consulados en Veracruz (17 de enero de 1795) y en Guadalajara el 6 de junio de 1795. Pero por decreto del Congreso el 16 de octubre de 1824 serían suprimidos los consulados y por una ley del 15 de Noviembre de 1841 se crean los tribunales mercantiles.

Dichas ordenanzas continuarían vigentes hasta que fueron derogadas por el Código de Comercio del 16 de mayo de 1854, conocido como Código Lares (con algo de influencia española), en honor al ministro de Santanna Teodosio Lares a quién se le atribuye la paternidad de dicho Código. Sería de efímera existencia, siendo derogado por la ley de 22 de noviembre de 1855, que restaura las Ordenanzas de Bilbao y suprime los Tribunales de Comercio. Desde entonces su jurisdicción se atribuiría a los de Comunes. Para los tiempos del imperio se restaura su vigencia mediante decreto del 15 de julio de 1863, aunque por un breve periodo.

Los movimientos históricos que se dieron en nuestro país en el siglo XIX tendientes a cambiar el sistema central a uno federal para imitar al sistema Estadounidense, tuvieron influencia directa en el comercio. Las constituciones de 1824 y 1857 hacen de la facultad legislativa en materia comercial una facultad local y no federal como lo fue antes. Aunque la respuesta de los Estados a esto fue nula. Tabasco sería el único Estado que se preocuparía por "legislar" en esta materia, aunque su Código sería una copia del de 1854 y Puebla simplemente declaró vigente el mismo, sin considerarlo ley del Estado.

Ante tal panorama, la materia mercantil volvió a ser federal, gracias a una reforma constitucional a la fracción X del artículo 73 del 15 de diciembre de 1883, promulgándose un nuevo Código de Comercio el 20 de abril de 1884; que sería substituido por el del 15 de septiembre de 1889 que aunque reformado casi totalmente y mutilado por la creación de numerosas leyes sigue vigente hasta nuestros días. En la creación de este último Código se tomaron ideas del ordenamiento italiano de 1882 y del español de 1885, que como ya mencionamos son de influencia francesa.

Hemos expuesto brevemente la historia de cómo la actividad comercial ha tratado de ser regulada mediante agrupaciones u ordenamientos de naturaleza jurídica. Como ya mencionamos, también podíamos considerar a esto los antecedentes históricos del Derecho Mercantil, aunque el Derecho Mercantil abarca muchos más aspectos que lo expuesto en la exposición histórica anterior o

que el comercio en general. Esta claro que no es lo mismo comercio que Derecho Mercantil, ¿qué es el Derecho Mercantil entonces? Para continuar nuestra exposición se hace necesario un concepto de Derecho Mercantil que nos guíe a lo largo de nuestro estudio.

Derivados de las diferentes corrientes existentes para entender al Derecho Mercantil tenemos los siguientes conceptos:

Para Vivante el Derecho Mercantil es "aquella parte del derecho privado que tiene principalmente por objeto regular las relaciones jurídicas que surgen del comercio"¹¹

Para el maestro Raúl Cervantes Ahumada, el Derecho Mercantil es "el conjunto coordinado de estructuras ideales, pertenecientes al ordenamiento jurídico general y destinadas a realizarse o actualizarse principalmente en la actividad de la producción o de la intermediación en el cambio de bienes o servicios destinados al mercado general."¹²

Ignacio Quevedo Coronado opina que el Derecho Mercantil es "el conjunto de normas jurídicas que se aplican a los actos de comercio legalmente calificados como tales y a los comerciantes en el ejercicio de su profesión"¹³

El Diccionario de Derecho de Rafael de Pina lo define como "El Conjunto de normas relativas a los comerciantes como tales, a los actos de comercio y a las relaciones jurídicas derivadas de la realización de estos"¹⁴

El maestro Mantilla Molina a su vez lo define como "El sistema de normas jurídicas que determinan su campo de aplicación mediante la calificación de mercantiles dadas a ciertos actos, y regulan estos y la profesión de quienes se dedican a celebrarlos"¹⁵

Consideramos que las definiciones presentadas son escuetas, pues en la mayoría de ellas se hace gran hincapié en la intermediación y algunos otros conceptos que aluden al comercio en su concepción económica. Y si bien las nociones económicas son el antecedente histórico del comercio, no definen el contenido actual del Derecho Mercantil. Mientras que otras toman al acto de comercio y al comerciante como los únicos elementos que integran al Derecho Mercantil; excluyen con esto a otros factores importantes de lo que se considera Derecho Mercantil como son: la actividad profesional del comerciante, la constitución de la empresa y otras funciones relativas a está con fines no comerciales, entre otras

¹¹ Cervantes Ahumada, Raúl. *Ob. cit.* p.20

¹² *idem.* p. 21

¹³ Quevedo Coronado, Ignacio. *Compendio de Derecho Mercantil Mexicano.* Addison Wesley Longman de México, México, 1998. p 11

¹⁴ De Pina, Rafael. *Diccionario de Derecho.* 24ª ed Porrúa.. México, 1997 p. 236

¹⁵ Mantilla Molina, Roberto L. *Ob. cit.* p.23

Opinamos que un verdadero concepto de Derecho Mercantil no solo debería basarse en nociones de comerciante, comercio o acto de comercio, también debe atender a cuestiones de medular importancia para el derecho mercantil como la empresa (todos sus actos de constitución, operación, etc.) y la actividad profesional de comerciante, entre otros. Creemos que la definición que más se acerca, aunque no cumple en su totalidad lo que consideramos Derecho Mercantil, sería la del maestro Mantilla Molina, y es la que para efectos prácticos podríamos utilizar para referirnos al Derecho Mercantil.

1.1.2. Los Actos de Comercio

El recuento histórico emprendido en el apartado anterior, nos lleva hasta la época de las modernas codificaciones que inician con el código elaborado por los juristas franceses de la época napoleónica, para los cuales, el Derecho Mercantil deja de ser una institución de carácter subjetivo (basado en la calidad del sujeto que lo realiza), para convertirse en una que atienda más al sistema objetivo (cimentado en el carácter intrínseco del acto).

Este cambio de orientación en el Derecho Mercantil, se reflejó en las naciones europeas y latinoamericanas de tradición jurídica romanista; entre ellas la nuestra, que en su código de 1889 (vigente hasta nuestros días) adopta un sistema predominantemente objetivo. Ya que a decir de algunos autores, un sistema totalmente objetivo es imposible. Aunque al leer con detenimiento nuestro código vemos que nuestro sistema no es objetivo.

Porque si bien nuestro precepto enuncia categóricamente en su primer artículo “los actos comerciales sólo se registrarán por lo dispuesto en este Código y las demás leyes mercantiles aplicables”. Dicho ordenamiento contiene también disposiciones aplicables a los comerciantes en el ejercicio de su actividad, como el artículo tercero que reza: “Se reputarán en derecho comerciantes: (...)” Lo que nos hace deducir que nuestro código, a pesar de lo que traten de afirmar los autores (“el derecho mercantil en México es –principalmente- el derecho de los actos de comercio”.¹⁶) No es objetivo, si no mixto.

Para que esto sea entendido debemos de hablar de la situación de los sistemas legales mercantiles en otros países.

1.1.2.1. Sistemas Legales

La mayoría de las legislaciones actuales se inclinan por un sistema predominantemente objetivo, subjetivo o bien mixto; para la codificación de su derecho mercantil.

¹⁶ De Pina Vara, Rafael. Derecho Mercantil Mexicano, 28ª ed. Porrúa. México, 2002. p.22

Alemania es ejemplo de un sistema de codificación subjetivo, que atiende a la calidad del sujeto que realiza el acto. Mientras que naciones como España y México adoptan un sistema predominantemente objetivo. En tanto que Venezuela tiene un sistema mixto.

Independientemente del sistema de codificación que adopten, para especificar al acto de comercio algunos abrazan el sistema de la definición al tiempo que otros toman el de la enumeración. El primero enuncia un concepto global que intenta establecer las características fundamentales de los diversos actos que se pueden considerar como mercantiles; en tanto que el segundo da un listado de incidentes que se encuentran en dicha posición.

España ha adoptado el sistema de definición; por su parte Italia, Alemania, Francia y nuestro país utilizan el de enumeración. (Véase artículo 75 de nuestro ordenamiento mercantil).

Empero de nuestro sistema, la enumeración utilizada por nuestro Código en ningún momento es limitativa o taxativa, muy por el contrario es ejemplificativa; si bien da algunos casos, en la última fracción del artículo 75 expresa "XXV. Cualesquiera otros actos de naturaleza análoga a los expresados en éste código". Dejando abierta la posibilidad de adjuntar más casos que la necesidad económica o histórica haga necesarios.

1.1.2.2. El Acto de Comercio

Es evidente que en el presente trabajo no podemos tratar a todo el Derecho Mercantil, puesto que eso sería labor de dos o más cursos completos de esa materia. Por lo que partiremos del acto de comercio con el propósito sentar algunas bases jurídicas necesarias para nuestro estudio, que además servirán de introducción a otras figuras jurídicas mercantiles que abordaremos posteriormente.

Reiteramos que el acto de comercio, no abarca todo el Derecho Mercantil (que contempla infinidad de figuras) es una mera referencia a la legislación mercantil general. Ya que como bien señala Joaquín Garrigues " No quiere significar que el acto de comercio absorba por completo al Derecho mercantil. Significa que el acotamiento del Derecho mercantil se realiza por medio de los actos de comercio, porque son ellos los que reclaman un tratamiento distinto al de los actos sometidos al Derecho civil"¹⁷

Por lo que para iniciar nuestro estudio sería propio dar una definición de acto de comercio; pero nos encontramos con que nuestro Código no da una definición, simplemente enumera una serie de supuestos de mercantilidad en el artículo 75:

¹⁷ Garrigues, Joaquín. Curso de Derecho Mercantil. Tomo I. 9ª ed. 2ª reimpr. Porrúa. México, 1990. p. 138

“La Ley reputa actos de comercio:

I.- Todas las adquisiciones, enajenaciones y alquileres verificados con propósito de especulación comercial, de mantenimientos, artículos, muebles o mercaderías, sea en estado natural, sea después de trabajados o labrados;

II.- Las compras y ventas de bienes inmuebles, cuando se hagan con dicho propósito de especulación comercial;

III.- Las compras y ventas de porciones, acciones y obligaciones de las sociedades mercantiles;

IV.- Los contratos relativos y obligaciones del Estado ú otros títulos de crédito corrientes en el comercio;

V.- Las empresas de abastecimientos y suministros;

VI.- Las empresas de construcciones, y trabajos públicos y privados;

VII.- Las empresas de fábricas y manufacturas;

VIII.- Las empresas de transportes de personas o cosas, por tierra o por agua; y las empresas de turismo;

IX.- Las librerías, y las empresas editoriales y tipográficas;

X.- Las empresas de comisiones, de agencias, de oficinas de negocios comerciales y establecimientos de ventas en pública almoneda;

XI.- Las empresas de espectáculos públicos;

XII.- Las operaciones de comisión mercantil;

XIII.- Las operaciones de mediación de negocios mercantiles;

XIV.- Las operaciones de bancos;

XV.- Todos los contratos relativos al comercio marítimo y a la navegación interior y exterior;

XVI.- Los contratos de seguros de toda especie, siempre que sean hechos por empresas;

XVII.- Los depósitos por causa de comercio;

XVIII.- Los depósitos en los almacenes generales y todas las operaciones hechas sobre los certificados de depósito y bonos de prenda librados por los mismos;

XIX.- Los cheques, letras de cambio o remesas de dinero de una plaza a otra, entre toda clase de personas;

XX.- Los vales ú otros títulos a la orden o al portador, y las obligaciones de los comerciantes, a no ser que se pruebe que se derivan de una causa extraña al comercio;

XXI.- Las obligaciones entre comerciantes y banqueros, si no son de naturaleza esencialmente civil;

XXII.- Los contratos y obligaciones de los empleados de los comerciantes en lo que concierne al comercio del negociante que los tiene a su servicio;

XXIII.- La enajenación que el propietario o el cultivador hagan de los productos de su finca o de su cultivo;

XXIV. Las operaciones contenidas en la Ley General de Títulos y Operaciones de Crédito;

XXV.- Cualesquiera otros actos de naturaleza análoga a los expresados en este código.

En caso de duda, la naturaleza comercial del acto será fijada por arbitrio judicial".

Además de esta enumeración del código, hay otras leyes de naturaleza mercantil como la Ley de Títulos y Operaciones de Crédito, La ley del Mercado de Valores, La Ley de Protección al Consumidor, etc. Que reputan ciertos actos como mercantiles por el simple hecho de estar contenidos en sus páginas.

¿Qué es el acto de comercio entonces? Para entender al acto de comercio debemos ir más allá de lo expuesto en la lista dada por nuestro legislador. Para descifrar al acto debemos examinar nociones fundamentales de derecho como la de hecho y acto jurídico, para posteriormente a llegar desentrañar la naturaleza del acto de comercio.

El hecho jurídico "lato sensu", sería todo suceso, sea un hecho del ser humano o una manifestación de la naturaleza, que el régimen jurídico toma en cuenta para imputarle efectos jurídicos. Estos se clasifican en:

- a) Hechos jurídicos stricto sensu
- b) Actos jurídicos

El hecho jurídico stricto sensu a su vez puede ser:

- a) De la naturaleza (muerte, accesión natural de bienes, nacimiento)
- b) Del ser humano (lícitos o ilícitos)

Por su parte el acto jurídico sería una expresión de la voluntad con el fin de extinguir, transmitir, crear o modificar obligaciones y derechos y produce diversos efectos. Tiene elementos de existencia y de validez. La falta de los primeros da como resultado la inexistencia del acto; que éste no produzca efectos legales y lo hace no ser susceptible de confirmación ni prescripción. La falta de los segundos produce nulidad absoluta o relativa, según sea el caso.

Los elementos de existencia son: la voluntad o acuerdo de voluntades, el objeto y la forma. Los de validez: capacidad, ausencia de vicios de la voluntad, licitud en el objeto o causa, y forma.

Aclarados estos puntos sobre lo que en derecho son considerados hecho y acto, la búsqueda del concepto de acto de comercio.

1.1.2.3 Concepto

Varios han sido los intentos a lo largo de la historia del Derecho Mercantil moderno de dar una definición de acto de comercio. Pero definir los actos de comercio es tarea difícil puesto que, a decir de algunos autores, la rápida transformación histórica del Derecho mercantil, el continuo ensanchamiento del ámbito comercial y la insistente especialización de dicho Derecho. Hacen que el intento de dar una definición de que se ajuste a todos los tiempos y circunstancias sea prácticamente imposible.

Para algunos estudiosos como el maestro Mantilla Molina dar un concepto de Acto de Comercio es una vana y absurda ilusión, debido a lo amplio y mutante de esta figura. Lo que resulta lamentable, ya que como él mismo expresa "el acto de comercio es la clave del sistema mercantil, pues a más de que su celebración determina la aplicabilidad de esta rama del derecho, la figura misma del comerciante no existe, según la opinión dominante, sino en función del acto de comercio"¹⁸

En contra posición al maestro Mantilla Molina otros autores como Elvia Arcelia Quintana Adriano creen poder llegar a delimitar el acto de comercio dentro de un concepto, ya que consideran que "El acto de comercio en esencia es el mismo; sin embargo, el avance tecnológico –industrial, entre otros, ha hecho que el referido acto se encuentre matizado con las características y elementos que en un determinado tiempo y espacio han regulado, tanto al comercio como a la actividad del comerciante. (...)"¹⁹. Esto no es un concepto, simplemente, la opinión de estos autores se encamina a considerar que aunque el acto de comercio sufre variantes que se derivan del avance tecnológico, éstas no afectan la naturaleza

¹⁸ Mantilla Molina, Roberto L. *Ob. cit.* p. 57

¹⁹ Quintana Adriano, Elvia Arcelia. *Ciencia del Derecho Mercantil*. Porrúa. México, 2002 p. 201

esencial del acto de comercio. Por lo que es posible conceptualizar al acto de comercio.

Las posiciones acerca de un concepto válido se van a los extremos de pensar en un concepto absoluto a negar por completo la existencia de tal, aun así haremos un intento más para tratar de puntualizar a esta compleja figura jurídica mercantil.

Entre los que han emprendido la titánica labor de desentrañar la naturaleza del acto de comercio hay quienes tratan de explicarlo ya bien solo o apoyándose en otros conceptos, mientras que otros simplemente lo definen. Entre las definiciones que podemos encontrar está la de Joaquín Rodríguez y Rodríguez para quien los actos de comercio son "los realizados en masa por las empresas"²⁰. Definición que nos pone en el aprieto de preguntarnos ¿qué es una empresa? y ¿qué es un acto en masa?

La empresa según el artículo 15 del Ley Federal del Trabajo es "la unidad económica de producción o distribución de bienes o servicios". Sin embargo, algunos teóricos al tratar de definir a la empresa la unen a la figura del comerciante (empresario) y dicen de ella, que es la conjunción de componentes personales y patrimoniales que utiliza el comerciante como medio para concurrir al mercado con servicios o bienes con fines lucrativos. Aunque debemos aclarar que, a pesar que terminologicamente empresa se confunde con empresario, esto no es correcto; el termino empresa usándolo como sinónimo de sociedad, hace referencia a la unidad económica, a esa universalidad de bienes sobre los que actúa el empresario; o bien, empresa también significa una actividad que desde el punto de vista económico es la coordinación de factores de la producción, capital y trabajo; pero para fines de la definición anterior adoptaremos el criterio del la Ley Federal del Trabajo

Ahora bien, se dice que la empresa realiza actos en masa, es decir una serie "actos conectados con la organización y explotación de las empresas, que se suceden iguales, en continuidad, y que constituyen la conducta, el quehacer dentro de la negociación o empresa de su titular (empresario) y de su personal"²¹; en contraposición a los actos ocasionales o aislados que suelen ser esporádicos, pudiendo ser mercantiles por fines especulativos, tener forma o tipo comerciales; o bien por tener por objeto algo de comercial.

A todas luces un concepto de acto de comercio basado en la concepción de empresa y actos en masa (conceptos de por si difíciles de concretar) es insuficiente, ya que debemos abordar figuras como el empresario, el personal, etc. Quizás este concepto podría ser válido si solo atendiéramos a algunas fracciones del artículo 75 que se refieren a la empresa mercantil (y aun así tendremos que observarlo con detenimiento) como fuente de donde emanan los actos de

²⁰ Citado por Quintana Adriano, Elvia Arcelia. *Ob. cit.* pág. 206

²¹ Barrera Graf, Jorge. *Instituciones de Derecho Mercantil*. Porrúa, México, 1989. p. 74

comercio (V, VI, VII, VIII y IX entre otras), pero sería hacer a un lado fracciones como las XIX y XXIV que otorgan el carácter de acto de comercio a diversas transacciones en las que no media la figura de la empresa, por las que acto de comercio tiene nociones aun más amplias.

Por su parte Jacinto Pallares, no define simplemente expresa que “son actos de comercio todos aquellos que menciona el Código y cualesquiera otros de naturaleza análoga dejando la clasificación de los hechos según vayan apareciendo en la escena mercantil al buen sentido de los comerciantes y a la experiencia y espíritu prácticos de los jueces y Magistrados”²². Definición que resulta insuficiente y no aclara para nada el concepto.

En tanto que Genaro Góngora Pimentel considera que el “acto de comercio es la expresión de la voluntad humana susceptible de producir efectos jurídicos dentro del ámbito de la realidad reservada a la regulación de la legislación mercantil”.²³ Esta definición simplemente toma el concepto de acto jurídico y le confiere consecuencias mercantiles, pero creemos que el concepto de acto de comercio va más allá.

Para Rafael de Pina Vara es “la expresión de la voluntad humana susceptible de producir efectos jurídicos dentro del ámbito de la realidad reservada a la regulación de la legislación comercial.”²⁴ Este concepto nos parece muy similar al anterior, es decir, con demasiadas referencias al acto jurídico y pocas alusiones a los actos materiales (como las actividades empresariales) que como ya vimos, también son considerados dentro de los actos de comercio. En todo caso, las definiciones anteriores no nos parecen lo suficientemente completas ya que plantean la disyuntiva de: ¿el acto de comercio es solo un acto jurídico o son también son actos materiales?

Mientras que el Diccionario de Derecho Privado lo define como “todo hecho voluntario que origina relaciones regidas por el Derecho Mercantil. Estrictamente se comprende bajo esta denominación todos aquellos actos que se hallan bajo el dominio de las leyes comerciales y son juzgados por los Tribunales con arreglo a ellas”²⁵. Este otro concepto es erróneo desde el momento que en su definición tratar al hecho como acto, lo que en Derecho (como señalamos anteriormente) es diferente. Además de que, como sucede en los conceptos anteriores, esta definición hace alusión al acto jurídico para tratar de definir al acto de comercio. Lo que como dijimos anteriormente, no es exacto, ya que el acto de comercio va más allá; debido a que existen actividades que no son consideradas “estrictamente” actos de comercio y aun así están comprendidos por las leyes mercantiles.

²² Citado por Quintana Adriano, Elvia Arcelia.Ob. cit. pág. 206

²³ Citado por Quintana Adriano, Elvia Arcelia.Ob. cit. pág. 208

²⁴ De Pina, Rafael.Ob. cit. Pág. 52

²⁵ Citado por Quintana Adriano, Elvia Arcelia.Ob. cit. p. 209

Por su parte, el maestro Felipe de Jesús Tena piensa que “todo contrato por el que se adquiere a título onerosos un bien de cualquiera especie con la intención de lucrar mediante su transmisión así como el contrato también onerosos, a cuya virtud esta transmisión se verifica”²⁶. Sobre este concepto pensamos, que si bien el Código de Comercio Vigente considera a algunos contratos como actos de comercio; en ningún momento podría una definición de este tipo ser válida, ya que los contratos de la naturaleza mercantil no son la totalidad (ni siquiera la mayor parte) de lo que consideramos como acto de comercio; por lo que esta definición también resulta insuficiente.

El estudioso Rocco juzga que “es un acto que realiza o facilita la interposición en el cambio”²⁷. Estas dos últimas definiciones atienden demasiado al comercio en su acepción económica como una actividad de intermediación, por lo que una vez más aseveramos, que ni comercio, ni Derecho Mercantil, ni acto de comercio son sinónimos; comparten características comunes, pero distan mucho unos de otros.

Lorenzo Mossa ve al acto de comercio como “el conjunto de las relaciones jurídicas en las cuales vive y a las cuales se aplica el derecho mercantil”²⁸. Este concepto desde nuestra perspectiva es demasiado general, porque consideramos que no todas las relaciones en las que vive y aplica el derecho mercantil son actos de comercio, existe otro mundo de relaciones mercantiles en las que éste vive y se aplica (como las referentes a la actividad profesional del comerciante) donde vive y se aplica el Derecho Mercantil y no son considerados actos de comercio.

Duque, Justino F. considera que el acto de comercio “en sentido amplio es todo acontecimiento, natural o humano, y, en sentido estricto, todo negocio jurídico, unilateral o bilateral, o acto ilícito, el cual, por reunir alguno de los caracteres individualizados por la doctrina (intermediación, ánimo de lucro, pertenencia a la empresa), está sometido al Derecho mercantil, produciendo efectos específicos, en cuanto a su perfección, prueba, interpretación, presunción de solidaridad, etc.”²⁹. Este autor también toma como base al acto jurídico en general para llegar al acto de comercio, aceptando las consecuencias de éste aunque legalmente sea considerado como ilícito (supuesto que muchos juristas rechazan); pero no se queda ahí incluye además algunos elementos del concepto económico de comercio como intermediación y lucro, además de que alude al elemento empresa a la que ya nos habíamos referido al analizar el concepto de Joaquín Rodríguez y Rodríguez. Pero una vez más se queda corto al tratar de comprender al acto de comercio, que abarca muchas más cosas.

Para Elvia Arcelia Quintana Adriano debemos considerar como acto de comercio a la “actividad propia del ser humano, manifestada por la voluntad

²⁶ De J. Tena, Felipe. Derecho Mercantil Mexicano. 19ª ed. Porrúa.. México, 2001 p. 22

²⁷ García Rodríguez, Salvador. Derecho Mercantil. 7ª ed. Porrúa. México. 2003. p. 6

²⁸ Citado por Quintana Adriano, Elvia Arcelia. Ob. cit., p. 208

²⁹ Citado por Quintana Adriano, Elvia Arcelia. Ob. cit., p. 209

dirigida a la producción de consecuencias jurídicas. (...) Cuando esta actividad se reduce al marco jurídico de lo que la ley señala como comerciante, y lo enmarca como acto de comercio, estamos hablando de actividades comerciales del Derecho Mercantil³⁰ Esta definición ni siquiera se da a la tarea de definir al acto de comercio; simplemente nos hace pensar que según el criterio de la autora no deberíamos hablar de actos de comercio, si no de actividades comerciales, que incluirían tanto al acto de comercio como al comerciante.

Tal vez se podría aclarar el concepto atendiendo a lo expuesto con respecto al acto de comercio por otros códigos de países con tradición jurídica romanista, como son el España y Alemania. Sobre esto, el Sistema legal español siguiendo la doctrina de Gay de Montellá Langle y otros. En el artículo 2º de su Código de Comercio establece "Serán reputados actos de comercio los comprendidos en este Código y cualesquiera otros de naturaleza análoga"³¹. Dicha aseveración como vemos no define nada, hace una simple prescripción.

En tanto que el Código de Comercio Alemán de 1897, en su artículo 343, expone "actos de comercio son todos los actos de un comerciante que pertenezca a la explotación de la industria mercantil"³² Lo que resulta demasiado amplio, tan amplio (o aun más) como el concepto de empresa como fuente de los actos jurídicos de Joaquín Rodríguez y Rodríguez; además de que ambos conceptos aluden a criterios subjetivos, pues es tan subjetivo decir que el Derecho Mercantil es el derecho de los comerciantes como que acto de comercio es lo que hacen los comerciantes.

Como podemos observar los criterios de definición son muy diversos y atienden a diferentes criterios, consideramos que en general (con las variantes que cada autor introduce en su concepto) hay tres tendencias para tratar de definir al acto de comercio entre los autores anteriormente expuestos: Por una parte están los que delimitan al acto de comercio partiendo de puntos de vista económicos como intermediación, fines de lucro. Otros ven al acto de comercio referido a la empresa y por lo tanto al comerciante. En tanto que los últimos equiparan al acto de comercio al acto jurídico, al que para ponerlo en el nivel del primero le dan consecuencias mercantiles. Lo que sí es de resaltarse es que la mayoría de los tratadistas mexicanos consideran mercantiles a los actos observados como tales por el Derecho Mercantil (que no sólo esta contenido en el Código de Comercio, si no en otros ordenamientos mercantiles) y que producen consecuencias en la realidad jurídica mercantil de nuestra nación.

Por nuestra parte concluimos que el acto de comercio es bastante amplio y complejo como para poder ser delimitado en un concepto de unas cuantas líneas; las figuras mercantiles, como el acto de comercio, son mutantes y intrincadas; podemos allegarnos de ciertas características y criterios que nos sirvan de guía

³⁰ Quintano Adriano, Elvia Arcelia, Derecho Mercantil, Mc Graw-Hill/Interamericanas, México, 1997 p.20

³¹ Garrigues, Joaquín. Curso de Derecho Mercantil, Tomo 1 pág. 143

³² Idem. p. 142

para entenderlo, pero finalmente para saber si un acto puede ser considerado de comercio o no, deberá ser observado particularmente. Por lo que en caso de sernos requerido un concepto al respecto no intentaríamos definirlo, simplemente invocaríamos al hecho de ser observados como tales por el Derecho Mercantil y que producen consecuencias en la realidad jurídica mercantil de nuestra nación.

1.1.2.4 Clasificación

Así como para tratar de definir el acto de comercio, han surgido muchas teorías y controversias, el intento de sistematizar doctrinalmente el contenido del artículo 75°, ha dado pie a otro mar de disertaciones jurídicas. Sin embargo al pretender clasificar el acto de comercio, aunque los criterios no sean universalmente unánimes, si han alcanzado más puntos de acuerdo (por lo menos en la doctrina mexicana) que los dados para definirlo.

En cuanto a los criterios legales; el contenido de estos obedece a lo declarado mercantil por el Código de Comercio y otros ordenamientos análogos.

1.1.2.4.1. Doctrinaria

Sobre los tratadistas mercantiles más reconocidos en el medio internacional podemos decir:

Para los italianos Rocco y Vivante³³ los actos de comercio pueden clasificarse tomando en consideración su "naturaleza intrínseca" o "los actos mercantiles por conexión". En los primeros la intermediación, característica de los actos de comercio se realiza; y los segundos se consideran actos de comercio por ir unidos a los primeros de forma accesoria. Aunque aclaran que dicha clasificación no comprende a todos los actos de comercio planteados en el Código Italiano de 1882.

Arcangelli³⁴, los clasifica en "legales o extrínsecos" y "substanciales o intrínseco". Siendo que son absolutamente comerciales los que la ley determina como tales sin tener en cuenta quien los realice, la finalidad o el modo.

Bolaffio³⁵ a su vez los divide en "actos de mero derecho comercial" y "actos mercantiles por su conexidad con el acto de comercio", Los primeros son parte del Derecho Mercantil cuando se observa una situación preexistente.

Rotondi³⁶ cree que "actos absolutos" y "actos relativos". Los primeros invariablemente son mercantiles, sin considerar fines extrañas al acto mismo.

³³ cf. Quintana Adriano, Elvia Arcelia.Ob. cit., p. 220

³⁴ cf. Mantilla Molina, Roberto L. Ob. cit. p. 61

³⁵ cf. Quintana Adriano, Elvia Arcelia.Ob. cit., p. 221

Mientras que los relativos son aquellos donde un suceso exterior es la razón de la comercialidad; esta a su vez se divide en tres tipos: actos relativos a la forma peculiar del ejercicio, actos relacionados al carácter especulativo del sujetos y actos relacionados con la conexión de otro acto.

En Alemania e Italia, la teoría dominante es la que atiende al carácter intrínseco del acto de comercio, es sobre todo producto de la evolución histórica del concepto de acto de comercio que divide a los actos de comercio en objetivos y subjetivos. Los primeros se consideran mercantiles debido a la naturaleza del acto, independientemente de la persona que lo realiza; y el Segundo son considerados así porque los comerciantes son quienes los realizan

El jurista francés Langle³⁷, habla de los diferentes tipos de actos de comercio. De algunos dice que son actos de comercio por que constituyen un cambio de cosa, otros son actos de que auxilian operaciones comerciales, de cambio y para el cambio. Asimismo hace una enumeración de actos de comercio: los que son considerados tales por mandato de la ley (*juris et de jure*), a los mixtos los llama actos mixtos por intención del agente, y finalmente llama actos accesorios a los que se relacionan o tienen conexión con un acto de comercio.

Para el sistema legal francés existen dos tipos de actos de comercio: los que están enumerados por su Código, que son llamados "actos de comercio por su naturaleza"; y los que se forman por declaración expresa de otras leyes, actos de comercio por accesoriedad, sociedades, letras de cambio, etc., que son los "actos de comercio objetivos". Al respecto del sistema francés diversos doctrinarios del derecho han establecido teorías.

Autores franceses como Boisrel, Thaller y Lyon Caen, así como los españoles Blanco, Constant, Alvarez de Manzano y Bonill³⁸. Postulan que los actos accesorios son los que se conectan de alguna manera con la función comercial, aunque dicha relación sea sólo de carácter económico y no jurídico.

Mientras que Julliot de la Morandiére, Rodière y Houin³⁹, opinan que los actos de comercio por su naturaleza, permiten definir al comerciante, que hace de estos su ocupación cotidiana. En tanto que a los actos de comercio objetivos los llama actos de comercio por su forma, los que a pesar de no ser desarrollados por un comerciante entran a la jurisdicción del derecho mercantil.

Los doctrinarios argentinos. Encabezados por Fontanosa divide a los actos de comercio en: "naturales, aquellos que manejan la interposición en el cambio de mercaderías como la compraventa, o de dinero como la operación bancaria; conexos, tendentes a demostrar en cada caso, como el mandato o presumidos por

³⁶ cf. Felipe de J. Tena. *Ob. cit.* p. 20 y Quintana Adriano, Elvia Arcelia. *Ob. cit.* p. 221

³⁷ cf. Quintana Adriano, Elvia Arcelia. *Ob. cit.* p. 222

³⁸ *Idem* p. 223

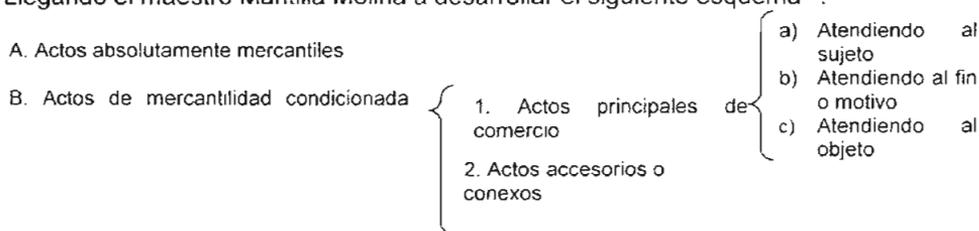
³⁹ *Idem* p. 224

la ley como los actos de los empleados, por disposición de la ley según sean las sociedades anónimas y/o unilaterales.⁴⁰

Los venezolanos que cuentan con un sistema mixto. Lo Objetivo, son las actividades reguladas por el Código de Comercio, y lo Subjetivo, que comprende al comerciante y su actividad reglamentada por el código y en concomitancia se presume el carácter comercial de otros actos. Siendo así que el legislador venezolano toma como mercantiles tanto las obligaciones contenidas en el concepto general de acto de comercio, y las operaciones que tengan relación a ésta.

En nuestro país contamos con varios esfuerzos de clasificación. Entre los más importantes se encuentran los hechos por los maestros Roberto L. Mantilla Molina y Felipe de J. Tena⁴¹, así como el realizado por el Profesor Jorge Barrera Graf.

Los primeros toman como base lo expuesto por el jurista italiano Arcangelli. Llegando el maestro Mantilla Molina a desarrollar el siguiente esquema⁴²:



Siendo que los llamados actos absolutamente mercantiles: Son los que por su naturaleza son considerados como tales, no importando el sujeto que los ejecuta y el fin que busca. Mientras que los actos de mercantilidad condicionada o relativamente mercantiles, dependen de la realización de determinada situación; estas se dividen en principales y accesorios o conexos.

En cuanto a las principales la sistematización atiende al sujeto, al fin o motivo y al objeto. El sujeto será cuando las personas que lo celebren tengan la condición de comerciantes. El fin o motivo dependerá de que el acto implique una intermediación con el interés de obtener un lucro, es decir con la idea de la especulación. Y por el objeto es cuando el acto es considerado de comercio porque la ley así lo dice.

Los actos accesorios y conexos serán aquellos que derivan de un acto absoluto o relativo de comercio.

⁴⁰ Quintano Adriano, Elvia Arecelia. Ob. cit. p. 224

⁴¹ Cf. De J. Tena, Felipe. Ob. cit.

⁴² Mantilla Molina, Roberto L. Ob. cit. p. 60 y s.s.

En tanto el maestro Jorge Barrera Graf⁴³ propone una clasificación basada en dos supuestos: los llamados actos de comercio principales y los actos de comercio por conexión o por accesión.

Los actos de comercio principales son considerados así en función de diversos factores del negocio jurídico; que a saber son: Sujetos, Objeto, Causa y Forma.

La clasificación conforme al Sujeto atiende a criterios de capacidad y consentimiento; es el empresario o comerciante que celebra un acto o participa en un contrato. En cuanto al objeto, se trata del ente materia de la obligación. La Causa, que es la finalidad de la actividad o del acto, en el caso de lo mercantil es la especulación, la organización de una empresa u otro fin de naturaleza comercial; es una de las categorías más amplias. Y finalmente la forma, que es el esquema o tipo elegido para la ejecución de un acto de comercio

Los actos de comercio por conexión o accesión, son aquellos cuya característica de mercantiles depende de su nexa a un acto principal o por ser accesorios de éste.

1.1.2.4.2. Legal

Gran parte de los actos que nuestra legislación considera mercantiles, son los enumerados en el artículo 75° del Código de Comercio Vigente. Pero como mencionamos anteriormente, no son los únicos existentes en el ordenamiento jurídico mexicano. Encontramos más definiciones de actos considerados como mercantiles en leyes como la Ley de Títulos y Operaciones de Crédito, La ley del Mercado de Valores, La Ley Federal de Protección al Consumidor, entre otras. Se añade además de los expresamente señalados están los que "derivan" de estos actos legalmente considerados mercantiles.

Las distintas fracciones del artículo 75, junto con otras normas de materia mercantil, han sido agrupadas por el maestro Rafael de Pina Vara en una tentativa de reunir todos los actos que nuestra legislación llama comerciales. El esquema⁴⁴ considera actos de comercio a:

- a) La Compraventa. Abordada por el artículo 75, fracción II, III y XXIII del Código de Comercio.
- b) La Permuta. Mencionada en el artículo 388 del Código de Comercio.
- c) El Arrendamiento. Visto en la fracción I del artículo 75 del Código de Comercio.

⁴³ cf. Barrera Graf, Jorge. Ob. cit. p. 75 y ss

⁴⁴ De Pina Vara, Rafael. Ob. cit., pág. 23 y ss.

- d) La Cesión. Artículo 389 del Código de Comercio.
- e) La Comisión. Artículo 75 fracción XII del Código de Comercio
- f) La Mediación. Artículo 75 fracción XIII del Código de Comercio
- g) El Préstamo. Artículo 358 del Código de Comercio
- h) El Transporte. Artículo 576 del Código de Comercio
- i) El Depósito. Artículo 75, fracciones XVII y XVIII, y 332 del Código de Comercio y 1° de la Ley de Títulos y Operaciones de Crédito.
- j) Los Seguros. Artículo 75, fracción XVI del Código de Comercio.
- k) El Crédito y la Banca. Artículo 75, fracciones XIV y XXIV de Código de Comercio; y 1°, 259, 267, 276, 288, 291, 302, 311, 317,321, 323 y 346 de la Ley de Títulos y Operaciones de Crédito.
- l) La Prenda Mercantil. Artículo 1° y 334 de la Ley de Títulos y Operaciones de Crédito.
- m) La Fianza. Artículo 12 de la Ley de Instituciones de Fianza.
- n) Títulos de Crédito. Artículo 75, fracciones II, IV, XVIII, XIX y XX del Código de Comercio.
- o) Operaciones Bursátiles. Ley del Mercado de Valores.
- p) Sociedades Mercantiles. Ley General de Sociedades Mercantiles.
- q) Contrato de Asociación en participación. Artículo 253 de la Ley de Sociedades Mercantiles.
- r) Empresas. Artículo 75 fracciones V, VI, VII, VIII, IX y X del Código de Comercio; y 16 de la Ley de Navegación.
- s) Comercio Marítimo. Artículo 75, fracción XV del Código de Comercio; y 95, 98, 106, 110 y 222 de la Ley de Navegación.
- t) Las Obligaciones de los comerciantes y sus empleados y las obligaciones entre comerciantes y banqueros. Artículo 75, fracciones XX, XXI y XXII del Código de Comercio.

El principio analogía que establece en su fracción XXV dicho artículo hace surgir así mismo muchas controversias. Respecto a la analogía, los dos supuestos legales para que esta exista (establecidos por jurisprudencia de la

Suprema Corte): "la falta de expresión de la norma al caso concreto" y "la igualdad esencial de los hechos".

Como mencionamos anteriormente todos estos esquemas y clasificaciones son una buena guía para entender al acto de comercio (que nos parece imposible de definir). Las clasificaciones (legales o doctrinarias) son quizás más claras que los conceptos y definiciones; en cuanto a las doctrinarias adoptariamos para nuestro estudio la hecha por el Maestro Mantilla Molina siguiendo los criterios del jurista Italiano Arcangelli, no por considerarla más o menos valiosa que la del maestro Barrera Graf, si no porque para nosotros resulta la más clara; y en cuanto a las legales consideramos que la clasificación hecha por el maestro Rafael de Pina Vara resulta muy útil para su aplicación en casos prácticos.

1.2 Comercio Electrónico

1.2.1. La Cibernética

Establecimos que la concepción de acto de comercio en parte varía o se amplía con el desarrollo tecnológico humano. Puesto que el Derecho Mercantil debe adaptarse a su contexto histórico y responder a las necesidades que se le plantean. En los últimos tiempos uno de los campos de mayor desarrollo en la comunidad mundial ha sido la tecnología; especialmente la relacionada con las computadoras y las redes.

Dicho desarrollo ha generado nuevas modalidades de expansión comercial, como lo es el comercio electrónico. Con una nueva gama de instrumentos, mecanismos, dispositivos y tecnologías, que hacen necesario emprender una revisión a la legislación comercial existente con el fin de adecuar la actual regulación jurídica para que responda a las necesidades de este nuevo tipo de comercio.

Por lo que para entender al comercio electrónico, sus mecanismos, y a las figuras jurídicas (como la de la **entidad certificadora**) derivadas de éste se hace necesario hacer un repaso a conceptos tecnológicos y un poco de historia que nos auxiliaran en nuestro estudio de las nuevas necesidades jurídicas que las recientes tecnologías traen aparejadas.

El ser humano está lleno de inquietudes, ya vimos a una de ellas que es el intercambio lucrativo, primitivo origen de lo que hoy en día conocemos como comercio. Otra de las inquietudes del ser humano han sido las matemáticas y la filosofía, ambas muchas veces en busca de causas últimas, y en ocasiones de realidades intangibles.

Las búsquedas filosóficas lo han llevado a profundas teorías tratando de explicar el cómo, donde y porque de la realidad conocida. Sus búsquedas

matemáticas lo han llevado a numerosas vertientes entre las que se encuentran las tecnológicas y las complicadas operaciones de cálculo de la actualidad.

Pero en los últimos tiempos han surgido nuevas tendencias que conciben al conocimiento como algo Holístico. Es la llamada Teoría de Sistemas que se auxilia de teorías filosóficas como la epistemología para tratar de dar una explicación global del nuestro mundo, donde todas las ciencias de unen.

De la mano de este enfoque interdisciplinario del conocimiento, han surgido nuevas ramas de la investigación como lo es la cibernética. Esta última vislumbró sus primeras luces en 1942 con motivo de un congreso de inhibición cerebral celebrado en Nueva York, del que se tomó la idea de que la colaboración entre fisiólogos y técnicos en mecanismos de control podría rendir grandes frutos.

Se trataban de buscar las causas mediante las cuales la información se transforma en la actuación deseada. Se vio impulsada por la Segunda Guerra Mundial (tristemente grandes invenciones humanas son impulsadas por necesidades bélicas) donde se hacían necesarios cerebros electrónicos y mecanismos de control automático para equipos militares.

Para 1948 Norbert Wiener le da nombre a esta retroalimentación entre las ciencias: "Cibernética". La denominación la toma del griego "kybernes" que significa timonel o pilotear un navío; aunque dicha palabra también fue utilizada por Platón en la República como "arte de dirigir a los hombres" o "arte de gobernar". Pero está claro que para Wiener la cibernética es la ciencia que trata de los sistemas de control y comunicación entre animales y máquinas, según su obra: "Cybernetics, or control and communication in the animal and machine". La Cibernética estudia y aprovecha los mecanismos comunes entre las máquinas y los seres vivos.

Y eso es lo que hace la Cibernética; contempla a la comunicación y el control de los organismos vivos y las máquinas por igual. Por lo que para obtener determinada respuesta ya sea de un ser vivo o bien de una máquina, es necesario proporcionarle la información correspondiente a los resultados reales de la acción prevista. En los seres humanos dicha información es ordenada por el cerebro y el sistema nervioso, lo que nos permite determinar la conducta a seguir. En el caso de las máquinas los mecanismos de autocorrección y control hacen las veces del cerebro y del sistema nervioso humano. Este principio recibe el nombre de retroalimentación (feedback), base fundamental de la automatización.

La cibernética como ya lo mencionamos, alude a la información y a nuestra concepción del conocimiento. Este último ha sido muy cuestionado recientemente por la epistemología o teoría del saber. El antiguo método científico propuesto por Descartes basado en la observación, ha sido confrontado por la aseveración de que las propiedades de los objetos no son otra cosa, más que simples construcciones mentales, y su existencia está subordinada a la observación del

individuo. Dicho enfoque filosófico llamado constructivismo se proyecta en las concepciones cibernéticas de los objetos.

Para la cibernética la información es estadística y se mide de acuerdo a las leyes de la probabilidad. "La información es concebida como una medida de la libertad de elección implícita en la selección. A medida que aumenta la libertad de elección, disminuye la probabilidad de que sea elegido un determinado mensaje. La medida de la probabilidad se conoce como entropía."⁴⁵ Según la segunda ley de la termodinámica en los procesos naturales existe la tendencia la desorganización o el caos. Por lo que atendiendo a los principios de la cibernética el desorden es lo más probable y el orden lo menos. Es ahí donde entran los mecanismos de control; como medios para mantener el orden en las conductas intencionadas de las máquinas y las personas; contrarrestando su tendencia natural al desorden.

Además de Wiener otros científicos han hecho importantes aportes a esta ciencia. Como John von Neumann, Warren McCulloch y Claude Shannon. Neumann hizo importantes contribuciones a la cibernética en su división informática; Shannon sentó las bases teóricas para el desarrollo de las telecomunicaciones digitales (entre ellas Internet); mientras que McCulloch colocó los cimientos de la actual orientación de la cibernética al llamarla "ciencias cognitivas".

El desarrollo y aplicación de la cibernética en las décadas de los 50 y 60 permitió el desarrollo de las máquinas, ampliando sus potenciales a niveles tales como: la robótica, máquinas lavadoras, puertas automáticas, la informática, la inteligencia artificial; y el Internet. También ha prestado auxilio a la biología, psicología, la economía, la ingeniería de sistemas, los sistemas sociales y la neurofisiología; pero el desarrollo en éstos campo ha sido más lento.

1.2.2. La Informática

El término informática o computación puede ser utilizado indistintamente. Computación procede del Inglés y se alude a la realización de cálculos, mientras que Informática proviene del francés y apunta al procesamiento de información. A pesar de los razonamientos etimológicos la diferencia de aplicación radica (como otros términos computacionales) en la zona geográfica donde nos encontremos. En Latinoamérica por influencia estadounidense es más utilizado el término computadora y en España se aplica más el de Informática. No obstante la tarea esencial de las computadoras no es el cálculo, sino el procesamiento de información.

⁴⁵ Cibernética. Enciclopedia Microsoft Encarta, 2002

En general podemos decir que es la ciencia que se encarga del tratamiento automatizado y racional de la información por medio de computadoras o ordenadores.

Al emplear computadoras para sus fines, las estudia profundamente. Las examina desde simples aspectos de diseño, utilización y funcionamiento hasta aspectos como la robótica y la inteligencia artificial. Para conseguir sus fines se vale de aspectos teóricos y prácticos de la ingeniería, electrónica, teoría de la información, matemáticas, lógica y comportamiento humano.

1.2.2.1 La Computadora

1.2.2.1.1. Antecedentes Históricos

Las primeras operaciones de cálculo entre los seres humanos se realizaban con los dedos y la memoria, y solo se trataba de conteos de animales, pertenencias, objetos de caza, etc. Con este propósito civilizaciones antiguas como los mayas y árabes, entre otros desarrollaron sistemas de cálculo.

Aproximadamente en el 830 D.C., el matemático árabe Al'Khwarizmi, escribe un libro de Aritmética, donde presenta el sistema numérico indio y los métodos para calcular con él. Dicho libro sería traducido al latín como Algoritmi de numero Indorum. De dicha versión latina proviene la palabra algoritmo.

Con el paso del tiempo las comunidades humanas aumentaron su tamaño, organización social y comercio. En consecuencia los cálculos requeridos por dichas comunidades se hacen cada vez más complicados, por lo que los seres humanos se ven en la necesidad de auxiliarse de artefactos que los ayuden en el desempeño de sus funciones dentro de su grupo.

Uno de los primeros dispositivos auxiliares del cálculo humano fue el ábaco. Su nombre proviene del vocablo griego abakos, que quiere decir superficie plana. Los más antiguos vestigios de la utilización de éste se encuentran en las civilizaciones griega y romana, alrededor del año 4000 a.C. Es un artefacto en realidad simple. Cuenta con varias cuentecillas engarzadas en varias barras engastadas en un marco rectangular. Al deslizar las cuentecillas sobre las barras, su colocación simboliza valores almacenados, así, por medio de diversas posiciones se pueden representar y almacenar datos. No lo podemos considerar una computadora, ya que carece de uno de los elementos fundamentales de dichos dispositivos, que es el programa.

Otro mecanismo utilizado por los antiguos para calcular fue el Dispositivo de Antikythera, construido por el 80 a.C. en la isla de Rodas. Se utilizaba para cálculos astronómicos de precisión. Era tal su sofisticación que algunos la han llamado "la primera computadora de occidente". Con la ayuda de una perilla se

accionaba un simulador miniatura del desplazamiento de la luna, el sol y algunos planetas, obteniendo como resultado la fecha que daría tal combinación

Los siguientes intentos del ser humano por poner orden lógico a su realidad cotidiana serían las tablas de logaritmos de John Napier en 1614 y las reglas de cálculo de 1630. Pero la idea de la creación de una máquina capaz de realizar complejas operaciones matemáticas seguiría latente en los seres humanos.

Ya Leonardo Da Vinci (1452-1519) se había planteado la idea de crear una sumadora mecánica, pero sería el científico francés Blaise Pascal (1623 – 1662), quien vendría a cristalizar estos esfuerzos, con la invención de la llamada "Pascalina" en 1642, a la que se considera la primera máquina semiautomática construida por el hombre. Media lo mismo que una caja de zapatos, dentro de ella se encontraban ruedas dentadas que unidas entre sí formaban una cadena de transmisión. Su funcionamiento consistía en datos representados mediante la posición de engranajes, "las ruedas representaban el sistema decimal de numeración; cada rueda constaba de diez pasos, para lo cual estaba convenientemente marcada con números del 0 al 9. El número total de ruedas ascendía a ocho, distribuidas de la siguiente manera: 6 ruedas para representar los números enteros, y 2 ruedas más en el extremo derecho para indicar dos posiciones decimales. Con esta disposición se podía manejar números entre 0.01 y 999,999.99. Para sumar o restar, se hacía girar una manivela en el sentido apropiado, con lo que las ruedas corrían los pasos necesarios"⁴⁶. Las cantidades se insertaban de modo manual esto hacia que se establecieran las ubicaciones finales de las ruedas, tal y como leeríamos el cuentakilómetros de un automóvil.

La máquina fue altamente apreciada en Europa, pero su alto costo (para ese entonces los cálculos aritméticos manuales eran mucho más baratos) y el hecho del que el único capaz de repararla fuera el propio Pascal, la hicieron inservible. Aun así hubo algunos intentos por mejorarla, entre los que se encuentran el del filósofo y científico alemán Gottfried Wilhelm von Leibniz (1646 – 1716), quién tras estudiar el dispositivo de Pascal construyó su Calculadora Universal, capaz además de sumar y restar, de dividir un multiplicar. Del mismo modo, Leibniz crea el sistema binario, que en un futuro se convertirá en el lenguaje de las computadoras.

En 1804 Joseph Marie Jacquard (1753-1834), un fabricante textil, diseña un telar que descifraba tarjetas de papel rígido perforadas que contenían información. Pudiendo con esto reproducir automáticamente patrones de tejido

Para 1834 Charles Babbage (1793-1871), un profesor de Cambridge, apoyado por el gobierno Británico, había diseñado una máquina de diferencias capaz de solucionar los problemas que generaban la elaboración de las engorrosas tablas matemáticas, mediante la realización de sumas repetidas (un

⁴⁶ <http://concytec.gob.pe/fanning/pc/tiempo.htm>

gran adelanto para el hardware computacional). Trabajaba en el mejoramiento de dicho dispositivo cuando se enteró de la invención de Jacquard.

Decide entonces emprender un proyecto aun más ambicioso: el de la máquina analítica (que de haberse ejecutado hubiera sido la primera computadora de aplicación general), la cual se podría programar mediante tarjetas perforadas, para realizar cualquier cálculo con una precisión de 20 dígitos, a una velocidad de 60 sumas por minuto. En 1843, Lady Ada Augusta Lovelace, sugirió la preparación de diversas tarjetas perforadas para dar instrucciones a mecanismo de Babbage, con el fin de que repitiera ciertas operaciones. Gracias a ésta sugerencia algunos consideran a Lady Ada la primera programadora. Pero la escasa tecnología de la época y los grandes requerimientos del diseño no permitió ver realizado su proyecto que hubiera adelantado cien años la tecnología.

El siguiente avance en el campo de las computadoras obedecería más a una necesidad inmediata que a profundos razonamientos humanos. El Censo estadounidense de 1880 no pudo ser completado sino hasta 1888; la oficina encargada del censo concluyó que ante tal panorama el censo de 1890 necesitaría de más de diez años para poder completarse. Por lo que se vieron en la necesidad de nombrar a un especialista para que encontrara la solución a éste problema. Existía un experto en estadística llamado Herman Hollerith, quien había desarrollado un sistema de procesamiento de datos basado en tarjetas perforadas y una máquina tabuladora de tarjetas perforadas. Contrario a lo que podría pensarse su sistema no estaba basado en las ideas de Jacquard, si no en un sistema de identificación de pasajeros a través de perforaciones ideada por los empleados ferroviarios.

La aplicación de la máquina para el procesamiento automático de los datos del censo resulto ser un éxito; pudiendo ser completado en menos de tres años y con un tremendo ahorro económico. El éxito alcanzado por Hollerith en tal empresa lo catapulto a la fama, tanto que decidió fundar la Tabulating Machine Company. Sus productos fueron vendidos en muchos países. En Rusia su máquina fue utilizada para el censo ruso de 1897.

No obstante, para el censo de 1910, el sistema de Hollerith fue reemplazado por uno desarrollado por James Powers. En 1911 James Powers constituyó la Power's Tabulating Machine Company, convirtiéndose en el principal competidor de Hollerith. Éste en lugar de luchar, decide unirse a Powers y juntos constituyen la Computing Tabulating Recording Company.

Una nueva innovación sería presentada en 1919 por la compañía, que presenta la primera impresora/listadora (antes de esto los datos obtenidos de la tabuladora debían recolectarse a mano). Para 1924 la empresa cambia de denominación para llamarse International Business Machines Corporation (IBM). Que sería la compañía líder en el procesamiento de datos con tarjeta perforada. Y posteriormente se convertiría en una de las primeras compañías de computadoras electrónicas.

A lo largo de los treinta, cuarenta, cincuenta y sesenta las máquinas que utilizaban tarjetas se desarrollarían y perfeccionarían, llegando a generarse alrededor de una máquina electromecánica de contabilidad (EAM) electromechanical accounting machine, toda una industria de procesamiento de datos que consumía gran cantidad de empleados y dispositivos auxiliares (la perforadora de tarjetas, el verificador, el reproductor, la perforación sumaria, el intérprete, el clasificador, el cotejador, el calculador y la máquina de contabilidad). Al procesamiento a través de tarjetas perforadas, también se le conocería como Procesamiento de Registro Unitario: una tarjeta, un registro.

Pero las mentes matemáticas del mundo seguían inquietas. En el Congreso Internacional de Matemáticas de París en 1900. David Hilbert (1862 –1943) pronunció una conferencia sobre problemas matemáticos, en la que trataba de 23 problemas de matemáticas estaban sin solución.

Cuestiones como ¿es la matemática completa? y ¿es la matemática consistente? Fueron resueltas por el matemático Kurt Gödel (1906 –1978) en 1931, quien demostró que cualquier sistema formal suficientemente potente es inconsistente o incompleto.

Otras como la entscheidungsproblem. Es decir ¿hay un método definido que pueda aplicarse a cualquier sentencia matemática y que nos diga si esa sentencia es cierta o no? O mejor dicho ¿son las matemáticas decidibles?. Tuvieron varias réplicas.

Alan Turing (1912 –1954) en 1936 escribió un artículo a propósito de ésta titulado On Computable Numbers. Construyó un modelo de computador (la máquina de Turing) para demostrar que había problemas que la máquina era incapaz de resolver. Mientras que en Estados Unidos Alonzo Church, tratando de resolver la misma pregunta creó el cálculo lambda, que se basaba en la notación formal y trataba de convertir todas las fórmulas matemáticas a una forma estándar.

El ingeniero alemán Konrad Zuse (1910 –1957), retoma los resultados de Church y con base en éstos, entre 1936 y 1941 diseñó y construyó varios computadores electromagnéticos binarios (del Z1 al Z3). Pero dichas computadoras nunca tuvieron gran difusión, ya que el entonces gobernante régimen nazi nunca confirmó los trabajos de Zuse.

Para 1938, Claude Shannon (1916 -) probó que las operaciones booleanas elementales, se podían representar por medio de circuitos conmutadores eléctricos, y la conjunción de circuitos permitía representar operaciones aritméticas y lógicas complejas. Al mismo tiempo demostró que el álgebra booleana podía utilizarse para simplificar los circuitos conmutadores.

1.2.2.1.2. Las Generaciones

Existen muchas controversias acerca de la quien fue el primero en desarrollar la computadora digital electrónica. Algunos consideran que atribuirle el desarrollo de la máquina a una sola persona es absurdo; ya que la miran más como un producto de las investigaciones de todos los científicos en este campo; que como el producto de una mente o un equipo en solitario. Pero la mayoría de las fuentes coinciden en señalar a John Atanasoff y Clifford Berry como los creadores de la que se considera la primera computadora.

Entre los años 1937 y 1942 el Dr. Atanasoff, catedrático de la Universidad Estatal de Iowa (Iowa State College – E.U.A.) junto con un estudiante graduado Clifford Berry, trabajaron en el desarrollo de la primera computadora. Al producto de su investigación la llamo la computadora Atanasoff-Berry o ABC (Atanasoff Berry Computer)

Pero los descubrimientos hechos por Atanasoff y Berry (cuyas investigaciones se realizaron en secreto) se verían apocados durante muchos años por el desarrollo de ENIAC (Electronic Numerical Integrator and Computer) en 1946. Al que durante mucho tiempo se le considero la primera computadora, hasta 1973, cuando una decisión de la Suprema Corte Estadounidense acabo con la patente de éste dispositivo reconociendo la prelación de la ABC sobre ENIAC

En Europa también hubo investigaciones importantes en el terreno de las computadoras. Durante la Segunda Guerra Mundial (1939 –1945), en Londres (Bletchley Park), un grupo de matemáticos y científicos trabajaban en el desarrollo de la primera computadora digital totalmente electrónica. Sus esfuerzos rindieron fruto hacia 1943, con la creación de Colossus. Ésta computadora empleaba 1.5000 tubos de vacío o válvulas. Su principal función fue descodificar los mensajes de radio cifrados por los alemanes.

La Segunda Guerra Mundial también hizo apresurar el desarrollo de la tecnología en los Estados Unidos. ENIAC, de la que hablamos anteriormente, fue creada originalmente para calcular tablas de trayectoria para el gobierno de los Estados Unidos. Para su desarrollo, los científicos a cargo del proyecto: el Dr. John W. Mauchly y J.Presper Eckert, Jr. Platicaron con el Dr. Atanasoff, repasaron sus apuntes sobre la ABC y la examinaron personalmente. La máquina tardó en desarrollarse 30 meses, finalmente salió a la luz en 1946, una computadora electrónica completamente operacional a gran escala.

La máquina pesaba 30 toneladas, ocupaba un espacio de 450 metros cuadrados (todo el sótano de la Universidad de Pennsylvania), contenía 18,000 bulbos y llenaba un cuarto de 12m por 6 m. Su programación era manual y terriblemente lenta (llegaba tardar semanas encargar un programa), por medio de tres tableros con más de 6000 interruptores. Para su operación 200 KW de energía eléctrica y todo un sistema de aire acondicionado para su enfriamiento.

Operaba con un sistema decimal y podía realizar cinco mil operaciones aritméticas por segundo.

Al equipo que desarrolló esta máquina con apoyo del departamento de Defensa, se unió el ingeniero y matemático húngaro John von Neumann (1903 – 1957) quien había publicado un artículo en 1946 en colaboración con Arthur W. Burks y Herman H. Goldstine que hablaba del almacenamiento de programas (Preliminary Discussion of the Logical Design of an Electronic Computing Instrument). Dicho concepto permitía la lectura de un programa dentro de la memoria de la computadora, para posteriormente ejecutar las instrucciones de dicho programa sin necesidad de ser escritas nuevamente. La coexistencia de datos e instrucciones, idea tan fundamental para las computadoras de nuestros días, hace que muchos consideren a von Neumann padre de las computadoras.

Estas ideas dieron como resultado una nueva computadora: la EDVAC (Electronic Discrete Variable Automatic Computer = Computadora Automática de Variable Discreta). En ésta los datos y las instrucciones se compenetraban, la computadora podía ser programada por medio de un lenguaje, sustituyendo a los antiguos alambres que por medio de electricidad interconectaban varias secciones de control. La máquina tenía 4000 bulbos y su memoria se basaba en tubos llenos de mercurio por donde circulaban señales eléctricas. Dicha memoria la liberaba de las limitaciones de velocidad impuestas por el lector de cintas de papel.

Para 1944 un equipo de científicos capitaneado por Howard H. Aiken, con apoyo de IBM, crea en la Universidad de Harvard la Mark I. Su nombre oficial era Automatic Sequence Controller Calculator (ASCC). Muchos no la consideran computadora electrónica ya que no era de propósito general y su funcionamiento estaba basado en unos dispositivos electromecánicos para regular y dirigir la corriente de un circuito, llamados relevadores o relés.

Tenía un aproximado de 700,000 relés, trabajaba con un código decimal, ejecutaba las cuatro operaciones básicas, con una velocidad que podía multiplicar dos números de once cifras en dos segundos y dividía en cuatro segundos. La memoria se dirigía de modo manual por una serie de interruptores, las instrucciones se introducían a través de cintas perforadas. Los resultados se obtenían a través de dos listadoras/impresoras o directamente a la cinta perforada. Pesaba 10 toneladas.

La historia de las computadoras es realmente corta, no han pasado muchos años desde que las primeras aparecieron. Por lo que medir la historia de éstas en décadas o años es algo absurdo. En consecuencia se ha tomado a los avances tecnológicos en ellas como paradigma para medir su historia; sus avances se miden en generaciones. Y para que se de un cambio de generación debe haber un desarrollo, ya sea en sus características constructivas (hardware) o los programas con los que opera (software). Se habla de la existencia de cuatro generaciones y una quinta en desarrollo.

Como ya hemos visto en la Primera Generación, las computadoras se servían de bulbos de alto vacío como factores esenciales de sus circuitos internos; el uso de dichos bulbos las hacía demasiado grandes; eran programadas a través del lenguaje de máquina (donde el programa debía escribirse mediante un conjunto de códigos binarios) por medio de tarjetas; consumían gran cantidad de energía y producían mucho calor; además de ser lentas, con poca capacidad de almacenamiento y no muy confiables. Además eran terriblemente costosas

Entre las más famosas de esta época están las ya mencionadas: Mark I (1937 –1944), Eniac (1943 –1945) y Edvac (1945 –1952); Así como la Univac (1951) y otras de las que hablaremos más adelante.

El equipo formado por el Dr. John W. Mauchly y J. Presper Eckert, Jr. que creara la ENIAC. Permaneció unido y fundó una compañía privada (Universal Computer) que construiría y sacaría al mercado público la UNIVAC I, cuyo primer cliente fue la oficina del Censo Estadounidense de 1950. Tenía mil palabras de memoria central y podía leer cintas magnéticas.

La IBM, que como vimos anteriormente era la encargada de suministrar máquinas de procesamiento de datos a dicho departamento, al verse desplazada de su posición (a pesar de seguir siendo exitosa con otros clientes) comienza a construir computadoras electrónicas. La primera sería la IBM 701 en 1953, que fue regularmente exitosa en el mercado (se vendieron 18 unidades entre 1953 y 1957).

La competencia directa de la 701 de IBM, sería el modelo 1103 de la compañía Remington Rand. La IBM trató de contraatacar con un nuevo modelo (la IBM 702), pero éste presentaba problemas de memoria, por lo que pronto salió del mercado.

Para 1954 fue sustituida por la IBM 650 a diferencia de la anterior fue todo un suceso en el mundo de la informática; ya que incorporaba un novedoso mecanismo de almacenamiento de memoria secundario llamado tambor magnético (antecedente directo del disco magnético). Resultó ser la computadora más exitosa de la primera generación (se vendieron a unas 100)

Para mediados de los cincuenta las computadoras habían sido aceptadas por compañías privadas y gobiernos (únicos capaces de costear el gasto que implicaban). IBM y Remington dominaban el mercado; algunos de los modelos de principios de la primera generación y finales de la segunda serían: la UNIVAC 80, 90 y 1105; y la Burroughs 220.

La segunda generación de computadoras vendría de la mano con el cambio de componentes. Los bulbos serían sustituidos por los transistores, así como nuevas memorias de ferrita; los avances en software también son de resaltar.

Dichos descubrimientos atacaron directamente a las desventajas de tamaño, memoria y gaste energético; aumentando las ventajas enormemente. Algunas de las computadoras de ésta generación fueron: la TRADIC, de los Laboratorios Bell en 1954, la TX-0 del laboratorio LINCOLN del MIT (Instituto Tecnológico de Massachusetts), las IBM 704, 709 y 7094, la Philco 212 (esta compañía se retiró del mercado en 1964) y la UNIVAC M460, la Control Data Corporation modelo 1604, seguida por la serie 3000, la National Cash Register presento el modelo NCR 315 (para uso comercial). La Radio Corporation of America presentó el modelo 501, que operaba con el lenguaje COBOL, para procedimientos administrativos y comerciales. Después apareció en el mercado la RCA 601.

En 1947 John Bardeen, Walter Brattain y William Shockley inventan el transistor y reciben el premio Nobel de física en 1956 por este descubrimiento. El transistor contiene un material semiconductor (regularmente silicio), que es capaz de cambiar su estado eléctrico. En estado normal el semiconductor no es conductivo, pero al aplicársele un determinado voltaje se hace conductivo y la corriente eléctrica fluye a través de éste, tal como un interruptor eléctrico lo haría.

Los transistores hicieron a las computadoras producir menos calor, más rápidas y pequeñas. Sembrando el camino a los posteriores microprocesadores. En contra posición a las máquinas que se hacían más pequeñas aparecen las supercomputadoras, llamadas así por ser más potentes que sus contemporáneas; estaban diseñadas para cálculos de aplicaciones científicas. Entre ellas estuvieron el Livermore Atomic Research Computer (LARC) y la IBM 7030.

Gran parte de estas computadoras se programaban a través de cintas perforadas, otras más a través de cableado en un tablero. Los programas eran diseñados a la medida por un grupo de expertos. No eran fáciles de usar, ya que se requería saber programarlas para lograr resultados, y era difícil que alguien quisiera dedicarse a programar, correr el programa y verificando los errores o bugs existente. Además de tener que guardar el programa resultante en una grabadora de cassette para no perderlo (porque no había discos flexibles). Empleaban redes de núcleos magnéticos para el almacenamiento primario. Los mencionados núcleos tenían diminutos aros de material magnético, vinculados entre sí, en los que se podían guardar datos e instrucciones. El beneficiario final de la información no estaba en contacto directo con las computadoras.

Pero esto cambia en 1951, Grace Murray Hooper (1906-1992) da a conocer los primeros rudimentos de los compiladores, llegando a desarrollar más tarde el COBOL. Aunque sería John Backus, en 1957, quien crea el primer compilador para FORTRAN. Los avances no paran y en 1958, John MacCarthy presenta el LISP (un lenguaje abocado a la ejecución de usos en el medio de la Inteligencia Artificial) Casi al mismo tiempo, Alan Perlis, John Backus y Peter Naur conciben el lenguaje ALGOL.

Dichos lenguajes (llamados de alto nivel) cambian la forma de comunicarse con las computadoras para siempre. Junto a estos nuevos lenguajes hacen su aparición programas procesadores de palabras, hojas de cálculo, entre otros (Word Star, spreadsheet, Visicalc, etc). A partir de entonces el hardware y el software intentarían ir de la mano en adelantos. Estos adelantos hacen que el usuario promedio de las computadoras cambie; de estar totalmente ajeno a ellas pasará a ser el objeto a satisfacer a la hora de crear las nuevas tecnologías (la interface humana). A partir de entonces los nuevos hardware y software buscaran por su comodidad y mejor desenvolvimiento. Pero aún faltaba mucho camino por recorrer.

De la mano de los avances técnicos están los teóricos. El famoso Alan Turing que con sus teorías ayudara al desarrollo de las computadoras de la primera generación; para 1950 publica un nuevo artículo Computing Machinery and Intelligence en la revista Mind, donde presenta el Test de Turing. Los razonamientos de Turing desatan un interés en la investigación y filosofía de la inteligencia artificial.

Aunque el personaje más importante en el desarrollo y análisis de algoritmos sería Edsger Dijkstra (1930-), que en 1956, saca a la luz pública dos algoritmos trascendentales: el algoritmo para la determinación de los caminos mínimos en un grafo, y el algoritmo del árbol generador minimal. Y como siempre sucede en el campo de la ciencia, el aporte de Dijkstra es semillero de nuevas teorías. Para 1961, N. Brujin presenta la notación O, la cual sería metodizada y extendida por D. Knuth. Siguen los avances y en 1957, hace su aparición la Programación Dinámica de R. Bellman. Para 1960, S. Golomb y L. Baumet exponen "las Técnicas Backtracking para la exploración de grafos". Y en 1962 son divulgados los primeros algoritmos: el *QuickSort* de Charles Hoare y el de la multiplicación de grandes enteros de A. Karatsuba e Y. Ofman. (Del tipo Divide y Vencerás).

Las computadoras de esta generación aun eran caras (pero no tanto como las de la primera), no obstante, fueron utilizadas por las empresas para el manejo de inventarios, contabilidad y nominas. Mientras que el Gobierno Estadounidense las utilizó para crear el primer simulador de vuelo. Las grandes compañías de computación de ésta generación fueron: la ya presente IBM, Burroughs, Univac, NCR, CDC y HoneyWell (mejor conocidos por sus siglas como el BUNCH)

El siguiente descubrimiento importante en el campo de la informática lo haría Jack Kilby (1923-) en 1959, cuando expone a la opinión pública y científica del mundo el primer circuito integrado monolítico. Compuesto de una serie de transistores interconectados con resistencias, en una minúscula pastilla de silicio y metal, llamada chip. Con este descubrimiento una vez más las computadoras disminuirían su tamaño, se harían todavía más rápidas, veloces y de menor costo. Con el paso del tiempo mayor número de transistores serían colocados dentro de un chip, haciendo a las computadoras más y más pequeñas.

La aparición de los circuitos integrados, junto con adelantos en comunicación usuario –máquina (los lenguajes de control de los sistemas operativos) marca el inicio de la siguiente generación de computadoras: la tercera generación.

El Circuito Integrado permite ensanchar la flexibilidad de los programas y estandarizar los modelos. La computadora se había hecho tan veloz que podía al mismo tiempo realizar operaciones numéricas de administración, y procesar archivos. Es decir, correr más de un programa a la vez (multiprogramación). Además los nuevos modelos de computadoras eran escalables, podían crecer y seguir corriendo sus antiguos programas.

El Circuito es un gran adelanto para el hardware, mientras que para el software, las computadoras se seguirán programando con los lenguajes de alto nivel, pero se establece un método de comunicación con el programador (una interfaz) conocida como sistema operativo.

En el ámbito comercial las computadoras que reflejan estos adelantos técnicos son: la serie 360 de IBM (que acapara casi el 70% del mercado) con los modelos 20, 22, 30, 40, 50, 65, 67, 75, 85, 90, 195. Respecto al hardware se valían de sistemas especiales del procesador, paquetes de discos magnéticos, unidades de cinta de nueve canales, entre otras utilidades (las aplicaciones variaban en cada modelo). En cuanto al software contaban con un sistema operativo llamado OS, que incluía diversas configuraciones; así como varias técnicas para el manejo de memoria y del procesador.

Contemporánea de la serie de IBM están: la SOLOMON creada por la Westinghouse Corporation y la ILLIAC IV, concebida en conjunción por Burroughs, el Ministerio de Defensa de los E.U.A. y la Universidad de Illinois.

Para 1964, Seymour Cray (1925-1996) presenta la serie 6000, con la computadora 6600, que podía efectuar un millón de operaciones por segundo (la más rápida de su tiempo). Pero se supera a sí mismo en 1969 con el modelo CDC 7600, diez veces más rápida que la anterior gracias a la inclusión de un procesador vectorial.

En cuanto a avances tecnológicos, uno de los logros más destacados de ésta generación fue el desarrollo del lenguaje PASCAL por el profesor de Ciencias de la Computación Niklaus Wirth y el artículo Fuzzy Sets del profesor de la Universidad de Berkeley que versa sobre la Teoría de Control o la Arquitectura de Computadores, que revoluciona el campo de la Inteligencia Artificial.

Para principios de los setentas. IBM lanza una nueva serie: la 370, que incluía los modelos: 115, 125, 135, 145, 158 y 168. Mientras que UNIVAC rivaliza con los modelos 1108 y 1110, que son máquinas en gran escala. En tanto que CDC produce la serie 7000 con el modelo 7600. Las características primordiales de éste grupo de computadoras son la potencia y la velocidad.

La compañía Intel (famosa hasta nuestros días) presenta el primer microprocesador en 1971: el 4004, que podía procesar 4 bits de datos a la vez. Estaba formada por 2300 transistores interconectados, soldados sobre un único sustrato de silicio, capaces de realizar 60,000 operaciones por segundo. Contaba con su propia unidad lógicoaritmética, dos chips de memoria y su propia unidad de control. Pero pronto se vio sustituido por el modelo 8008, también de Intel, capaz de procesar el doble de datos que el 4004.

Dicho microprocesador es posible gracias a las tecnologías de integración a gran escala (LSI acrónimo de Large Scale Integrated) y de integración a muy gran escala (VLSI acrónimo de Very Large Scale Integrated). Por medio de las cuales procesadores muy complicados podían colocarse dentro de un diminuto chip. Dichas tecnologías hacen posible la aparición en el mercado de las minicomputadoras o computadoras de tamaño mediano, que son mucho menos costosas que las grandes o mainframes, pero igual de útiles. Algunos de los modelos más conocidos fueron: la VAX (Virtual Address eXtended), la PDP - 8 y la PDP - 11 de Digital Equipment Corporation; la NOVA y ECLIPSE de Data General, la serie 3000 y 9000 de Hewlett - Packard con los modelos el 36 y el 34; la Wang y Honey - Well -Bull; la alemana Siemens; la inglesa ICL y la rusa US (Sistema Unificado, Ryad).

Y para fines de la década IBM produce nuevos modelos para la serie 370: 3031, 3033, 4341. Al tiempo que Burroughs compite los modelos 6500 y 6700 de su serie 6000, que finalmente son remplazadas por la serie 7000. En tanto que Honey -Well con varios modelos de su DPS.

Hasta ese entonces las computadoras se habían visto restringidas a los campos de los organismos gubernamentales, militares, a las universidades y a las grandes empresas. Pero a partir de éstos cambios, que las hicieron más rápidas, pequeñas y baratas, el campo de aplicación y el mercado de las computadoras se amplió enormemente.

Llega entonces la cuarta generación con los microchips (microcircuitos integrados en plaquetas de silicio), los microprocesadores, la integración a larga escala (LSI) y la búsqueda de la miniaturización de los componentes. Estos adelantos hacen posibles las primeras microcomputadoras mucho más pequeñas y baratas. Nacen entonces las computadoras personales que poco a poco van inundando los hogares modernos.

Una de las primeras (o la primera para algunas fuentes) microcomputadora fue la Altair 8800 (que aparece en la portada de Popular Electronics), producida por la compañía Micro Instrumentation and Telemetry Systems (MITS) cuyo precio realmente bajo (397 dólares) la popularizó en el mercado.

Aunque requería conocimientos en programación para poder ser utilizada, pues empleaba lenguaje de máquina y tenía 256 bytes de memoria. En búsqueda

de una forma de hacer a la Altair más fácil para el usuario; MITS compra el software Basic a sus creadores William Gates y Paul Allen. El software es un éxito, por lo que Allen y Gates crean una empresa dedicada solo al software a la que llaman Microsoft.

Por su parte Steven Wozniak y Steven Jobs, casi al mismo tiempo que Allen y Gates, también inspirados en la Altair (a la que sólo habían visto en una revista), para 1976 construyen la Apple I, a la que deciden comercializar por si mismos; Para lo cual el 1 de abril de 1976 fundan Apple Computer, Al año siguiente lanzan la Apple I, que es tan exitosa que Apple Computer se convierte en la segunda compañía más importante del mercado. Algunas de las innovaciones que incluye la Apple II son armazón de plástico y gráficos a color.

En 1981, IBM lanza un nuevo modelo y filosofía al mercado: la IBM Personal Computer, por medio de la cual pretendían que las computadoras antes relegadas a empresas y universidades se integren totalmente al hogar como un componente más del menaje casero.

La máquina contaba con un procesador Intel (el 8088), 16 kb de memoria (escalable a 256) y un sistema operativo creado por la Microsoft de Allen y Gates; el famoso MS-DOS, Microsoft Disk Operating System, que la hacía más fácil de usar y le proporcionaba mejores gráficos. Esta computadora será posteriormente conocida como la PC-XT, y le seguirán otras series, también de IBM, como AT (de 1984 con el procesador Intel 80286) y PS/2 (de 1988 con el procesador Intel 80386).

Para 1984, Apple saca un nuevo modelo a mercado: la Macintosh, que contaba el primer Mouse (o ratón) y una interfaz gráfica para el usuario. La facilidad con la que podía ser operada la hizo muy popular en el mercado.

Las computadoras empiezan a venderse por millares a partir de entonces.

Para 1991 surgen los microprocesadores de alto rendimiento. Varias empresas lanzan sus modelos: Intel el 80486, Motorola el 68040, y la alianza de Apple, IBM y Motorola crea el Microprocesador Power PC (Performance Optimization With Enhanced RISC PC)

En 1993 Intel presenta el procesador 80586, conocido como Pentium, que inicia la serie Pentium I, II, III y (hasta el momento de ser escrita esto) IV

Actualmente los circuitos integrados pueden contener apartados completos de la computadora (alguna vez toda), independientemente de los medios de almacenamiento y comunicación.

A la par de las microcomputadoras, las minicomputadoras y los grandes sistemas continúan desarrollándose; sobre todo para usos gubernamentales, militares y de grandes industrias. Ya no requieren instalaciones tan costosas y son

mucho más rápidas que sus antecesoras. Entre éstas grandes computadoras están: las series CDC, CRAY, Hitachi o IBM. Que son capaces de realizar miles de operaciones por segundo.

A partir de entonces el desarrollo en materia de hardware y software en las computadoras personales no ha parado. Cada día los programas y equipos se hacen más interactivos, las empresas de computación se afanan en hacer más fácil la labor al usuario.

Actualmente se está en la búsqueda de la quinta generación. Puesto para que haya un cambio de generación se necesita de una transformación fundamental en la estructura y composición de las computadoras. La quinta generación se plantea dos objetivos fundamentales: La comunicación con las computadoras a través de un lenguaje más cotidiano, sin tener que recurrir a lenguajes o códigos especializados; así como un procesamiento de datos por medio de diseños especiales, arquitectura y circuitos de alta velocidad.

En 1989, Japón lanza el proyecto "quinta generación", la competencia en materia informática deja de verse como una rivalidad entre compañías, para convertirse en una lucha entre naciones que buscan la supremacía en mercado mundial de computadoras; los dos principales contendientes de esta contienda son Japón y Estados Unidos.

En cuestiones de computacionales al decir futuro es ahora.

1.2.2.1.3. Concepto

Antes que nada, debemos puntualizar que a lo largo de este trabajo, emplearemos la denominación computadora que deriva del término en Inglés "Computer", atendiendo a que es el término con la que la mayoría de los mexicanos estamos familiarizados y por lo tanto se adapta más a nuestra realidad nacional. Aunque en estricto español la Real Academia la denomina Ordenador (atendiendo a la complejidad de operaciones que realiza la máquina).

Las computadoras u ordenadores están presentes en cada aspecto de nuestras vidas. Desde la computadora que detecta los precios a través de los códigos del supermercado hasta las modernas aplicaciones en materia de gobierno electrónico. Pero, ¿qué es una computadora? ¿Qué concepto adoptar? Al respecto hay varias opiniones.

Según el maestro Julio Téllez Valdés la computadora es "una máquina automatizada de propósito general, integrada por elementos de entrada, procesador central, dispositivo de almacenamiento y elementos de salida"⁴⁷.

⁴⁷ Téllez Valdés, Julio. Derecho Informático, p. 5

Para otros la computadora es "Máquina capaz de efectuar una secuencia de operaciones mediante un programa, de tal manera, que se realice un procesamiento sobre un conjunto de datos de entrada, obteniéndose otro conjunto de datos de salida"⁴⁸.

La enciclopedia Encarta la define como: "Un dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información."⁴⁹

Las tres definiciones nos hablan de un ingreso de datos, un procesamiento de estos y la obtención de resultados. Un proceso que ha estado presente desde las primeras generaciones de computadoras. La definición del maestro Téllez Valdés quizás atienda demasiado al hardware, que bien pueden variar con el paso del tiempo y generaciones. La tercera definición sentimos se queda un poco escueta con respecto a todas las funciones de la computadora. Por lo que para efectos prácticos adoptaremos la segunda definición que trata sobre el programa, que es básico en una computadora.

1.2.2.1.4. Clasificación

En la revisión histórica de las computadoras vimos que una primera clasificación de ellas se hace con base en generaciones. A continuación presentaremos otras clasificaciones de basadas, ya bien en su tamaño o en su modo de operación.

La clasificación de las computadoras atendiendo a su tamaño las distribuye en cuatro categorías: las Supercomputadoras, Macrocomputadoras, Minicomputadoras y las Microcomputadoras o PC's.

La Supercomputadora es la más rápida y potente actualmente. Son diseñadas para una tarea específica y para procesar una cantidad colosal de información en poco tiempo; algunas de estas tareas son: la búsqueda de yacimientos petrolíferos con base en datos sísmicos, la búsqueda de armas nucleares, el estudio y predicción del clima, la simulación de vuelo, entre otras. Son muy caras debido a la gran cantidad de componentes que emplean (sus precios llegan a alcanzar los 30 millones de dólares). Por lo que son pocas las que se llegan a construir.

Las macrocomputadoras o mainframes son las segundas en tamaño. Se emplean para controlar a cientos de usuarios al mismo tiempo, así como miles de dispositivos de entrada y salida. Las macrocomputadoras son más poderosas que

⁴⁸ <http://www.monografias.com/trabajos/histocomp/histocomp.shtml>

⁴⁹ Ordenador. Enciclopedia Microsoft Encarta 2002

las supercomputadoras, puesto que pueden soportar más programas simultáneamente, sin embargo las supercomputadoras pueden ejecutar un programa más rápido que una mainframe. En cuanto a tamaño, actualmente son más pequeñas que las supercomputadoras. Su costo es alto pero mucho menor que una supercomputadoras (de 350,000 hasta varios millones de dólares).

Las minicomputadoras son versiones pequeñas de las macrocomputadoras surgidas en los sesentas. Se orientan a tareas específicas, que hacen innecesarios la gran cantidad de periféricos de la mainframe, lo que reduce considerablemente su costo y mantenimiento. Es capaz de soportar de 10 a 200 usuarios al mismo tiempo. Son utilizadas para aplicaciones multiusuario, almacenar grandes cantidades de datos y automatización industrial- En cuanto a tamaño y poder son el punto intermedio entre la mainframe y la microcomputadora.

La microcomputadora o PC (Personal Computer = Computadora Personal) es con la que la mayoría de nosotros estamos familiarizados. Aquella basada en los chips y microprocesadores. Sus raíces más antiguas las encuentra en la IBM PC de 1981. Están dedicadas al uso personal y su costo comparado con las super, macro y mini es reducido. Hay numerosas variaciones de estas: las de escritorio, las laptop o notebook, etc. Hasta a las Macintosh que no son propiamente PC se les considera como tales por estar destinadas al uso personal.

Actualmente, se emplean dos tipos de computadoras: las analógicas y las digitales. Aunque el término computadora a secas se utiliza para las digitales. En todos ellos se maneja la ausencia o presencia de voltajes

Las análogas pueden ser electrónicas o hidráulicas. Se valen de la semejanza matemática entre los fenómenos físicos, utilizando circuitos hidráulicos o eléctricos para representar el problema físico. Las electrónicas utilizan señales eléctricas, se emplean en problemas de simulación, su programación está esculpida en los circuitos que la integran (por ejemplo: en termómetro = la temperatura). Son rápidas; el inconveniente es que al cambiar el problema hay que cambiar el hardware.

Las digitales se programan por medio de lenguajes que emplean un alfabeto llamado código binario. El que se vale de cadenas de unos y ceros para representar cualquier información o carácter. Se basan en dispositivos que únicamente pueden tomar el valor de 0 o 1 (alta o baja tensión). Son capaces de ejecutar diferentes programas para diferentes problemas sin necesidad de modificarlas como las analógicas, aunque no son tan rápidas.

Hay una tercera categoría especial llamada Híbrida. Que es una combinación de las analógicas y las digitales. Se utilizan para resolver problemas complejos, tomando lo mejor de las dos.

1.2.2.1.5. Componentes

Actualmente las computadoras personales o microcomputadoras (las más comunes en nuestra vida cotidiana) cuentan con gran cantidad de componentes para su operación. Por motivos prácticos (o quizás teóricos) los componentes han sido divididos en dos categorías: hardware y software.

Se le llama hardware a todos los componentes físicos de la computadora (todo aquello visible y tangible). Son cuatro las actividades fundamentales del hardware: la entrada, el procesamiento, la salida y el almacenamiento secundario. Para poder realizarlas en general se vale de cinco elementos principales: la unidad central de proceso, los dispositivos de almacenamiento de memoria, los de entrada, salida y una red de comunicaciones (bus) que une a todos los elementos y los conecta con el mundo exterior.

Software se llama a los programas, reglas, procedimientos o cualquier documentación relativa a la operación del Sistema de Computo, aquellos que emplean para manipular datos (elementos intangibles). Un conjunto de instrucciones individuales que se le proporcionan a la computadora para que pueda procesar datos y obtener resultados. Al software se le suele clasificar en cuatro categorías: sistemas operativos, lenguaje de programación, software de aplicación y software de uso general (hay algunos que unen estos dos en una única categoría).

En cuanto a los elementos del Hardware tenemos:

La Unidad Central de Proceso o CPU por sus siglas en inglés. Es un chip o un grupo de chips que efectúan que controlan y temporizan las operaciones de los demás elementos del sistema; así como ejecutan cálculos lógicos y aritméticos. A su vez los chips están compuestos por cuatro secciones: una unidad aritmética/lógica (que proporciona la capacidad de cálculo y ejecución de operaciones); unos registros (áreas de almacenamiento temporal de datos, seguimiento de instrucciones y conservación de resultados); una sección de control (regulariza y temporiza toda la actividad del sistema informático; descodifica las instrucciones para convertirlas en actividad; y regula el tiempo que el C.P.C. utilizará para determinada actividad) y un bus interno (que es una red que conecta los elementos internos y los externos del procesador). Uno de éstos chips es el microprocesador, que acoge a un sistema de memoria y circuitos adicionales.

Los dispositivos de almacenamiento de memoria. Estos pueden almacenar la memoria ya sea de manera interna (en la memoria) o en los dispositivos de almacenamiento externo. También se les denomina áreas de almacenamiento primario y secundario. En la primera encontramos a la memoria ROM (read only memory) o memoria de sólo lectura, donde se almacena información y datos necesarios por la computadora de forma permanente y que no pueden ser modificados por el programador; así como la RAM (random access memory) o

memoria de acceso aleatorio, es la que el usuario emplea mediante los programas y es volátil. La segunda es un almacenamiento definitivo, no volátil como el RAM, y generalmente se da a través de dispositivos portátiles. Actualmente existen diferentes dispositivos de almacenamiento: los magnéticos (comprende a los discos flexibles, los duro, las cintas magnéticas o cartuchos), los ópticos (que emplean el láser CD ROM y WORM) y los mixtos (fusionan ambas tecnologías).

Los dispositivos de entrada permiten ingresar información, programas y comandos a la Unidad Central de Proceso. Son muy amplios, entre los más comunes tenemos a los teclados, el mouse o ratón, lápices ópticos, joysticks, las pantallas sensibles al tacto, el escáner o incluso módulos de reconocimiento de voz.

Mientras que los dispositivos de salida permiten al usuario obtener los resultados de sus manipulaciones de datos u operaciones ingresadas a la computadora. Entre estos tenemos a: la unidad de visualización (monitor) o VDU (Video Display Unit), casi idénticos a los de un televisor; las impresoras o los módem (que enlazan a dos ordenadores)

De los elementos que integran al Software tenemos a:

El sistema operativo, es un programa (quizás el más importante) de control principal; encargado de coordinar las actividades de la computadora; está almacenado permanentemente en la memoria central de la computadora. Es un "interprete" de los comandos que el usuario introduce a la máquina para obtener resultados. Originalmente fueron creados para trasladar y coordinar los flujos de datos que procedían de diferentes fuentes (diferentes unidades del disco). El sistema operativo proporciona una plataforma de software, sobre la cual otros programas (llamados aplicaciones) pueden correrse. Algunos de los sistemas operativos más populares son DOS, OS/2, Linux y Windows.

Por medio de los programas se le indica a las computadoras las tareas a efectuar y la forma de hacerlo, pero para que esto sea posible es necesario introducir las instrucciones a la máquina en un lenguaje que ésta pueda entender; es entonces que entran los lenguajes de programación. Existen tres tipos principales de lenguajes: el lenguaje de máquina, los lenguajes de bajo nivel (o ensamblador) y los lenguajes de alto nivel.

El lenguaje de máquina es aquel que sólo la computadora puede entender, dicho lenguaje ordena a la computadora ejecutar sus operaciones fundamentales una por una. Utiliza un sistema binario y es difícil de emplear para una persona común.

El lenguaje de bajo nivel o ensamblador, utiliza pequeñas abreviaturas de palabras en inglés (por lo general de tres letras), agiliza y facilita la labor de los programadores. Para su empleo se crearon programas traductores para convertir el lenguaje ensamblador a lenguaje máquina. Pero el lenguaje ensamblador sólo

se podía utilizar para un solo tipo de chip o microprocesador, por lo que cada que surgía un nuevo microprocesador tenían que cambiarlo, por lo que resultaba demasiado inconveniente.

Los lenguajes de alto nivel aceleran aun más la programación, pues emplean enunciados completos para la realización de tareas (términos como: PRINT o LIST), los comandos se insertan por medio de algún dispositivo de entrada, almacenamiento o un programa residente en la memoria y son interceptados por un programa que los traduce a lenguaje máquina. Existen dos tipos de programas traductores: los compiladores y los intérpretes.

Un compilador lee el código escrito en cierto lenguaje (lenguaje de origen), para después traducirlo a un programa semejante escrito en otro lenguaje (lenguaje objetivo) y de paso señala al usuario los errores en el código fuente del programa. Obtenido el lenguaje objeto, el compilador conjura al linker que convierte al archivo objeto en ejecutable. Es diez o veinte veces más rápido que un traductor.

En tanto que el intérprete simplemente realiza la operación que debió realizar el lenguaje origen, lee el lenguaje tal y como está escrito, para posteriormente convertirlo en acciones, lo ejecuta al instante.

Algunos de los principales lenguajes de programación que ha existido son: "Fortran (1957, fórmula traductora), Algol (1959, lenguaje algorítmico), Basic (1958, código de instrucciones simbólicas para principiantes de todo propósito), Cobol (1960, lenguaje orientado a los negocios comunes) y posteriormente el PASCAL, ADA, PL/I, APL, PROLOG, LISP, Visual Basic, HTML, Javascript, etcétera."⁵⁰

El Software de aplicación son programas que ejecutan una tarea específica; manejan información que el usuario necesita procesar. Su objetivo es permitir al usuario ejecutar su trabajo con agilidad, facilidad, rapidez y precisión. Hay diferentes tipos de software de aplicación (agendas, bases de datos, procesadores de texto, programas de contabilidad, etc.), algunos de ejemplos de estos son: Excel, Word, Corel Draw, etc.

El Software de uso general presenta al mercado la estructura para una gran cantidad de aplicaciones personales, científicas y empresariales, por lo general se vende como paquetes (el software con la documentación dirigida al usuario). Ejemplos de éste tipo de software son: hoja de cálculo, Diseño asistido por computadoras, etc.

⁵⁰ Téllez Valdés, Julio. Derecho Informático p. 5

1.2.2.2. Redes

1.2.2.2.1. Antecedentes

Al tiempo que las computadoras se volvieron cada vez más comunes y compactas (recordemos el gran desarrollo de las microcomputadoras a partir de mediados de los ochentas) se pensó en lo útil que resultaría poder interconectar estas diminutas unidades, para que compartieran recursos e intercambiaran información, entre otras funciones. Con el fin de que el trabajo que antes era realizado por una sola computadora que respondía a todas estas necesidades de cálculo, y que por lo general era una mainframe (mucho más costosa que varias microcomputadoras), pudiera ser dividido entre varias PCs, que se vería directamente reflejado en la disminución de costos, y además de otorgar la insospechada ventaja adicional de la comunicación a distancia.

Las guerras, fueron (y siguen siendo) el motor impulsor para el desarrollo de nuevos dispositivos tecnológicos, como es el caso de computadoras; mientras que el mejoramiento en componentes y la disminución de costos marcaron un hito en cuanto a la historia de éstas, haciendo que la venta y construcción de las computadoras se disparara en cuestión de años. La creación de las primeras redes de computadoras, su crecimiento y desarrollo responde al igual que las computadoras a factores bélicos, tecnológicos y económicos.

Como ya mencionamos, las redes de computadoras se desarrollaron con varios propósitos en un principio: *el compartir recursos*, hacer que los equipos, programas y datos estuvieran disponibles para cualquiera dentro de la red, sin importar la ubicación física del usuario y del recurso, haciendo posible el trabajo conjunto a distancia; *la alta fiabilidad*, que hace posible que ante cualquier error de alguna computadora o suministro hubiera otra que permitiera continuar la labor; y el *ahorro económico* que representa el uso de pequeñas computadoras, además de la posibilidad de expandir la red a placer con la simple anexión de nuevos equipos a ésta, que no implica el mismo gasto que tener que sustituir una mainframe por otra nueva que mejor a las nuevas necesidades de una empresa o grupo.

De manera oficial el Instituto de Ingenieros Eléctricos y Electrónicos o IEEE (una de las máximas autoridades en cuanto a Redes y normatividad de éstas) en su comisión 802 define a la red como “un sistema de comunicaciones que permite que un número de dispositivos independientes se comuniquen entre sí”⁵¹

Para Tanenbaum es una Red de Computadoras es una “colección interconectada de ordenadores autónomos”⁵². La interconexión entre computadoras alude al hecho de que éstas puedan intercambiar información, en

⁵¹ Rábago, José Félix. Introducción a las redes locales. Anaya Multimedia América. México 1995. p.19

⁵² Tanenbaum, Andrew S. Redes de Ordenadores. 2ª ed. Prentice –Hall Hispanoamericana, S.A. México, 1991. p. 2

tanto que la autonomía hacer referencia al hecho de que una computadora pueda controlar, parar y arrancar por si misma, es decir sin estar subordinado a las ordenes de otra.

Al tiempo que para Félix Rábago es “un sistema de transmisión de datos que permite compartir recursos e información por medio de ordenadores, o redes de ordenadores”⁵³

Consideramos que los dos elementos esenciales de cualquier definición de red son la interconexión y la autonomía o independencia, por lo que el concepto de Tanenbaum que nos parece bastante claro es el que adoptamos para posteriores referencias a cerca de redes.

Las primeras redes de computadoras eran Redes Locales, es decir se ubicaban dentro de un mismo edificio, a este tipo de redes se la llamo LAN (Red de Área Local), mientras que a las redes que posteriormente se desarrollaron, que se extendían fuera de un edificio o local, que tenían un mayor alcance se les llamo WAN (Red de Área Extendida).

1.2.2.2.2. Estructura de la red

Siguiendo la terminología empleada por ARPANET (de la que hablaremos más adelante). El punto de partida en toda disposición de red son los hostales o sistemas terminales, que son máquinas abocadas a correr aplicaciones o programas de usuario; dichas máquinas se unen mediante una subred, que está encargada de despachar mensajes entre hostales.

Para el caso de las redes de área extendida, la subred se integra por líneas de transmisión (también conocidas como troncales, canales o circuitos) y elementos de comunicación (o IMP = Procesadores de Intercambio de Mensajes). Las primeras se encargan de desplazar bits entre los hostales y las segundas son computadoras especializadas que se emplean para enlazar dos o más troncales.

En general existen dos prototipos para la subred de comunicación: Los canales de punto a punto y los canales de difusión. El primero patrón es empleado por lo regular para las WAN; las IMP para este tipo de red pueden estar unidas por medio de un cable común, pero en caso de no estarlo, se pueden transmitir datos de forma indirecta a través de otra IMP intermediaria. Los datos (o paquete) se transmiten completamente de IMP a IMP por lo que si en algún punto de la transmisión no existe canal de salida, el paquete se almacenará en la IMP hasta que encuentre salida.

El segundo patrón se emplea para las LAN y algunas WAN. En ellas hay un hostal por IMP (a diferencia de las punto a punto donde puede haber más de un

⁵³ Rábago, José Félix. Ob. cit. p.19

hostal por IMP), sólo hay un canal de comunicación concurrente para todas las IMP, por lo que los paquetes que una IMP envía son admitidos por todas, pero en el campo de dirección que contiene el paquete detalla hacia quien va dirigido lo que hace que las máquinas no destinatarias automáticamente lo ignoren (aunque existen paquetes de dirección que permiten ser enviados a todas las IMP).

1.2.2.2.3. Arquitectura de las Redes

Las redes están constituidas por medio de capas o niveles; el contenido, número y funciones de dichas capas varía de red a red. Pero en general la función de cada nivel es proporcionar servicios al nivel superior, eximiéndolo del entendimiento de cómo realiza dicha asistencia. En tanto que la comunicación entre capas de diferentes máquinas se realiza a través de convenciones y reglas de comunicación conocidas como protocolo; pero para que esta conversación entre máquinas sea posible, debe ser entre capas correspondientes o procesos pares. Mientras que para la comunicación entre capas inferiores y superiores en una misma máquina se utilizan las llamadas interfaces. A la combinación de protocolos y capas se le llama arquitectura de red.

Existen muchos diseños en cuanto a redes, pero con la finalidad de contar con un prototipo base que permita a diferentes máquinas ser capaces de comunicarse a través de protocolos, la Organización Internacional de Normas o ISO, ha establecido un arquetipo llamado "Modelo de Referencia OSI (interconexión de sistemas abiertos)" en cuanto a arquitectura de redes.

Dicho modelo se compone de siete capas: la física, la de enlace, la de red, la de transporte, la de sesión, la de presentación y la de aplicación; cada una ejecuta una función definida.

La capa física es la que se encarga de la transmisión de bits a través de un canal de comunicación. En ella, los aspectos a considerar son los eléctricos, mecánicos, los procesos de interfase y el medio de transmisión física. El especialista dominante de esta fase es el ingeniero eléctrico.

La capa de enlace se encarga de crear una línea de transmisión sin errores para la capa red. Para desarrollar esta tarea divide la entrada de datos en tramas de datos, que son transmitidas en forma sucesiva, al mismo tiempo que procesa las tramas de asentimiento que son abonadas por el receptor.

La capa red atiende la operación de la subred. Es decir, encamina los paquetes desde su destino hasta su origen.

La capa de transporte toma los datos de la capa de sesión, los divide (en caso necesario) los conduce a la capa red, al mismo tiempo que se asegura que llegue bien al otro extremo. Esta capa establecerá que clase de servicios dará a la capa de sesión e indirectamente a los usuarios de la red

La capa sesión hace posible que los usuarios de diversas máquinas puedan instaurar cesiones entre ellas; lo que les hace factible transmitirse datos. Algunas de sus funciones son: la gestión del control de diálogo, permitiendo que el tráfico de información corra entre ambas direcciones, o una sola; así como la administración testigo que consiste en evitar que dos protocolos traten de realizar la misma función en el mismo instante, para que esto sea posible, proporcionan testigos intercambiables, siendo así que solo el extremo con testigo puede realizar la operación crítica; así como la sincronización que es la inserción de puntos de verificación en el flujo de datos.

La capa de presentación se ocupa de la sintaxis y semántica de la información que es transmitida. Codifica los datos conforme a lo pactado anticipadamente. Maneja disposiciones abstractas de datos, las convierte de los símbolos manejados por la computadora en representaciones de red. En esta capa es donde se hacen presentes los aspectos de compresión de datos y la criptografía por razones de seguridad.

La capa de aplicación es la encargada de resolver las compatibilidades de la máquina, contiene los protocolos más utilizados. Entre otras cosas se encarga del correo electrónico, la transferencia de archivos, la entrada de trabajo a distancia, entre otros servicios de propósito general.

La transmisión de datos en el modelo OSI es vertical, pero las capas son programadas como si se tratara de una transmisión horizontal. Alguna de la terminología empleada por el sistema OSI es la que habla de los elementos activos que se localizan en cada capa, a las que llama entidades; que pueden ser hardware o software. Dependiendo de la capa que ocupen pueden ser entidades de Sesión, Transporte, etc. Si ocupan la misma capa pero en máquinas distintas se les llama entidades pares o iguales. A la entidad que auxilia a una capa superior se le llama proveedor de servicio y a la capa que es auxiliada usuario de servicio. Al lugar en el que una capa puede acceder a un servicio se le llama SAP (punto de acceso al servicio).

1.2.2.2.4. Ejemplos de Redes

Actualmente existe una gran cantidad de redes, cuya historia, servicios, administración y diseño es muy distinto. Las hay privadas y públicas, por lo general las públicas operan por medio de PTT o proveedores de servicios portadores comunes.

Muchas de las redes públicas son dedicadas exclusivamente al comercio o a la investigación, la mayoría de ellas se vale del modelo OSI y los cánones del Comité Consultivo Internacional telegráfico y telefónico (CCITT) para el desarrollo de su estructura interna. Existen muchas redes públicas, entre las más conocidas tenemos a:

1.2.2.2.4.1. Red de la Agencia de Proyectos de Investigación Avanzada (ARPANET)

La Red de la Agencia de Proyectos de Investigación Avanzada (ARPANET). Es de las primeras redes, al igual que las computadoras, surgiría por responder a cuestiones bélicas. En este caso sería la guerra fría que a mediados del siglo pasado sostenían el bloque socialista encabezado por la entonces Unión de Repúblicas Soviéticas Socialistas y el bloque capitalista capitaneado por los Estados Unidos de Norteamérica. La situación de espionaje y la latente amenaza de un conflicto nuclear entre las dos naciones hizo reflexionar al Departamento de Defensa Estadounidense, acerca de la necesidad de crear una red de comunicación nacional, capaz de sobrevivir a un conflicto de grandes dimensiones.

Algunas de las necesidades que debía cubrir dicha red era la de ser capaz de conservarse, es decir "la información debía encontrar más de una ruta desde su origen hasta su destino, obviando así cualquier 'hueco' que se pudiera suceder en la red"⁵⁴, asimismo la red debía ser de fácil establecimiento con las tecnologías de ese entonces y por último debía ser descentralizada, para así evitar un centro de información fácilmente destructible en caso de conflicto.

Se trabajó mucho en la búsqueda de soluciones; a principios de la década de los sesentas del siglo pasado, arranca un proyecto del Departamento de Defensa que canaliza recursos del gobierno compañías privadas y a los departamentos de ciencias de la comunicación de varias universidades con el objetivo de alentar la investigación en redes computacionales.

Algunos de los primeros en desarrollar el concepto de una red global fueron: Leonard Kleinrock, que en 1961, presenta uno de los primeros trabajos en comunicación de paquetes, concepción que revoluciona los conceptos de comunicación entre computadoras, ya que hasta entonces los investigadores trataban de interconectarlas por medio de circuitos; le sigue muy de cerca Licklider, que para 1962, desarrolla la idea de una Red Galáctica (Galactic Network); así como Ivan Sutherland, Bob Taylor, y Lawrence G. Roberts (la mayoría de ellos eran investigadores del Instituto Tecnológico de Massachusetts) este último en 1965 logra el primer dialogo entre computadoras al conectar una computadora que se encontraba en Massachusetts con otra de California por medio de una línea telefónica conmutada de baja velocidad, el sistema de comunicación a través de línea telefónica no resultó el más adecuado por lo que este retoma las ideas de Kleinrock.

Para 1969 aparece una red experimental de cuatro nodos ("la Universidad de Utah, el Instituto de Investigaciones de Stanford {Stanford Research Institute} y

⁵⁴ Téllez Valdés, Julio. Ob. cit. p. 83

dos servidores de la Universidad de California: Santa Barbara y los Angeles"⁵⁵). Con el paso de los años se aumentan más nodos, para 1971 son 15 en total y al año siguiente llegaron a 40. El crecimiento de la red es constante, a la vez que surgen redes alternas: aparece en Estados Unidos MILNET, una red militar que emplea la tecnología de ARPANET; los europeos no se quedan atrás y crean MINET, que es una extensión de MILNET; ambas están conectadas a ARPANET, pero el flujo de datos entre ellas es más restringido que el resto de las transmisiones de ARPANET. Más tarde se unirán dos redes satelitales: SATNET y WIDEBAND. Posteriormente redes LAN de diversas universidades y empresas privadas se enlazan con los IMPs, creando la interred ARPA. Entre los primeros organismos que se unen esta la NSF (National Science Foundation o Fundación Nacional de Ciencias). La aparición de las primeras computadoras personales (de lo que ya hablamos anteriormente) en la década de los ochenta, hace que la red se expanda más.

El avance tecnológico trajo diversos cambios en la red, los mayores cambios se reflejaron en los IMPs. Algunos de los IMPs originales han sido substituidos por otros más poderosos llamados PSN o nodos de conmutación de paquetes, que ejecutan las mismas funciones que un IMP. Otros IMPs se han dispuesto de tal forma que dejan que los terminales usuarios los llamen directamente, sin tener que recurrir al hostal intermediario. A este tipo de IMPs se les conoce como TIP (procesador de mensajes con interconexión de terminales) o TAC (controlador de acceso a terminal).

En cuanto a su estructura interna la red ARPANET no sigue el modelo OSI, en gran medida debido a que es muy anterior a la aparición de dicho modelo. Utiliza diversos protocolos: el orientado para la red se llama IP (protocolo de redes); el de transporte esta orientado a la conexión y se le llama TCP (protocolo de control de transmisión); otros como el FTP (protocolo de transferencia de archivo), SMPT (protocolo simple de transferencia de correo y TELNET (de conexión remota) se encargan de servicios tales como la transferencia de archivos, conexión remota, correo electrónico entre otros.

La primitiva ARPANET dura hasta 1990. Para mediados de los ochenta la NSF había creado su propia red mediante el enlace de seis centros de computación, a dicha red se le llamo NSFNET. El gran mérito de dicha red fue la reducción de costos, "NSF desarrollo un sistema de direcciones que permitía que los centros de supercomputo se conectaran con sus vecinos más próximos para retransmitir información"⁵⁶

Para fines de esa década la NSF transfiere dicha red a un grupo de universidades: el MERIT (Michigan Educational Research Information Triad), que en conjunción con IBM y MCI crean ANS (Advanced Network Services), y abren

⁵⁵ Randall, Neil. Trad. Sanchez Garcia, Gabriel. Aprendiendo Internet en 21 días. Prentice Hall Hispanoamericana. México, 1995. p. 38

⁵⁶ Téllez Valdés, Julio. Ob. cit. p. 83

dicha red a fines comerciales. Este cambio hace que ARPANET quede discontinuado, tomando NSFNET su lugar. Pero en un impredecible cambio de circunstancias, en 1991 durante la administración del presidente George Bush, el gobierno norteamericano retoma el control de las redes informáticas mediante la creación de NREN (National Research and Education Network), que utiliza a NSFNET como base, que abre por completo la red a fines comerciales y gubernamentales.

Dichos cambios nos hacen llegar hasta la actual Internet con la inclusión de algunas modificaciones como el hipertexto (desarrollado en 1993 por el suizo Tim Berners-Lee); la utilización de browser necesarias para la navegación en la red. A esta nueva red de alcances mundiales se le llamo World Wide Web (Red de Alcance Mundial).

1.2.2.2.4.2. Computer Science Network (CSNET) Y Because It's Time Network (BITNET)

Paralelas a ARPANET; NSFNET y demás surgen CSNET y BITNET. La primera como un esfuerzo de la NSF de dotar a los departamentos de ciencias de la computación de las universidades estadounidenses que no tenían acceso a NSFNET de un medio de comunicación. Es una "metared que utiliza los servicios de transmisión brindados por otras redes y añade una capa de protocolo uniformada en la parte superior, para hacer que todo ello parezca como una sola red lógica para usuarios"⁵⁷ Aunque dicha red era muy limitada, ya que solo contaba con el servicio de correo electrónico.

BITNET (Because It's Time NETWORK = Porque ya es hora) se crea a iniciativa de las Universidades Yale y de Nueva York, con el propósito de dotar a todos los departamentos de las universidades (no sólo a los de ciencias de la computación) de una red. Ofrecía servicios tales como: capacidades de transferencia de archivos, correo electrónico y otras; pero al no utilizar el protocolo IP se vio en la necesidad de crear un medio de comunicación con NSFNET.

Finalmente al ver que buscaban los mismos fines CSNET y BITNET decidieron unirse para crear CREN (Corporation for Research and Educational Networking). Actualmente trabajan en su integración a la NREN.

1.2.2.2.4.3. USENET

Esta red nace de la mano del sistema UNIX. La tecnología base de esta red es el sistema uucp, que fue creado con el propósito de copiar archivos de un sistema UNIX a otro. Posteriormente con la integración de los módems de llamada

⁵⁷ Tanenbaum, Andrew S. Ob. cit p.48

automática a los equipos UNIX, la comunicación entre computadoras a distancia fue posible.

Las primeras redes de computadoras que empleaban el sistema UNIX se valían de una computadora central que contaba con un marcador telefónico automático, encargado de llamar a un conjunto de computadoras, para así transferir información entre ellas; siendo una especie de intermediario de la información.

La simplicidad de la red UNIX, que solo precisaba de una computadora con sistema UNIX y un módem, la hizo muy popular, contando con miles de usuarios, a la red formada se le llamo UUCP. Esta red solo ofrecía el servicio de correo electrónico, pero posteriormente una red compañera creada por las universidades de Carolina del Norte y Duke ofreció un servicio llamado red de noticias, a esta red se le llamó USENET.

1.2.3. Comercio Electrónico

En apartados anteriores hablamos ampliamente del comercio "tradicional". En los últimos tiempos han aparecido técnicas novedosas de comercio, el objetivo es el mismo que en el comercio tradicional, lo original viene con la técnica empleada para lograr el objetivo comercial.

Algunas de las primeras "novedades" en materias de ventas fueron los catálogos de productos, que aparecieron por primera vez en la década de los veinte del siglo pasado en los Estados Unidos. Dichos catálogos llenos de fotos ilustrativas hicieron posible entre otras cosas la exposición de los productos de los grandes almacenes (creadores de los catálogos) a clientes en alejadas zonas rurales, además de permitir a los clientes potenciales la adquisición de los productos desde la comodidad de sus hogares, e incluso proporciona anonimato entre cliente y vendedor. Esta modalidad se vería doblemente impulsada con la aparición de la tarjeta de crédito.

El siguiente gran salto vendría con las ventas por televisión de mediados de 1980. Donde los productos eran exhibidos a un mayor grupo de compradores de forma más realista que en un catálogo impreso. Las operaciones en esta clase de comercio se concretaban mediante una llamada telefónica, y cubriendo el costo del producto por lo general mediante una tarjeta de crédito.

Las primeras relaciones comerciales que hacen uso de la computadora para la transmisión de datos, se dan a principios de los años 1970. Para entonces no existían estándares para este tipo de operaciones, por lo que las empresas privadas de un mismo sector se vieron en la necesidad de establecerlos (distintos para cada rama de la industria) al tiempo que mejoraron sus equipos, técnicas y demás cuestiones relativas a estas primitivas relaciones electrónicas comerciales.

Ejemplo de esto fue el supermercado mayorista Amigazo, que a mediados de la década de 1980 crea un sistema de procesamiento de pedidos electrónicos, que permite a las empresas clientes del establecimiento ordenar pedidos desde sus empresas y enviarlas de modo electrónico a Amigazo. En la práctica dicho sistema demostró su efectividad al reducir los tiempos de procesamiento de pedidos, así como los errores en las entregas. Tal fue el beneficio que el supermercado instaló un equipo en cada una de las oficinas de sus clientes regulares.

Pero hay los que consideran que no es el uso de la computadora lo que le da la acepción de comercio electrónico a una transacción; opinan que tecnologías tales como: télex, teléfono y fax, empleadas para fines comerciales también deben ser consideradas comercio electrónico.

De lo expuesto anteriormente deducimos que la introducción de las tecnologías informáticas en el ámbito comercial por lo general se haría con la búsqueda de beneficios en organización, reducción de costos, rapidez y exactitud. Hasta el día de hoy la informática ha demostrado su efectividad para lograr dichos objetivos, por lo que el futuro del comercio electrónico está asegurado.

1.2.3.1. Concepto

Los especialistas en sistemas de computadoras consideran que debemos llamar comercio electrónico a aquel "que se efectúa exclusivamente mediante formato electrónico"⁵⁸. Este concepto no hace solo referencia a la realización de negocios, si no también a las funciones electrónicas que auxilian a la empresa a la realización de transacciones comerciales. A menudo se confunde al comercio electrónico con el comercio por Internet, pero éste es un subconjunto del primero. El comercio por Internet solo comprende a aquel que se verifica por medio de un formato electrónico por Internet.

Los juristas en general adoptan dos posturas al respecto de lo que es comercio electrónico. Por un lado están los que ven al comercio electrónico como "cualquier forma de transacción o intercambio de información comercial basada en la transmisión de datos sobre redes de comunicación como Internet"⁵⁹. Este concepto sólo aborda a las redes como medios de comercio electrónico, dejando de lado otras tecnologías informáticas, lo que nos hace pensar que el autor de tal definición más que referirse a comercio electrónico, hace alusión al comercio por redes como lo es el comercio por Internet.

Mientras que otros consideran no solo la parte respectiva a redes, y lo definen como "todo intercambio de datos que se realiza por medios electrónicos,

⁵⁸ Smith, Rob, et. al. Trad. Martínez, Miguel Angel. Comercio Electrónico. Pearson Education. México. 2001. p. 50

⁵⁹ Téllez Valdés, Julio. Ob. cit. p. 188

ópticos o cualquier otra tecnología relacionada estrictamente con la actividad comercial”⁶⁰ Este último nos parece un poco más completo y mucho más cercano al dado por los especialistas en sistemas de computadoras.

Otras opiniones como la del especialista Juan Fernández (coordinador de la Comisión Nacional de Comercio Electrónico de Cuba) apuntan a ver al comercio electrónico como: "cualquier forma de transacción de negocios en la cual las partes interactúan electrónicamente en lugar de mediante intercambios materiales o contacto físico directo"⁶¹ En esta definición una vez más se alude al elemento a la interacción por medios electrónicos.

En tanto que la Organización Mundial de Comercio define al comercio electrónico como "la producción, distribución, comercialización, venta y entrega de bienes y servicios por medios electrónicos"⁶² Que a nuestro parecer es una mezcla del concepto económico de comercio, con la novedad de la intromisión del concepto medio electrónico. Anteriormente abordamos al comercio; y en lo que se refiere a electrónico, siguiendo lo expresado por el maestro Julio Téllez Valdés lo puntualizamos como "la infraestructura mundial de tecnologías y redes de la informática y las telecomunicaciones que permiten el procesamiento y la transmisión de datos digitalizados"⁶³. Si desentrañamos el concepto de la Organización Mundial de comercio con auxilio de las definiciones anteriormente anotadas resulta tan o más completo que los primeros conceptos mencionados.

Para fines prácticos utilizaremos esta última definición, ya consideramos que comprende lo expresado por las anteriores definiciones, además de ser la desarrollada por un organismo tan importante para el comercio mundial, como lo es la Organización Mundial de Comercio.

Otros puntos que abordaremos con mayor profundidad en apartados posteriores del presente trabajo son E-commerce y E-business. Por el momento basta con aclarar que E-commerce es la denominación en Inglés para el Comercio Electrónico, es por así decirlo, un sinónimo de comercio electrónico. En tanto que el E-business hace referencia "toda la organización del negocio, vista desde el punto de aplicación de las nuevas tecnologías de la informática"⁶⁴.

1.2.3.2. Clasificación

Existen muchos criterios para clasificar al comercio electrónico, nosotros adoptamos los dos más utilizados por la mayoría de los autores de la materia, que

⁶⁰ Quintano Adriano, Elvia Arcelia. *Ob. cit.* p. 243

⁶¹ <http://www.monografias.com/trabajos13/comel/comel.shtml>

⁶² Citado por Patroni Vizquerra, Ursula. *Apuntes de Derecho Electrónico*. http://v2.vlex.com/es/ppv/doctrina/resultados.asp?query_doc=178122&n_orden=0&

⁶³ Téllez Valdés, Julio. *Ob. cit.* p. 185

⁶⁴ Patroni Vizquerra, Ursula. *Apuntes de Derecho Electrónico*. http://v2.vlex.com/es/ppv/doctrina/resultados.asp?query_doc=178122&n_orden=0&

son: la clasificación dependiendo de los agentes implicados y la que atiende a la clasificación por la forma de relacionarse.

1.2.3.2.1. Dependiendo de los Agentes Implicados

Esta se divide para su estudio al comercio electrónico en dos categorías:

- El Comercio Electrónico Indirecto: que consiste en la adquisición de "bienes tangibles que necesitan luego ser enviados físicamente usando canales tradicionales de distribución"⁶⁵
- El Comercio Electrónico Directo: donde "el pedido, pago y envío de los bienes intangibles y/o servicios se produce on-line"⁶⁶ (ej. Compra de música, software, etc. en línea)

1.2.3.2.2. Por la forma de relacionarse

Esta clasificación hace alusión a los agentes que actúan en el comercio electrónico, que en general son: empresas, consumidores y administradores. La unión e interconexión de estos tres elementos básicos pueden surgir muchas combinaciones de comercio electrónico, entre las más básicas están:

- "Entre empresas o B2B (Business to Business)
- Entre empresa y consumidor o B2C (Business to Consumers)
- Entre empresa y la Administración o B2A (Business to Administration)"⁶⁷
- Entre consumidor y consumidor o C2C (Consumers to Consumers)
- Entre consumidor y administrador o C2A (Consumers to Administration)

La categoría B2B hace referencia la interrelación que se da entre las empresas que generalmente hacen uso de los medios electrónicos para realizar actividades tales como la recepción de facturas, hacer ordenes de compra a sus proveedores, efectuar pagos, etc. Las empresa se valen para esto de medios tales como: EDI ("Electronic Data Interchange") sobre redes privadas o redes de valor agregado ("Value added Networks-VAN").

La categoría B2C trata de es la venta al detalle o venta electrónica, que se ha vuelto muy popular en los últimos tiempos; sobre todo desde la introducción de la Internet a los particulares.

En cuanto a la categoría B2A aborda a las transacciones entre empresas y el gobierno (administración pública). Por medio de esta las empresas pueden

⁶⁵ <http://www.mecon.gov.ar/comercio/electronico/indirec.htm>

⁶⁶ Ibidem

⁶⁷ Téllez Valdés, Julio. Ob. cit. p. 189

realizar operaciones como el pago de impuestos, presentar declaraciones fiscales, etc.; es un campo en desarrollo en nuestro país.

La categoría C2C nos remite a una transacción comercial entre consumidores, esto suena absurdo porque una de las partes (en todo caso el vendedor) se convertiría en empresa al ofrecer, dejando a un lado su calidad de consumidor. El objeto de esta categoría es hacer una distinción entre personas lo que nosotros llamaríamos personas físicas y las personas morales (las empresas) en Internet.

La última categoría C2A al igual que la B2A esta en etapa de desarrollo, administraciones estatales como Chiapas se han dado a la tarea de crear un gobierno electrónico que permita una reducción de la burocracia y la corrupción, así como la una agilización de tramites.

1.3. DERECHO INFORMATICO

El desarrollo de las tecnologías informáticas ha afectado a numerosos campos del conocimiento humano; ha acelerado el manejo de la información, revolucionado la forma de comunicarnos, y hasta podríamos decir que ha hecho más cortas las distancias; podríamos aventurarnos a decir que es en parte responsable de fenómenos como la globalización (con todos sus pros y contras, detractores y defensores) que la humanidad enfrenta hoy en día. Es indudable que la Informática ha influido en prácticamente todos los campos del desarrollo humano, entre estos el del Derecho.

Hoy en día es innegable la influencia ejercida por la Informática en el Derecho; aunque hace algunas décadas cualquier insinuación de Informática en el campo jurídico nos habría parecido fantástica. Aun así ya en las décadas cuarenta y cincuenta del siglo pasado hubo quienes visionariamente pensaron en la relación que algún día podría darse entre Informática y Derecho.

El primero de ellos puede ser Norbert Wiener, que para 1949 en su libro *Cibernética y Sociedad* dedica un capítulo entero (el cuarto) a la relación entre el Derecho y las comunicaciones. En el mismo año, un juez Norteamericano, Lee Loe Vinger difunde el artículo "The Next Step Forward" (el siguiente paso adelante) en la revista "Minnesota Law Review. En el cual explica que "... El próximo paso adelante en el largo camino del progreso del hombre, debe ser el de la transición de la Teoría General del Derecho hacia la Jurimetría, que es la investigación científica acerca de los problemas jurídicos"⁶⁸

⁶⁸ Loe Vinger, Lec. Jurimetrics, The Next Step Forward, Minnesota Law Review, XXXIII, 1949. Citado por Piña Libien, Hiram Raúl. El Derecho Informático v su Autonomía como Nueva Rama del Derecho. www.ordenjuridico.gob.mx/Congreso/pdf/78.pdf

Pero ¿en qué consiste esta nueva rama del Derecho? En caso de que la podamos considerar una rama del Derecho; ya que algunos consideran que el Derecho Informático no es una rama autónoma del Derecho.

Los que no consideran al Derecho Informático como una materia independiente en el campo jurídico, apelan a que en cada una de las materias jurídicas la informática se encuentra presente de alguna manera, por lo que les parece imposible la integración de todas estas normas en un cuerpo jurídico aislado.

En tanto que los que abogan por la existencia autónoma del Derecho Informático consideran que éste "constituye un cuerpo autónomo de normas jurídicas que tienen por objeto regular las actividades que derivan de la informática, dentro de un orden eficiente y justo"⁶⁹. Esta postura recibió gran apoyo a partir de la década de los ochenta del siglo pasado cuando se vio cuan conveniente era la unión de las normas relacionadas a la informática con el fin de constituir una nueva ciencia, con nuevos enfoques y métodos y métodos.

Al respecto de estas dos posturas los especialistas jurídicos han llegado a la conclusión de que el Derecho Informático es autónomo ya que "cuenta con los elementos mínimos (Materia, Teoría y Método propios) para ser considerada como disciplina jurídica"⁷⁰. Concordamos esta postura, ya que consideramos que a pesar de que son necesarios aun más estudios doctrinales y codificaciones sobre la materia, el Derecho Informático reúne todas las características para ser una rama independiente del Derecho.

Basados en esta postura de la autonomía de Derecho Informático con respecto de otras materias jurídicas, se hace necesario dar un concepto que nos guíe a lo largo de nuestro estudio. Pero para entender al Derecho Informático debemos comprender primeramente su composición como disciplina.

Llamamos ciencia al "cuerpo de doctrina metódicamente formando que constituye una rama del humano saber"⁷¹. A decir de algunos para que un paradigma del conocimiento pueda ser considerado ciencia debe contar con tres elementos fundamentales: Una Materia, Teoría y Método propios. La Materia a su vez cuenta con un objeto material y objeto formal. Llamamos material al objeto del estudio, la cosa a estudiar; en tanto que el objeto formal es el punto de vista desde el cual se estudia al objeto material.

En el caso de la Informática y el Derecho (o Ciencia Jurídica). Si el Derecho es estudiado por la Informática, hablamos de la Informática Jurídica; al tiempo que si la Informática es utilizada como herramienta para aplicar, realizar o materializar

⁶⁹ Piña Libien, Hiram Raúl. El Derecho Informático y su Autonomía como Nueva Rama del Derecho. www.ordenjuridico.gob.mx/Congreso/pdf/78.pdf

⁷⁰ Ibidem

⁷¹ Raluy Poudevida, Antonio. Diccionario Porrúa de la Lengua Española. 48ª ed. Porrúa, México, 2003 p.170

el Derecho, hablamos del Derecho de la Informática, el derecho se convierte en el punto de vista desde el cual se estudia a la informática.

Partiendo de los supuestos anteriores podríamos definir al Derecho Informático como "una rama de las ciencias jurídicas que considera a la Informática como instrumento (Informática Jurídica) y objeto de estudio (Derecho de la Informática)"⁷².

Existen otras definiciones más generales que consideran al Derecho Informático como una "Disciplina social que procura analizar y proponer respuestas jurídicas a los problemas jurídicos creados por el desarrollo y crecimiento de la informática moderna"⁷³

Otros autores lo definen de forma más extensa como "una interdisciplina que estudia el uso y desarrollo de las tecnologías informáticas, encaminadas a la investigación científica de los problemas jurídicos y como un factor estratégico para el desarrollo de una sociedad, con el fin de lograr su pleno aprovechamiento y como instrumento de apoyo para elevar la productividad, la competitividad, la eficiencia, la administración y procuración del derecho en los sectores público, privado y social, y con ello proporcionar bienestar común"⁷⁴

Para efectos del presente trabajo emplearemos la definición dada por el maestro Julio Téllez Valdés, ya que consideramos es lo bastante clara y concisa para la comprensión de esta rama jurídica.

Algunos de los campos de estudio que se plantean como objetivos a abordar por esta nueva rama del Derecho son: Administración de Justicia y Nuevas Tecnologías, Banca y Dinero Digital, Censura en Internet, Libertad de Expresión online, Firma Electrónica, Habeas Data, Impuestos e Internet, Informática Jurídica, Manifestación de la Voluntad por Medios Electrónicos, Protección de Datos de Carácter Personal, Publicidad e Internet, Relación entre el Derecho y la Informática, Sociedad Civil e Internet, Sociedad de la Información, Telefonía y Voz sobre IP, Wireless Application Protocol (WAP), Medidas Cautelares sobre Equipos Informáticos, Nombres de Dominio y Direcciones IP, Notas Bibliográficas y de Eventos, Notificación por Medios Electrónicos, Privacidad en Soportes Lógicos, Comercio Electrónico, Contratos Informáticos, Delitos Informáticos, Derecho en la Era Digital, Derecho de las Telecomunicaciones, Derecho Laboral e Informática, Documento Electrónico, EDI y Factura Electrónica, E-government, e-Learning del Derecho y Nuevas Tecnologías, Profesionales del Derecho en la Era Digital, Propiedad Intelectual y Propiedad Industrial e Internet, Programas: Software Jurídico. Bases de datos y Gestión de Bufetes

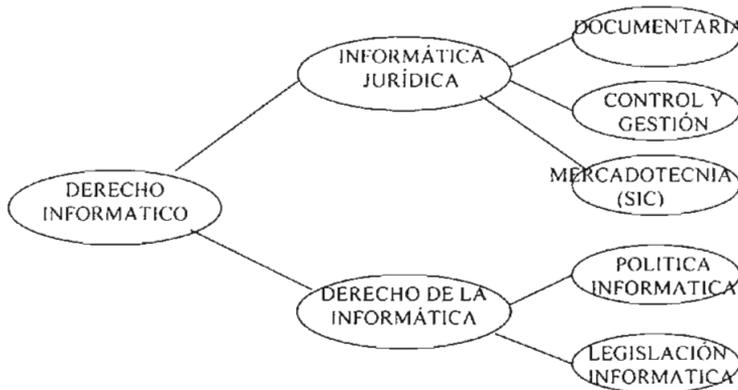
⁷² Téllez Valdés, Julio. Ob. cit. p. 17

⁷³ <http://www.hess-cr.com/cursos/diccionario/d.html>

⁷⁴ Piña Libien, Hiram Raúl. El Derecho Informático y su Autonomía como Nueva Rama del Derecho. www.ordenjuridico.gob.mx/Congreso/pdf/78.pdf

En cuanto a la naturaleza de el Derecho Informático ésta es mixta, ya que en parte es público por abarcar campos como el Derecho Internacional Público, al regular de manera internacional datos informáticos, hablar de jurisdicciones, etc.; así como el Derecho Constitucional, al tratar de proteger (aunque en nuestro país aun no lo hace expresamente) las garantías individuales de las posibles agresiones que puedan sufrir éstas por parte de la tecnología informática (preservación de información personal, derecho a la información, etc.); así como de Derecho Penal al tratar los delitos informáticos. En tanto que puede hablarse de Derecho Público en ciertas ramas como la contratación informática, la protección de software, entre otras.

Esquemáticamente el Derecho Informático ha sido clasificado por el maestro Julio Téllez Valdés de la siguiente forma⁷⁵:



1.3.1. Informática Jurídica

La Informática Jurídica puede ser definida como una rama de la informática que busca "el tratamiento lógico y automático de la información legal"⁷⁶. O bien como "la técnica interdisciplinaria que tiene por objeto el estudio e investigación de los conocimientos de la informática general, aplicables a la recuperación de información jurídica, así como la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de la información jurídica necesarios para lograr dicha recuperación"⁷⁷

Esta rama del Derecho Informático puede ser clasificada en tres categorías: la informática documentaría, que atiende al almacenamiento y recuperación (es decir automatización) de textos jurídicos como legislación, jurisprudencia y

⁷⁵ Téllez Valdés, Julio Ob. cit. p. 20

⁷⁶ http://es.wikipedia.org/wiki/Derecho_inform%Etico

⁷⁷ Téllez Valdés, Julio Ob. cit. p. 19

doctrina. En tanto que la informática jurídica de control y gestión, que se ocupa del desarrollo de actividades jurídicas “tendientes a la automatización de las tareas rutinarias que se efectúan en... cualquier despacho jurídico”⁷⁸; y la informática metadocumentaria que constituye un apoyo en la decisión, educación, investigación, redacción y previsión de los conflictos jurídicos.

Los primeros antecedentes de esta rama se remontan a la década de los cincuenta en los Estados Unidos (específicamente 1959) cuando se llevan a cabo las primeras investigaciones enfocadas a la recuperación de documentos jurídicos con el auxilio de computadoras (es decir de forma automatizada).

Esto marca un hito ya que las computadoras se apartan de sus tradicionales fines matemáticos, para enfocarse en objetivos lingüísticos. Uno de los primeros proyectos enfocados a este campo fue el emprendido por la Universidad de Pittsburg, por medio del Health Law Center, donde el director desarrolla elabora una serie de cintas magnéticas por medio de las cuales se hace posible el acceso automatizado a la información legal. Este sistema es presentado en 1960 a la American Association Boreau of Lawyars, en su reunión anual en Washington D.C.

A partir de entonces la evolución en este campo no se detendrá. En 1964 se lanza al mercado un sistema de procesamiento de datos legislativos desarrollado por la American Corporation of Data Recovery. Tres años después la Data Corporation de Datos de Dayton, Ohio suscribe un acuerdo con la barra de abogados del mismo Estado, mediante el que desarrollan el sistema OBAR (Ohio Bar of Automatized Reserch, dicho sistemas actualizado constantemente. Hasta 1973 cuando Mead Data Central toma el control y comercializa el sistema LEXIS, que se convierte en uno de los más rentables a nivel mundial.

En nuestro país la Ley Orgánica de la Administración Pública Federal, establece en su artículo 27, fracción XXXI, como facultad y obligación de la Secretaría de Gobernación: “Compilar y sistematizar las leyes, tratados internacionales, reglamentos, decretos, acuerdos y disposiciones federales, estatales y municipales, así como establecer el banco de datos correspondiente, con objeto de proporcionar información a través de los sistemas electrónicos de datos”⁷⁹

Para cumplir con dicho objetivo, la Secretaría de Gobernación crea la Dirección General de Compilación y Consulta del Orden Jurídico Nacional, dependiente de la Secretaria de Asuntos Jurídicos y Derechos Humanos. Actualmente, se puede consultar el orden jurídico nacional a través de la página de la Secretaría de Gobernación y de la página de la dirección general de compilación y consulta del orden jurídico nacional, quienes dirigen la búsqueda a otras páginas de los poderes públicos que las contengan.

⁷⁸ www.ordenjuridico.gob.mx/Congreso/pdf/79.pdf

⁷⁹ Ley Orgánica de la Administración Pública Federal

1.3.2. Derecho de la Informática

Siempre se pensó en los beneficios de la Informática, pero nunca en sus consecuencias. Es tratando de solucionar los problemas ya existentes y en un intento de prevenir los futuros que surge el Derecho de la Informática; "como una inevitable respuesta social al fenómeno informático y que por lo mismo es un Derecho en el que su existencia precede a su esencia"⁸⁰.

Para efectos del tema de la presente tesis nuestros estudios se ubicaran en el campo del Derecho de la Informática, ya que nos ocuparemos de algunas "normas, principios e instituciones que regulan el tratamiento automatizado de la información"⁸¹

El Derecho de la Informática puede ser definido como "el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la Informática"⁸²

A decir de algunos autores, podríamos considerar fuentes de Derecho de la Informática a la legislación, jurisprudencia y doctrina, sólo que en el caso particular del Derecho de la Informática el contenido de éstas sería de temas alusivos a la informática. Además de auxiliarse para el diseño y elaboración de los contenidos de dicho derecho de ciencias tales como: la Sociología, la Economía, la Filosofía, la Estadística, la Política Económica, etc.

Es importante aclarar que el Derecho de la Informática se encuentra aun en "construcción" por lo que necesita de muchos aportes en el campo doctrinal y dogmático. Será la labor de los juristas del futuro la construcción del Derecho de la Informática del Futuro.

1.3.2.1. Contratos Electrónicos

1.3.2.1.1. El Contrato en General

Entre las fuentes tradicionales de las obligaciones nos encontramos con los contratos; para el caso de las transacciones comerciales electrónicas, el contrato se ha perfilado como uno (quizás el más) importante de los instrumentos empleados en esta nueva modalidad comercial. Ya que es capaz de generar vínculos entre las partes; pero además es una figura lo suficientemente flexible para cumplir con las necesidades comerciales particulares de las transacciones electrónicas.

⁸⁰ Flores Gómez, Oswaldo. El Derecho Informático y su Autonomía como Nueva Rana del Derecho. www.ordenjuridico.gob.mx/Congreso/pdf/77.pdf

⁸¹ http://es.wikipedia.org/wiki/Derecho_inform%Etico

⁸² Téllez Valdés, Julio. Ob. cit. p. 21

De acuerdo con las leyes de nuestro país, el contrato es una especie de convenio, siendo este último de acuerdo con el artículo 1792 del Código Civil Vigente "(...) el acuerdo de dos o más personas para crear, transferir, modificar o extinguir obligaciones", en tanto que el artículo 1793 aclara que "los convenios que producen o transfieren las obligaciones y derechos toman el nombre de contratos".

"El contrato como todo convenio es un acto jurídico, una manifestación exterior de la voluntad tendiente a la producción de efectos de derecho sancionados por la ley"⁸³.

El contrato electrónico formalmente reconocido por la legislación de nuestro país debe de cumplir con los requisitos legales, solo que estos requisitos se verán matizados por las particularidades del medio donde se desarrolla el contrato. También es importante señalar que además de los anteriores el contrato electrónico requerirá de ciertos requisitos adicionales que el mismo medio donde se desarrolla, le exige para su mejor desenvolvimiento. Pero sin dejar de lado que sigue siendo un acuerdo de voluntades, lo único que cambia es la forma en que se expresa.

Aunque entre los teóricos hay opiniones discrepantes. Sobre el Contrato electrónico, una de ellas versa sobre la diferencia entre contratación electrónica y contratación informática. Existen dos corrientes doctrinales que hablan de ellas, la primera sostiene que la contratación electrónica es la que se "realiza mediante la utilización de elementos electrónicos que tienen incidencia en la formación de la voluntad, el desarrollo y la interpretación futura de algún acuerdo"⁸⁴, en tanto que la contratación informática es aquella "cuyo objeto o materia de una de las prestaciones, es un bien informático, servicio informático, o ambos"⁸⁵.

La segunda corriente encabezada por autores como Salvador Dario Bergel o Valentin Carrascosa López sostiene que "el término contratación informática se presenta en una doble acepción ya que en sentido amplio incluiría tanto la contratación de bienes y servicios, como la realizada a través de estos medios, y en un sentido más restringido se limitarían a la contratación de bienes y servicios"⁸⁶.

Por nuestra parte adoptaremos el primer criterio, ya que es el favorecido por la mayoría de los autores (incluso los mexicanos, como Julio Téllez), y el mayormente utilizado en el Derecho de la Informática Internacional. Aunque no podemos dejar de lado que la segunda corriente nos parece bastante interesante y visionaria, creemos que quizás en un futuro cuando la doctrina del Derecho de la Informática alcance un mayor desarrollo, dicha corriente será retomada y acogida por más juristas informáticos.

⁸³ Bejarano Sánchez. Manuel. *Obligaciones civiles*. 5ª ed. Oxford. México 1999 p. 27

⁸⁴ http://v2.vlex.com/es/ppv/doctrina/resultados.asp?query_doc=171892&n_orden=0

⁸⁵ *Ibidem*

⁸⁶ <http://www.injef.com/php/index.php?option=content&task=view&id=414&Itemid=35>

Otro punto de discrepancia entre los teóricos de la contratación electrónica es sobre la búsqueda una definición de contrato electrónico (aunque por nuestra parte insistimos que para el caso del contrato electrónico, lo único que cambia es el medio de expresión). Pero dada la controversia existente, es preciso tocar el tema.

Existen muchas definiciones de contrato electrónico, entre ellas tenemos: la que sostiene que los contratos electrónicos son "los contratos celebrados a distancia o sin que las partes - comprador y vendedor - estén presentes, que se realizan a través de equipos electrónicos de tratamiento y almacenamiento de datos (que son los medios de expresión de la voluntad)"⁸⁷. La definición anterior, igualmente afirma que existen ciertos tipos de contratos que no pueden ser celebrados vía electrónica, como son: 1. La compraventa de bienes inmuebles y creación de derechos sobre ellos. 2. Actividades que exigen la intervención de tribunales, autoridades públicas, notarios o registradores. 3. Contratos de crédito y caución. 4. Contratos que regulan relaciones familiares y de sucesiones.

Para otros es "todo contrato en que al menos la aceptación se trasmite por medio de equipos electrónicos de tratamiento y almacenamiento de datos, conectados a una red de telecomunicaciones"⁸⁸.

Incluso siendo más simplistas algunos consideran así al "contrato mundo real acordado en mundo virtual"⁸⁹.

En tanto que otros aseguran que es "todo contrato celebrado sin la presencia física simultánea de los factores, prestando este consentimiento en origen y destino por medio de equipos electrónicos de tratamiento y almacenamiento de datos, concertados por medio de cables, radio, medios ópticos o cualquier otro medio. No existe la presencia de las partes. El consentimiento se presta por medio electrónico y el soporte del documento queda de manera electrónica"⁹⁰.

Algunos más juzgan que se puede considerar como electrónico a "todo contrato celebrado sin la presencia física simultánea de las partes, prestando éstas su consentimiento en origen y destino por medio de equipos electrónicos de tratamiento y almacenaje de datos, concretados por medio de cable, radio, medios ópticos o cualquier otro medio"⁹¹ Esta definición es muy similar a la anterior.

"Por su parte el Profesor español Miguel Angel Davara Rodríguez, la considera como aquella que se realiza mediante la utilización de algún elemento

⁸⁷ <http://www.expansiondirecto.com/2000/02/10/tecnologia/5tec.html>

⁸⁸ <http://www.injef.com/php/index.php?option=content&task=view&id=414&Itemid=35>

⁸⁹ <http://www.utem.cl/cyt/derecho/contratacion.html>

⁹⁰ <http://www.injef.com/php/index.php?option=content&task=view&id=414&Itemid=35>

⁹¹ <http://www.utem.cl/cyt/derecho/contratacion.html>

electrónico cuando éste tiene, o puede tener, una incidencia real y directa de la voluntad o el desarrollo o interpretación futura del acuerdo"⁹²

Otros más piensan que el contrato electrónico es exactamente igual a un contrato "normal" la única diferencia radica en que "los elementos básicos de todo contrato se suman, en este caso, los aspectos particulares de la contratación electrónica y, en concreto, aquellos referentes a la identidad y representación de las partes, la simultaneidad de las comunicaciones o los requisitos de firma y documento escrito a efectos de prueba"⁹³

Del análisis de las anteriores definiciones concluimos que coinciden en los siguientes aspectos: En primer lugar la utilización en algún punto de la formación del contrato de medios electrónicos, ya sea por que el consentimiento de las partes se presta mediante estos sistemas, por un soporte documental electrónico u otro aspecto relacionado a los medios electrónicos. Y como segundo punto hablan de la ausencia física de las partes o mejor dicho la "no presencia simultanea". Aunque para nosotros el contrato electrónico es igual a cualquier contrato tradicional (por lo que la definición de contrato dada por nuestro Código Civil es válida para éste) sólo cambia la forma de expresión de la voluntad en éste, que en todo caso es por medios electrónicos.

1.3.2.1.2. Requisitos de Existencia

De acuerdo con nuestra legislación, los contratos precisan de ciertos requisitos para su existencia. De acuerdo con el artículo 1794 del Código Civil para el Distrito Federal *para la existencia de un contrato se requiere:*

- I. *Consentimiento*
- II. *Objeto que pueda ser materia del contrato.*

El Consentimiento, es "un acuerdo de voluntades (dos declaraciones unilaterales: oferta (o propuesta) y la aceptación): dos querer que se reúnen y constituyen una voluntad común"⁹⁴

El Objeto según la doctrina mexicana puede tener tres acepciones:

- 1- "El objeto directo del contrato, que es el *crear o transferir derechos y obligaciones.*
- 2- El objeto indirecto del contrato, que es el objeto de las obligaciones engendradas por él, y que puede consistir en *dar, hacer o no hacer, y*
- 3- *La cosa misma que se da*"⁹⁵

⁹² <http://www.injef.com/php/index.php?option=content&task=view&id=414&Itemid=35>

⁹³ <http://www.alfa-redi.org/revista/data/53-7.asp>

⁹⁴ Bejarano Sánchez, Manuel. *Obligaciones civiles*. 5ª ed. Oxford. México 1999 p. 47

Al respecto, la segunda acepción es la que corresponde a lo prescrito por el Código Civil para el Distrito Federal Vigente en su artículo 1824, que señala:

Son objeto de los contratos:

- I. *La Cosa que el obligado debe dar*
- II. *El hecho que el obligado debe hacer o no hacer*

Aplicando éstas y otras previsiones a los contratos electrónicos podríamos decir que un contrato electrónico tiene como los contratos tradicionales un objeto (en sus tres acepciones), dicho objeto debe de existir en la naturaleza (aún tratándose de bienes informáticos); ser determinado o determinable y estar dentro del comercio; así como ser lícito y posible.

Entre las particularidades que podría presentar a este respecto el contrato electrónico, son que existen ciertas materias que debido a su naturaleza y al consenso internacional no pueden ser tratadas en el marco de la contratación electrónica. La última versión del Anteproyecto de convención sobre la utilización de mensajes de datos en (el comercio internacional)(el contexto de los contratos internacionales) {A/CN.9/WG.IV/WP.108} de la Comisión de las Naciones para el Derecho Mercantil Internacional (CNUDMI); en su artículo 2° dedicado a las exclusiones señala:

La presente Convención no se aplicará a la utilización de los mensajes de datos (en relación con los siguientes contratos, bien sean existentes o previstos) (en el contexto de la formación o ejecución de los siguientes contratos):

- a) *Los contratos celebrados para fines personales, familiares o domésticos (salvo que la parte que ofrezca los bienes o servicios no supiera ni debiera haber sabido, en cualquier momento previo a la celebración del contrato o en el momento de su celebración, que estaban destinados a dicho uso).*
- b) *Los contratos por los que se autorice un uso ilimitado de derechos de propiedad intelectual*

El otro elemento que nuestra legislación exige para la existencia de un contrato es el consentimiento, que no es otra cosa que la declaración de la voluntad de las partes para la celebración de un contrato. Para la formación del consentimiento se requiere de "dos declaraciones unilaterales de la voluntad: la oferta (o propuesta) y la aceptación".⁹⁵ De este concepto que parecería tan simple se desprenden numerosas implicaciones jurídicas que afectan de forma muy clara a los contratos electrónicos.

Por lo que analizaremos ciertos puntos del consentimiento para el caso de los contratos electrónicos, haciendo de lado otros que son igual de importantes,

⁹⁵ Idem. p. 57

⁹⁶ Bejarano Sánchez, Manuel. *Obligaciones civiles*. 5ª ed. Oxford. México 1999 p. 47

pero que resultan irrelevantes para el presente estudio, ya que nuestro objetivo es desentrañar la Naturaleza Jurídica de la Entidad Certificadora, y no así del Contrato Electrónico, que aunque substancial, no nos ocupa directamente en este estudio.

En primer lugar el principio de autonomía de la voluntad (es decir el principio de libertad contractual) es reconocido plenamente por nuestra legislación en materia de comercio electrónico, ya que el artículo 89 del Código de Comercio Vigente estipula:

*... Las actividades reguladas por este título se someterán en su interpretación y aplicación a los principios de neutralidad tecnológica, **autonomía de la voluntad**, compatibilidad internacional y equivalencia funcional del mensaje de datos en relación con la información documentada en los medios no electrónicos y de la firma electrónica en relación con la firma autógrafa...*

De manera internacional, el ya mencionado Anteproyecto sobre contratación electrónica de la CNDUMI en su artículo 4° declara:

Las partes podrán excluir la aplicación de la presente Convención o establecer excepciones a cualquiera de sus disposiciones o modificar sus efectos

En cuanto a la expresión del consentimiento de las partes (o agentes electrónicos, como los llama el anteproyecto de la CNUDMI) en los contratos electrónicos, ésta puede ser expresada por medio de mensajes de datos a los que nuestro código mercantil vigente en su artículo 89 define como *"la información generada, enviada, recibida o archivada por medios electrónicos, ópticos o cualquier otra tecnología"* Se dice que el mensaje de datos proviene del emisor cuando como señala nuestro Código de Comercio Vigente:

ARTICULO 90. *Se presumirá que un mensaje de datos proviene del emisor (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 ESTE ES EL CASO, PERO QUE NO HAYA ACTUADO A TITULO DE INTERMEDIARIO) si ha sido enviado:*

I. Por el propio emisor;

II. Usando medios de identificación, tales como claves o contraseñas del emisor o por alguna persona facultada para actuar en nombre del emisor respecto a ese mensaje de datos, o

III. Por un sistema de información (TODO SISTEMA UTILIZADO PARA GENERAR, ENVIAR, RECIBIR, ARCHIVAR O PROCESAR DE ALGUNA OTRA FORMA MENSAJES DE DATOS) programado por el emisor o en su nombre para que opere automáticamente.

ARTICULO 90 BIS. *Se presume que un mensaje de datos ha sido enviado por el emisor y, por lo tanto, el destinatario o la parte que confía, en su caso, podrá actuar en consecuencia, cuando:*

I. Haya aplicado en forma adecuada el procedimiento acordado previamente con el emisor, con el fin de establecer que el mensaje de datos provenía efectivamente de éste, o

II. El mensaje de datos que reciba el destinatario (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) o la parte que confía (PERSONA QUE, SIENDO O NO EL DESTINATARIO, ACTUA SOBRE LA BASE DE UN CERTIFICADO O DE UNA FIRMA ELECTRONICA), resulte de los actos de un intermediario que le haya dado acceso a algún método utilizado por el emisor para identificar un mensaje de datos como propio..

Lo dispuesto en el presente artículo no se aplicará:

I. A partir del momento en que el destinatario o la parte que confía, haya sido informado por el emisor de que el mensaje de datos no provenía de éste, y haya dispuesto de un plazo razonable para actuar en consecuencia, o

II. A partir del momento en que el destinatario o la parte que confía, tenga conocimiento, o debiere tenerlo, de haber actuado con la debida diligencia o aplicando algún método convenido, que el mensaje de datos no provenía del emisor.

Salvo prueba en contrario y sin perjuicio del uso de cualquier otro método de verificación de la identidad del emisor, se presumirá que se actúo con la debida diligencia si el método que uso el destinatario o la parte que confía cumple con los requisitos establecidos en este Código para la verificación de la fiabilidad de las firmas electrónicas.

El momento en que las partes se ponen de acuerdo, es muy importante, ya que en ese instante surge el consentimiento y por lo tanto nace el contrato con todos sus efectos jurídicos. En el caso de los contratos electrónicos a los que se les podría considerar (como lo hemos señalado en definiciones anteriores) contratos entre no presentes.

Al tratarse de contratos entre no presentes, tendremos que remitirnos a la doctrina que maneja diversas teorías para tratar de explicar cuando se forma un contrato entre no presentes. Que son: La teoría de la Declaración (cuando el destinatario de la oferta declara, en cualquier forma, aceptarla), La Expedición (cuando el destinatario de la oferta contesta al proponente y expide su respuesta por algún medio), de la Recepción (cuando el proponente recibe en su domicilio o buzón la respuesta del aceptante) y La de la Información (Cuando el proponente se informa de la respuesta que contiene la aceptación).

La teoría que es adoptada por el Código de Comercio Vigente (y por lo tanto suponemos por las disposiciones en materia de Comercio Electrónico en el mismo Código) es la de la recepción; ya que de acuerdo a su artículo 80:

Los convenios o contratos mercantiles que se celebren por correspondencia, telégrafo o mediante el uso de medios electrónicos, ópticos o de cualquier otra tecnología, quedaran perfeccionados desde que se reciba la aceptación de la propuesta o las condiciones con que esta fuere modificada.

Pero veamos que dicen los artículos de nuestro Código de Comercio Vigente relativos al Comercio Electrónicos al respecto:

ARTICULO 91. *Salvo pacto en contrario entre el emisor y el destinatario, el momento de recepción del mensaje de datos se determinara como sigue:*

I. Si el destinatario ha designado un sistema de información para la recepción de mensaje 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 aún cuando el sistema de información este ubicado en un lugar distinto de donde se tenga por recibido el mensaje de datos conforma al artículo

ARTICULO 91 BIS. *Salvo pacto en contrario entre el emisor y el destinatario, el mensaje de datos se tendrá por expedido cuando ingrese en un sistema de información que no este bajo el control del emisor o del intermediario (TODA PERSONA QUE, ACTUANDO POR CUENTA DE OTRA, ENVIE, RECIBA O ARCHIVE UN MENSAJE DE DATOS O PRESTE ALGUN OTRO SERVICIO CON RESPECTO A EL.).*

ARTICULO 92. *En lo referente a acuse de recibo de mensajes de datos, se estará a lo siguiente:*

I. Si al enviar o antes de enviar un mensaje de datos, el emisor solicita o acuerda con el destinatario que se acuse el recibo del mensaje de datos, pero no se ha acordado entre estos una forma o método determinado para efectuarlo, se podrá acusar recibo mediante:

A) Toda comunicación del destinatario, automatizada o no, o

B) Todo acto del destinatario, que baste para indicar al emisor que se ha recibido el mensaje de datos.

II. Cuando el emisor haya indicado que los efectos del mensaje de datos estarán condicionados a la recepción de un acuse de recibo, se considerara que el mensaje de datos no ha sido enviado en tanto que no se haya recibido el acuse

de recibo en el plazo fijado por el emisor o dentro de un plazo razonable atendiendo a la naturaleza negocio, a partir del momento de envío del mensaje de datos;

III. Cuando el emisor haya solicitado o acordado con el destinatario que se acuse recibo del mensaje de datos, independientemente de la forma o método determinado para efectuarlo, salvo que:

A) El emisor no haya indicado expresamente que los efectos del mensaje de datos estén condicionados a la recepción del acuse de recibo, y

B) No se haya recibido el acuse de recibo en el plazo solicitado o acordado o, en su defecto, dentro de un plazo razonable atendiendo a la naturaleza del negocio.

El emisor podrá dar aviso al destinatario de que no ha recibido el acuse de recibo solicitado o acordado y fijar un nuevo plazo razonable para su recepción, contado a partir del momento de este aviso. Cuando el emisor reciba acuse de recibo del destinatario, se presumirá que éste ha recibido el mensaje de datos correspondiente;

IV. Cuando en el acuse de recibo se indique que el mensaje de datos recibido cumple con los requisitos técnicos convenidos o establecidos en ley, se presumirá que ello es así.

Como podemos ver en los citados artículos se respeta la teoría de la recepción adoptada por el Código Mercantil, pero adicionalmente se nos habla de acuses de recibo y otros mecanismos, que pensamos viene a apoyar la certidumbre en las transacciones electrónicas, lo cual creemos es sumamente importante para su cabal y futuro desarrollo.

Además del momento se concreta un contrato electrónico, también es importante la ubicación de las partes (o agentes electrónicos) que celebran el contrato, ya que esto auxiliará a la delimitación de jurisdicciones (un dolor de cabeza frecuente en las transacciones electrónicas). Nuestra legislación, habla de la ubicación de las partes en el artículo 94 del ya mencionado Código de Comercio

ARTICULO 94. *Salvo pacto en contrario entre el emisor y el destinatario, el mensaje de datos se tendrá por expedido en el lugar en donde el emisor tenga su establecimiento y por recibido en el lugar donde el destinatario tenga el suyo. Para fines del presente artículo:*

I. *Si el emisor o el destinatario tienen más de un establecimiento ¿, su establecimiento será el que guarde una relación más estrecha con la operación subyacente, su establecimiento principal, y*

II. *Si el emisor o el destinatario no tiene establecimiento, se tendrá en cuenta su lugar de residencia habitual.*

En cuanto a la oferta y la aceptación desde el punto doctrinal; podemos definir a la oferta como "una declaración unilateral de la voluntad, recepticia,

expresa o tácita, hecha a persona presente o no presente, determinada o indeterminada, con la expresión de los elementos esenciales de un contrato cuya celebración pretende el autor de esa voluntad, seria y hecha con ánimo de cumplir en su oportunidad"⁹⁷ la aceptación podíamos definirla como "una declaración unilateral de la voluntad en plena concordancia con los términos de la oferta"⁹⁸

Podríamos ahondar en la oferta y la aceptación en los contratos electrónicos, pero como mencionamos anteriormente eso sería materia de otro estudio; simplemente concluiremos con la oferta y la aceptación en los contratos electrónicos diciendo que a pesar de las particularidades del medio en el que se desarrollan los contratos electrónicos, tanto la primera como el segundo pueden ser claramente expresadas por medios electrónicos (con algunas de las particularidades referidas a ubicación y aceptación que mencionamos anteriormente).

1.3.2.1.3. Requisitos de Validez

La ley nos habla también de los requisitos necesarios para que un contrato sea considerado; el Código Civil, señala en su artículo 1795 que *el contrato puede ser invalidado*:

- I. *Por incapacidad legal de las partes o de una de ellas,*
- II. *Por vicios del consentimiento;*
- III. *Por su objeto, o su motivo o fin, sea ilícito;*
- IV. *Porque el consentimiento no se haya manifestado en la forma que la ley establece.*

"...Esta norma interpretada a contrario sensu, exige éstos:

1. - Capacidad de las partes que intervienen en el acto,
2. - Voluntad de esas personas, libre o exenta de vicios,
3. - Licitud en el objeto, motivo o fin del acto que se celebra,
4. - Observancia de las partes, de la forma que exija la ley, para externar la voluntad"⁹⁹

Para el caso de los contratos electrónicos, más que ahondar en teorías tradicionales de contratos, solamente mencionaremos las particularidades que presentan los contratos electrónicos en este campo.

En cuanto a la Capacidad de las partes que intervienen en el acto, ésta se ve afectada por ser un medio electrónico, ya que es difícil conocer quien en realidad realiza las transacciones. Pero se ha tratado de solucionar problemas

⁹⁷ Gutierrez y Gonzalez. Ernesto. Derecho de las obligaciones. 5ª ed. Cajica, S.A. México. 1984 p.209

⁹⁸ Bejarano Sánchez, Manuel. Obligaciones civiles. 5ª ed. Oxford. México 1999 p. 50

⁹⁹ Gutierrez y Gonzalez, Ernesto. Ob.cit. p.185

como estos mediante la creación de instrumentos de seguridad en las transacciones electrónicas como certificados, firma electrónica, entidades de certificación (de los que hablaremos más adelante) entre otros. Gracias a mecanismos de seguridad como los anteriores es prácticamente imposible que en una transacción electrónica entre grandes empresas o entidades gubernativas, se pueda falsear identidades. Pero no podemos decir lo mismo para el caso de pequeñas transacciones (transacciones al menudeo o entre particulares), por lo que para estos casos, legislaciones internacionales han buscado diversas soluciones.

En Francia valiéndose de una llamada "teoría de la apariencia", se responsabilizan a los padres por los actos celebrados por sus hijos menores de edad en virtud de que ellos "aparentan" ser mayores de edad en los medios electrónicos. Mientras que en Chile "se le denomina dolo de incapacidad por inducir a contratar. El Código Civil establece que si la parte incapaz ha manipulado fraudulentamente para inducir al acto o contrato, en este caso ni actor, ni los herederos o cesionarios podrán alegar nulidad, obligando al titular a realizar la obligación realizada por el menor"¹⁰⁰

Respecto a los vicios de la voluntad que de acuerdo a nuestra legislación son error, dolo, lesión, violencia, y mala fe. En cuanto al error en los contratos electrónicos, el Anteproyecto de CNUDMI en su artículo 14 relativo al error en las comunicaciones electrónicas enuncia:

1. *(Salvo acuerdo {expreso} en contrario de las partes) el contrato celebrado por una persona que acceda al sistema de información automatizado de otra persona no surtirá efecto jurídico alguno ni será ejecutorio si el iniciador cometió un error en su mensaje de datos y si el sistema de información automatizado no le brindó oportunidad alguna de prevenir o rectificar su error. La persona que invoque un error deberá notificarlo a la otra parte lo antes posible, haciendo saber que ha cometido un error en su mensaje de datos*
2. *Para poder invocar un error con arreglo al párrafo 1, toda persona deberá:*
 - a) *haber tomado medidas razonables, y haber seguido las instrucciones de la otra parte, para devolver los bienes o servicios recibidos, de haber recibido alguno, como consecuencia del error o, si se le ordena hacerlo, destruir dichos bienes o servicios; o*
 - b) *no haber utilizado los bienes o servicios recibidos de la otra parte, de haber recibido alguno, ni haber sacado de ellos ventaja o provecho material alguno.*

De esto debemos decir que el modelo e anteproyecto aún está en discusión; así que solo debemos observarlo como guía y tal vez tomar algunas ideas para lo que podría ser nuestra legislación en materia de contratación electrónica en un futuro.

¹⁰⁰ <http://www.injcf.com/php/index.php?option=content&task=view&id=414&Itemid=35>

Como vemos el Dolo, la Lesión, la Violencia y la Mala Fe pueden hacerse presentes en los contratos electrónicos. Conforme al artículo 1815 del Código Civil para el Distrito Federal entendemos a éstos como:

Se entiende por dolo en los contratos cualquier sugestión o artificio que se emplee para inducir a error o mantener en él a algunos de los contratantes, y por mala fe la disimulación del error de los contratantes, una vez conocido.

Pero debemos hacer hincapié en que, si hay algo que se trate de impedir en los contratos vía electrónica, es la presencia del Dolo y la Mala Fe. Es esencial que las transacciones electrónicas se desarrollen de forma lícita y normal, ya que de ello depende su incremento. Por lo que hablar de la licitud para la validez de un contrato electrónico sería redundar, ya que como hemos expresado en párrafos anteriores es un requisito "esencial" en los contratos electrónicos actuales.

En cuanto a las formalidades de que la ley puede exigir, se revista un contrato electrónico, existen artículos expresos en nuestro multicitado Código de Comercio Vigente que a saber rezan:

ARTICULO 93. *Cuando la ley exija la forma escrita para los actos, convenios o contratos, este supuesto se tendrá por cumplido tratándose del mensaje de datos, 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.*

Cuando adicionalmente la ley exija la firma de las partes, dicho requisito se tendrá por cumplido tratándose de mensajes de datos, siempre que sea atribuible a dichas partes.

En los casos en que la ley establezca como requisito que un acto jurídico deba otorgarse en instrumento ante fedatario público, este y las partes obligadas podrán, a través del mensaje 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 atribuyen dichos mensajes a las partes y conservar bajo su resguardo una versión íntegra de los mismos para su ulterior consulta, otorgando dicho documento de conformidad con la legislación aplicable que lo rige.

ARTICULO 93 BIS. *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, este requisito quedara satisfecho respecto a un mensaje de datos:*

l. Si existe alguna garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se genero por primera vez en su forma definitiva, como mensaje de datos 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 considerara que el contenido de un mensaje de datos 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. El grado de confiabilidad requerido será determinado conforme a los fines para los que se genero la información y de todas las circunstancias relevantes del caso.

Además de los anteriores un contrato electrónico requiere de elementos como la autenticidad, el no rechazo, sistemas de seguridad (tales como la firma digital avanzada), confidencialidad, entre otros, que lo respalden.

1.3.2.1.4. Contratación Electrónica en diversos códigos mexicanos

Respecto al punto vista legal; nuestra legislación reconoce como válida a la realización de actos previamente pactados en contratos escritos, en diversos códigos; como son: La Ley de Instituciones de Crédito, La Ley del Mercado de Valores, el Código de Comercio, el Código Civil Federal, la Ley Federal de Protección al Consumidor, Los Códigos Civiles de los Estados de Baja California Sur, Coahuila, Jalisco, Puebla, Yucatán; entre otros

En la Ley de Instituciones de Crédito, se autoriza en el artículo 31 *“Las instituciones de Banca de Desarrollo, proporcionaran a las autoridades y al público en general, información referente a sus operaciones utilizando medios electrónicos, ópticos o cualquier otra tecnología que les permita dar a conocer dicha información de acuerdo a las reglas de carácter general que la Secretaría de Hacienda y Crédito Público emita para tal efecto, en el cumplimiento de esta obligación, las Instituciones de Banca de Desarrollo observaran lo dispuesto en el artículo 117 de la ley de Instituciones de Crédito”*. Asimismo en su artículo 52 autoriza a las instituciones de crédito para *“pactar la celebración de sus operaciones y a 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, establecimiento de 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 al 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.*

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 sujetaran a las reglas de carácter general que en su caso, emita la Comisión Nacional Bancaria y de Valores.

Lo anterior, 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”.

El artículo 91 inciso II, segundo párrafo de la Ley del Mercado de Valores al reglamentar el contrato de intermediación bursátil, establece que *“las partes podrán convenir libremente el uso de carta, telégrafo, telex, telefax o cualquier otro medio electrónico, de computo o de telecomunicaciones para el envío, intercambio o en su caso confirmación de las ordenes 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”*; en el inciso V del mismo artículo establece: *“En caso de que las partes convengan el uso de medios electrónicos, de computo o de telecomunicaciones para el envío, intercambio y en su caso confirmación de las ordenes y demás avisos que deban darse, habrán de precisar las claves de identificación recíproca y las responsabilidades que conlleve su utilización.*

Las claves de identificación que se convenga utilizar conforme a este artículo sustituirán a la firma autógrafa por lo que las constancias documentales o técnicas en donde aparezcan, producirán los mismos efectos que las leyes otorguen a los documentos suscritos por las partes y, en consecuencia, tendrán igual valor probatorio.”

Las primeras reformas en materia de comercio electrónico en nuestro país datan de mayo del 2000, se aplicaron a diversos artículos del Código de Comercio, al Código Civil Federal, al Código Federal de Procedimientos Civiles y Ley de Federal de Protección al Consumidor. Nuevas reformas se introducirían en agosto de 2003 (que entrarían en vigor hasta el 27 de Agosto de ese mismo año) al Código de Comercio. Dichas reformas anexarían un Título Segundo que versa sobre el comercio electrónico. En estas reformas se autoriza el uso de medios electrónicos, ópticos y de cualquier otra tecnología en los actos de comercio y en la formación de ellos. Muestra de ello es el artículo 89 que reza *“en los actos de comercio podrán emplearse los medios electrónicos, ópticos o cualquier otra tecnología para efecto del presente código, a la información generada, enviada, recibida, archivada o comunicada a través de dichos medios se le denomina mensaje de datos”*. Las mencionadas reformas además de permitir la contratación electrónica tratan a figuras tales como el mensaje de datos, la firma electrónica, el prestador de servicios de certificación, el certificado; que son de medular importancia para la presente tesis, por lo que hablaremos con mayor profundidad de ellas en apartados posteriores.

La Ley Federal de Protección al Consumidor, dedica el capítulo VIII bis a los *"derechos de los consumidores en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología"* En dicho capítulo desglosa diversos derechos de los consumidores *"en línea"*.

El Código Civil Federal, al hablar de consentimiento en los contratos en su artículo 1803 menciona que *"será expreso cuando se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos..."*. Al mismo tiempo según lo señalado en su artículo 1805b equipara la oferta hecha entre presentes a la realizada por medios electrónicos, ópticos o de cualquier otra tecnología que permita la expresión de la oferta y la aceptación de ésta en forma inmediata. Finalmente al hablar de la forma de los contratos en su artículo 1834 bis, señala que los supuestos en cuanto a forma *"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 accesibles para su ulterior consulta"*;

En el panorama legislativo general de la contratación electrónica en nuestro país puede observarse una falta de uniformidad de vocablos y criterios para las nacientes tecnologías; así como la necesidad de un mayor desarrollo legislativo en campos como la contratación electrónica (aspectos como identidad, capacidad, legal existencia y facultades de representantes, etc.). Así también un mayor estudio de entidades tales como el "Prestador de Servicios de Certificación".

CAPITULO SEGUNDO. FIRMA ELECTRÓNICA

En el capítulo anterior nos ocupamos entre otros temas del comercio y la contratación electrónica; los cuales traen al Derecho tradicional nuevas modalidades integradoras de obligaciones; no es que hablemos de una nueva fuente de obligaciones, si no una forma distinta de expresar la voluntad proveniente de los avances tecnológicos que hacen posible que las transacciones comerciales sean mucho más rápidas, puedan desarrollarse a grandes distancias e incluso sean menos costosas, entre otros beneficios.

Pero la tecnología no ha traído sólo beneficios, el uso de medios electrónicos para transacciones comerciales, hace que éstas carezcan de un soporte documental tan tangible como podría ser el papel, que es el medio usualmente utilizado como elemento probatorio de las transacciones comerciales; lo que provoca que el contenido y validez de un documento electrónico que de fe de alguna transacción comercial pueda ser objeto de duda.

Por lo que en un afán de otorgar seguridad a esta nueva modalidad comercial, y permitir con esto un mejor desarrollo la tecnología ha traído diversas formas de protección de información, como lo son la firma electrónica y los certificados digitales. Que el Derecho se ve en la necesidad de regular, por la importancia que han adquirido en los últimos tiempos en el ámbito comercial.

Las primeras reformas en nuestros Códigos en materia comercial electrónica fueron publicadas en el Diario Oficial el 29 de mayo del 2000; adicionando varias disposiciones del Código Federal de Procedimientos Civiles, el Código Civil Federal, la Ley Federal de Protección al Consumidor y el Código de Comercio. Dichas reformas (de las que hablamos en el capítulo anterior) sólo fueron un pequeño esbozo de lo que en realidad se planeaba establecer en nuestro Códigos en cuanto a transacciones comerciales electrónicas, ya que los involucrados en la creación de normas en materia de comercio electrónico esperaban la aprobación de la Ley Modelo de CNUDMI de Firmas Electrónicas; para que sus disposiciones no fueran discordantes a las de este importante organismo comercial internacional.

Finalmente, para el 2001 la Ley Modelo sobre Firmas Electrónicas fue aprobada por la CNUDMI, ese mismo año (5 y 6 de Septiembre) el Congreso Convoco a un Foro sobre "Avances en la Legislación en Materia de Comercio Electrónico", en el que ahondaremos posteriormente, cuando hablemos de la historia de la firma electrónica en México.

Resultado de dicho foro se integró el Grupo de Trabajo encargado de elaborar la iniciativa de Reformas y Adiciones al Código de Comercio en Materia de Firma Electrónica; que fue presentada el 15 de Mayo de 2002, aprobada el 26 de noviembre por la Cámara de Diputados por 422 votos a favor y 1 abstención, en tanto que en la Cámara de Senadores fue aprobada el 8 de abril del 2003, por

unanimidad, verificándose entonces su publicación el 29 de agosto de 2003 y estableciéndose una vigencia de 90 días después de haber sido publicada en el Diario Oficial de la Federación.

Estas reformas versarían sobre figuras que ya aparecían en diversos ordenamientos, como la Ley del Mercado de Valores; pero que requerían de una regulación más extensa. Por lo que en estas reformas se trato con más detenimiento a figuras como la firma electrónica, el certificado digital, la entidad certificadora, etc. Tal como hemos mencionado anteriormente el objetivo del presente trabajo de Tesis es desentrañar la naturaleza jurídica de una de las figuras surgidas de dichas reformas: la entidad encargada de otorgar los certificados digitales; pero para poder llegar a este punto debemos abordar previamente otras figuras del Derecho y de la Tecnología, para que así el alcance de ésta sea comprendido. Entre las figuras necesarias para descifrar a la entidad certificadora está la firma electrónica, de la que se ocupará el presente capítulo.

2.1 Los mensajes de datos o documentos electrónicos

Al hablar de firmas electrónicas uno de los primeros puntos que se hace necesario abordar son los mensajes de datos o documentos electrónicos. Ya que la firma electrónica es utilizada principalmente para "firmar" un mensaje de datos o documento electrónico.

El artículo 89 del Código de Comercio Vigente en su segundo párrafo puntualiza que de acuerdo con el principio de equivalencia funcional, se establece la semejanza "*...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...*". De la misma forma dicho artículo en párrafos posteriores define al mensaje de datos como "*la Información generada, enviada, recibida, o archivada por medios electrónicos, ópticos o cualquier otra tecnología*".

Por lo expresado en dicho artículo un mensaje de datos o documento electrónico para efectos jurídicos tendría la misma validez que un documento en el sentido jurídico tradicional y la firma electrónica equivaldrá a una autógrafa.

El documento jurídicamente es una "Representación material idónea para poner de manifiesto la existencia de un hecho o acto jurídico (acontecimiento de la vida independientemente de la voluntad humana, contrato, testamento, sentencia, etc.), susceptible de servir en caso necesario como elemento probatorio."¹⁰¹. El Código de Procedimientos Civiles Vigente para el Distrito Federal nos habla de dos tipos de Documentos: los documentos públicos y los documentos privados.

¹⁰¹ De Pina Vara, Rafael. Diccionario de Derecho. 24ed. Porrúa, México, 1997. p. 255

De acuerdo con doctrinarios del derecho “el documento es de carácter público, cuando es producido por un órgano de la autoridad en ejercicio legítimo de sus atribuciones”¹⁰². El Código de Procedimientos Civiles en su artículo 327 nos hace una enumeración de los documentos que legalmente son considerados públicos como son:

- I. *Las escrituras públicas, pólizas y actas otorgadas ante notario o corredor público y los testimonios y copias certificadas de dichos documentos;*
- II. *Los documentos auténticos expedidos por funcionarios que desempeñen cargo público, en lo que se refiere al ejercicio de sus funciones;*
- III. *Los documentos auténticos, libros de actas, estatutos, registros y catastros que se hallen en los archivos públicos, o los dependientes del Gobierno Federal, de los Estados, de los Ayuntamientos o del Distrito Federal;*
- IV. *Las certificaciones de las actas del estado civil expedidas por los jueces del Registro Civil, respecto a constancias existentes en los libros correspondientes;*
- V. *Las certificaciones de constancias existentes en los archivos públicos expedidas por funcionarios a quienes compete;*
- VI. *Las certificaciones de constancias existentes en los archivos parroquiales y que se refieran a actos pasados, antes del establecimiento del Registro Civil, siempre que fueren cotejadas por notario público o quien haga sus veces con arreglo a derecho;*
- VII. *Las ordenanzas, estatutos, reglamentos y actas de sociedades o asociaciones, universidades, siempre que estuvieren aprobados por el Gobierno Federal o de los Estados, y las copias certificadas que de ellos se expidieren;*
- VIII. *Las actuaciones judiciales de toda especie;*
- IX. *Las certificaciones que expidieren las bolsas mercantiles o mineras autorizadas por la ley y las expedidas por corredores titulados con arreglo al Código de Comercio;*
- X. *Los demás a los que se les reconozca ese carácter por la ley;*

Siendo así que los documentos privados por exclusión serían “todos aquellos que no son públicos y que por lo tanto son producidos o elaborados por los particulares”¹⁰³. El artículo 334 del citado Código señala que “*Son documentos privados los vales, pagarés, libros de cuentas, cartas y demás escritos firmados o formados por las partes o de su orden y que no estén autorizados por escribanos o funcionario competente*”

Por lo que el mensaje de datos al ser equiparado a cualquier otro documento jurídico puede ser privado o público. Privado cuanto como hemos visto sea otorgado por particulares. En tanto que serán públicos cuando cumplan con los requisitos que la ley prescribe para tal tipo de documentos. En todo caso, como lo señala el artículo 89 bis. “*No se negaran efectos jurídicos, validez o fuerza obligatoria a cualquier tipo de información por la sola razón de que esté contenida en un mensaje de datos*”.

¹⁰² Gómez Lara, Cipriano. *Teoría General del Proceso*. 9ª ed. Oxford. México, 200. p. 276

¹⁰³ *Ibidem*

En todo caso, como habíamos mencionado anteriormente el código mercantil vigente en su artículo 89 define como *“la información generada, enviada, recibida o archivada por medios electrónicos, ópticos o cualquier otra tecnología”*.

Otro de los Códigos que se ocupa de los documentos digitales es el Código Fiscal Vigente; que en su artículo 17-D, señala que *“Se entiende por documento digital todo mensaje de datos que contiene información o escritura generada, enviada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología”* Dicha definición es idéntica a la del Código de Comercio; esto nos habla de una coherencia legislativa en materia de normatividad electrónica, lo que resulta muy positivo ya que una unificación de reglas permite un sano desarrollo gubernamental y/o comercial; además de dar lugar a la existencia de una confianza entre partes; que es esencial para el desarrollo de las transacciones vía electrónica, que si de algo sufren es de incertidumbre por el medio en que se desarrollan.

En tanto que la Norma Oficial Mexicana NOM-151-SCFI-2002, Sobre Prácticas comerciales - Requisitos que deben observarse para la conservación de mensajes de datos; define al mensaje de datos como *la información generada, enviada, recibida, archivada o comunicada a través de medios electrónicos, ópticos o cualquier otra tecnología*.

Pero es preciso señalar que muchas de las definiciones adoptadas por nuestros legisladores están basadas en reglas aceptadas internacionalmente; con el fin de facilitar la tarea a las empresas mexicanas en las transacciones internacionales.

Uno de los documentos que los legisladores mexicanos tomaron como base para la elaboración nuestra legislación en materia electrónica, es la ley modelo de la CNUDMI sobre comercio electrónico con la guía para su incorporación al derecho interno de 1996. Que en su artículo segundo al abordar algunas definiciones, precisa que *“por ‘mensaje de datos’ se entenderá la información generada, enviada, recibida o archivada o comunicada 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”*

Las similitudes entre ambas definiciones son claras; sin embargo existen algunas modificaciones introducidas por nuestros legisladores, como son el no hablar de “información comunicada”, lo que consideramos un acierto, ya que al hablar de enviar y recibir, se sobreentiende el hecho de comunicar. Otro punto en que la definición dada en nuestro ordenamiento dista de la CNUDMI, es la enumeración que ésta hace, para simplemente limitarse nuestro ordenamiento a decir “cualquier otra tecnología”

Posterior a la ley de comercio electrónico, la CNUDMI da a conocer La Ley Modelo de la CNUDMI sobre Firma Electrónicas, que en su artículo 2 al tocar las definiciones dice que *“por mensaje de datos se entenderá la información*

generada, enviada, recibida o archivada o comunicada 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". Esta definición es idéntica a la de la ley modelo sobre comercio electrónico, y en el Anteproyecto de Convención sobre Contratación Electrónica, la definición es similar, lo único que cambia es que al igual que en nuestra legislación, las palabras: "o comunicada" han sido suprimidas. Consideramos que estas definiciones obedecen a que la CNUDMI, lo hace con un afán de uniformidad de criterios comerciales internacionales.

Para efectos de la presente tesis adoptaremos la definición que da el Código de Comercio Vigente.

En el capítulo pasado al hablar de contratación electrónica, citamos diversos artículos del Código Mercantil Vigente que hacen alusión al mensaje de datos. Por lo que sería reiterativo volverlos a citar, simplemente abordaremos algunos puntos que consideramos trascendentales de cada artículo así como de los requisitos que consideramos necesarios para que un mensaje sea considerado legalmente válido.

Dentro de los temas más importantes que trata en apartado dedicado a los mensajes de datos dentro del Comercio Electrónico del Código de Comercio Vigente; tenemos lo dispuesto en el artículo 89 que cita cuatro principios por los que se interpretaran y aplicaran las normas de naturaleza electrónica. Dichos principios son: el de Neutralidad Tecnológica, el de Compatibilidad Internacional, Equivalencia Funcional y el de Autonomía de la Voluntad.

Ya habíamos abordado un poco a los principios de Equivalencia Funcional y Autonomía de la voluntad. La Autonomía de la voluntad estará presente en mucha de las transacciones que se lleven por vía electrónica, ya que cuestiones como domicilios de envío, recepción, acuses de recibo, entre otras; podrán ser objeto de acuerdo entre las partes.

La Equivalencia funcional, que hace posible la equiparación de los mensajes de datos con los documentos escritos tradicionales. Para ser considerado equiparable, el mensaje debe de ser reconocido por la ley como válido (además servir la validez para funciones probatorias y prácticas). Para ser considerado como válido tenemos que hay tres requisitos principales que debe llenar un mensaje de datos: la Integridad, la Atribución y la Accesibilidad.

La Integridad, que a su vez se subdivide en dos categorías: la primera que alude a la fiabilidad del método para generar, recibir, comunicar y archivar los mensajes de datos; y la segunda que se refiere a la forma de garantizar que la información en él contenida no fue alterada.

Para que este requisito dispuesto por el segundo párrafo del artículo 49, pueda ser cumplido cabalmente, la Secretaría de Economía elaboró una Norma

Oficial (NOM-151-SCFI-2002) que versa sobre los requisitos que deben de observarse para la conservación de los mensajes de datos, que a la fe reza: *“...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 Comercio y Fomento Industrial emitirá la Norma Oficial Mexicana que establezca los requisitos que deberán observarse para la conservación de los mensajes de datos”*

El texto final de la norma fue firmado el 19 de marzo de 2002, y su publicación se llevó a cabo en el Diario Oficial de la Federación el 4 de junio del 2002, para su entrada en vigor se estableció que debía existir la infraestructura necesaria, además de darse un aviso oficial en el Diario Oficial de la Federación.

La estructura del Reglamento a grandes rasgos es la siguiente:

0. Introducción
1. Objetivo
2. Campo de aplicación
3. Definiciones
4. Disposiciones generales
5. Elementos que intervienen en la conservación de mensajes de datos
6. Vigilancia
7. Apéndice normativo
8. Bibliografía
9. Concordancia con normas internacionales

La Atribución hace referencia a la forma de asegurar que las partes unidas por una relación jurídica expresan su voluntad sin ningún vicio y acreditan su personalidad cabalmente. Para lograr esto se ha recurrido a medidas de seguridad en las transacciones electrónicas como la firma electrónica. De esto hablaremos con más profundidad en apartados posteriores, baste decir que esta puede ser simple o avanzada.

En tanto que la Accesibilidad versa sobre el hecho de que el contenido de un mensaje de datos, pueda ser consultado posteriormente por cualquier usuario interesado en conocer el texto (autoridad, juez, emisor, auditor, receptor, etc.). Siempre y cuando dicho texto reúna los requisitos de Integridad y Atribución, mencionados anteriormente. El medio material en el cual se creo el mensaje puede variar del medio de consulta (por ejemplo: de un disco duro a un disquete)

Actualmente no existe una legislación federal que aborde la forma de presentar la información a los usuarios de los mensaje de datos; por lo que será

labor de los legisladores establecer las reglas necesarias en el futuro para que este requisito se revista de la normatividad necesaria.

En cuanto a los dos principios restantes que rigen a los mensajes de datos, podemos decir que; la Neutralidad Tecnológica hace referencia a que, en las transacciones comerciales electrónicas no se debe de privilegiar a ningún tipo de tecnología, porque esto sería discriminatorio, además que podría dar pie a la creación de monopolios tecnológicos para las transacciones comerciales entre otras consecuencias.

En tanto que la Compatibilidad Internacional trata de la obligación de los agentes involucrados en los actos de comercio electrónicos de cumplir con los estándares internacionales, como son las normas de la CNUDMI, la OMPI, ISO, entre otras; con el fin lograr una congruencia internacional y evitar futuros conflictos.

Sobre la presunción de envío, recibo y acuses de recibo a los que aluden los artículos del Código Mercantil citados anteriormente, podemos decir que en general se presume que un mensaje proviene del emisor si: éste utiliza medios de identificación propios; o bien se vale de un sistema de identificación programado por el emisor o en su nombre para que opere automáticamente. En cuanto a la recepción, los Acuses de recibo podrán ser requeridos en las transacciones electrónicas por disposición legal o convenio entre las partes. Para el caso de ser utilizados se tendrá por enviado un mensaje de datos cuando se reciba el acuse de recibo; así como se tendrá por recibido cuando el emisor reciba el acuse de recibido.

Para el caso de que la ley establezca la necesidad de instrumento público; el fedatario deberá conservar una versión íntegra para ulteriores consultas, además de consignar los elementos para atribuir el acto.

En cuanto al lugar de expedición y envío, en cualquiera de los dos casos las partes pueden acordar el lugar que se tomará como legalmente válido para cualquier efecto, o en todo caso, como lugar de emisión se tomará el del domicilio del emisor y como de recepción el del domicilio del receptor.

El mensaje de datos será admisible como un medio de prueba, y su valoración como tal dependerá de la fiabilidad de la forma de generación del archivo, su conservación y comunicación.

2.2 La Firma Autógrafa.

Etimológicamente "el vocablo firma proviene del latín *firmare* que significa afirmar, dar fuerza y el vocablo *autógrafa* significa grabar o escribir por sí mismo y se aplica al escrito de mano de su propio autor en el entendido que los signos o

trazos han de ser hechos por la mano del autor sin que la impresión se realice por medios mecánicos”¹⁰⁴

Desde el punto de vista filológico el Diccionario Porrúa de la Lengua española define a la firma como “Nombre y apellido o título de una persona que ésta pone, con su rúbrica, al pie de un documento para darle autenticidad..”¹⁰⁵

En tanto que el Diccionario de Derecho de Rafael de Pina Vara la define como “Nombre y apellido (o apellidos) que una persona pone, con rúbrica o sin ella, al pie de un escrito, como señal de autenticidad”¹⁰⁶

Si nos remontamos a los orígenes de la humanidad; “la organización primitiva del hombre es comunal, con igualdad de derechos y de propiedades entre todos los miembros del grupo. Todos participaban en la recolección, la caza y la pesca. Sólo hay una división del trabajo muy sencilla, fundamentalmente entre hombres y mujeres. Se inicia apenas la existencia de los artesanos especializados, en los magos y artistas del Paleolítico; posteriormente aparecen los alfareros, metalúrgicos y otros especialistas”¹⁰⁷ Posteriormente “La creciente productividad y la mayor división del trabajo da lugar en el cuarto milenio a.C., a la aparición de las ciudades: centro artesanales, comerciales, administrativos y religiosos”¹⁰⁸

“El mejoramiento de la producción y el incremento del comercio traen consigo la necesidad de llevar cuentas y de apuntar algunos hechos. Se desarrolla la numeración y después la escritura, que principia en forma pictográfica (se dibujan ciertas cosas, lo que dificulta la representación de ideas abstractas), para dar lugar, a través de una evolución bastante larga y compleja, a la escritura fonética, en la cual cada signo representa un sonido. Esta escritura permite apuntar todo lo que puede expresarse en palabras”¹⁰⁹

Históricamente se considera que la historia nace con el desarrollo de la escritura, que permite la preservación de la memoria humana en documentos escritos. El desarrollo de la escritura da pie a medios de identificación personales como la firma. Por lo que siguiendo lo expuesto por el maestro Miguel Acosta Romero¹¹⁰, los primeros antecedentes históricos de la firma los podemos encontrar en los alfabetos de los fenicios, egipcios y griegos; así como en las civilizaciones tan antiguas como la cretense y sumeria.

¹⁰⁴ Bravo Machado, Antonio: Seguridad en transacciones por Internet: Universidad Panamericana; Tesis para obtener el título de licenciado en derecho: 2001 cit. por Reyes Krafft, Alfredo Alejandro. La firma electrónica y las entidades de certificación. Porrúa., México 2003 p.85

¹⁰⁵ Raluy Poudevida, Antonio. Diccionario Porrúa de la Lengua Española. 48ª ed. Porrúa. México. 2003

¹⁰⁶ De Pina Vara, Rafael. Ob. cit.

¹⁰⁷ Brom, Juan. Esbozo de Historia Universal. 19ª ed. Grijalbo. México. 1998 p.36

¹⁰⁸ Ibidem

¹⁰⁹ Idem p. 35

¹¹⁰ Cfr. Acosta Romero, Miguel. Nuevo Derecho Mercantil. 2ª ed. Porrúa. México. 2003 p.50

Ya hemos hablado del Antiguo Imperio Romano; para el caso de la firma, ésta no era una costumbre ni una necesidad en esta civilización, sin embargo existía una ceremonia denominada “manufirmatio” en la cual tras la lectura de un documento por el “notarius” o su creador, éste era tendido sobre una superficie donde posteriormente era recorrido por la mano a forma de aceptación; después de lo cual se estampaban, ya bien tres cruces o el nombre del autor, así como de los testigos.

Posteriormente en los tiempos del Imperio Visigodo surgiría la confirmación de un documento por diversos métodos: la subscripción o signatura (stipulatio, firmatio, roboratio) y el tocamiento (chartam tangere). Pero la primera se hace especialmente importante a partir de la era euriciana en las que se establecen regulaciones específicas para esta; se establecieron la “subscriptio” (que era la indicación de la fecha y el nombre del signante) y el “suscriptio” (un rasgo de suplencia que hacía las veces de subscriptio para aquellos que no podían o no sabían escribir), la primera daba pleno valor probatorio a un documento; mientras que la segunda debía de ser completada por un juramento de veracidad de algún testigo¹¹¹.

El analfabetismo de los gobernantes de la Edad Media (no así de los ministros religiosos) hacía que figuras como Carlo Magno se vieran en la necesidad de utilizar rasgos arbitrario, letras, cruces u otro tipo de inscripciones para hacer patente su consentimiento en documentos públicos. Casi al mismo tiempo surge “el sello” que hace las veces de la inscripción manuscrita, que se vuelve muy popular entre los nobles iletrados.

La situación cultural no mejoraría durante el periodo, a pesar de ello, en documentos posteriores de la Edad Media, junto con el sello se haría costumbre utilizar las firmas (aunque fueran simples cruces) para autenticar los documentos. Llegando esto a hacerse oficial como en el caso de Carlos V de Francia, que en Octubre de 1358, hizo obligatorio a los escribanos (considerados oficiales públicos), suscribir en los actos que pasasen por sus manos además de sus signos, sus firmas.

Con el tiempo se establecería una diferenciación entre signos y firmas, viendo que estas últimas, eran “más que simples signos eran la inscripción manuscrita de del nombre o de los apellidos”¹¹². El desarrollo del comercio y una mayor instrucción de la población hicieron que la firma “fuera adquiriendo la importancia y uso que con el transcurso del tiempo se fue consagrando como un símbolo de identificación y de enlace entre el autor de lo escrito o estampado y su persona”¹¹³

¹¹¹ Ctr. Reyes Krafft, Alfredo Alejandro. La firma electrónica y las entidades de certificación. Porrúa, México 2003 p. 86

¹¹² Acosta Romero, Miguel. Nuevo Derecho Mercantil. 2ª ed. Porrúa, México, 2003 p. 560

¹¹³ Idem p. 561

Además de los usos comerciales, los artistas se valieron de las firmas para identificar a sus obras como propias, como el famoso artista renacentista Miguel Ángel, o del pintor Alberto Durero, entre otros miles; incluso los artistas orientales se valieron de la firma en sus creaciones artísticas.

2.2.1 Concepto

Siguiendo lo expresado por el maestro Miguel Acosta Romero "la firma es el conjunto de letras y signos entrelazados, que identifican a la persona que la estampa, con un documento o un texto."¹¹⁴. La firma puede ser de diversas clases como son:

- a) Autógrafa.
- b) En facsímil
- c) Mecánica
- d) De la persona física
- e) De la persona jurídica colectiva (a través de sus órganos de administración o representación)
- f) Con lápiz o con tinta
- g) Con otros instrumentos de escritura
- h) La firma electrónica

Para el caso de la firma autógrafa podemos definirla como aquella "que suscribe la persona física con su propia mano y consiste en un conjunto de letras o bien algún componente de su nombre y a veces el nombre y el apellido, aunado a una serie de trazos que pueden abarcar toda gama de evoluciones del instrumento de escritura, que señalan e identifican al sujeto y lo separan de otros, en los documentos que suscribe y es un elemento que refleja permanentemente su voluntad de expresar lo que firma, o de obligarse al tenor del texto que suscribe"¹¹⁵

Autores clásicos del Derecho como Mustapich, así como Planiol y Ripert¹¹⁶ al hablar de firma establecen que ésta debe de contener ya bien el nombre del suscriptor, o bien caracteres alfabéticos, lo que nos haría pensar que las firmas actuales (que muchas veces son simples trazos) no serían en derecho firmas, ya que no cumplirían con los elementos anteriormente planteados. Por lo que la búsqueda de una definición de firma autógrafa que se adapte a la realidad de nuestros tiempos debe ser menos estricta.

Actualmente el hecho de que los signos expresados de forma manuscrita contengan caracteres alfabéticos, o bien, el nombre y/o los apellidos del autor no es importante. El punto medular al que los juristas deben atender al tratar a las

¹¹⁴ Ibidem

¹¹⁵ Reyes Krafft, Alfredo Alejandro Ob. Cit., p. 87

¹¹⁶ Véase. Reyes Krafft, Alfredo Alejandro Ob. Cit. y Acosta Romero, Miguel. Ob. cit.

firmas es “el ánimo de obligarse al reconocimiento del contenido del escrito en que se estampe”¹¹⁷

Para el caso de las personas morales, también llamadas personas jurídicas colectivas, podrán firmar por medio de sus legítimos representantes, que así hayan sido autorizados por los órganos de representación y administración.

Las personas físicas o jurídicas individuales, no representan mayor problema, al poder suscribir personalmente. En todo caso los impedimentos vendrían para las personas que por problemas físicos o falta de instrucción no pudieran hacerlo; en cuyo caso estaríamos frente al uso de la Huella Digital como medio de identificación; así como la firma a ruego.

Algunos de los preceptos de nuestro ordenamiento jurídico, que establecen las características de la firma en los documentos son: el artículo 1165 del Código de Comercio que reza:

*“El documento privado que contenga deuda líquida y sea de plazo cumplido, permitirá al acreedor, promover medios preparatorios a juicio, exhibiendo el documento al juez a quien se le hará saber el origen del adeudo, solicitándole que ordene el **reconocimiento de la firma**, monto del adeudo y causa del mismo.*

*Para tal fin, el juez ordenará al actuario o ejecutor que se apersona en el domicilio del **deudor para que se le requiera que bajo protesta de decir verdad, haga reconocimiento de su firma**, así como del origen y monto del adeudo, y en el mismo acto se entregue cédula de notificación en que se encuentre transcrita la orden del juez, así como copia simple cotejada y sellada de la solicitud.*

De no entenderse la diligencia personalmente con el deudor cuando se trate de persona física o del mandatario para pleitos y cobranzas o actos de dominio tratándose de personas morales o del representante legal, en otros casos, el actuario o ejecutor se abstendrá de hacer requerimiento alguno, y dejará citatorio para que ese deudor, mandatario o representante legal, lo espere para la práctica de diligencia judicial en aquellas horas que se señale en el citatorio, la que se practicará después de las seis y hasta las setenta y dos horas siguientes. También el actuario o ejecutor podrá, sin necesidad de providencia judicial, trasladarse a otro u otros domicilios en el que se pueda encontrar el deudor, con la obligación de dejar constancia de estas circunstancias. Si después de realizadas hasta un máximo de cinco búsquedas del deudor éste no fuere localizado, se darán por concluidos los medios preparatorios a juicio, devolviéndose al interesado los documentos exhibidos y dejando a salvo sus derechos para que los haga valer en la vía y forma que corresponda.

¹¹⁷ Acosta Romero, Miguel. *Ob. cit* p. 562

Cuando fuere localizado el deudor, su mandatario o representante, e intimado dos veces rehuse contestar si es o no es suya la firma, se tendrá por reconocida, y así lo declarará el juez.

Cuando reconozca la firma, más no el origen o el monto del adeudo, el actuario o ejecutor lo prevendrá para que en el acto de la diligencia o dentro de los cinco días siguientes exhiba las pruebas documentales que acredite su contestación. De no exhibirse, el juez lo tendrá por cierto en la certeza de la deuda señalada, o por la cantidad que deje de acreditarse que no se adeuda, al igual que cuando reconozca la firma origen o monto del adeudo.

Cuando el deudor desconozca su firma se dejarán a salvo los derechos del promovente para que los haga valer en la vía y forma correspondiente pero de acreditarse la falsedad en que incurrió el deudor, se dará vista al Ministerio Público.

Lo mismo se hará con el mandatario o representante legal del deudor que actúe en la misma forma que lo señalado en el párrafo anterior.

Cuando se tenga por reconocida la firma o por cierta la certeza de la deuda, se ordenará la expedición de copias certificadas de todo lo actuado a favor del promovente y a su costa.

El actor formulará su demanda en vía ejecutiva, ante el mismo juez que conoció de los medios preparatorios acompañando la copia certificada como documento fundatorio de su acción, copias simples de éstas y demás que se requieran para traslado al demandado, y se acumularán los dos expedientes y en su caso se despachará auto de ejecución.

Cuando se despache auto de ejecución, se seguirá el juicio en la vía ejecutiva como marca la ley para los de su clase.

La resolución que niegue el auto de ejecución será apelable en ambos efectos, y en caso contrario se admitirá en el efecto devolutivo."

Tras analizar el precepto concluimos que la ley en ningún momento establece requisitos específicos como ciertos caracteres o nombre, para que un documento pueda considerarse firmado; jurídicamente la importancia reside en el reconocimiento de cierto signo como propio, como ya lo habíamos mencionado anteriormente, es el llamado "animus signandi".

Es de mencionar que no toda firma tiene efectos jurídicos, pero existen algunos que acarrea el colocar nuestra firma en algún documento, escrito u obra de arte, de acuerdo con los artículos 204 y 206 del Código Federal de Procedimientos Civiles:

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 suscripción la colocación, al pie del escrito, de las palabras que, con respecto al destino del mismo, sean idóneas para identificar a la persona que suscribe.

La suscripción 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 suscripción

Artículo 206

Se considerará autor de los libros de comercio, registrados domésticos y demás documentos que no se acostumbra suscribir, 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 objeto, 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."

A decir de autores como Carnelutti¹¹⁸ la firma de nuestros días funde en sí, la declaración del patronato y la manifestación del autor, que originalmente eran dos elementos aislados. Todo para identificar a aquel que suscribe un documento.

Por lo que debemos concluir que conforme a lo expresado por los ordenamientos de nuestro país, un documento vale en cuanto está firmado y si no está firmado, no tiene ninguna validez.

¹¹⁸ Cfr. Reyes Krafft, Alfredo Alejandro Ob. Cit p.91

2.2.2 La firma en el derecho bancario mexicano¹¹⁹

Para hablar de la firma autógrafa en el Derecho Bancario Mexicano, citaremos diversos artículos de la ley Bancaria en los que se trata a la firma autógrafa, quizás no sea un estudio exhaustivo de la firma autógrafa en el Derecho Bancario Mexicano, pero al menos nos dará bases y guías para el presente estudio.

Existe un criterio generalizado entre diversos autores, por el que afirman que a pesar de que la firma para el Derecho Bancario cuenta con ciertas características que la hacen distinta de la firma en general; existen ciertos criterios de ésta que pueden ser aplicados para el caso de la firma autógrafa.

Una de las normas que durante mucho tiempo fue aplicada con éxito en el sistema bancario, era la que establecía diversos requisitos de validez para el caso de operaciones bancarias y depósitos. Estaba contenida en el artículo 102 de la Ley General de Instituciones de Crédito y Organizaciones Auxiliares (abrogada el 15 de enero de 1985, esto es por lo que se refiere a Organizaciones Auxiliares) que decía:

*"Salvo convenio en contrario, las condiciones generales establecidas por la institución de crédito, respecto a los depósitos en cuenta de cheques, se entenderían aplicables a todos los depósitos de esta clase, y podrán ser cambiadas libremente por la institución, previo aviso con cinco días de anticipación dado a los depositantes por escrito, o mediante publicación de avisos o su fijación en lugares abiertos al público en las oficinas de la institución. Todo documento o título de crédito expedido para disponer de depósito bancario de dinero, y los endosos, avales y demás actos que en ellos se consignen, **deberán contener escritos o impresos con tinta, los requisitos necesarios para su validez y la firma o firmas de quien o quienes lo suscriban.**"*

De lo expuesto por este artículo podemos obtener diferentes conclusiones: En primer lugar, el precepto aclara que los requisitos señalados sólo serán aplicables para el caso de los títulos de crédito o documentos necesarios para disponer de depósitos bancarios; pero consideramos que esto no puede tomarse literalmente ya que por consideraciones de prueba y seguridad jurídica los requisitos señalados son válidos para toda clase de documentos bancarios.

Como segundo punto, al señalar que los requisitos de validez deben estar impresos en tinta quiere decir, que estos deben estar impresos mediante "medios mecánicos"; los requisitos a imprimir deberán de ser los que para cada caso en específico señalen el Código de Comercio o bien las Leyes Especiales Mercantiles.

¹¹⁹ Véase. Reyes Krafft, Alfredo Alejandro *Ob. Cit.* y Acosta Romero, Miguel. *Ob. cit.*

Y por último, en lo referente a las firmas, por lo señalado en el precepto podemos inferir que éstas deben estamparse con tinta y ser autógrafas. La falta de estos requisitos crearía una ausencia de formalidad, cuya consecuencia jurídica sería una nulidad relativa; ya que el acto sería existente porque el consentimiento y el objeto se cumplen y no sería una nulidad absoluta, ya que ésta solo “se origina con el nacimiento del acto; cuando el acto va en contra del mandato o de la prohibición de una ley imperativa o prohibitiva, esto es, una ley de orden público”¹²⁰ Para este caso de acuerdo con lo señalado por el artículo 78 del Código de Comercio Vigente “*En las convenciones mercantiles cada uno se obliga en la manera y términos que aparezca que quiso obligarse, sin que la validez del acto comercial dependa de la observancia de formalidades o requisitos determinados*”

A pesar de la utilidad jurídica que este artículo proporcionó a las cuestiones bancarias prácticas; en la Ley Reglamentaria del Servicio Público de Banca y Crédito de 1985 y la Ley de Instituciones de Crédito de 1990, se suprime toda referencia a él.

Además de estipulado en el extinto artículo; existen otros apartados (que no han sido derogados) de la Ley de Instituciones de Crédito vigente que hacen referencia a la firma autógrafa, algunos de los cuales ya hemos abordado al hablar de contratación electrónica en el capítulo anterior y que se hace necesario volver a tratar para en este apartado.

El primero es el artículo 52 (citado textualmente en capítulos anteriores) que establece como otros ordenamientos mercantiles, la equivalencia entre el uso de los medios de identificación con la firma autógrafa para efectos legales y probatorios.

En tanto que el artículo 57 de la misma ley establece que: *En las operaciones a que se refieren las fracciones I y II del artículo 46 de esta Ley, los depositantes o inversionistas podrán autorizar a terceros para hacer disposiciones de dinero, bastando para ello la **autorización firmada en los registros especiales** que lleve la institución de crédito.*

Las instituciones de crédito podrán cargar a las cuentas de sus clientes, el importe de los pagos que realicen a proveedores de bienes o servicios autorizados por dichos clientes, siempre y cuando:

I. Cuenten con la autorización del cliente de que se trate, o

II. El cliente autorice directamente al proveedor de bienes o servicios y éste a su vez instruya a la institución de crédito para realizar el cargo respectivo. En este caso, la autorización podrá quedar en poder del proveedor de los bienes o servicios.

¹²⁰ Gutierrez y Gonzalez, Ernesto. Derecho de las Obligaciones. 5ª ed. Cajica, México 1984 p.134

En el evento de que el cliente cuya cuenta hubiere sido cargada en términos del párrafo anterior, objete dicho cargo dentro de los noventa días naturales siguientes a la fecha en que éste se haya realizado, la institución de crédito respectiva deberá abonarle en la cuenta de que se trate, a más tardar el día hábil bancario inmediato siguiente a aquél en que se efectúe la objeción, la totalidad de los cargos.

Para efectos de cumplir con la obligación a que se refiere el párrafo anterior, la institución de crédito estará facultada para cargar a la cuenta que lleve al proveedor de los bienes o servicios, el importe correspondiente. Cuando la cuenta del proveedor de bienes o servicios la lleve una institución de crédito distinta, ésta deberá devolver a la institución en que tenga su cuenta el cliente los recursos de que se trate, pudiendo cargar a la cuenta del proveedor de los bienes o servicios respectivo el importe de la reclamación. Para estos efectos, la institución de crédito y el proveedor deberán pactar los términos y condiciones que serán aplicables.

Las instituciones de crédito deberán pactar con los proveedores el procedimiento para efectuar los cargos a que se refiere el párrafo anterior, cuidando en todo momento que no causen daño al patrimonio de dichas instituciones.

*Las autorizaciones, instrucciones y comunicaciones a que se refiere este artículo podrán llevarse a cabo **por escrito con firma autógrafa o a través de los medios electrónicos, ópticos o de cualquier otra tecnología que previamente convengan las partes, debiendo contar las instituciones de crédito con los registros, archivos u otros medios que les permitan presentar ante la autoridad competente, la fecha y demás características principales de las reclamaciones que, en su caso, presenten los usuarios.***

Como vemos, las referencias a firma autógrafa en este artículo, son respecto a terceros, para hacer cargos a una cuenta a la que han sido autorizados; señalando que dicha autorización debe de estar firmada y guardada en los archivos de la Institución de Crédito. Además de que en estas operaciones, también se autoriza el uso ya sea de firma autógrafa o medios electrónicos.

Por último el artículo 68 de la Ley de Instituciones de Crédito reza: "Los contratos o las pólizas en los que, en su caso, se hagan constar los créditos que otorguen las instituciones de crédito, junto con los estados de cuenta certificados por el contador facultado por la institución de crédito acreedora, serán títulos ejecutivos, sin necesidad de **reconocimiento de firma ni de otro requisito.**

El estado de cuenta certificado por el contador a que se refiere este artículo, hará fe, salvo prueba en contrario, en los juicios respectivos para la fijación de los saldos resultantes a cargo de los acreditados o de los mutuatarios.

El estado de cuenta certificado antes citado deberá contener nombre del acreditado; fecha del contrato; notario y número de escritura, en su caso; importe del crédito concedido; capital dispuesto; fecha hasta la que se calculó el adeudo; capital y demás obligaciones de pago vencidas a la fecha del corte; las disposiciones subsecuentes que se hicieron del crédito, en su caso; tasas de intereses ordinarios que aplicaron por cada periodo; pagos hechos sobre los intereses, especificando las tasas aplicadas de intereses y las amortizaciones hechas al capital; intereses moratorios aplicados y tasa aplicable por intereses moratorios.”

En este artículo simplemente se hace alusión a la certificación en los estados de cuenta hecha por un contador facultado, que en conjunción a los contratos en que se asienten los créditos otorgados por la Institución, servirán como elemento probatorio en juicio.

Los anteriores son solo algunos artículos que tratan a la firma. Para entender el alcance de la firma autógrafa en el Derecho Bancario Mexicano, se hace necesario un estudio más profundo, que dado el tema que ocupa la presente tesis no nos es posible emprender.

2.2.3 La firma en títulos de crédito¹²¹

Para el caso de los títulos de crédito, a los requisitos establecidos para la firma autógrafa en otros ordenamientos mercantiles se agregaran los dispuestos por diversos artículos de la Ley de Títulos y Operaciones de Crédito Vigentes sobre firma autógrafa, que a continuación citaremos:

Está el artículo 8º fracción II que reza: *“Contra las acciones derivadas de un título de crédito, sólo pueden oponerse las siguientes excepciones y defensas: ... II.- Las que se funden en el hecho de no haber sido el demandado **quien firmó** el documento”*

Le sigue el artículo 11 que dice: *“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 concurren las demás circunstancias que en este artículo se expresan.”*

Asimismo tenemos el artículo 29, fracción II que trata sobre endoso y al respecto señala: *“El endoso debe constar en el título relativo o en hoja adherida al mismo, y llenar los siguientes requisitos: ... II.- **La firma** del endosante o de la persona que suscriba el endoso a su ruego o en su nombre.”*

¹²¹ Véase. Reyes Krafft, Alfredo Alejandro Ob. Cit. y Acosta Romero, Miguel. Ob. cit.

Así como el artículo 76 fracción VII que aborda a la letra de cambio que expone: *“La letra de cambio debe contener:.... VII.- La **firma** del girador o de la persona que suscriba a su ruego o en su nombre.”*

Le sigue el artículo 85, párrafo segundo, que versa sobre el aval menciona: *“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.”*

En tanto que el artículo 170, fracción VI que trata al pagaré estipula: *“El pagaré debe contener: ... VI.- **La firma** del suscriptor o de la persona que firme a su ruego o en su nombre”*

Mientras que la fracción VI del artículo 176 relativa al cheque textualmente advierte: *“El cheque debe contener:... VI.- **La firma** del librador.”*

Al tiempo que el artículo 203 relativo a los cheques de viajero nos dice: *“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.”*

Así tenemos al artículo 210, relativo a las obligaciones que en sus fracciones X y XI, señala: *“Las obligaciones deben contener: X.- **La firma autógrafa** de los administradores de la sociedad, autorizados al efecto, o bien la firma impresa en facsimil 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 facsimil 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.”*

Otro de los artículos que trata a la firma es el 228-N, fracciones II y X, que respecto de los certificados de participación reza: *“El certificado de participación deberá contener: II.- La designación de la sociedad emisora y la **firma autógrafa** del funcionario de la misma, autorizado para suscribir la emisión correspondiente; X.- **La firma autógrafa** del representante común de los tenedores de certificados.”*

Mientras los artículos 231, fracción II y 232 fracción V relativos al certificado de depósito y bono de prenda que dicen: *“Tanto el certificado de depósito como el bono de prenda, deberán contener: ... II.- La designación y la firma del almacén.”* *“El bono de prenda deberá contener, además: V.- La firma del tenedor del certificado que negocie el bono por primera vez”*

En cuanto a los títulos de Crédito contemplados por la Ley de Instituciones de Crédito; nos encontramos que la firma está presente en los artículos:

El 62 que versa sobre los requisitos de los certificados de depósito bancario a plazo y dice: *“Los depósitos a plazo podrán estar representados por certificados que serán títulos de crédito y producirán acción ejecutiva respecto a la emisora, previo requerimiento de pago ante fedatario público. Deberán consignar: la mención de ser certificados de depósito bancario de dinero, la expresión del lugar y fecha en que se suscriban, el nombre y la firma del emisor, la suma depositada, el tipo de interés pactado, el régimen de pago de interés, el término para retirar el depósito y el lugar de pago único”.*

En tanto que el artículo 63 menciona en el acta de emisión de los bonos bancarios, y al respecto tenemos que su fracción III estipula: *“Los bonos bancarios y sus cupones serán títulos de crédito a cargo de la institución emisora y producirán acción ejecutiva respecto a la misma, previo requerimiento de pago ante fedatario público. Se emitirán en serie mediante declaración unilateral de voluntad de dicha institución que se hará constar ante la Comisión Nacional Bancaria, en los términos que ésta señale y deberán contener: ... III. El nombre y la firma de la emisora”*

Y el párrafo tercero del artículo 64 que trata a las obligaciones subordinadas, nos remite a los artículos posteriores, por lo que consideramos que lo anteriormente aplicado para las firmas es igualmente válido para ésta. El artículo textualmente dice: *“Las obligaciones subordinadas y sus cupones serán títulos de crédito con los mismos requisitos y características que los bonos bancarios, salvo los previstos en el presente artículo...En el acta de emisión relativa, en el prospecto informativo, en cualquier otra clase de publicidad y en los títulos que se expidan deberá constar en forma notoria, lo dispuesto en los párrafos anteriores.”*

Por lo citado en los artículos anteriores podemos concluir que la firma es un elemento sumamente importante para los títulos de crédito, ya que la falta de ésta los hace simplemente inexistentes.

Según los usos bancarios, cuando un ordenamiento habla de “firma” se entiende por ésta, a la firma autógrafa, que conforme a los usos mercantiles es la que se estampa “de puño y letra de quien la estampa”¹²². Este criterio con

¹²² Reyes Krafft, Alfredo Alejandro. *Ob. cit.* p. 96

respecto a la firma, no sólo es adoptado en el ámbito bancario, si no en el ámbito de los usos mercantiles en general.

En todo caso la firma estampada en los títulos de crédito, no requiere del reconocimiento de un fedatario público o autoridad para ser ejecutivo.

Por lo visto podemos afirmar que "el origen de toda obligación en materia de títulos de crédito, es la firma autógrafa"¹²³ que no podrá ser reemplazada por una firma a ruego o una impresión digital. Siendo así que el principio de equivalencia funcional que menciona el artículo 93 (citado anteriormente) del Código de Comercio Vigente es contradictorio, debido a la imposibilidad de sustituir la firma autógrafa para el caso de los títulos de crédito; en la ley de Títulos y Operaciones de Crédito no se hace ninguna mención al respecto. Lo que nos hace suponer que siguiendo el principio de especialización de la ley, la firma en los títulos de crédito en cualquier caso debe ser autógrafa.

En todo caso para que un título de crédito pueda ser suscrito por un tercero a nombre y cuenta de otro, debe de cumplir con algunos requisitos que menciona el maestro Miguel Acosta Romero¹²⁴, que son:

1. Si es una persona jurídica colectiva, o una persona física que sepa leer y escribir, tendrá que cumplir con los requisitos establecidos en los artículos 9^o¹²⁵ y 8^o, párrafo segundo de la Ley General de Títulos y Operaciones de Crédito, este último aplicable a las letras de cambio.
2. En el supuesto de una persona física que no sepa, o no pueda leer, o escribir, tendrá que recurrirse a un fedatario ante el cual se otorgará el poder correspondiente a un tercero, para que éste firme los títulos de crédito.¹²⁶

En cuanto a las excepciones oponibles por no haber firmado un documento, según criterio de la Suprema Corte de Justicia podemos ver que:

"La excepción opuesta por el demandado de que él no firmó el título de crédito base de la acción deducida, corresponde demostrarla al propio demandado, porque de igual manera que al actor toca probar los hechos constitutivos de su acción, al demandado corresponde la prueba de los que integran sus excepciones (artículo 8^o, fracción II de la Ley General de Títulos y Operaciones de Crédito); tanto más que, si bien la excepción consiste en la negativa de haber firmado en la demanda la letra base de la acción cambiaría ejercida, se advierte sin dificultad que

¹²³ Ibidem

¹²⁴ Cfr. Acosta Romero Miguel. Ob.cit. p.57

¹²⁵ Artículo 9. 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.

¹²⁶ Acosta Romero, Miguel. Ob. cit. p. 567

se trata de una negociación que envuelve la afirmación, que dicha parte si estuvo en posibilidad de acreditar, de que la firma que, como suya, aparece en el documento, es falsa; aparte de que la misma Ley, atendiendo a las necesidades de la rápida circulación de los títulos de crédito, al suprimir la exigencia legal anterior de la ratificación de las firmas de los suscriptores de tales documentos, entonces establecida como condición para que se consideren ejecutivos, lo hizo partiendo de la base de presumir, salvo prueba en contrario cuya carga recae en el demandado que la objete, la autenticidad de las susodichas firmas."

Directo 4019/1956 Dolores Guadarrama Vda. De Reza. Resuelto el 17 de julio de 1957, por unanimidad de 5 votos. Ponente: ministro García Rojas. Secretario: Lic. Alfonso Arbitia A.¹²⁷

2.2.4 La firma en materia de fianzas¹²⁸

En materia fianzas, las pólizas de fianzas llevan la firma de las personas así autorizadas por el Consejo de Administración o la Asamblea General. Las firmas autorizadas se clasifican en dos ramas: "A" y "B" donde se establece que puede una firma obligar a cierta empresa, los alcances que ésta puede tener (a ese sistema se le conoce como catalogo de firmas).

Como en otros casos, la ley especializada: la "Ley Federal de Instituciones de Fianzas", hace referencia en diversos artículos a las firmas y facsimiles ("calco o reproducción perfecta de una firma, escrito, dibujo, impreso, etc."¹²⁹) de éstas, en las pólizas de fianza.

En el artículo 13 de dicha ley establece "*Las autoridades federales o locales están obligadas a admitir las fianzas, aceptando la solvencia de las instituciones de fianzas, sin calificar dicha solvencia ni exigir la constitución de depósitos, otorgamiento de fianzas o comprobación de que la institución es propietaria de bienes raíces, ni la de su existencia jurídica...*"

Lo sigue el artículo 82 que reza "Las instituciones de fianzas realizarán su objeto social **por medio de uno o más funcionarios** que se designen especialmente al efecto y de **cuyos actos responderá directa e ilimitadamente la institución**, sin perjuicio de las responsabilidades civiles o penales en que ellos incurran personalmente.

*La Comisión Nacional de Seguros y Fianzas, con acuerdo de su Junta de Gobierno, podrá en todo tiempo determinar que se proceda a la remoción o suspensión de los miembros del consejo de administración, contralor normativo, directores generales, comisarios, directores y gerentes, delegados fiduciarios funcionarios que puedan **obligar con su firma** a la institución, cuando considere que no cuentan con la suficiente calidad técnica, honorabilidad e historial crediticio satisfactorio para el desempeño de sus funciones, no reúnan los requisitos al efecto establecidos o incurran de manera grave o reiterada en infracciones a la*

¹²⁷ Citado por Acosta Romero Miguel. *Ob. cit.* p. 566

¹²⁸ Véase. Reyes Krafft, Alfredo Alejandro *Ob. Cit.* y Acosta Romero, Miguel. *Ob. cit.*

¹²⁹ Raluy Poudevida, Antonio. *Diccionario Porrúa de la Lengua Española*. 4ª ed. Porrúa, México, 2003

presente Ley o a las disposiciones de carácter general que de ella deriven. En los dos últimos supuestos, la propia Comisión podrá además, inhabilitar a las citadas personas para desempeñar un empleo, cargo o comisión dentro del sistema financiero mexicano, por un periodo de seis meses hasta cinco años, sin perjuicio de las sanciones que conforme a éste u otros ordenamientos legales fueren aplicables. Antes de dictar la resolución correspondiente, la citada Comisión deberá escuchar al interesado y a la institución de fianzas de que se trate...”

En el artículo 84 se nos dice que “Los documentos que acrediten la facultad de los representantes de las instituciones de fianzas para otorgar fianzas, así como **los facsímiles de sus firmas**, deberán registrarse en la Comisión Nacional de Seguros y Fianzas”

Y finalmente el artículo 96 que enuncia: “El documento que consigne la obligación del solicitante, fiado, contrafiador u obligado solidario, acompañado de una copia simple de la póliza y de la certificación de la o **las personas facultadas por el consejo de administración de la institución de fianzas de que se trate**, de que ésta pagó al beneficiario, llevan aparejada ejecución para el cobro de la cantidad correspondiente así como para el cobro de primas vencidas no pagadas y accesorios. La certificación a que se refiere el párrafo anterior, hará fe en los juicios respectivos, salvo prueba en contrario”

Con el fin de otorgar mayor seguridad al sistema de fianzas; cada año la Comisión Nacional de Seguros y Fianzas, mediante oficio circular que se publica en el Diario Oficial de la Federación; hace del conocimiento de las autoridades y del público en general las firmas autorizadas por cada compañía aseguradora, así como del facsímil respectivo.

2.2.5 La firma en pólizas de seguros¹³⁰

Los procedimientos entre pólizas de seguro y las de fianza son muy distintos. Para el caso de los seguros, no se hace uso de los facsímiles, la firma empleada es en todos los casos autógrafa.

No cumplen con tantas formalidades como las pólizas de fianza, y en general son aceptadas en el campo mercantil sin grandes problemas, en todo caso un agente de seguros autorizado puede llegar a refrendar su firma.

2.2.6 Características de la firma¹³¹

Conforme a lo expuesto por el teórico Alfredo Reyes Krafft la firma autógrafa tiene tres características: el ser Identificativa, Probatoria y Declarativa.

¹³⁰ Véase. Reyes Krafft. Alfredo Alejandro Ob. Cit. y Acosta Romero, Miguel. Ob. cit.

¹³¹ Véase. Reyes Krafft, Alfredo Alejandro Ob. Cit

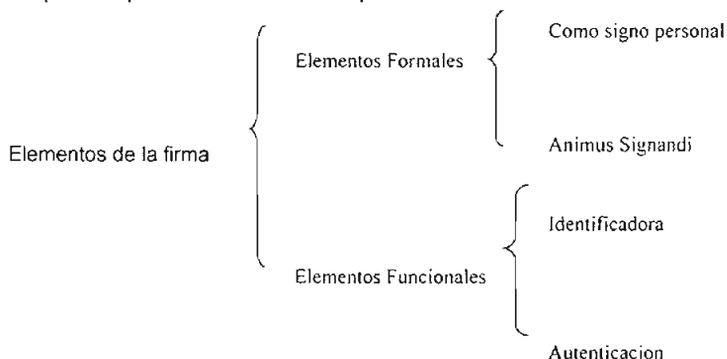
La característica Identificativa de la firma permite establecer o "identificar" al autor de algún documento.

El ser Probatoria hace posible determinar si el signatario, es aquel que ha sido reconocido como tal en el hecho de la firma

Por último al decir que es Declarativa, se hace alusión a el signatario asume el contenido del documento, al suscribirlo; especialmente importante para el caso del que firma al final de un contrato.

2.2.7 Elementos de la firma¹³²

Basándonos en la teoría de Alfredo Reyes Krafft elaboramos el siguiente esquema que a continuación explicaremos.



Los elementos formales son los elementos instrumentales de la firma, relativos a los procedimientos usados para firmar, y el mismo grafismo de ésta. Al tiempo que los elementos funcionales hacen referencia a la firma, cuando se toma a ésta como un signo o un conjunto de signos.

Dentro de los elementos formales, nos encontramos con la firma "como un signo personal", esto quiere decir que la firma se convierte en un signo distintivo y personal, al ser colocada de puño y letra por el signante. El otro elemento es el "animus signandi", que es el factor intelectual o intencional de la firma; y estriba en la voluntad de contraer el contenido de un documento (muy diferente a la voluntad de contratar).

En cuanto a los elementos funcionales. Al hablar de la "Identificadora" se consolida la relación jurídica entre la persona firmante y el acto firmado, ya que la

¹³² Véase. Reyes Krafft, Alfredo Alejandro Ob. Cit

identificación de una persona permite la atribución de derechos y obligaciones, aunque no acaba de ser un método de autenticación totalmente fiable ya que el contenido del documento puede ser objeto de alteraciones, y la firma de falsificaciones.

En tanto que la autenticación se refiere a que "el autor del acto expresa su consentimiento y hace propio el mensaje"¹³³. Esta puede ser activa o pasiva. Es activa cuando "alguien se identifica conscientemente en cuanto al contenido suscrito y se adhiere al mismo"¹³⁴; siendo pasiva cuando "no requiere del consentimiento, ni del conocimiento siquiera del sujeto identificado"¹³⁵. La firma se convierte en un vínculo entre firmante y documento

2.3 La Firma Electrónica. Recuento Histórico

El reconocimiento de medios tecnológicos para fines jurídicos en codificaciones nacionales comienza con el código de comercio de 1884, en el que se reconoce al telégrafo, que para ese entonces era un medio de comunicación sumamente novedoso. En 1928, el Código Civil reconoce al teléfono; para 1990 diversas leyes financieras y bancarias reconocen a los medios telemáticos; posteriormente la ley de Protección Federal al Consumidor de 1992 establece diversas normas que protegen a los consumidores en las ventas a distancia y Telemarketing (las ventas realizadas por medios de comunicación masiva como T.V. y Radio); seis años después, en las leyes fiscales de 1998 se dan a conocer diversas disposiciones sobre declaraciones y pagos en formato electrónico.

El 17 de Mayo de 1999, se hace una reforma al Código Penal Federal, donde se establece el delito de acceso ilícito a sistemas y equipos de informática, con penas de 3 meses a 8 años de prisión y 100 a 900 días de multa. El 4 de Enero del 2000 la Ley de Adquisiciones Arrendamientos y Servicios del Sector Público y la Ley de Obras Públicas y Servicios Relacionados con las mismas disponen "Las proposiciones presentadas deberán ser firmadas autógrafamente por los licitantes o sus apoderados; en caso de que éstas sean enviadas a través de medios remotos de comunicación electrónica, en sustitución de la firma autógrafa, se emplearán medios de identificación electrónica, los cuales producirán los mismos efectos que las leyes otorgan a los documentos correspondientes y, en consecuencia, tendrán el mismo valor probatorio".

Hasta finales del siglo pasado nuestra legislación exigía la firma autógrafa y un soporte escrito para que un acto jurídico fuera considerado válido; lo que resultaba arcaico; ya que en nuestro país se venían realizando transacciones (70% de ellas por las empresas) mediante el uso de sistemas electrónicos de seguridad como la firma electrónica y los certificados; aun sin el reconocimiento

¹³³ www.cem.itesm.mx/dacs/publicaciones/logos/libros/firma.pdf

¹³⁴ Ibidem

¹³⁵ Ibidem

legal necesario; "A falta de una regulación específica en el ámbito del Comercio Electrónico, en México se habían resuelto los conflictos que se habían presentado a través de la aplicación de figuras similares establecidas en diversos ordenamientos jurídicos"¹³⁶.

La Firma Electrónica y los Certificados Digitales en nuestro país hasta ese momento habían sido desarrollados por La Asociación Nacional del Notariado Mexicano (ANNM) en conjunción con el Colegio Nacional de Contaduría Pública Mexicana y las empresas SeguriDaTA e Infosel. El trámite que el usuario interesado en obtener un certificado digital era el siguiente:

- El Usuario genera en su computadora su Requerimiento de Certificación y sus Claves.
- Con el Requerimiento de Certificación y la documentación que compruebe su identidad, acude con un Fedatario Público.
- El Fedatario Público revisa la información presentada por el usuario, da fe de su identidad y procede a emitir un Certificado Digital; por medio de un proceso en línea, el Fedatario Público se enlaza con la Agencia Certificadora y ésta, a su vez, con la Agencia Registradora, para la emisión del Certificado Digital definitivo, verificando que no exista duplicidad de claves.
- El Fedatario Público recibe el Certificado Digital y lo entrega al usuario. A partir de ese momento el Usuario podrá celebrar operaciones a través de Comercio Electrónico seguro.

Para poder ingresar a la Red de Certificación Digital se requiere:

- Ser Notario Público miembro de la Asociación Nacional del Notariado Mexicano.
- Acreditar el curso de "Certificación Digital" impartido por SeguriDATA e Infosel.¹³⁷

En un esfuerzo por establecer bases legales en materia de comercio electrónico y algunos medios de seguridad informática, En abril de 1999 el Partido Acción Nacional presenta ante el congreso una iniciativa del texto de la Ley Modelo de CNUDMI en materia de Comercio electrónico; para marzo del 2000 el Partido Revolucionario Institucional expone una iniciativa de texto abreviado y adicionado con disposiciones relativas a la ley de Protección del Consumidor.

Tras varios meses de discusión y análisis de diversos bosquejos; para el periodo de sesiones de Marzo - Abril del 2000 se discute el proyecto oficial en ambas cámaras. En la de diputados el 26 de abril del 2000 recibe 390 votos a favor, 0 en contra y 3 abstenciones; y en la de senadores se aprueba el 29 de abril por una unanimidad de 88 votos. Por lo que el decreto donde se reforman y

¹³⁶ Academia de Estudios Fiscales de Contaduría Pública A.C. Comercio Electrónico – Principios Jurídicos y Marco Fiscal. Dofiscal Editores, México, 2001 p.38

¹³⁷ Idem. p.52

adicionan diversas disposiciones del Código Civil Federal, Código de Procedimientos Civiles, Código de Comercio y la Ley Federal de Protección al Consumidor con el propósito de instaurar un esquema jurídico para proporcionar mayor certeza a las operaciones vía digital o electrónica, es publicado en el Diario Oficial de la Federación el 29 de mayo de 2000. Su entrada en vigor se establece para el 7 de junio del 2000.

A diferencia de otras naciones donde se establecen todos los temas relativos a transacciones vía electrónica en un solo ordenamiento, nuestros legisladores no los incluyeron en un documento único (aunque se presentó una iniciativa con tales características, pero no fue aprobada por considerarse demasiado general y amplia); si no que dividieron los temas relativos a contratación electrónica en diversos códigos, donde se contemplan aspectos básicos como: "la atribución de la persona (indudablemente cada quien es quien dice ser); la integridad no alterabilidad del acuerdo de voluntades; los contratos con soporte informático tienen la misma validez jurídica que aquellos soportados en papel; el consumidor siempre recibirá información clara, veraz y suficiente para realizar su compra"¹³⁸

Entre las reformas hechas al Código de Comercio en materia de contratación están los artículos 1803 donde se añade el concepto de mensaje de datos, a la vez de conferirle validez como "consentimiento expreso"; mientras que en el artículo 1811 se le otorga validez y obligatoriedad a la aceptación y propuesta realizada por medio de un mensaje de datos; y en el artículo 1834 se equipara al mensaje de datos con un contrato escrito para el caso de ser atribuible y disponible para ulterior consulta.

En tanto que en el Código de Procedimientos Civiles, en el artículo 210-A se reconoce la fuerza obligatoria, la validez del mensaje de datos y su carácter probatorio, en caso de que éste pueda ser conservado íntegramente y sea accesible para su ulterior consulta. En el artículo 210 -B se estipulan los mecanismos a emplear la valoración probatoria de un mensaje de datos. Y en el 217 se hace alusión a que el valor probatorio de los mensajes de datos se entenderá según lo dispuesto en los artículos 210-A y 210-B del mismo Código.

Mientras que el artículo 49 del Código de Comercio versa sobre la conservación de mensajes de datos; en el 89 se trata del uso de medios electrónicos en los actos de comercio, en el 90 de la atribución del mensaje de datos (es decir de quien proviene el mensaje); en el 91 de la recepción del mensaje de datos; en el 92 del acuse de recibo; en el 94 de la recepción del mensaje de datos; así como el 1205 y 1298 del mensaje de datos como prueba.

Por último la Ley Federal de Protección al Consumidor en su artículo primero garantiza la protección de los datos empleados en las transacciones electrónicas, así como de las mismas transacciones electrónicas. En tanto que en

¹³⁸ <http://www.travel-center.com/Legal/Mexican-Ecommerce-Regulations-Spanish.htm>

el 24 se hace alusión a utilizar, difundir u formular códigos de ética entre los proveedores de servicios. En el 76 se precisa la forma que deberá tener la relación entre proveedor y consumidor, estableciendo los derechos y obligaciones de las partes. Y en el 128 se habla de los montos económicos de las sanciones por el incumplimiento de el mencionado ordenamiento.

Las reformas hechas no fueron tan amplias y exhaustivas como los legisladores hubieran deseado, en parte porque la CNDUMI aun no aprobaba su ley modelo sobre firmas electrónicas y los legisladores mexicanos no se aventuraron a establecer conceptos y procedimientos de seguridad informática, sin antes conocer el espíritu internacional al respecto.

Otros intentos por legislar en materia electrónica en esos años, fueron hechos por diversas Secretarías: la Secretaría de Economía el 29 de Mayo del 2000, después la Secretaría de la Función Pública (antes SECODAM) el 17 de Enero del 2002; y finalmente la Secretaría de Hacienda y Crédito Público (SHCP) realiza diversas modificaciones al Código Fiscal de la Federación, publicadas en 5 de Enero del 2003.

En el artículo 17- D (entre otros) del mencionado Código Fiscal establece que todos los documentos que se presenten a través de un medio digital contengan una Firma Electrónica Avanzada, exceptuándose de esto únicamente los contribuyentes dedicados a actividades agrícolas, ganaderas, pesqueras y silvícolas.

Dichas modificaciones al ordenamiento fiscal han dado pie a varias aplicaciones en el ámbito fiscal. La mas reciente es la Firma Electrónica Avanzada (Tu firm@), otorgada por el Sistema de Administración Tributaria (SAT); es "un conjunto o bloque de caracteres que viajan junto con un documento o mensaje y que puede acreditar quién es el emisor del mismo, a diferencia de una firma electrónica simple, que puede ser hasta la inclusión de su nombre al final de un correo electrónico."¹³⁹ Por medio de la cual se pueden realizar diversos trámites fiscales ante la Secretaría de Hacienda, además de otorgar la posibilidad de expedir comprobantes fiscales a través del SAT, o un prestador de servicios de Certificación Autorizado por el Banco de México.

Por el momento su uso sólo es obligatorio para las personas físicas que durante 2003 obtuvieron ingresos mayores a 300,000 pesos y aquellas con actividad empresarial que percibieron ingresos por arriba de 1,750,000 pesos, están obligadas a tramitar la firma electrónica. Siendo obligatoria definitivamente para el 2005.

No obstante tras la aprobación en el 2001 de la Ley Modelo de Firmas Electrónicas, la Comisión de Comercio y Fomento Industrial de la LVIII legislatura, emprende la tarea de "completar" la legislación existente. Con este objetivo la

¹³⁹ <http://www.red.com.mx/scripts/redArticulo.php?idNumero=65&articuloID=7465>

legislatura celebra el Foro "Avances en la Legislación en materia de Comercio Electrónico" los días 5 y 6 de septiembre de 2001 con el siguiente programa:

Tema	Ponente	Organismo
El Internet en México	Lic. Alejandro Rodríguez	Asociación Mexicana de la Industria Publicitaria y Comercial en Internet
La legislación Vigente a Nivel Nacional	Lic. Philip Bienvenu y Dr. Alfredos Reyes K	Asociación de Banqueros de México
Norma de Conservación de Mensajes de Datos	Lic. Sergio Carrera	Secretaría de Economía
Firmas Electrónicas en su ámbito legal	Lic. Luis Manuel Meján	Grupo Gilce
Firmas Electrónicas en su ámbito técnico	Mat. Ignacio Mendivil	Director General de Seguridata
Panorama Internacional	Lic. José Ma. Abascal	Representante de México ante la O.N.U.
Factura Electrónica	Lic. Ramón López Castro	Miembro del Grupo Gilce
Delitos Informáticos	Lic. Luis Manuel Ramírez Perches	L. Ramírez y Asociados, S.C.
Posibles Modificaciones a la Constitución	Lic. Luis Vera Vallejo	Amiti
Nombres de Dominio	Lic. Arturo Azuara	Nic México
Páginas de Internet	Ing. Alejandro Diego	Director General de Interware
Legislación en materia de propiedad Industrial e Intelectual	Lic. Flor Ma. Cuellar	Coordinadora del Proyecto E-Commerce Gobierno de Guanajuato

El objetivo del foro era reseñar las problemáticas más recurrentes en el comercio electrónico, el contexto en el que se desarrollo, las demandas de los usuarios, y los lineamientos a seguir para el desarrollo de un marco normativo que satisfaga las necesidades de este nuevo medio comercial.

Como resultado del foro se constituyó un Grupo de Trabajo, conformado por representantes de organizaciones del sector académico, publico y privado; así como empresas privadas. Tras un año de trabajos el grupo da como resultado una iniciativa de Reformas y Adiciones al Código de Comercio en Materia de Firma Electrónica, presentada el 15 de mayo del 2002 por el Dip. Diego Alonso Hinojosa Aguerreverre (presidente de la comisión). Siendo aprobada el 26 de noviembre por la Cámara de Diputados por 422 votos a favor y 1 abstención, en tanto que en la Cámara de Senadores fue aprobada el 8 de abril del 2003, por unanimidad, verificándose entonces su publicación el 29 de agosto de 2003 y estableciéndose una vigencia de 90 días después de haber sido publicada en el Diario Oficial de la Federación. Dando como resultado el ordenamiento jurídico que rige las transacciones comerciales actuales.

Las reformas hechas a 30 artículos del Código de Comercio introducen varios conceptos de firma electrónica que analizaremos más adelante.

2.3.1 La Firma Electrónica

Técnicamente la firma electrónica es el resultado constante de 128 bits; que se generan mediante un algoritmo matemático de una sola vía casi o prácticamente imposible de falsificar; capaz de ser almacenado para futuras verificaciones y auditorías.

Como vimos en el recuento histórico emprendido en el capítulo primero, gran parte de los descubrimientos tecnológicos responden a necesidades prácticas (Las computadoras y el Internet, tristemente a razones bélicas). La firma electrónica, responde a una necesidad de seguridad en las transacciones vía electrónica. El incremento en el uso de las redes para fines comerciales, también aumentó el número de incidentes delictivos en ellas; de 2002 a 2003 estos crecieron en un 80%; por lo que era casi seguro que surgirían tecnologías de protección para responder a las necesidades prácticas.

Algunos de los beneficios que proporciona la firma electrónica son: el ser equivalentemente funcional a la firma autógrafa; asegurar la identidad de las partes en las transacciones electrónicas; garantizar el contenido de un mensaje durante su transmisión; permitir la certificación (o no repudio) de un mensaje de datos; hacer posible la detección de cualquier intento de modificación o detección de un mensaje; ofrecer medidas de garantía contra fenómenos como el web spoofing o hacker en páginas web; realizar operaciones comerciales vía electrónica (compra - venta, pedidos, facturas, contratos, etc.); declaraciones de impuestos vía electrónica; transparencia, ahorro en costos de transacción y almacenamiento de procesos gubernamentales; y transacciones bancarias, entre otras.

Existen numerosas definiciones de firma electrónica, pero antes de enunciar algunas de las más importantes, debemos aclarar la diferencia entre la firma electrónica y la llamada firma digital (aunque existen autores que no hacen distinción al respecto). De acuerdo al criterio del doctrinario mexicano Julio Téllez Valdés: "Firma Electrónica es el término genérico y neutral para referirse al universo de las tecnologías mediante las cuales una persona puede firmar un mensaje de datos.." ¹⁴⁰, en tanto que la Firma Digital es "cierto tipo de firma electrónica basada en el uso de criptografía" ¹⁴¹.

De acuerdo con el artículo segundo de la Ley Modelo de la CNDUMI sobre firmas electrónicas del 2001, en la que se basaron nuestros legisladores para

¹⁴⁰ Téllez Valdés, Julio. *Ob. cit.* p.203

¹⁴¹ Ibidem

nuestro ordenamiento; por firma electrónica se entenderán los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, pueden 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.

La Norma Oficial Mexicana NOM-151-SCFI-2002, Practicas Comerciales - Requisitos Que Deben Observarse Para La Conservación De Mensajes De Datos, define a la Firma Electrónica como *"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 tanto que el artículo 89 del Código de Comercio Mexicano Vigente define a la firma electrónica como: *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.*

Entre la definición de la NOM-151-SCFI-2002 y la de la CNDUMI, no existen muchas diferencias, podría decirse que son casi idénticas; el único elemento de novedad que introduce la NOM-151-SCFI-2002 es un enunciado al final que prescribe *"La firma electrónica establece la relación entre los datos y la identidad del firmante"* que quizás después de todos los elementos dados por la definición resulta redundante. Donde encontramos mayor número de elementos discrepantes es en la definición del Código de Comercio Vigente, que en comparación con las de la NOM-151-SCFI-2002 y la CNDUMI, además de las descripciones básicas, incluye otros enunciados que introducen nuevos elementos. Los enunciados discordantes son: *"...por cualquier tecnología..."; "...que son utilizados..."; "...y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio"*.

El hablar de "cualquier tecnología", hace alusión al principio de Neutralidad Tecnológica (mencionado anteriormente), consignado en el artículo 89 del Código de Comercio Vigente; que se refiere a que para el caso de las transacciones comerciales electrónicas no se debe de privilegiar a ningún tipo de tecnología, porque esto sería discriminatorio, además que podría dar pie a la creación de monopolios tecnológicos para las transacciones comerciales entre otras consecuencias.

En cuanto al párrafo que utiliza la expresión "que son", dista de las definiciones anteriores, porque en éstas se habla de un "puede ser". Otro de los

principios consignados por el Artículo 89 del Código de Comercio Vigente es el de Equivalencia Funcional que hace alusión a la equiparación de los mensajes de datos con los documentos escritos tradicionales y encuentra expresión en la definición de firma electrónica del Código de Comercio al decir “...y que produce los mismos efectos jurídicos que la firma autógrafa”

Por último, en la definición de Firma Electrónica de Comercio, se establece el pleno valor probatorio de la firma electrónica en juicio al decir de ésta: “...siendo admisible como prueba en juicio”.

Al igual que con otros conceptos para los fines de la presente tesis nos valdremos del concepto de firma electrónica dado por el Código de Comercio Vigente por considerarlo el más adecuado para nuestros propósitos.

2.3.1.1. La Firma Electrónica Avanzada

Hemos mencionado que entre las funciones de la firma electrónica están: el “identificar a la persona que realiza la transacción, es decir proporciona el servicio de autenticación (verificación de la autoridad del firmante para estar seguro de que fue él y no otro el autor del documento) y no de repudio (seguridad de que el autor del documento no puede retractarse en el futuro de las opiniones o acciones asignadas en él)”.¹⁴² Además de que “es la garantía de detención de cualquier modificación de los datos firmados, proporcionando una integridad total ante alteraciones fortuitas o deliberadas durante la transmisión telemática del documento firmado”¹⁴³

“Cuando esta identificación es altamente fiable y permite revelar cualquier alteración del documento no autorizada permitiendo también notar si los dispositivos empleados en la creación de la firma son seguros, por cumplir ciertas exigencias técnicas, y porque el prestador de servicios de certificación que ha intervenido está ‘acreditado’, entonces se habla de ‘firma electrónica avanzada’”¹⁴⁴

La firma electrónica avanzada es creada por su signatario a través de medios que éste mantiene bajo su exclusivo control, lo que permite que dicha firma sólo pueda ser vinculable a él, haciendo posible la detección de cualquier modificación ulterior de ésta o los datos contenidos en ella; está basada en un certificado reconocido emitido por un prestador de servicios de certificación autorizado para ello por el gobierno a través de la Secretaría de Economía.

Entre los medios electrónicos empleados para la creación de una firma electrónica avanzada; tenemos a la criptografía asimétrica, que se basa en el uso

¹⁴² <http://www.cem.itesm.mx/dacs/publicaciones/logos/libros/libros/firma.pdf>

¹⁴³ Ibidem

¹⁴⁴ <http://www.cimm.com.mx/cimm/clave.html>

de un par de claves únicas: una pública y otra privada; relacionadas entre si de forma matemática; haciendo que del conocimiento de la clave pública se derive la clave privada.

En general, podemos decir que la diferencia entre ambas firmas, radica en el grado de protección legal que producen. A la firma avanzada, también se le conoce como firma digital, para fines teóricos ambos términos son utilizados indistintamente.

Los cuerpos jurídicos mexicanos se ocupan de la firma electrónica avanzada o firma digital. Entre ellos está la NOM-151-SCFI-2002 que puntualiza que la firma digital es *“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”*.

Está también el artículo 89 del Código de Comercio Vigente que define a la firma electrónica avanzada como: *“Aquella firma electrónica que cumpla con los requisitos contemplados en las fracciones I a IV del artículo 97”*. Dichos requisitos son: *“I. Los datos de creación de firma, en el contexto en que son utilizados, 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 esta hecha después del momento de la firma”*.

A pesar que el artículo 89 del Código de Comercio Vigente hace una enumeración de características; en tanto la NOM-151-SCFI-2002, da una “definición”; ambas descripciones son idénticas. Y nos parecen por demás correctas, porque atienden a los criterios adoptados internacionalmente por diversas naciones y organismos de comercio internacional, entre ellos la CNDUMI en su Ley Modelo sobre firmas electrónicas del 2001¹⁴⁵. Esto es un acierto de nuestros legisladores, ya que al establecer reglas claras que siguen los criterios

¹⁴⁵ Artículo 6

...3) La firma electrónica se considerará fiable a los efectos del cumplimiento del requisito a que se refiere el párrafo 1) si:

- a) los datos de creación de la firma, en el contexto en que son utilizados corresponden exclusivamente al firmante;
- b) los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante;
- c) es posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma; y
- d) cuando uno de los objetivos del requisito legal de firma consista en dar seguridades en cuanto a la integridad de la información a que corresponde, es posible detectar cualquier alteración de esa información hecha después del momento de la firma...

adoptados universalmente, se facilita el desarrollo del comercio electrónico en México, ya sea en el plano nacional o en el internacional.

Técnicamente, el modelo de firma electrónica avanzada que operará en México se basa en el estándar propuesto por la Unión Internacional de Telecomunicaciones (UIT), y la Organización para la Cooperación y el Desarrollo Económico, (OCDE), opera sobre el sistema de seguridad X.509 versión 3, que ofrece niveles de encriptación de datos de 128 bits.

Cuando se cumple con todos los requisitos legales estamos frente a una firma electrónica avanzada, que hace posible entre otras cosas: la Autenticación (Identifica al usuario que ha enviado el mensaje); la Autorización (el asegurar que es la persona indicada para llevar a cabo la operación concreta); la Privacidad (Garantizar que nadie más vea los mensajes); la Integridad: (Garantiza que no se ha alterado el mensaje) y el No repudio (Nadie excepto el emisor podría haber firmado el documento)

2.3.1.1.1. Criptografía

El diccionario de la Real Academia de la Lengua define a la criptografía como el arte de escribir con clave secreta o de modo enigmático. Al tiempo que la Norma Oficial Mexicana NOM-151-SCFI-2002, prácticas comerciales – requisitos que deben observarse para la conservación de mensaje de datos, en su punto 3.19 aclara que es *un conjunto de técnicas matemáticas para cifrar información*. Algunos otros la definen como “la ciencia de la seguridad de la información”¹⁴⁶

La Criptografía es una de las ramas de la Criptología, que es la “ciencia que estudia la ocultación, disimulación o cifrado de la información, así como el diseño de sistemas que realicen dichas funciones”¹⁴⁷. Además de la criptografía, la criptología comprende al criptoanálisis, que se encarga de “transformar un criptograma en un texto claro original pero sin conocer inicialmente el sistema de cifrado utilizado y/o clave”¹⁴⁸; y a la criptofonía que es la ocultación de la voz.

Etimológicamente la palabra criptografía proviene del griego *kryptos*, que significa oculto y *graphae* que quiere decir escritura; que juntos significan escritura en clave. El término fue empleado por primera vez en el siglo XVII, pero el concepto de ocultar mensajes es muy antiguo. Las primeras tentativas criptográficas no son escritas, sino orales; las personas que hablaban más de una lengua, se valían de ello para intercambiarse información delante de personas que desconocían dicha lengua. De ahí viene la palabra *criptolalia*, de raíz *krypto* que quiere decir yo oculto, y de *laleo*; que significa yo hablo; y en conjunto quiere decir:

¹⁴⁶<http://www.cem.tesm.mx/dacs/publicaciones/logos/libros/libros/firma.pdf>

¹⁴⁷ Reyes Krafft, Alfredo Alejandro. *Ob cit.* p.178

¹⁴⁸ *Ibidem*

alteración de la lengua hablada con el fin de que no pueda ser comprendida si no se conoce la clave.

Los antecedentes más remotos del uso de métodos (manuales) que podríamos considerar como criptográficos, los encontramos entre la antigua civilización egipcia, hacia el año del 2000 a.C. El sistema de escritura egipcio estaba basado en jeroglíficos, que eran una serie de pictogramas complejos cuyo significado solo podía ser interpretado por algunos cuantos.

El siguiente precedente lo encontramos en la antigua Grecia, donde los militares desarrollaron un sistema llamado *SCYTALE*, que se valía de enredar un listón delgado en un pequeño báculo hasta ferrarlo; sobre éste escribían el mensaje a enviar, al ser desenrollado el mensaje se volvía indescifrable, pero al volver a enredarse en un báculo con dimensiones idénticas podía ser leído nuevamente.

Posteriormente, en los tiempos del Imperio Romano, el famoso general Julio Cesar (100 a.C. –44 a.C.) concibe un sistema de comunicación con sus oficiales y gobernadores, donde "los caracteres eran remplazados por el tercer carácter siguiente del alfabeto romano"¹⁴⁹. Otras civilizaciones antiguas como los vikingos y árabes también harían uso de métodos criptográficos para ocultar información.

La ciencia de la criptografía adquiriría un carácter más formal hacia 1379, cuando Gabriel de Lavinde publica su primer manual de criptografía. En 1832 Samuel Morse desarrolla el Código Morse, que aunque no es un código es una forma de cifrar las letras del alfabeto dentro de sonidos largos y cortos.

En la antigüedad la criptografía fue utilizada con fines militares, pero a medida que a la información entre la gente común adquirió más y más importancia el uso de ésta entre la comunidad no castrense se popularizó. Además de extenderse, las aplicaciones tecnológicas, hicieron evolucionar a la criptografía de métodos manuales a mecánicos y posteriormente a medios electrónicos.

Actualmente la criptografía se ocupa de modificar los datos de un mensaje, mediante un algoritmo o una clave, de tal manera que el mensaje original quede ilegible. Haciendo posible que dado un texto cifrado, y conocido el algoritmo o la clave utilizada para su transformación, se puede descifrar el mensaje. A este proceso se le conoce como encriptamiento, que significa "hacer que determinada información sea ininteligible para alguien no autorizado a acceder a ella"¹⁵⁰

La técnica de encriptación comprende dos subcategorías: la simétrica o de clave privada (sólo existe una clave); y la asimétrica o de clave pública (donde "se utiliza un par de llaves: una privada -que es secreta- usada para asegurar la firma

¹⁴⁹ <http://www.cem.tesm.mx/dacs/publicaciones/logos/libros/libros/firma.pdf>

¹⁵⁰ Téllez Valdés, Julio. *Op. cit.* p.203

digital y otra pública -a la que todos tienen acceso- que se usa para verificar la firma¹⁵¹).

En ambas técnicas se valen del uso de algoritmos para realizar la encriptación. Un algoritmo es una "serie de reglas que no pueden ser ambiguas y deben tener una meta clara. Los algoritmos pueden ser expresados por cualquier lenguaje, de el inglés al francés hasta lenguajes de programación de computadoras"¹⁵²

2.3.1.1.1. Simétrica

Los sistemas de encriptación simétrica surgen a finales de los años 70, se basan en el uso de una clave secreta que aplicada a un algoritmo convierte un mensaje original en uno cifrado. La clave para cifrar y descifrar mensajes es la misma, o bien es fácilmente calculable a partir de la otra.

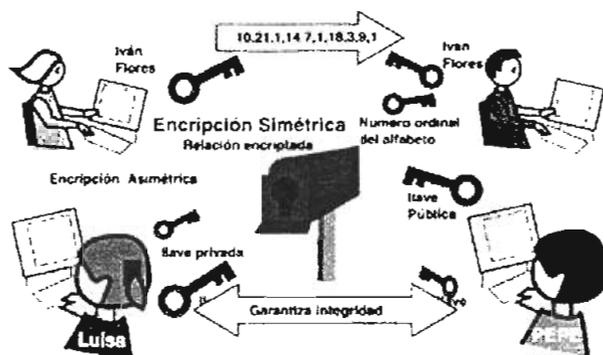
La criptografía simétrica es rápida en comparación con la criptografía asimétrica; pero el hecho de que la clave tenga que ser conocida por ambos usuarios la hace poco segura, por lo mismo no se cumple con la autenticación y el no repudio; haciendo que su uso en redes públicas sea escaso, ya que en cierta medida se requiere que los usuarios se conozcan previamente; aunque es popular en redes pequeñas, dado el número reducido de usuarios y la comunicación que exista entre ellos.

Ejemplos de sistemas simétricos son: el RC2, RC4, RC5, 3DES, AES, ECC (Criptografía de Curva Elíptica) SkipJack, y el DES (Data Encryption Standard) o DEA (Algoritmo de Encriptación de Datos). Este último fue creado en 1976 por la IBM, adoptado inicialmente por las oficinas gubernamentales de los Estados Unidos Americanos, rápidamente adquirió popularidad, llegándose a convertir en el estándar a seguir por más casi veinte años. "Es un bloque cifrado, encriptando los datos en bloques de 64 bits... La clave tiene un tamaño de 56 bits"¹⁵³. Este sistema ha sufrido ciertas mejoras, que han recibido el nombre de IDEA.

¹⁵¹ <http://www.monografias.com/trabajos13/contelec/contelec.shtml>

¹⁵² <http://www.cem.tesm.mx/dacs/publicaciones/logos/libros/libros/firma.pdf>

¹⁵³ *Ibidem*



2.3.1.1.1.2. Asimétrica

También conocida como criptografía de llave pública, la criptografía asimétrica se basa en el uso en una pareja de claves conocidas como clave pública y clave privada relacionadas matemáticamente. La firma electrónica avanzada se basa en este tipo de criptografía, por lo que nuestros legisladores se han ocupado de definir a ambas. De acuerdo con la NOM-151-SCFI-2002, debemos entender como clave pública a *la cadena de bits perteneciente a una entidad particular y susceptible de ser conocida públicamente, que se usa para verificar las firmas electrónicas de la entidad, la cual está matemáticamente asociada a su clave privada*; en tanto que por clave privada se comprende *A la cadena de bits conocida únicamente por una entidad, que se usa en conjunto con un mensaje de datos para la creación de la firma digital, relacionada con ambos elementos.*

La clave privada solo es del conocimiento y uso del propietario, es secreta, se genera mediante un algoritmo fuerte y se utiliza para firmar mensajes. La clave pública está contenida en certificado electrónico, pero igualmente puede almacenarse en directorios públicos y es utilizada para cifrar mensajes. El uso de dos claves provoca que teniendo la clave para descifrar no se pueda calcular la clave para encriptar; pero un mensaje cifrado con una de las claves solamente puede ser descifrado por la otra. De tal manera que si un usuario cifra determinada información con su llave pública, cualquier persona que conozca su llave pública podrá descifrar la misma, probando con esto la autoría del mensaje. Aunque debemos aclarar que cifrar y firmar no es lo mismo. La firma electrónica garantiza la autenticación, la integridad y el no repudio; en tanto que el cifrado asegura la confidencialidad de un mensaje.

En la práctica, dado que toma mucho tiempo a los algoritmos de clave pública cifrar documentos largos, "los protocolos de firma digital se implementan

junto con funciones unidireccionales de resumen (funciones hash)¹⁵⁴, de tal forma que se firma un resumen, en lugar de tener que firmar todo el documento.

La coherencia entre el certificado de firma digital y el contenido puede ser verificado mediante las mismas funciones Hash; que consisten en funciones matemáticas a través de las que un conjunto de información es transfigurada en una suma decimal. "Estas sumas se utilizan para notar una coherencia cercana entre los contenidos y la firma digital... Si solo una letra del mensaje original es cambiado, se vera una suma que es diferente de la calculada y firmada inicialmente, conformando así su alteración luego de ser enviado"¹⁵⁵.

Quedando claro con esto que firmar electrónicamente un documento estriba en pasar un algoritmo sobre el texto a cifrar, tomando como base la clave privada del signatario electrónico. Para el caso que el texto debe transmitirse firmado, el algoritmo circula los datos electrónicos, y, junto a la clave privada obtiene un valor hash, lo que constituye la llamada firma digital. "En la transmisión, se envía por una parte un documento cifrado, y por otra el hash. Cuando el receptor recibe ambos documentos, debe actuar bajo las siguientes pautas: 1. Descifra el texto del destinatario con la clave pública. 2. Con este texto calcula el hash. 3. Si el hash calculado y el enviado coinciden, eso significa que el documento que ha llegado lo envía quien dice ser (ha sido descifrado con su clave 'contraria') y que además no ha sido alterado por el camino, por lo contrario los dos hash no coincidirían"¹⁵⁶.

Algunos de los algoritmos de encriptación asimétrica más utilizados en la actualidad son: el DH, el RSA, el DSA y el MD5. El DH o Diffie-Hellman es el más antiguo algoritmo de clave pública (1976), tiene un rango de clave de 1536 bits; su "secreto" radica en la dificultad de calcular algoritmos discretos infinitamente, se emplea primordialmente para generar claves secretas, mas no para desencriptar o encriptar.

Le sigue el RSA (Sistema Criptográfico de Clave Pública) desarrollado en 1977 por Adi Shamir, Ron Rivest y Lonard Adleman (profesores del M.I.T.). Cuenta con un rango de clave de 1024 bits para uso corporativo y 2048 para claves valiables; con él se sientan las bases para la moderna firma electrónica avanzada, ya que es el primero en emplear el sistema de dos claves para la encriptación de documentos.

Más reciente (1994) tenemos al DSA (Digital Signature Algorithm o Algoritmo de Firma Digital) producto del gobierno de los Estados Unidos Americanos a través de su Instituto Nacional de Tecnología y Estándares (NIST); basado en el estándar DSS (Digital Signature Standard o Estándar de Firma Digital); consiste en tomar un problema de logaritmos discretos, derivados de los sistemas criptográficos propuestos por ElGamal y Schnorr. Cuenta con un rango de clave de

¹⁵⁴ Reyes Krafft, Alfredo Alejandro. *Ob cit.* p. 182

¹⁵⁵ <http://www.monografias.com/trabajos13/contelec/contelec.shtml>

¹⁵⁶ Reyes Krafft, Alfredo Alejandro. *Ob cit.* p. 184

56 bits; el 19 de Mayo de 1994 fue oficialmente seleccionado para convertirse en el estándar de autenticación digital del gobierno de E.U.A.

En cuanto a los algoritmos encargados de las funciones Hash de una sola dimensión, tenemos al MD5, desarrollado en 1992 con un rango de clave de 128 bits. "Después de un proceso inicial, MD5 procesa el texto insertado en bloques de 512 bits, divididos en bloques de 32 bits. El resultado del algoritmo son 4 bloques de 32 bits, que juntos forman un bloque de 128 bits"¹⁵⁷

Al hablar de los diferentes sistemas de criptografía asimétrica abordamos el tamaño de las claves, esto es importante, dado que "el tamaño de las claves determina la seguridad del sistema de encriptación... Cuanto más larga sea la clave más segura será la transmisión"¹⁵⁸. Por ejemplo, una clave de 128 bits genera mensajes que son 309,485,009,821,341,068,724,781,056 veces más difíciles de descifrar que una clave de 40 bits.

Por último, es necesario aclarar que la criptografía asimétrica forma parte de los siguientes estándares internacionales:

- *ISO9796*, International Standards Organization u Organización de Estándares Internacionales, la norma ISO9796 versa sobre Tecnología de la Información – Técnicas de Seguridad – Mecanismo de Firma Digital.
- *ANSI X9.31* Instituto Americano de Estándares Nacionales o American National Standards Institute, estándar X9.31 de Autenticado de Mensajes para Instituciones Financieras (Financial Institution Message Authentication) para el sistema bancario estadounidense.
- *ITU-T X.509*. Unión Internacional de Telecomunicaciones, Sector de Estandarización de Telecomunicaciones o Internacional Telecommunication Union, Telecommunication Standardization Sector, estándares X.509 de Tecnología de la Información, -Interconexión de Sistemas Abiertos – El Directorio : Marco para el Autenticado (Information Tecnology –Open Systems Interconnection - The Directory: Authentication Framework).
- *PKCS*. Estándares de Criptografía de Clave Pública o Public Kay Cryptography Standards, desarrollados por RSA Corporation en forma conjunta con Apple, Microsoft, Digital, Lotus, Sun y Massachusetts Institute of Tecnology
- *SWIFT*. Sociedad para las Telecomunicaciones Financieras Interbancarias Mundiales o Society for Worldwide Interbank Financial Telecommunications
- *ETEBAC*: Sistemas Financiero Francés, estándar 5¹⁵⁹

¹⁵⁷ <http://www.cem.tesm.mx/dacs/publicaciones/logos/libros/libros/firma.pdf>

¹⁵⁸ Kent, Peter. *Internet ¡Fácil!* 3ª ed. Prentice - Hall Hispanoamericana, S.A., México, 1996 p.52

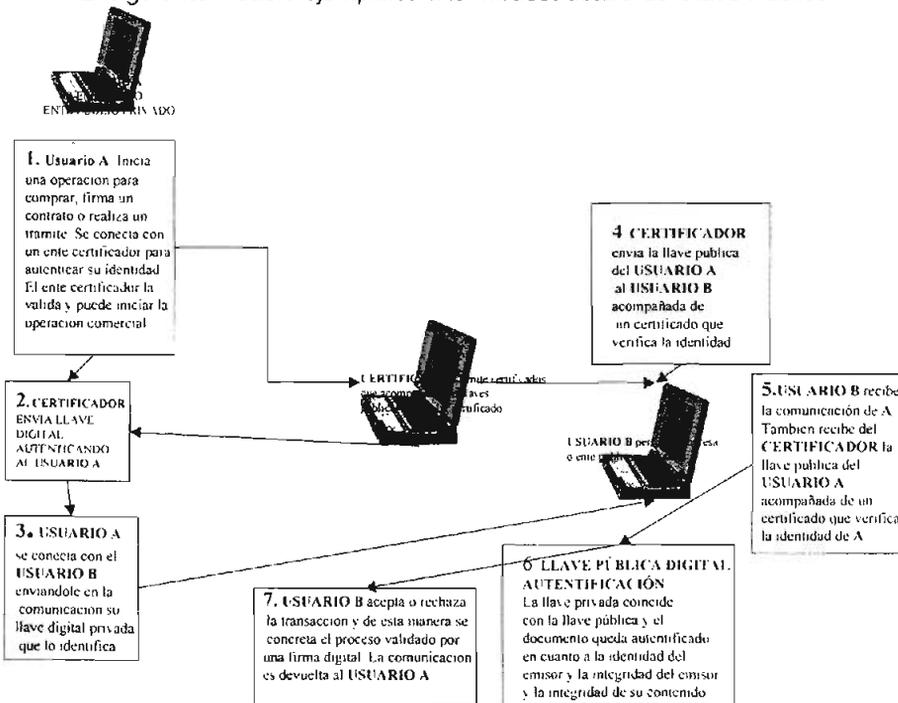
¹⁵⁹ http://www.informatica-juridica.com/trabajos/firma_digital.asp

2.3.1.1.1.2.1. La Infraestructura de Clave Pública

Como vemos los primeros pasos hacia la seguridad en materia electrónica nos lo dan los sistemas de encriptación asimétrica basados en complejos sistemas matemáticos y tecnológicos. Pero, no son suficientes, para lograr que una firma electrónica avanzada sea lo bastante confiable para las transacciones vía electrónica se necesita de una estructura más compleja. Es aquí donde entra la "Open Public Key Infrastructures (PKI) o Infraestructura de Clave Pública.

La PKI es una "arquitectura de seguridad que ha sido desarrollada para proveer de un nivel mayor de confidencialidad al intercambiar información en Internet"¹⁶⁰. Es una estructura mediante la cual las llamadas Entidades de Certificación (a las que dedicaremos un capítulo completo posteriormente) asegura que la clave pública corresponde a una determinada persona a través de ciertas políticas operativas, el otorgamiento de certificados, entre otros métodos que hacen posible un mayor rango de seguridad en las transacciones vía electrónica.

El siguiente modelo ejemplifica a la Infraestructura de Clave Pública¹⁶¹:



¹⁶⁰ <http://www.cem.tesm.mx/dacs/publicaciones/logos/libros/libros/firma.pdf>

¹⁶¹ Cfr. Téllez Valdés, Julio. *Op.cit.* p.204

2.4. La firma electrónica mundialmente

2.4.1. Estados Unidos Norteamericanos

Comenzamos nuestro recuento mundial con los Estados Unidos Norteamericanos (E.U.A.) debido a que es una de las naciones pioneras en la regulación de la temas de Derecho Informático (entre ellos la firma electrónica).

Como mencionamos anteriormente, al hablar de sistemas criptográficos; uno de sus primeros intentos de establecer regulaciones en el campo informático por parte del gobierno de los E.U.A. fue el sistema DES (Data Encryption Standard) o DEA (Algoritmo de Encriptación de Datos), de 1976, que el gobierno adoptó para ser usado en sus comunicaciones no clasificadas, pero sensibles.

Sería en los mismos E.U.A. donde surgiría la primera ley en Materia de Firma Digital en el Mundo. El 27 de Febrero de 1995, es dada a conocer la "Utah Digital Signature Act" (modificada en 1996) por el Estado de Utah. Algunos de los objetivos que se plantea van encaminados sobre todo a la búsqueda de seguridad, confiabilidad, autenticación y rapidez en los mensajes de datos y la firma electrónica; con el objetivo de agilizar las transacciones via electrónica, y evitar cualquier tipo de fraudes.

Entre otras cosas esta ley establece la equivalencia funcional entre la firma digital y la manuscrita (siempre y cuando ésta cumpla con los requisitos legales) por lo que se admite su valor probatorio. La define como la *"transformación de un mensaje empleando un criptosistema asimétrico tal, que una persona posea el mensaje inicial y la clave pública del firmante pueda determinar con certeza si la transformación se creó usando la clave privada que corresponde a la clave pública del firmante, y si el mensaje ha sido modificado desde que se efectuó la transformación"*. Al tiempo que al criptosistema asimétrico lo concreta como *aquel "algoritmo o serie de algoritmos que brindan un par de claves confiables"*.

Esta ley, no ha sido el único documento estadounidense en materia de firma electrónica. La American Bar Association (ABA) que ha emitido diversas resoluciones sobre firma electrónica: "La Resolución sobre Cibernetario: Un especialista internacional en transacciones vía computadora" (Resolution concerning the CyberNotary: an International computer – transaction specialist) del 2 de agosto de 1994, y la "Guía de Firmas Digitales" (Digital Signature Guidelines) del 1 de agosto de 1996.

Para el 16 de abril de 1993, el gobierno estadounidense lanza el proyecto Clipper; una iniciativa criptográfica para asegurar la seguridad en las transacciones electrónicas entre civiles. Dos son sus bases: "Un chip cifrador a prueba de cualquier tipo de análisis o manipulación (el Clipper chip o EES (Escrowed Encryption Standard) y Un sistema para compartir las claves secretas (KEY –Key Escrow System) que, en determinadas circunstancias, otorgaría el

acceso a la clave maestra de cada chip, y que permite conocer las comunicaciones cifradas en él”¹⁶².

Posteriormente, el 15 de agosto de 1997, la Conferencia Nacional de Comisionados sobre Derecho Estatal Uniforme (NCCSL) se reúne para elaborar una ley uniforme en materia de comercio electrónico, fruto de lo cual tenemos a la "Uniform Electronic Transactions Act" (UETA), que es aprobada el 30 de julio de 1999. Esta misma asociación crea la "Uniform Computer Information Transactions Act" (UCITA), aprobada el 4 de agosto del 2000.

Por parte de la presidencia estadounidense tenemos a la "Electronic Signatures in Global and National Commerce Act" (E-Sign Act) emitida en 30 de junio del 2000; que entró en vigor, el 1 de Octubre del 2000; donde se establece legalmente la equivalencia funcional entre la firma electrónica y el documento electrónico, respecto a la firma autógrafa y documento de papel.

Actualmente cada una de las legislaciones estadounidenses estatales cuenta con una definición de firma electrónica y firma digital (o firma electrónica avanzada).

2.4.2. Argentina

Los primeros antecedentes legales de regulación en materia de Firma Electrónica en Argentina los encontramos en la Resolución MTSS N° 555/97 del Ministro de Trabajo y Seguridad Social – Normas y Procedimientos para la Incorporación de Documentos y Firma Digital. En ella se define a la firma digital, el documento digital, el certificador de clave pública, la clave privada, el certificado y la clave pública; además de establecer la validez, eficacia, plenos efectos probatorios y legales de los documentos digitales que estén firmados electrónicamente.

El mismo año es la resolución SAFJP N° 293/97 de la Superintendencia de Administradoras de Fondos de Jubilación y Pensiones – Incorporación del Correo Electrónico con Firma Digital. "Establece que los CD – ROMs remitidos por el Sistema, serán válidos y eficaces, surtiendo todos los efectos legales y probatorios, a partir de la fecha y hora en que queden enmienda o raspadura que altere la información escrita sea visible y evidente;

2. El documento posee márgenes razonable que contienen los renglones escritos, tal que cualquier escritura sea visible y evidente;
3. La firma manuscrita se coloque delimitando la información escrita, tal que no sea posible agregar texto escrito excepto a continuación de la firma manuscrita;
4. El firmante utiliza siempre la misma o similar firma manuscrita para firmar los documentos de su autoría;
5. La firma manuscrita es suficientemente compleja tal que su falsificación deviene no trivial, y

¹⁶² http://www.informatica-juridica.com/trabajos/firma_digital.asp

6. Existen peritos caligráficos que pueden detectar las falsificaciones con un razonable grado de certeza”¹⁶³

En tanto que el decreto N° 427/98 de 1998 del Poder Ejecutivo – Firmas Digitales para la Administración Pública Nacional. Elaborado por el Sub-Comité de Firma Digital del Comité de Usuarios de Procesamiento de Imágenes (CUPI), en el que participaron representantes de diversos organismos estatales y el Banco Central de la República de Argentina. Autoriza el uso de la firma digital (a la que se equipara con la manuscrita) en la instrumentación de actos internos del sector público nacional argentino. Asimismo, se habla de figuras como la entidad certificadora, sus condiciones; el certificado de clave pública, entre otras cosas.

La firma digital es definida como “el resultado de una transformación de un documento digital empleando un criptosistema asimétrico y un digesto seguro de forma que una persona que posea el documento digital inicial y la clave pública del firmante pueda determinar con certeza si la transformación se llevo a cabo con la clave privada que corresponde a la clave pública del firmante, lo que impide su repudio; si el documento digital ha sido modificado desde que se efectuó la transformación, lo que garantiza su integridad. La conjunción de los dos requisitos anteriores garantiza su no repudio y su integridad.”¹⁶⁴ Al tiempo que al documento digital se le define como “la representación digital de actos, hechos o datos jurídicamente relevantes. Un documento digital firmado es al que se le ha aplicado una firma digital”¹⁶⁵

Para marzo de 1999, la comisión jurídica creada por el decreto 685/95 se encarga de la redacción de un Proyecto de Código Civil que se ocupará de las materias electrónico comerciales. Estas reformas entre otras cosas amplian la referencia jurídica argentina de escrito, considerándose como tal también a lo que se produce, consta o lee a través de medios electrónicos; se define a la firma y se habla de los procedimientos a seguir para que ésta sea considerada como legalmente válida; así como se establece la posibilidad de que puedan existir tanto documentos digitales públicos, como privados.

Tras el estudio de todos los documentos previos (como el Decreto N° 427/98) y ponencias se redacta un anteproyecto de Ley de Firma Digital, por la Comisión Redactora del Ministerio de Justicia. Aprobado por media sanción por la Cámara de Diputados el 15 de Agosto del 2001, y finalmente sancionada el 14 de Noviembre del 2001; siendo promulgada el 11 de diciembre del 2001, la Ley N° 25.506 – de Firma Digital de la Nación Argentina.

Consta de 53 artículos. En el artículo 2° de esta ley se establece que por firma digital se entiende “al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del

¹⁶³ http://www.informatica-juridica.com/trabajos/firma_digital.asp

¹⁶⁴ Téllez Valdés, Julio, *Ob cit.* p. 207

¹⁶⁵ *Ibidem*

firmante, encontrándose éste bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, al que dicha verificación simultáneamente permite identificar el firmante y detectar cualquier alteración del documento posterior a su firma". En el artículo 3° se habla de la equivalencia funcional entre la firma digital y la manuscrita; salvo las excepciones establecidas en el artículo 4°: a) a las disposiciones por causa de muerte, b) a los actos jurídicos del derecho de familia; c) a los actos personalísimos en general; y d) a los actos que deban ser instrumentados bajo exigencias o formalidades incompatibles con la utilización de la firma digital; ya sea como consecuencia de las disposiciones legales o acuerdo de partes.

Se hace también la distinción entre la firma digital y la electrónica; entendiéndose por esta última como el "conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizados por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital". Fruto de esta diferencia, en los artículos 7° y 8° se establecen los efectos jurídicos de la firma digital, que en virtud de su naturaleza, goza de autoria y de integridad, siendo así que la carga de la prueba recaerá sobre la persona que alega la falsedad de un documento firmado digitalmente o que el mismo ha sido firmado por interpósita persona; en contrario sensu cuando se desconoce la firma electrónica la carga de la prueba sobre su validez recaerá sobre quien la alega. En el artículo 12° se habla de la conservación de documentos registros y datos digitales.

Este es a grandes rasgos el panorama argentino de en materia de firma electrónica al momento de ser escrito el presente apartado.

2.4.3. Colombia

En un intento de adaptarse a las realidades internacionales; la nación sudamericana se dio a la tarea de elaborar una ley sobre comercio electrónico que abarcara todos los temas relacionados. Por lo que a iniciativa de los Ministerios de Justicia, Comercio Exterior, Transporte y Desarrollo; se convocó a una Comisión Redactora conformada por sectores públicos y privados. Dicha comisión se dio a la tarea de estudiar las diversas legislaciones internacionales, y doctrinas sobre comercio electrónico hasta ese entonces.

Producto de sus esfuerzos el 18 de Agosto de 1999, Colombia promulga su Ley 527 sobre Comercio Electrónico, cuyo objetivo es "definir y reglamentar el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, así como establecer las entidades de certificación"¹⁶⁶. En ella se define a diversas figuras de comercio electrónico de la siguiente manera:

¹⁶⁶ Téllez Valdés, Julio. *Ob cit.* p. 205

- a) Mensaje de datos. La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el fax;
- b) Comercio electrónico. Abarca las cuestiones suscitadas por toda relación de índole comercial, sea o no contractual, estructurada a partir de la utilización de uno o más mensajes de datos o de cualquier otro medio similar. Las relaciones de índole comercial comprenden, sin limitarse a ellas, las siguientes operaciones: toda operación comercial de suministro o intercambio de bienes o servicios; todo acuerdo de distribución; toda operación de representación o mandato comercial; todo tipo de operaciones financieras, bursátiles y de seguros; de construcción de obras; de consultoría; de ingeniería; de concesión de licencias; todo acuerdo de concesión o explotación de un servicio público; de empresa conjunta y otras formas de cooperación industrial o comercial; de transporte de mercancías o de pasajeros por vía aérea, marítima y férrea, o por carretera¹⁶⁷;
- c) Firma digital. Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación; y
- d) Entidad de Certificación. Es aquella persona que, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales.

2.4.4. Chile

La primera vez que Chile habla de Firma electrónica es en el decreto 81 del 10 de junio de 1999, presentado por el presidente Eduardo Frei, donde se reglamenta la utilización de la firma digital y los documentos electrónicos en la Administración del Estado. En este se define a la *firma electrónica* como un código informático que permite determinar la autenticidad de un documento electrónico y su integridad, impidiendo a su transmisor desconocer la autoría de un mensaje en forma posterior. La *firma digital* es la que resulta de un proceso informático validado, implementado a través de un sistema criptográfico de claves públicas y privadas. El *documento electrónico* es toda representación informática que da testimonio de un hecho. Y *certificado de firma digital* señala que es todo

¹⁶⁷ Cfr. Reyes Krafft, Alfredo Alejandro. *Ob cit.* p133

documento electrónico por el ministro de fe del servicio respectivo que acredita la correspondencia entre una clave pública y la persona que es titular de la misma.

Pero dicho decreto al limitarse simplemente a la implementación de tecnologías electrónicas en la administración pública, hace a un lado las necesidades de los particulares, ya que ni siquiera las toca. Por lo que en afán de dotar a los particulares de regulaciones en materia electrónica el 9 de agosto del 2000 en Chile se inicio la elaboración de un proyecto de ley sobre firma electrónica, que finalmente fue aprobado por unanimidad en el 2002. En dicho proyecto entre otras cosas se reconoce la validez legal del documento electrónico y de los contratos electrónicos; así como a la firma electrónica avanzada; entre otros temas. Los conceptos en ella utilizados son retomados del decreto 81.

Casi simultánea a ésta tenemos la Ley Marco de Comercio Electrónico que reconoce la contratación Electrónica, Firma Electrónica, la Fuerza probatoria de los Documentos; fruto de un proyecto suscrito por Jorge Muñoz Zinches, aprobado a través de la ley 27269 publicada el 28 de mayo del 2000, ella establece entre otras cosas que: "Si la transformación se hizo utilizando la clave privada correspondiente a la clave pública del firmante. Si el mensaje firmado ha sido alterado desde que la transformación fue hecha. Para la transformación de un mensaje se deben cumplir los siguientes requisitos: Depende de la persona que firma; y solo el titular de las firmas es capaz de crear la firma digital para un mensaje específico. Cualquiera será capaz de verificar la firma digital pues tiene acceso a la clave pública del firmante"¹⁶⁸.

2.4.5. Ecuador

Para marzo del 2001 "se presentó un Proyecto de Ley de Comercio Electrónico y firmas digitales, en términos muy similares a la chilena, utilizando el modelo mexicano"¹⁶⁹

2.4.6. Panamá¹⁷⁰

Este país también cuenta con una regulación sobre comercio electrónico, firma electrónica, entidades de certificación e intercambio de documentos electrónicos, es la llamada Ley número 43 del 31 de julio del 2001, que hace las siguientes definiciones:

¹⁶⁸ <http://www.monografias.com/trabajos13/contelec/contelec.shtml>

¹⁶⁹ Reyes Krafft, Alfredo Alejandro. *Ob cit.* p.153

¹⁷⁰ Publicada en la Gaceta Oficial No. 24.359 del 3 de agosto de 2001. Citado por Reyes Krafft, Alfredo Alejandro. *Ob cit.* p.153

Certificado: Manifestación que hace la entidad de certificación, como resultado de la verificación que efectúa sobre la autenticidad, veracidad y legitimidad de las firmas electrónicas o la integridad de un mensaje.

Destinatario: Persona designada por el iniciador para recibir el mensaje, pero que no esté actuando a título de intermediario con respecto al mensaje.

Documento electrónico: Toda representación electrónica que da testimonio de un hecho, una imagen o una idea.

Entidad de certificación: Persona que emite certificados electrónicos en relación con las firmas electrónicas de las personas, ofrece o facilita los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos y realiza otras funciones relativas a las firmas electrónicas.

Firma electrónica. Todo sonido, símbolo o proceso electrónico vinculado a o lógicamente asociado con un mensaje, y otorgado o adoptado por una persona con la intención de firmar el mensaje que permite al receptor identificar a su autor.

Iniciador: Toda persona que, a tenor del mensaje, haya actuado por su cuenta o en cuyo nombre se haya actuado, para enviar o generar ese mensaje antes de ser archivado, si éste es el caso, pero que no haya actuado a título de intermediario con respecto a ese mensaje.

Intermediario: Toda persona que, actuando por cuenta de otra, envíe, reciba o archive un mensaje o preste algún otro servicio con respecto a él.

Mensaje de datos: Información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax.

Repositorio: Sistema de información utilizado para guardar y recuperar certificados u otro tipo de información relevante para la expedición de éstos.

Revocar un certificado: Finalizar definitivamente el periodo de validez de un certificado, desde una fecha específica en adelante.

Sistema de información: Todo sistema utilizado para generar, enviar recibir, archivar o procesar de alguna forma mensajes de datos.

Suscriptor: Persona que contrata con una entidad de certificación la expedición de un certificado, para que sea nombrada o identificada en él. Esta persona mantiene bajo su estricto y exclusivo control el procedimiento para generar su firma electrónica.

Suspender un certificado: Interrumpir temporalmente el periodo operacional de un certificado, desde una fecha en adelante.

2.4.7. Perú

Dentro del seminario Respondiendo a los obstáculos legales para el comercio electrónico en América Latina o "Responding to the Legal Obstacles to Electronic Commerce in Latin America" convocado del 29 de Septiembre al 1 de Octubre de 1999 por National Law Center Inter American Free Trade. The organization of American States Business Software Alliance; con sede en Washington DC, se presentó el proyecto de ley 5070 –99 elaborado el 9 de agosto de 1999 por el gobierno Peruano, que entre otras cosas regula a la firma electrónica.

El proyecto es aprobado (basado en la legislación colombiana, argentina, chilena y mexicana) al año siguiente tomando el nombre de Ley 27269 de Firmas y Certificados Digitales, en ésta se establece la equivalencia funcional entre firma electrónica y la firma manuscrita; la vinculación de un mensaje al signatario electrónico de éste; así como la integración y autenticación de los documentos electrónicos. Entre sus definiciones tenemos:

Firma digital, que para esta ley es la que utiliza una técnica de criptografía asimétrica, basada en el uso de un par de claves único; asociadas una clave privada y una clave pública relacionadas matemáticamente entre sí, de forma que las personas que conocen la clave pública no pueden derivar de ella la clave privada.

Certificado digital, es el documento electrónico generado y firmado digitalmente por una entidad de certificación, la cual vincula un par de claves con una persona determinada confirmando su identidad.

Entidad de Certificación cumple con la función de emitir y cancelar certificados digitales, así como brindar otros servicios inherentes al propio certificado o aquellos que brinden seguridad ala sistema de certificados en particular o del comercio electrónico en general; podrán también asumir las funciones de entidades de registro y verificación.

La Entidad de Registro o Verificación, cumple con la función de levantamiento de datos y comprobación de la información de un solicitante de certificado digital; identificado y autenticación del suscriptor de firma digital; aceptación y autorización de solicitudes de emisión y cancelación de certificados digitales.

2.4.8. Venezuela

El proyecto de Ley Orgánica de Tecnologías de la Información del 26 de abril del 2000, es el primer documento venezolano que se ocupó de la firma electrónica y los documentos digitales, al igual que en el caso Chileno, no hablaban de una regulación de medios electrónicos para fines comerciales o particulares; sino de sus usos en la administración Estatal.

Pero igual que en el caso Chileno, más adelante se crea una ley para satisfacer los intereses de los particulares. En el 2001 aparece la Ley sobre Mensajes de Datos y Firmas Electrónicas; en ella se reconoce la eficacia y el valor jurídico de la firma electrónica, el mensaje de datos y cualquier información en formato electrónico. Sobre de diversas figuras electrónicas dice:

Firma electrónica es la información creada o utilizada por el signatario, asociada al mensaje de datos, que permite atribuirle su autoría bajo el contexto en el cual ha sido empleado.

Los mensajes de datos son toda información inteligible en formato electrónico o similar que puede ser almacenada o intercambiada por cualquier medio.

Certificado electrónico, es un mensaje de datos proporcionado por un proveedor de servicios de certificación que le atribuye certeza y validez a la firma electrónica.

Proveedor de Servicios de Certificación, es la persona dedicada a proporcionar certificados electrónicos y demás actividades previstas en el decreto – ley.

Sistema de Información, es aquel utilizado para generar, procesar o archivar cualquier forma de mensaje de datos.

2.4.9. Brasil

En materia electrónica cuenta con un proyecto de ley sobre creación, archivo y utilización de los documentos electrónicos.

2.4.10. Canadá

Tiene la propuesta de la Columbia británica 13 – 2001, ley de transacciones electrónicas. ("British Columbia Bill 13-2001, The Electronic Transactions Act"¹⁷¹)

¹⁷¹ <http://www.cem.itesm.mx/dacs/publicaciones/logos/libros/libros/firma.pdf>.

2.4.11. Europa

Como todos sabemos Europa se ha convertido en una Comunidad, algunas medidas económicas, como la adopción del euro como moneda única de los países miembros, han sido implementadas. Otras de las medidas son de carácter legal, buscando una unificación de normas entre los países miembros.

Los esfuerzos de unificación legal, se han encaminado a diversos campos, entre ellos el electrónico. Con el fin de lograr una armonía en cuestiones electrónicas para la comunidad, la comunidad europea hizo diversas previsiones acerca de procesos electrónicos en la Comunicación de la Comisión sobre Fomento de la seguridad y la confianza en las comunicaciones electrónicas, presentada al Consejo de la Unión Europea el 1 de diciembre de 1997, y la continuación de la Conferencia Ministerial de Bonn de julio de 1997.

Para octubre de 1997 la Comisión Europea presentó "una comunicación al Consejo, al Parlamento Europeo, al Comité Económico y Social y Al Comité de Regiones titulada 'Iniciativa Europea de Comercio Electrónico', con un subtítulo de 'Hacia un Marco Europeo para la Firma Digital y el Cifrado'¹⁷²

Más adelante a instancias del Gobierno de Dinamarca (por medio de su Ministerio de Investigación y Tecnología de la Información) y la Comisión de las Comunidades Europeas (DG XIII, Telecomunicaciones, Mercado de la Información y de Explotación de la Investigación), se celebró en Copenhague los días 23 y 24 de abril de 1998.

A dicha conferencia asistieron 102 representantes oficiales de todos los estados miembros de la comunidad europea; así como naciones invitadas (Barbados, E.U.A., Japón, Canadá, Corea, Suiza y Noruega), 29 expertos, 55 invitados y representantes de la prensa. "Se celebraron 7 sesiones, 4 dedicadas a la criptografía (tendencias del mercado, uso en la empresa, Industria europea y cumplimiento de la ley) y tres a la autenticación electrónica y firma digital (Requisitos comunes mínimos, Reconocimiento legal y Responsabilidad)¹⁷³

Ese mismo año, pero en el segundo trimestre, la comunidad europea habla de la necesidad de encauzar las propuestas a la elaboración de una Directiva de firma digital; con el propósito de dar un reconocimiento legal común a esta en Europa. Para finales de 1998 se preparó un borrador de propuesta de directiva sobre firma y servicios relacionados.

Resultado de esto al año siguiente (1999), la comunidad europea saca una Directiva del Parlamento Europeo y del Consejo que establece un marco común para la firma electrónica. El objetivo que se plantea es garantizar el buen funcionamiento del mercado interior en el área de la firma electrónica, instituyendo

¹⁷² http://www.informatica-juridica.com/trabajos/firma_digital.asp

¹⁷³ Nota informativa acerca de la audiencia europea de expertos sobre firma digital y cifrado

un marco jurídico homogéneo y adecuado para la Comunidad Europea y definiendo criterios que fundamenten su reconocimiento legal¹⁷⁴. En el se dan diferentes definiciones, entre ellas:

Firma electrónica como la firma en forma digital integrada en unos datos, ajena a los mismos o asociada con ellos, que utiliza un signatario para expresar conformidad con su contenido y que cumple los siguientes requisitos:

1. Estar vinculada al signatario de manera única.
2. Permitir la identificación del signatario.
3. Haber sido creada por medios que el signatario pueda mantener bajo su exclusivo control.
4. Estar vinculada a los datos relacionados de modo que se detecte cualquier modificación ulterior de los mismos.

Dispositivo de Creación de Firma a los datos únicos, como códigos o claves criptográficas privadas, o un dispositivo físico de configuración única para crear la firma electrónica.

Dispositivo de verificación de firma son los datos únicos, tales como códigos o claves criptográficas públicas, o un dispositivo físico de configuración única, utilizado para verificar la firma electrónica.

Certificado reconocido es el certificado digital que vincula un dispositivo de verificación de firma a una persona y confirma su identidad.

Proveedor de servicios de certificación es la persona o entidad que expide certificados o presta otros servicios al público en relación con la firma electrónica.

Esta ha sido una de las directivas comunitarias europeas relativas a medios electrónicos más importantes. Aunque existe una directiva posterior, la llamada "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"¹⁷⁵.

2.4.11.1. España

Legislación y jurisprudencia españolas son suficientemente holgadas como para acoger el concepto de firma electrónica (o cualquier otro tipo de firma) y todos sus derivados. Pero con el objeto de otorgar mayor certeza jurídica los legisladores españoles se ocuparon de estos nuevos conceptos electrónicos.

¹⁷⁴ Cfr. Téllez Valdés, Julio. *Ob. cit.* p. 208

¹⁷⁵ http://www.mineco.es/oficvirtual/firma_0.htm

Los primeros intentos de legislar al respecto los tenemos en el Real Decreto 2402/1985, del 18 de diciembre de 1985, que regula las facturas. En su artículo 3 menciona que no es necesaria "la firma ni ningún otro signo de validez" en las facturas o contratos; para ser consideradas como válidas. Lo importante de lo señalado en dicho decreto es que al hablar de "otro signo de validez" admite la posibilidad de utilizar a la firma electrónica como un signo de validez.

Le sigue una circular del Banco de España, la 8/88 del 14 de Junio de 1988, donde se reglamente el Sistema Nacional de Compensación Electrónica, donde se indica que "la información se cifrará, para que las entidades introduzcan un dato de autenticación con la información de cada comunicación, a lo que se le reconoce a este método el mismo valor que posee un escrito firmado por personas con poder bastante"¹⁷⁶

El siguiente paso es permitir el uso de medios electrónicos en la administración pública en cuestiones ciudadanas, esto se estableció finalmente en el artículo 45 de la Ley 30/1992 (26 de noviembre de 1992) del régimen jurídico de las Administraciones Públicas y del Procedimiento Administrativo. Al que el Real Decreto 263/1996 de febrero de 1996 donde se dice que "deberán adoptarse las medidas técnicas que garanticen la identificación y la autenticidad de la voluntad declarada, pero no hace ninguna regulación legal de la firma electrónica"¹⁷⁷

A partir de ahí España ha emitido más decretos, de entre todos ellos consideramos muy importantes al Real Decreto Ley 14/1999 del 17 de Septiembre de 1999 sobre firma electrónica. En el se regula a la firma electrónica, así como diversos aspectos relacionados. Algunas de las definiciones dadas por esta ley son: La firma electrónica es el conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge. (RD-L 14/1999 Art. 2).

En tanto que la firma electrónica avanzada es la que permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su 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. (RD-L 14/1999 art. 2 b). Debe basarse en un certificado reconocido, aquél que contiene determinadas informaciones (RD-L 14/1999 art. 8) y que ha sido emitido respetando determinadas cautelas (RD-L 14/1999 art. 12). El certificado reconocido tiene que haber sido expedido por un prestador de servicios de certificación acreditado (RD-L 14/1999 art. 6). Además esta firma electrónica tiene que haber sido generada empleando un dispositivo seguro de creación de firma (RD-L 14/1999 art. 19) debidamente certificado (RD-L 14/1999 art. 6).

¹⁷⁶ http://www.informatica-juridica.com/trabajos/firma_digital.asp

¹⁷⁷ *Ibidem*

El certificado es definido como la certificación electrónica que vincula unos datos de verificación de firma a un signatario y confirma su autenticidad.

Al tiempo que el prestador de servicios de certificación es la persona física o jurídica que expide certificados, puede prestar, además otros servicios en relación con la firma electrónica.

En el decreto se establece la equivalencia funcional entre la firma manuscrita y la electrónica avanzada al decir que se tendrá, respecto de los datos consignados de forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio. (RD-L 14/1999 art. 3).

Igual de importante que el Decreto Ley de 1999, tenemos a la Nueva Ley sobre firma electrónica que comenzó su vigencia el 20 de Marzo del 2004. Algunas de las novedades que introduce esta ley con respecto a lo dispuesto por su predecesora son: el Documento Nacional de Identidad, la llamada firma reconocida, certificados electrónicos para personas morales; etc.

2.4.11.2. Alemania

El primer proyecto de ley en materia de firma electrónica en Europa fue el proyecto alemán del 19 de septiembre de 1996, promulgada el 13 de junio de 1997, entró en vigor el 1 de noviembre del mismo año. Su reglamento (Law Governing Framework Conditions for Electronic Signatures and Amending Other Regulations) fue publicado el 7 de junio de 1997. La ley de firmas digitales "tiene como objetivo crear las condiciones generales para las firmas digitales bajo las cuales se las pueda considerar seguras y que las falsificaciones de firmas digitales y las falsificaciones de información firmada puedan ser verificadas sin lugar a dudas"¹⁷⁸.

La ley nos da las siguientes definiciones: Firma Digital es el sello creado con una clave privada de firma sobre información digital, el cual permite, mediante el uso de clave pública asociada rotulada por un certificado de clave de un certificador, o de una autoridad, que sean verificados el propietario de la clave firma y el carácter de no falsificador de la información.

Certificador es la persona física o jurídica, la cual da fe a la atribución de claves públicas de firma de personas físicas y mantiene una licencia para ese motivo. En tanto que certificado es la certificación digital rotulada con una firma digital con respecto a la atribución de una clave de firma pública a una persona física (certificado de clave de firma), o una certificación digital especial que se refiere inequívocamente a un certificado de clave de firma y contiene información adicional (certificado de atributos).

¹⁷⁸ Téllez Valdés, Julio. Ob. cit. p. 209

2.4.11.3. Bélgica

Bélgica contaba con algunas regulaciones en materia de medios electrónicos, como la Ley de telecomunicaciones: Régimen voluntario de declaración previa para los certificados de clave pública; así como algunos proyectos: El Proyecto de ley de certificadores de clave pública relacionados con la firma digital; El Proyecto de ley de modificación del Código Civil en materia de prueba digital; y el Proyecto de ley sobre la utilización de la firma digital en ámbitos de la seguridad social y la salud pública.

Pero las leyes que vinieron realmente a reglamentar a la firma electrónica fueron: Loi introduisant l'utilisation de mohines de télécommunication et de la signature électronique dans la procédure judiciaire et extrajudiciaire (Ley introductoria al uso de los medios de telecomunicación y la firma electrónica en el procedimiento judicial y extrajudicial), del 20 de Octubre del 2000; y la Loi fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification (Ley que establece ciertas reglas relativas al ambiente jurídico para las firmas electrónicas y los proveedores de servicios de certificación), del 29 de septiembre del 2001.

2.4.11.4. Dinamarca

En este país se dedicaron al desarrollo de un proyecto de ley de utilización segura y eficaz de la comunicación digital, que hizo posible el desarrollo de leyes posteriores como: Act 411 of 31May 2000 on Electronic Signatures. Bill L 229. Executive Order on Security Requirements etc. for Certification Authorities. Executive Order N° 923 of 5 October 2000. Executive Order on Reporting of Information to the National Telecom Agency by Certification Authorities and System Auditors. Executive Order N°922 of October 2000. (Acta 417 del 31 de Mayo del 2000 Sobre Firmas Electrónicas. Iniciativa L 229. Orden Ejecutiva sobre Requerimientos de Seguridad, etc. para Autoridades de Certificación. Orden Ejecutiva n° 923 del 5 de Octubre del 2000. Orden Ejecutiva sobre reporte de información al Dirección Nacional de Telecomunicaciones por Autoridades de Certificación y Auditores de Sistemas. Orden N° 922 de Octubre del 2000)

2.4.11.5. Finlandia

En Finlandia hasta este momento existen dos proyectos: uno sobre el intercambio electrónico de datos en la administración y los procedimientos judiciales administrativos; y otro por el que la Oficina del Censo hará las veces de certificador de clave pública.

2.4.11.6. Francia

El primer paso dado por Francia en la búsqueda de una regulación de las transacciones electrónicas es su Ley de Telecomunicaciones y disposiciones sobre uso interior cifrado. La mencionada ley habla de una normatividad sobre utilización de la firma digital en los ámbitos de seguridad social y la sanidad pública; así como del suministro de productos de firma digital sujeto a procedimientos de información; del mismo modo trata a la libertad de uso, importación y exportación de productos y servicios de firma digital.

Posteriormente Francia emitiría un decreto y una ley. El Decreto N° 2001 – 217 del 30 de marzo del 2001 Para la aplicación del artículo 1316 –4 del código civil y relativo a la firma electrónica; y la ley 2000-230 del 13 de marzo del 2000 portant adaptation du droit de la preuve aux technologies d'informtion et relative à la signature électronique.

2.4.11.7. Irlanda

En el año 2000, Irlanda publicó su ley sobre comercio electrónico (Electronic Commerce Act, 2000 – number 27 of 2000)

2.4.11.8. Italia

Italia publicó su ley N° 59 del 15 de marzo de 1997. En ella se reconoce la plena validez jurídica de los documentos electrónicos. Posteriormente se expide el Reglamento de Actos, documentos y contratos en forma electrónica aprobado el 5 de agosto de 1997, por el Consejo de Ministros. En él se establecen los principios generales de lo que debe entenderse por *documento electrónico*, llegando a las siguientes definiciones por representación informática de actos hechos o datos jurídicamente relevante, por *firma digital*, el resultado del proceso informático basado en un sistema de claves o llaves asimétricas pública y privada.

El artículo 5 del antes mencionado Reglamento establece que el documento informático firmado con firmas digitales, tiene eficacia de documento privado¹⁷⁹. Mientras que en el artículo 10.2, se "equipara a la firma digital sobre un documento informático a la firma escrita en soporte papel; y el art. 11.1 establece que los contratos realizados por medios telemáticos o informáticos mediante el uso de firma digital según las disposiciones del reglamento serán válidos y eficaces para los efectos legales"¹⁸⁰.

El notario juega un papel importante en la autenticación de la firma electrónica, siendo reconocido por el Reglamento en el artículo 16, en el que define que la *autenticidad de la firma* consistirá en la declaración por parte del

¹⁷⁹ <http://www.injef.com/php/index.php?option=content&task=view&id=414&Itemid=35>

¹⁸⁰ http://www.informatica-juridica.com/trabajos/firma_digital.asp

oficial público de que la firma digital ha sido puesta en su presencia por el titular, previo el aseguramiento de su identidad personal, de la validez de la llave pública y del hecho de que el documento firmado responde a la voluntad de la parte, no siendo contraria al ordenamiento jurídico"¹⁸¹.

Esta ley y su reglamento repercutieron en otros ámbitos, resultado de lo cual se publicaron una serie de leyes y decretos paralelos. Entre los que están: La ley general de reforma de los servicios públicos y simplificación administrativa promulgada; Principio de reconocimiento legal de los documentos digitales; el decreto de creación de archivo y transmisión de documentos y contratos digitales; el decreto regulador de productos y servicios; y el decreto sobre las obligaciones fiscales derivadas de los documentos digitales.

En últimas fechas Italia publico las reglas técnicas sobre firmas digitales (15 de abril de 1999) y la Ley sobre firma electrónica el 23 de enero del 2002.

2.4.11.9. Luxemburgo

Desde el 1º de Junio del 2001 cuenta con un reglamento relativo a la firma electrónica, a los pagos electrónicos y a la creación de un comité de comercio electrónico. También existe un proyecto de reglamento sobre la determinación de un sistema de acreditación de los organismos de certificación y de inspección, así como de los laboratorios de prueba y de patrones a través de la creación de la oficina luxemburguesa de acreditación y vigilancia, de un comité de acreditación y de una selección nacional de auditores de tecnologías y calidad.

2.4.11.10. Portugal

Tiene su Decree –Law 290 – D/99.

2.4.11.11. Reino Unido

La firma no alcanza en common law el nivel de solemnidad con el que cuenta en los sistemas de derecho romanistas.

“Es por ello que, el único impacto realmente apreciable de las Electronic Signatures Regulations en el Reino Unido ha sido el producido por el reconocimiento mutuo de certificados válidos a través del mercado interno... Por otra parte, el Reino Unido comenzó aprobando la Electronic Communications Act en el año 2000 y las Electronic Signatures Regulations, en transposición de la "Directiva de Firma Electrónica"¹⁸².

¹⁸¹ <http://www.injef.com/php/index.php?option=content&task=view&id=414&Itemid=35>

¹⁸² <http://www.alfa-redi.org/revista/data/53-7.asp>

2.4.11.12. Suecia

Se "organizó una audiencia pública sobre la firma digital en 1997"¹⁸³ Así como la "Qualified Electronic Signatures Act (FSF 2000-832)"¹⁸⁴

2.4.12. Otros países

2.4.12.1. Australia

Se encuentran desarrollando el Proyecto "Gatekeeper"; una estrategia para la creación de una infraestructura de firma digital que asegure la integridad y autenticidad de las transacciones efectuadas en el ámbito gubernamental y en su relación con el sector privado. Así también se prevé la creación de una autoridad pública que administre dicha infraestructura y acredite a los certificadores de clave pública.

2.4.12.2. Japón

El primero de abril del 2001 Japón promulgó su Ley sobre Firma Electrónica y Servicios de Certificación.

2.4.12.3. Malasia

Actualmente dicho país cuenta con una ley de firma digital, en la que se otorga efecto legal al uso de ésta; y regula el licenciamiento de los certificadores de clave pública. Así como un proyecto piloto de desarrollo de infraestructura de firma digital.

2.4.13. Organismos Internacionales

2.4.13.1. Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNDUMI)

La Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI o UNCITRAL, por sus siglas en inglés) es un órgano subsidiario de la Asamblea General de las Naciones Unidas. Establecido en 1966 con el objetivo de promover la unificación y armonización progresiva del derecho mercantil internacional. Con este objetivo siempre presente, se han desarrollado diversos instrumentos de derecho sustantivo, aplicables a las transacciones

¹⁸³ http://www.informatica-juridica.com/trabajos/firma_digital.asp

¹⁸⁴ <http://www.cem.itesm.mx/dacs/publicaciones/logos/libros/libros/firma.pdf>.

comerciales, y otros aspectos de derecho mercantil de interés para el comercio internacional.

La CNUDMI cuenta con sedes en Viena y Nueva York. Los estados miembros son escogidos entre: representación de diversas regiones geográficas, estados observadores, organizaciones intergubernamentales y organizaciones no gubernamentales de carácter internacional interesadas en la labor de la comisión. Actualmente se compone de 36 países. Nueve miembros son estados de África, seis de América Latina y el Caribe, siete son estados de Asia y catorce de Europa Occidental y Oriental.

Algunos de los textos elaborados y preparados por la CNUDMI son: la Convención sobre la prescripción en materia de compraventa internacional de mercaderías, 1974. 17 estados partes; La Convención sobre el Transporte Marítimo de mercancías, Hamburgo, 1978. 28 estados partes. La Convención de las Naciones Unidas sobre los Contratos de compraventa Internacional de Mercaderías, Viena, 1980. 62 estados partes. La Convención de las Naciones Unidas sobre letras de cambio internacionales y pagarés internacionales. Nueva York, 1988. 3 firmas, 3 ratificaciones y adhesiones. La Convención sobre el Reconocimiento y la ejecución de las Sentencias Arbitrales Extranjeras. Nueva York, 1958. 132 estados partes. Entre otras, leyes modelo Ley modelo sobre arbitraje comercial internacional, 1985; Sobre transferencias internacionales de crédito, 1992; sobre contratación pública de bienes, obras y servicios, 1994; sobre comercio electrónico, 1996; sobre insolvencia transfronteriza, 1997, guías jurídicas, guías legislativas, reglamentos y notas sobre determinadas prácticas.

Pero las que son de vital importancia son para el presente estudio son la Ley Modelo de Comercio Electrónico y la Ley Modelo de firma electrónica, de las que a continuación hablaremos con mayor profundidad.

Para el 24° periodo de sesiones de la CNUDMI (1991) se encargo al Grupo de Trabajo sobre Pagos Internacionales, un estudio sobre los problemas jurídicos del Intercambio electrónico de datos. El informe elaborado por dicho grupo fue elevado al rango de comisión, que posteriormente recibiría el nombre de Grupo de Trabajo sobre Intercambio Electrónico de Datos.

Para el siguiente periodo de sesiones (1992), la CNUDMI, tras examinar el informe del Grupo de Trabajo sobre Pagos Internacionales; encomendó al Grupo de Trabajo sobre Intercambio Electrónico de Datos la elaboración de una reglamentación jurídica del Intercambio Electrónico de Datos; hecho al que se abocaron, dando como resultado que el 14 de Junio de 1996 en su 29° periodo de sesiones celebrado en Nueva York, el Plenario de la CNUDMI "examinó y probó el proyecto de Ley Modelo sobre aspectos jurídicos de EDI bajo la denominación de Ley Modelo sobre el comercio electrónico. (Resolución General de la Asamblea 51/162 de 16 de diciembre de 1996)"¹⁸⁵.

¹⁸⁵ Reyes Krafft, Alfredo Alejandro. *Ob. cit.* p.161

La ley de comercio electrónico se divide en dos partes: en la primera se abordan los aspectos generales del comercio electrónico y en la segunda se aplica el comercio electrónico al transporte de mercancías específicamente. Se basa en el establecimiento del equivalente funcional de conceptos como: escrito, firma y original.

El Grupo de Trabajo sobre Intercambio Electrónico de Datos, sería rebautizado como Grupo de Trabajo sobre Comercio Electrónico; con esta nueva denominación la Comisión se abocó al estudio de las cuestiones jurídicas relativas a las firmas digitales y las autoridades de certificación. Más adelante y como resultado de un estudio encargado a la Secretaría del Grupo de Trabajo, se redactó el documento A/CN.9/WG.IV/WP.71 del 31 de diciembre de 1996. La Comisión en su 30º periodo de sesiones, celebrado en Viena del 12 al 30 de Mayo de 1997; hizo suyas las conclusiones a las que había llegado el grupo de trabajo sobre comercio electrónico, y en su 31º periodo de sesiones (celebrado en Nueva York del 18 al 28 de febrero de 1997) con respecto a la viabilidad y conveniencia de preparar un régimen uniforme sobre las cuestiones jurídicas relativas a las firmas digitales y las entidades certificadoras, y posiblemente sobre cuestiones conexas. La Comisión en su 32º periodo de sesiones (enero de 1998) encomendó al grupo de trabajo la preparación de un régimen uniforme para las firmas electrónicas sobre la base de una nota preparada por la secretaria.

Producto de lo cual, el 5 de julio de 2001 se adoptó la ley modelo de la Comisión de Naciones Unidas para el Derecho Mercantil Internacional sobre Firma Electrónica; que define los conceptos de mensaje de datos, firma electrónica, certificado digital, prestador de servicios de certificación, firmante, parte que confía. En la ley se da igual tratamiento a las diferentes tecnologías (principio de neutralidad tecnológica), establece los requisitos de firma, los actos requeridos del firmante y del prestador de servicios de certificación, así como de la fiabilidad de los recursos, el proceder de la parte que confía en el certificado y el reconocimiento de certificados extranjeros y de firmas electrónicas extranjeras.

La ley da una serie de definiciones: Se le llama 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 el firmante aprueba la información contenida en el mensaje de datos". Para que dicha firma sea considerada fiable, debe cumplir ciertos requisitos: a) los datos de creación corresponden exclusivamente al firmante, b) los datos de creación de la firma estaban en el momento bajo el control exclusivo del firmante, c) es posible detectar cualquier alteración de la firma hecha después del momento de la firma y si la firma da seguridad de la integridad de la información a que corresponde, y d) es posible detectar cualquier alteración hecha a la información luego de la firma. Sin perjuicio que cualquier persona demuestre de otra manera la fiabilidad de la firma electrónica o aduzca pruebas de no fiabilidad de una firma.

Algunos de los deberes que el firmante debe de cumplir de acuerdo con lo expuesto en la ley son: actuar con diligencia razonable para evitar la utilización no autorizada de los datos de creación de la firma; utilizar los medios que proporcione el prestador de los medios de certificación, y dar aviso a cualquier persona que pueda considerar la firma fiable, si el firmante sabe que los datos de creación de la firma han quedado en entredicho o si las circunstancias de que tiene conocimiento el firmante muestran un riesgo considerable que los datos de creación de la firma hayan quedado en entredicho. Deberá igualmente cerciorarse que todas las declaraciones que haya hecho en relación con el ciclo vital del certificado sean exactas y cabales.

La ley también habla de algunas obligaciones para los prestadores de servicios de certificación, como son: el actuar de conformidad con las normas y prácticas que imponga, con la diligencia razonable para cerciorarse que todas las declaraciones que haya hecho en relación con el ciclo vital del certificado o que estén consignadas en él son exactas y cabales, proporcionar a la parte que confía en el certificado los medios para identificar mediante el certificado la identidad del prestador de servicios de certificación, el método utilizado para comprobar la identidad del firmante, si los datos de creación de la firma son válidos y no están en entredicho, entre otros; deberá, de otro lado utilizar al prestar sus servicios, sistemas, procedimientos y recursos humanos fiables. Estarán a cargo del prestador de servicios de certificación las consecuencias jurídicas que entrañe el hecho de no haber cumplido los deberes.

2.4.13.2. Organización para la Cooperación y Desarrollo Económico (OCD)

El 27 de marzo de 1997, la Organización para la Cooperación y el Desarrollo Económico publicó su recomendación para el establecimiento de políticas sobre Criptografía, (Guidelines for Cryptography Policy) "sin embargo solo establece una serie de lineamientos que se sugiere a los gobiernos adoptar al momento de legislar en materia de firma digital y Entidades Prestadoras de Servicios de Certificación"¹⁸⁶.

2.4.13.3. Organización Internacional de Normas (ISO)

La International Standards Organization (ISO) o Organización Internacional de Normas, tiene la norma ISO/IEC 7498 – 2 (Arquitectura de Seguridad de OSI) en la que se basan "todos los desarrollos normativos posteriores, regula los servicios de seguridad sobre confidencialidad, integridad, autenticidad, control de accesos y no repudio. A través de su subcomité 27, SC 27, trabaja en una norma de firma digital"¹⁸⁷.

¹⁸⁶ <http://www.cem.itesm.mx/dacs/publicaciones/logos/libros/libros/firma.pdf>

¹⁸⁷ http://www.informatica-juridica.com/trabajos/firma_digital.asp

2.5. Aplicaciones mercantiles de la firma electrónica avanzada

En el capítulo primero, al hablar de comercio electrónico, concluimos que éste era según lo expresado por la organización mundial de comercio: la producción, distribución, comercialización, venta y entrega de bienes y servicios por medios electrónicos. Asimismo, aclaramos que e-commerce era la denominación en inglés para comercio electrónico, es decir lo mismo.

Posteriormente, al hablar de las diferentes clasificaciones de comercio electrónico, mencionamos una que se basa en la forma de relacionarse entre los agentes que actúan en los actos de comercio electrónico (empresas, consumidores y administradores); cuyas combinaciones hacen surgir diversas formulas como son: Entre empresas o B2B (Business to Business); entre empresa y consumidor o B2C (Business to Consumers); entre empresa y la Administración o B2A (Business to Administration)¹⁸⁸; entre consumidor y consumidor o C2C (Consumers to Consumers); entre consumidor y administrador o C2A (Consumers to Administration)

Revisado lo anterior, es pertinente mencionar; que antes de concluir el presente capítulo debemos aclarar que la firma electrónica avanzada, los certificados digitales, y toda esa serie de tecnologías de seguridad en las transacciones comerciales electrónicas; están enfocadas a la modalidad comercial B2B o Business to Business. Es decir a la interrelación que se da entre las empresas que generalmente hacen uso de los medios electrónicos para realizar actividades tales como la recepción de facturas, hacer ordenes de compra a sus proveedores, efectuar pagos, etc. O en todo caso a la modalidad B2A o Business to Administration; que aborda a las transacciones entre empresas y el gobierno (administración pública). Por medio de las cuales las empresas pueden realizar operaciones como el pago de impuestos, presentar declaraciones fiscales, etc. Pero que a fin de cuentas se enfocan a las empresas; tan solo en nuestro país "B2B representa cerca del 78% de las transacciones electrónicas que se hacen"¹⁸⁹

Esto debido a que las tecnologías, elementos materiales y jurídicos, utilizados para el desarrollo de dichos mecanismo; resultan muy costosos y complicados. Por lo que su uso se reserva a grandes transacciones comerciales (como las que se dan entre las empresas). Dichas tecnologías de seguridad empresarial y otros mecanismos electrónicos empleados por las empresas para su mejor desarrollo reciben el nombre de E-business (o e - negocio en español); que es definido como "toda la organización del negocio, vista desde el punto de aplicación de las nuevas tecnologías de la informática"¹⁹⁰. Implica la integración de varias tecnologías como Intranet, Extranet, comercio electrónico, administración de la relación con los clientes (customer relationship management o CRM),

¹⁸⁸ Téllez Valdés, Julio, *Ob. cit.* p. 189

¹⁸⁹ http://www.amece.org.mx/motor/contenidos/htmls/105_13_12_02.php?acceso

¹⁹⁰ Patroni Vizquerra, Ursula. *Apuntes de Derecho Electrónico.*

http://v2.vlex.com/es/ppv/doctrina/resultados.asp?query_doc=178122&n_orden=0&

servicio al cliente, centros de ayuda, entre otras actividades que proporcionan valor real a las organizaciones¹⁹¹. El e- business depende en gran medida de la seguridad y la confianza.

Para los particulares o consumidores finales existen otro tipo de mecanismos de protección como los Números de identificación personal o NIP bancarios ("claves de cuatro dígitos numéricos para utilizarlos en los cajeros automáticos, como medio de identificación conjuntamente con el uso de tarjetas de crédito o débito"¹⁹²), las tarjetas plásticas con chips, etc. Que quizás no son tan seguros como la firma electrónica, los certificados digitales y otras figuras de seguridad digital; pero son suficientemente seguras para las pequeñas transacciones comerciales.

¹⁹¹ http://www.ebconsultores.com.mx/sol_ebusiness.htm

¹⁹² Acosta Romero, Miguel. *Ob cit.* p. 576

CAPÍTULO TERCERO. FE PÚBLICA Y CERTIFICACIÓN

En el presente capítulo hablaremos sobre Fe Pública y Certificación; dos concepciones que deben de ser cabalmente comprendidas para que la naturaleza de la entidad certificadora pueda ser desentrañada. Definiremos ambos conceptos y posteriormente haremos un cotejo de figuras, con el fin de que el lector comprenda porqué un prestador de servicios puede otorgar certificados; pero como el mismo Código Civil Vigente señala en su artículo 100 "...la facultad de expedir Certificados no conlleva fe pública...". Todo ello para demostrar que a pesar de la carencia de fe pública, un prestador de servicios de certificación puede ayudar a crear mayor certidumbre en las transacciones mercantiles electrónicas.

3.1. Fe Pública

3.1.1. Aspecto filosófico

De acuerdo con algunos autores la fe es una "virtud teologal que nos hace creer lo que Dios dice y la Iglesia proponen"¹⁹³. Este concepto es seguido por la mayoría de las definiciones; todas ellas se enfocan a ver la fe como aspectos divinos y teológicos; es un "creer en algo, en alguien, es voluntario, es decir, un acto de adhesión libre e individual"¹⁹⁴. La fe divina tiene un aspecto objetivo y subjetivo. Objetivamente es "un conjunto de verdades reveladas por Dios"¹⁹⁵ y Subjetivamente es "un acto de fe"¹⁹⁶.

Sobre este acto de fe, San Agustín opina: "A la fe nadie puede ser obligado"¹⁹⁷; punto de vista apoyado por Schopenhauer que piensa "la fe, como el amor, no puede ser forzada"¹⁹⁸. Aunque hay autores más modernos con opiniones distintas, como Miguel de Unamuno que al respecto señala: "No creemos si no lo que esperamos, ni esperamos si no lo que creemos"¹⁹⁹.

Los filósofos también tienen su visión al respecto de la fe. Partiendo del punto de vista ontológico la conceptúan como: "un proceso intelectual, que puede ser en relación con: a) el hombre aislado, que se refiere a la convicción de cada individuo (cada quien tiene su fe muy particular); b) el hombre en la colectividad, se refiere a que cada individuo debe considerar algunos hechos o actos específicos que no presenció ni percibió con sus sentidos, procurándole un estado

¹⁹³ Raluy Poudevida, Antonio. *Ob. cit.* Fe

¹⁹⁴ Ríos Hellig, Jorge. *La práctica del Derecho Notarial*. 3ª ed. Mc. Graw-Hill, México, 1998. p. 45

¹⁹⁵ Carral y de Teresa, Luis. *Derecho Notarial y Derecho Registral*. 15ª ed. Porrúa, México, 1998. p. 51

¹⁹⁶ *Ibidem*

¹⁹⁷ http://www.eped.edu.mx/revista/INTRODUCCION__AL__DERECHO__NOTARIAL__PARTE__UNO.htm

¹⁹⁸ Carral y de Teresa, Luis. *Ob. cit.* p. 51

¹⁹⁹ *Diccionario Enciclopédico Saber 3*. Tomo 2. Fernández Editores. México, 1990. Fe

de certidumbre alejado de la duda o el error²⁰⁰. De esta última (la fe colectiva) es de donde podemos partir para tratar de entender que es la fe pública.

Con el paso del tiempo el crecimiento de los grupos humanos, llevó aparejado un desarrollo en tamaño y complejidad de las comunidades; lo que provocó que sus miembros se vieran imposibilitados de presenciar los actos jurídicos de otros conciudadanos; por lo que se tuvo que crear un sistema que obligara a la colectividad a tener como ciertas algunas afirmaciones; surgiendo así la fe pública como un medio para hacer que los actos celebrados por algunos debieran ser tomados como verdaderos por otros de manera obligatoria.

El sistema de fe pública se basaría en el "invertir a una persona de una función autenticadora, de modo que al expedir un documento, pudiera decirse que estaba presente el Estado mismo"²⁰¹

3.1.2. Concepto Fe Pública

Conforme a lo expresado por el artículo 44 de la Ley de la Comisión Estatal de Derechos Humanos de Jalisco debemos entender por Fe Pública a *"...la facultad de autenticar documentos preexistentes o declaraciones y hechos que tengan lugar o estén aconteciendo en presencia de dichos servidores públicos, sin perjuicio del valor probatorio que se les atribuya, en los términos de este ordenamiento y otras leyes aplicables. Las declaraciones y hechos a que se refiere el párrafo anterior, se harán constar en el acta circunstanciada que al efecto levantará el servidor público correspondiente"*.

Mientras que algunas definiciones doctrinales la ven como: "una presunción legal de verdad; un imperativo jurídico o verdad oficial impuesta por el Estado, vigente mientras no se pruebe su falsedad; la seguridad otorgada por el Estado para afirmar que un acto o hecho es verdadero; el imperativo jurídico o coacción que nos obliga a tener por válidos determinados hechos o acontecimientos sin decir originalmente sobre su verdad objetiva; o más ampliamente como un imperativo jurídico que impone el Estado a un pasivo contingente universal para considerar cierta y verdadera la celebración de un acto o el acaecer de un evento que no percibe este contingente por sus sentidos; también es el contenido del instrumento que lo contiene."²⁰²

Sea cual sea la definición que adoptemos para fe pública, debemos tener presentes varios aspectos: 1. la fe pública siempre debe constar en forma documental; 2. Proviene del Estado con el fin de otorgar seguridad jurídica a sus componentes; 3. Es un imperativo jurídico, por lo que debe ser tenido obligatoriamente como cierto por la colectividad; y 4. Es oponible ante cualquiera

²⁰⁰ Ríos Hellig, Jorge. *Ob. cit.* p.45

²⁰¹ Carral y de Teresa, Luis. *Ob. cit.* p. 52

²⁰² Cfr. Ríos Hellig, Jorge. *Ob. cit.* p.46

(erga omnes). Por lo que cualquier definición de fe pública que observe estos cuatro aspectos será válida para nosotros.

3.1.3. Requisitos de Fe pública

Para que exista la fe pública es necesario que cumpla los requisitos de Evidencia, Objetivación y Coetaneidad o Simultaneidad.

3.1.3.1. Evidencia

Se llama así a la "relación entre *el quien y el ante quien*, el notario {o la persona investida de fe pública} narra el hecho propio (certificación) y constata el hecho ajeno"²⁰³. En este requisito la importancia se ubica en el autor de la fe pública, y no en el documento o en el destinatario (de los que se ocupan otros requisitos). Del autor se requiere que sea una persona pública, y que vea el hecho ajeno o que narre el propio.

De dicho autor "no se precisa acto de fe, sino de conocimiento directo. Se trata del autor, de quien dimana el acto de fe pura al destinatario. El autor jamás produce un acto de fe, pues para él el hecho o el acto es evidente. El acto de fe se requiere para todos los demás entre los que debe surtir efectos ese acto, o sea, para los destinatarios del documento"²⁰⁴.

3.1.3.2. Objetivación

En el requisito de evidencia la importancia radicaba en el autor (la persona investida de fe pública); mientras que en este otro el punto medular es el documento donde se hace constar la fe pública. Este requisito exige que "todo lo percibido debe plasmarse en un instrumento, es decir, todo lo que el notario {o persona investida de fe pública} percibe de manera sensorial o por el dicho de otros, debe constar por escrito dentro de un protocolo"²⁰⁵

El documento es de suma importancia, ya que da al hecho un soporte material, evitando con esto que desaparezca con el paso del tiempo (ya que la memoria del autor puede llegar a fallar) "Emancipándolo" de alguna forma de su autor, al producirse una fe escrita "que está previamente valorada por la ley y que se subsiste íntegra, como hecho o documento auténtico, y como tal tiene que ser estimada por el juez"²⁰⁶. Previendo además que la fe pública sea objeto de requisitos exigibles a actos subjetivos (como el testimonio) como son: la fidelidad, lealtad, desinterés, percepción retenida (memoria), pasión, etc.

²⁰³ Ríos Hellig, Jorge. *Ob. cit.*, p. 49

²⁰⁴ http://www.eped.edu.mx/revista/INTRODUCCION_AL_DERECHO_NOTARIAL_PARTE_UNO.htm

²⁰⁵ Ríos Hellig, Jorge. *Ob. cit.*, p. 50

²⁰⁶ Carral y de Teresa, Luis. *Ob. cit.* p. 55

3.1.3.3. Coetaneidad o simultaneidad

Hace referencia a que los dos requisitos anteriores (objetivación y evidencia) deben darse al mismo tiempo; es decir, en un solo acto. "Es una relación temporal entre lo narrado por terceros, lo percibido por éstos o el notario (o la persona investida de fe pública) y su plasmación u otorgamiento en el instrumento notarial (o documento material)"²⁰⁷.

Pero esta coetaneidad debe darse bajo ciertas normas de forma (dirigidas al autor), obligatorias para el fedatario público y previstas por la ley. Con el fin de que el acto celebrado pueda surtir plenos efectos en el futuro, con lo que se garantiza su futuro valor probatorio. O mejor dicho "el valor de la prueba se alcanza por las garantías de su forma, esto es, por las garantías que acompañan a las fases de evidencia, objetivación y coetaneidad"²⁰⁸.

3.1.4. Notas o accidentes de la Fe Pública

Se denomina de esta manera a las "situaciones que tienden a determinar la identidad entre el hecho o acto y lo narrado"²⁰⁹.

3.1.4.1. Exactitud

La exactitud versa sobre la fidelidad que debe de existir entre lo puntualizado en el documento donde consta la fe pública y el hecho o acto que ahí se narra. "Es la identidad entre "actum" y "dictum", es la verdad del espejo, de la fotografía: la imagen en su actualidad"²¹⁰.

Entre los efectos jurídicos que la exactitud de la fe pública acarrea, está la eficacia "erga omnes"; aunque el documento donde conste la fe pública, puede presumiblemente no ser conocido por todos, pero para aquel tercero que llegará a conocerlo será plenamente válido, por lo que no podrá negarle valor probatorio (aunque no puede obligar a terceros como otros artículos).

3.1.4.1.1. Natural

Es la relación de exactitud entre el documento y el hecho; pero enfocándose a referencias espaciales, es decir, al tiempo y lugar. Es decir se

²⁰⁷ Ríos Hellig, Jorge. *Ob.cit.* p. 50

²⁰⁸ http://www.eped.edu.mx/revista/INTRODUCCION__AL_DERECHO_NOTARIAL_PARTE_UNO.htm

²⁰⁹ Ríos Hellig, Jorge. *Ob.cit.* p. 53

²¹⁰ Carral y de Teresa, Luis. *Ob.cit.* p. 56

narra completamente el hecho, pero dentro de determinados límites de tiempo: tiempo de presencia funcionalista o unidad de acto formal.

3.1.4.1.2. Funcional

Este punto hace referencia a que el hecho relatado en el documento debe concretarse "a lo que del hecho interesa a un asunto (unidad negocial) o la ley (circunstancias de un acto o de una inscripción)"²¹¹. Es decir, se debe relatar en el documento únicamente lo sobresaliente del hecho o acto; así como evitar a toda costa formas anticuadas o inútiles.

3.1.4.2. Integridad

Se refiere al "acto de materializar o estatizar el acto o hecho para el futuro"²¹² en un documento. Es la búsqueda de la exactitud proyectada hacia el futuro.

3.1.5. Tipos de Fe Pública

3.1.5.1. Originaria

Se le denomina originaria a la fe que es "captada directa y coetáneamente por la vista y el oído del funcionario 'de viso et auditu suis sensibus'"²¹³. Es decir, cuando el hecho o acto al que dará fe fue captado por el fedatario de forma sensorial (a través de sus sentidos) de forma directa e inmediata.

3.1.5.2. Derivada

Al tiempo que hablamos de fe derivada cuando el hecho objeto de la fe; no es una cosa, hecho o persona que el fedatario capte sensorialmente. Si no un documento o hecho de un tercero, preexistente.

3.1.6. Clases de Fe Pública

Antes de comenzar a hablar de la clasificación que se hace de la fe pública; debemos dejar claro, que "la fe pública es única, y el Estado la ejerce por sí mismo o la delega a servidores públicos o a particulares"²¹⁴. Si es que se llega a agruparse a ésta en categorías es con meros fines didácticos. Aclarado este

²¹¹http://www.eped.edu.mx/revista/INTRODUCCION_AL_DERECHO_NOTARIAL_PARTE_UNO.htm

²¹² Ríos Hellig, Jorge. *Ob cit.*, p. 53

²¹³ Carral y de Teresa, Luis. *Ob cit.*, p. 58

²¹⁴ Ríos Hellig, Jorge. *Ob cit.*, p. 58

punto, podemos proseguir con nuestro estudio de las diversas clasificaciones que se hacen de la fe pública.

3.1.6.1. Notarial

Llamamos Fe Pública notarial a aquella que es dada por los notarios. La ley del Notariado para el Distrito Federal Vigente, en su artículo 42 nos dice del Notario: **Artículo 42.** *Notario es el profesional del Derecho investido de fe pública por el Estado, y que tiene a su cargo recibir, interpretar, redactar y dar forma legal a la Voluntad de las personas que ante él acuden, y conferir autenticidad y certeza jurídicas a los actos y hechos pasados ante su fe, mediante la consignación de los mismos en instrumentos públicos de su autoría. El notario conserva los instrumentos en el protocolo a su cargo, los reproduce y da fe de ellos. Actúa también como auxiliar de la administración de justicia, como consejero, árbitro o asesor internacional, en los términos que señalen las disposiciones legales relativas.*

El notario es la persona investida de fe pública con la más extensa gama de facultades, ya que sus actuaciones son empleadas en la mayoría de las materias jurídicas; aunque su función de fedatario público también tiene algunas limitaciones conforme al artículo 45 de la citada Ley de Notariado para el Distrito Federal Vigente²¹⁵.

Es indudable el valor probatorio de los testimonios notariales, ya que "El derecho notarial satisface la necesidad general de toda prueba, ya que el notario actúa en el mismo instante en que se produce el hecho; en cambio, en los sistemas de prueba en general el hecho se comprueba generalmente después de que ocurrió"²¹⁶. El notario es el fedatario público por excelencia, pero existen otros de los que hablaremos en los siguientes apartados.

3.1.6.2. Judicial

Este tipo de fe pública está contenida en los documentos judiciales, los funcionarios competentes para dar fe en un proceso judicial serán de los secretarios de los juzgados (más no los jueces) ya que dan fe de los actos decretados por el juez, realizando diligencias, o expidiendo copias certificadas.

²¹⁵ Artículo 45. Queda prohibido a los notarios:

- I. Actuar con parcialidad(...)
- II. Dar fe de actos que dentro de los procedimientos legales respectivos corresponda en exclusiva hacerlo a algún servidor público(...)
- III. Actuar como notario en instrumentos o asuntos en que tengan interés, disposición a favor(...)
- IV. Actuar como notario sin rogación de parte(...)

²¹⁶ <http://www.prodigyweb.net.mx/bieleto/conclusiones.htm>

Esto conforme a los artículos 58 y 61 de la Ley Orgánica del Tribunal Superior de Justicia del Distrito Federal²¹⁷.

A decir de algunos autores "el Ministerio Público, ya sea local o federal, también tiene fe pública (ministerial) en relación a las diligencias en que debe intervenir"²¹⁸. Esto debido a las actas levantadas por ellos en desempeño de sus funciones; actuaciones de las que encontramos sustento legal en los artículos 124 del Código Federal de Procedimientos Penales y 265 del Código de Procedimientos Penales para el Distrito Federal²¹⁹.

3.1.6.3. Mercantil

Este tipo de fe pública está depositada en los corredores públicos, que pueden, ya bien, ser intermediarios en los actos de comercio; o bien, actuar como fedatarios imparciales en actos y hechos mercantiles. La función de correduría pública está regulada por la Ley Federal de Correduría Pública Vigente (Artículos 6 y 18²²⁰), donde se habla de las funciones del corredor público y de la póliza (instrumento donde hace constar sus actuaciones como fedatario).

²¹⁷ **Artículo 58.** - Son obligaciones de los Secretarios de Acuerdos:(...)

III. Autorizar los despachos, exhortos, actas, diligencias, autos y toda clase de resoluciones que se expidan, asienten, practiquen o dicten por el Juez;

IV. Asentar en los expedientes las certificaciones que procedan conforme a la ley o que el Juez ordene;

VI. Expedir las copias autorizadas que la ley determine o deban darse a las partes en virtud de decreto judicial;

Artículo 61. - Los Secretarios Actuarios estarán adscritos a cada Juzgado y tendrán las obligaciones siguientes:(...)

III. Hacer las notificaciones y practicar las diligencias decretadas por los Jueces, bajo la responsabilidad de la fe pública que les corresponda y dentro de las horas hábiles del día, entendiéndose por éstas las que median desde las siete hasta las diecinueve horas, devolviendo los expedientes dentro de las veinticuatro horas siguientes, previas las anotaciones en el libro respectivo, y

IV. En caso de existir imposibilidad para practicar las diligencias ordenadas, deberá asentar razón de ello y devolver las actuaciones dentro de las veinticuatro horas siguientes.

El Secretario Auxiliar Actuario de Sala tendrá las mismas obligaciones referidas en las fracciones anteriores.

²¹⁸ Ríos Hellig, Jorge. *Op.cit.*, p. 59

²¹⁹ **Artículo 265.** Al iniciar sus procedimientos, el Ministerio Público o la policía judicial, se trasladarán inmediatamente al lugar de los hechos, para dar fe de las personas y de las cosas a quienes hubiere afectado el acto delictuoso y tomarán los datos de las que lo hayan presenciado, procurando que declaren, si es posible, en el mismo lugar de los hechos, y citándolas, en caso contrario, para que dentro del término de veinticuatro horas comparezcan a rendir su declaración.

Artículo 124. En el caso del artículo anterior, se procederá a levantar el acta correspondiente, que contendrá: la hora, fecha y modo en que se tenga conocimiento de los hechos(...);

²²⁰ **Artículo 6.** Al corredor público corresponde:(...)

V.- Actuar como fedatario público para hacer constar los contratos, convenios, actos y hechos de naturaleza mercantil, excepto en tratándose de inmuebles; así como en la emisión de obligaciones y otros títulos valor; en hipotecas sobre buques, navíos y aeronaves que se celebren ante él, y en el otorgamiento de créditos refaccionarios o de habilitación o avío, de acuerdo con la ley de la materia;

VI.- Actuar como fedatarios en la constitución, modificación, fusión, escisión, disolución, liquidación y extinción de sociedades mercantiles y en los demás actos previstos en la Ley General de Sociedades Mercantiles; y

3.1.6.4. Registral

"La fe notarial se apoya en la publicidad de los actos por medio del Registro Público de la Propiedad y otros registro."²²¹; por lo que se deposita la llamada Fe Pública Registral en los directores de los registros (locales o federales). Esto conforma al artículo 6° del Reglamento del Registro Público de la Propiedad para el Distrito Federal²²².

3.1.6.5. Consular

Esta fe pública está depositada en los cónsules (no así los embajadores), que realizan funciones notariales en actos que pudieran llegar a tener efecto en nuestro país; como son: testamentos, otorgar poderes, legalización de firmas en documentos públicos, etc. Esto conforme a lo establecido en el artículo 44 de la Ley del Servicio Exterior Mexicano²²³.

El Reglamento de la Ley del Servicio Exterior Mexicano, es más específico acerca de las funciones consulares, sobre ella habla en varios de sus artículos (78, 80, 82 – 86)²²⁴. El procedimiento de legalización de que habla el artículo 86²²⁵,

Artículo 18. Póliza es el instrumento redactado por el corredor para hacer constar en él un acto, convenio o contrato mercantil en el que este autorizado a intervenir como funcionario revestido de fe pública. Acta es la relación escrita de un hecho jurídico en la que el corredor intervino con fe pública y que contendrá las circunstancias relativas al mismo. Las actas y pólizas autorizadas por los corredores son instrumentos públicos y los asientos de su libro de registro y las copias certificadas que expida de las pólizas, actas y asientos son documentos que hacen prueba plena de los contratos, actos o hechos respectivos. El corredor podrá expedir copias certificadas para hacer constar las actas o pólizas en que haya intervenido, siempre que obren en su archivo y que aparezcan debidamente registradas en el libro correspondiente

²²¹ <http://www.prodigyweb.net.mx/bieletto/conclusiones.htm>

²²² **Artículo 6°.** Corresponde al Departamento, por conducto del Director General:(...)

I Ser depositario de la fe pública registral para cuyo pleno ejercicio se auxiliará de los registradores y demás servidores públicos de la institución;

²²³ **Artículo 44.-** Corresponde a los jefes de oficinas consulares:(...)

III. Ejercer, cuando corresponda, funciones de Juez del Registro Civil;

IV. Ejercer funciones notariales en los actos y contratos celebrados en el extranjero que deban ser ejecutados en territorio mexicano, en los términos señalados por el Reglamento. Su fe pública será equivalente en toda la República, a la que tienen los actos de los notarios en el Distrito Federal;

Los jefes de oficina consular podrán delegar en funcionarios subalternos el ejercicio de una o varias de las facultades señaladas en el presente artículo, sin perder por ello su ejercicio ni eximirse de la responsabilidad por su ejecución. La delegación se hará en los términos que establezca el Reglamento de la presente Ley.

²²⁴ **Artículo 78.-** Además de las funciones consignadas en el artículo 44 de la Ley, corresponde a los jefes de oficinas consulares:

VI.- Cotejar los documentos públicos o privados que en original tengan a la vista y certificar las copias correspondientes. Para ello llevarán un libro de cotejos en los términos que determine la Secretaría;

Artículo 82.- Las oficinas consulares ejercerán las funciones del registro civil en los términos del Código Civil Federal y autorizarán en el extranjero las actas de registro civil concernientes al nacimiento, matrimonio y defunción de mexicanos y, en su caso, expedirán copias certificadas de las mismas. Los actos del estado civil de mexicanos en el extranjero se asentarán en las formas que proporcione la Secretaría.

Sólo se autorizarán actas de matrimonio cuando los dos contrayentes sean mexicanos.

es sustituido por el apostillamiento, que dimana de la Convención por la que se suprime el requisito de legalización de los documentos públicos extranjeros concluida en la 5 de octubre de 1961, durante la Novena Sesión de la Conferencia de la Haya de Derecho Internacional Privado; aprobada por la Cámara de Senadores del H. Congreso de la Unión, el 19 de diciembre de 1993, según decreto publicado en el Diario Oficial de la Federación el 17 de enero de 1994; y que fue finalmente fue promulgada el 14 de agosto de 1995 en el Diario Oficial de la Federación.

3.1.6.6. Administrativa

Es aquella fe pública, que tiene el Poder Ejecutivo, por medio de sus Secretarías de Estado, concedida (por técnica legislativa) a los oficiales mayores de éstas; se ejerce basados en certificaciones, y está limitada por los actos internos de la Secretaría.

Ejemplo de este tipo de fe pública lo encontramos en la Ley Orgánica de la Administración Pública del Distrito Federal, que establece en algunos de sus artículos:

Artículo 20. A la secretaria de gobierno corresponde primordialmente...

Las copias certificadas de las actas del Registro Civil expedidas por funcionarios consulares tendrán validez en México.

Las actas a que se refiere este artículo serán concentradas en la Oficina Central del Registro Civil en el Distrito Federal, en los términos y condiciones que señalen las disposiciones aplicables.

Artículo 83.- Los funcionarios consulares podrán legalizar firmas en documentos públicos extranjeros expedidos por autoridades residentes en sus respectivas circunscripciones consulares, o en documentos que hubieren sido certificados por fedatarios de su circunscripción.

La legalización consistirá en certificar que las firmas, los sellos o ambos, que consten en un documento expedido en el extranjero, sean los mismos que use en sus actuaciones el funcionario que lo haya autorizado y que dicho funcionario desempeñaba el cargo con el que se ostentó al firmar el documento de que se trate.

Al efecto, las oficinas consulares mantendrán un registro de las firmas y los sellos que usen los funcionarios que actúen en su circunscripción.

Las legalizaciones sólo se harán tratándose de documentos originales o de copias certificadas expedidas por funcionarios o fedatarios autorizados legalmente y se expedirán en la forma especial que proporcione la Secretaría, la cual se adherirá al documento respectivo. En ambos se imprimirá la firma del funcionario y el sello de la oficina que legalice.

Las legalizaciones efectuadas por las oficinas consulares surtirán sus efectos en la República Mexicana sin necesidad de que las firmas de dichos funcionarios requieran a su vez ser legalizadas por la Secretaría.

Artículo 85.- En el ejercicio de funciones notariales, las oficinas consulares podrán dar fe, autenticar y protocolizar contratos de mandato y poderes, testamentos públicos abiertos, actos de repudiación de herencias y autorizaciones que otorguen las personas que ejerzan la patria potestad o la tutela sobre menores o incapaces, siempre y cuando dichos actos jurídicos se celebren dentro de su circunscripción y estén destinados a surtir efectos en México.

²²⁵**Artículo 86.** Las oficinas consulares asentarán y autorizarán las escrituras que se otorguen ante su fe en su protocolo, autorizado previamente por la Secretaría, y elaborado conforme a las disposiciones de la Ley de Notariado para el Distrito Federal.

XV. Certificar en los términos de las leyes y reglamentos respectivos, documentos expedidos por los funcionarios del Distrito Federal en el Desempeño de sus funciones y expedir copias certificadas de los que obren en los archivos de la dependencia;...

Artículo 32. *Corresponde a las delegaciones del Distrito Federal;*

I. Legalizar las firmas de sus subalternos, y certificar y expedir copias y constancias de los documentos que obren en los archivos de la delegación;

3.1.6.7. Marítima

La fe pública marítima está depositada en el capitán del buque para ciertos casos especiales, esto conforme al artículo 25²²⁶ de la Ley de Navegación y otros relativos del Código Civil para el Distrito Federal (146 y 1583 a 1592)²²⁷.

3.1.6.8. Registro Civil

La fe pública también está depositada en los Jueces del Registro Civil, para los actos referentes al estado civil de las personas; esto conforme al artículo 35²²⁸ del Código Civil para el Distrito Federal.

3.1.6.9. Agraria

Sobre la fe pública en materia agraria, podemos decir que en varios artículos de la Ley Agraria se otorgan funciones de certificación (es decir, fe pública) a ciertas autoridades; así como también, el Reglamento Interno del Registro Agrario Nacional, puntualiza lo que se considera como fedatario para fines agrarios. Estamos hablando de los artículos 28, 58, 68, 80 y 114²²⁹ de la Ley Agraria y 13 del Reglamento Interno del Registro Agrario Nacional²³⁰.

²²⁶ **Artículo 25.** El capitán tendrá las siguientes funciones a bordo de las embarcaciones:

IV. Actuar como oficial del Registro Civil y levantar testamentos, en los términos del Código Civil para el Distrito Federal, en Materia Común, y para toda la República en Materia Federal; y(...)

²²⁷ **Artículo 1583.** Los que se encuentren en alta mar, a bordo de navíos de la Marina Nacional, sea de guerra o mercantes, pueden testar sujetándose a las prescripciones siguientes.

Artículo 1584. El testamento marítimo será escrito en presencia de dos testigos y del Capitán del navío, y será leído, datado y firmado, como se ha dicho en los artículos 1512 al 1519; pero en todo caso deberán firmar el Capitán y los dos testigos.

²²⁸ **Artículo 35.** En el Distrito Federal, estará a cargo de los Jueces del Registro Civil, autorizar los actos del estado civil y extender las actas relativas a nacimiento, reconocimiento de hijos, adopción, matrimonio, divorcio administrativo y muerte de los mexicanos y extranjeros en el Distrito Federal, al realizarse el hecho o acto de que se trate, así como inscribir las ejecutorias que declaren la ausencia, la presunción de muerte, el divorcio judicial, la tutela o que se ha perdido o limitado la capacidad legal para administrar bienes, siempre y cuando se cumplan las formalidades exigidas por los ordenamientos jurídicos aplicables.

²²⁹ **Artículo 80.** Los ejidatarios podrán enajenar sus derechos parcelarios a otros ejidatarios o a vecindados del mismo núcleo de población. Para la validez de la enajenación a que se refiere este artículo bastará la

3.1.6.10. Legislativa

Cuando hablamos de la fe pública del Poder Legislativo, pensamos en ésta como una fe pública intrínseca, "la cual surte efecto en los actos de publicación y promulgación de las leyes. Quienes reciben estas disposiciones deben tener por cierto, verdadero y obligatorio el texto de éstas (contenido en el Diario Oficial de la Federación y en las gacetas o periódicos oficiales de las entidades federativas)"²³¹ sobre esto tenemos el artículo 14 de la Ley Federal de Derecho de Autor Vigente²³².

3.1.6.11. De los archivos notariales

Para el caso de aquellos lugares donde exista un Archivo General de Notarías, se concederá a su titular fe pública para expedir copias certificadas a petición de parte o fedatario, o bien regularizar documentos incompletos en su poder, entre otras funciones. Esto conforme al artículo 238 de la Ley de Notariado para el Distrito Federal²³³.

conformidad por escrito de las partes ante dos testigos y la notificación que se haga al Registro Agrario Nacional, el que deberá expedir sin demora los nuevos certificados parcelarios. Por su parte el comisariado ejidal deberá realizar la inscripción correspondiente en el libro respectivo...

²³⁰ **Artículo 13.** Para efecto de lo dispuesto en el artículo 28 y demás relativos de la Ley, por fedatario público se entenderá, además del notario y corredor público, los funcionarios públicos que ejerzan funciones fedatarias de conformidad con la legislación aplicable

²³¹ Ríos Hellig, Jorge. *Ob.cit.* p. 65

²³² **Artículo 14.-** No son objeto de la protección como derecho de autor a que se refiere esta Ley:(...)

VIII. Los textos legislativos, reglamentarios, administrativos o judiciales, así como sus traducciones oficiales. En caso de ser publicados, deberán apegarse al texto oficial y no conferirán derecho exclusivo de edición; Sin embargo, serán objeto de protección las concordancias, interpretaciones, estudios comparativos, anotaciones, comentarios y demás trabajos similares que entrañen, por parte de su autor, la creación de una obra original;

²³³ **Artículo 238.-** El Consejero Jurídico y de Servicios Legales designará al titular del Archivo, quien ejercerá además de las facultades previstas en otros ordenamientos jurídicos, las siguientes:(...)

V.- Expedir y reproducir a solicitud de parte interesada los documentos públicos y privados que obren en los acervos en custodia del Archivo;

VI.- Certificar la documentación solicitada por autoridades judiciales, administrativas y legislativas, así como por los particulares que acrediten su interés legítimo, y que esté en custodia del Archivo;...

VIII.- Certificar la razón de cierre con respecto a la revisión previa a la que se refiere la fracción que antecede;...

XIII.- Regularizar y autorizar en definitiva, los instrumentos que hubieren quedado pendientes de autorización por parte de un notario;...

3.2. Certificación

Tratamos a la fe pública en el apartado anterior; por lo que ahora es pertinente hablar de la certificación, para así poder obtener los datos suficientes, que nos permitan realizar una comparación entre la función certificadora y la fedataria. Esto con el fin de acercarnos más a la naturaleza de las funciones de la Entidad Certificadora de los Actos de Comercio Electrónico para el sistema jurídico en nuestro país.

3.2.1. Concepto

La certificación en general, es definida por la mayoría de los autores, como una "acción llevada a cabo por una entidad reconocida como independiente de las partes interesadas, mediante la que se manifiesta la conformidad de una empresa, producto, proceso, servicio o persona con los requisitos definidos en normas o especificaciones técnicas"²³⁴

Esta entidad reconocida como independiente o tercera parte de la relación, por lo general asegura por escrito su conformidad (con la empresa, producto, proceso, servicio o persona). A este escrito se le conoce como certificado, y constituye una valiosa herramienta para las transacciones comerciales internacionales y nacionales, ya que es un generador de confianza entre las partes.

Conforme a lo expresado por el artículo 80 de la Ley de Metrología y Normalización, las actividades que debe comprender la certificación en general son: "I. Evaluación de los procesos, productos, servicios e instalaciones, mediante inspección ocular, muestreo, pruebas, investigación de campo o revisión y evaluación de los programas de la Calidad; II. Seguimiento posterior a la certificación inicial, para comprobar el cumplimiento con las normas y contar con mecanismos que permitan proteger y evitar la divulgación de propiedad industrial o intelectual del cliente; y III. Elaboración de criterios generales en materia de certificación mediante Comités de Certificación donde participen los sectores interesados y las dependencias. Tratándose de Normas Oficiales Mexicanas los criterios que se determinen deberán ser aprobados por la dependencia competente"²³⁵.

Mientras jurídicamente, Ley Federal de Metrología y Normalización en su **artículo 3°** define a la certificación como el: *procedimiento por el cual se asegura que un producto, proceso, sistema o servicio se ajusta a las normas o lineamientos o recomendaciones de organismos dedicados a la normalización nacionales o internacionales.*

²³⁴ <http://www.aenor.es/desarrollo/certificacion/quees/queescertificacion.asp>

²³⁵ <http://www.onnce.org.mx/>

Al tiempo que norma o lineamiento internacional según lo expuesto por este mismo artículo deben ser entendidas como: *la norma, lineamiento o documento normativo que emite un organismo internacional de normalización u otro organismo internacional relacionado con la materia, reconocido por el gobierno mexicano en los términos del derecho internacional.* En tanto, y según lo expresado por este mismo artículo, las normas mexicanas pueden ser oficiales y no oficiales, para el caso de las no oficiales, son definidas como: *la que elabore un organismo nacional de normalización, o la Secretaría, en los términos de esta Ley, que prevé para un uso común y repetido reglas, especificaciones, atributos, métodos de prueba, directrices, características o prescripciones aplicables a un producto, proceso, instalación, sistema, actividad, servicio o método de producción u operación, así como aquellas relativas a terminología, simbología, embalaje, marcado o etiquetado.* Siendo diferentes de las normas oficiales mexicanas, a las que se especifica como: *la regulación técnica de observancia obligatoria expedida por las dependencias competentes, conforme a las finalidades establecidas en el artículo 40, que establece reglas, especificaciones, atributos, directrices, características o prescripciones aplicables a un producto, proceso, instalación, sistema, actividad, servicio o método de producción u operación, así como aquellas relativas a terminología, simbología, embalaje, marcado o etiquetado y las que se refieran a su cumplimiento o aplicación.*

Sin embargo y tal como lo expone el **artículo 51-A** *Las normas mexicanas son de aplicación voluntaria, salvo en los casos en que los particulares manifiesten que sus productos, procesos o servicios son conformes con las mismas y sin perjuicio de que las dependencias requieran en una norma oficial mexicana su observancia para fines determinados. Su campo de aplicación puede ser nacional, regional o local.*

Como podemos ver no hay mucha discrepancia entre la definición de certificación dada por los teóricos y la expuesta por la ley mexicana; pero para efectos de esta tesis, tomaremos como concepto general de certificación el dado por el artículo 3° de la ley de metrología y normalización.

3.2.2. Características

Al hablar de certificación en general; las fuentes coinciden en señalar dos características fundamentales que ésta debe de llenar: el ser temporal y tener carácter voluntario.

Cuando decimos que la certificación es temporal, se hace alusión al certificado (o escrito de conformidad dado por el tercero certificador) que tiene cierto tiempo de vigencia; dependiendo de la empresa, producto, proceso, servicio o persona; y del tercero certificador. Al término del tiempo de vigencia del certificado, se debe de solicitar una nueva evaluación, con el fin de conseguir una renovación del mismo; pero esto no quiere decir que mientras este vigente el certificado, dejará de ser objeto de observación; por el contrario el tercero

certificador está obligado a dar seguimiento posterior al objeto de su certificación, para así otorgar la seguridad suficiente a terceros de que se está frente a un objeto confiable.

Por otra parte, cuando hablamos del carácter voluntario de la certificación, queremos decir, que en ningún caso existe una regla, norma o procedimiento coercitivo que haga que las partes se vean obligadas a seguir determinados lineamientos; debe quedar claro que la certificación es siempre solicitada por la parte interesada que por razones de seguridad interna o externa, o bien por cumplir con los lineamientos consensuales que mercado solicita, requiere a un organismo certificador sus servicios. El ordenamiento nacional reconoce este principio, tal es el caso de la Ley de Metrología y Normalización, que en su artículo 51-A (anteriormente citado) señala: "*Las normas mexicanas son de aplicación voluntaria...*"

3.2.3. Organismos de Certificación

La entidad reconocida como independiente o tercera parte de la relación para el procedimiento de certificación, es también conocida con organismo de certificación (encargado entre otras cosas de emitir un certificado). Su importancia es medular ya que debe ser una entidad lo suficientemente acreditada y confiable para que sus determinaciones y criterios sean reconocidos por las otras partes. En el presente apartado hablaremos de dichos organismos, así como de algunos organismos de certificación sumamente importantes en el medio internacional y nacional a manera de ejemplo.

Según el artículo 3° de la ley Federal de Metrología y Normalización; debemos entender como organismos de certificación a *las personas morales que tengan por objeto realizar funciones de certificación*. Estos organismos de certificación encuentran fundamento jurídico y regulaciones específicas en diversos ordenamientos nacionales; entre los que tenemos a la ya mencionada Ley Federal de Metrología y Normalización, que en sus artículos 3 fracción XV-A, 68, 70 fracción I, 70-C, 79, 80 y 88; hace referencia a ellos de la siguiente forma:

El artículo 3° nos dice que "*Para los efectos de esta Ley, se entenderá por: ... XV-A. Personas acreditadas: los organismos de certificación, laboratorios de prueba, laboratorios de calibración y unidades de verificación reconocidos por una entidad de acreditación para la evaluación de la conformidad...*"

El artículo 68 menciona "*La evaluación de la conformidad será realizada por las dependencias competentes o por los **organismos de certificación**, los laboratorios de prueba o de calibración y por las unidades de verificación acreditados y, en su caso, aprobados en los términos del artículo 70.*"

La acreditación de los organismos, laboratorios y unidades a que se refiere el párrafo anterior será realizada por las entidades de acreditación..."

"Artículo 70. *Las dependencias competentes podrán aprobar a las personas acreditadas que se requieran para la evaluación de la conformidad, en lo que se refiere a normas oficiales mexicanas, para lo cual se sujetarán a lo siguiente: I. Identificar las normas oficiales mexicanas para las que se requiere de la evaluación de la conformidad por personas aprobadas y, en su caso, darlo a conocer en el Diario Oficial de la Federación..."*

Mientras que el artículo 70 habla de diversos criterios que deberán seguir las entidades de acreditación y las personas acreditadas por éstas. El artículo 79° cita a los diversos criterios que deberán seguir las dependencias competentes para aprobar a los organismos de certificación acreditados por cada norma oficial mexicana. El artículo 80, trata a las actividades de certificación, que en todo caso deberán ajustarse a las reglas, procedimientos y métodos que se establezcan en las normas oficiales mexicanas, y en su defecto a las normas internacionales.

Y por último, el artículo 88, nos dice que "Las personas físicas o morales tendrán la obligación de proporcionar a las autoridades competentes los documentos, informes y datos que les requieran por escrito, así como las muestras de productos que se les soliciten cuando sea necesario para los fines de la presente Ley y demás disposiciones derivadas de ella. En todo caso, respecto a las muestras se estará a lo dispuesto en los artículos 101 al 108 de la presente Ley".

También encontramos referencias de los organismos de certificación en los artículos 75, 76, 87 y 88 del Reglamento de la Ley Federal sobre Metrología y Normalización, que al respecto nos dicen:

El artículo 75, menciona los casos en que las entidades de acreditación, previa opinión de las dependencias competentes, podrán suspender en forma parcial o total la acreditación de los organismos de certificación, laboratorios de prueba, laboratorios de calibración o unidades de verificación.

El artículo 76, hace referencia a los casos en que las entidades de acreditación, previa opinión de las dependencias competentes, podrán cancelar la acreditación de los organismos de certificación, laboratorios de prueba, laboratorios de calibración o unidades de verificación.

Mientras que el artículo 87, nos dice que "Los interesados en acreditarse y aprobarse como laboratorios de pruebas y calibración, organismos de certificación y unidades de verificación, deberán formular su solicitud a la entidad de acreditación en términos de lo dispuesto en los artículos 68 y, en su caso, 79 de la Ley".

Artículo 88. "Los laboratorios de pruebas y calibración, **organismos de certificación** y, en su caso, las unidades de verificación acreditados y aprobados deberán demostrar, en la forma que indique la entidad de acreditación, que operan bajo un procedimiento de aseguramiento de la calidad que se encuentre previsto en las normas oficiales mexicanas, normas mexicanas o normas o lineamientos internacionales, que actúan con imparcialidad, independencia e integridad, y que garantizan la confidencialidad y la solución a los posibles conflictos que puedan afectar la confianza que deben brindar..."

Otro ordenamiento que versa sobre los organismos de certificación es el Reglamento Federal de Seguridad, Higiene y Medio Ambiente de Trabajo; que en sus artículos 11 y 163 estipulan:

"Artículo 11. El cumplimiento de las Normas en los centros de trabajo se podrá comprobar a través de los dictámenes que sean expedidos por las unidades de verificación, laboratorios de prueba y **organismos de certificación acreditados** en los términos de la Ley Federal sobre Metrología y Normalización. Lo anterior, sin perjuicio de las atribuciones de la Secretaría para realizar visitas de inspección conforme a la Ley y a las disposiciones reglamentarias..."

"Artículo 163. Sin perjuicio de lo establecido en el artículo anterior, la vigilancia del cumplimiento de las Normas podrá realizarse por conducto de las unidades de verificación, laboratorios de pruebas y **organismos de certificación**, de conformidad con lo dispuesto por la Ley Federal sobre Metrología y Normalización y este Reglamento".

Además de todos los ordenamientos anteriores; existe una norma mexicana que trata de certificación; la NMX-EC-065-IMNC-2000 "Requisitos generales para organismos que operan sistemas de certificación de producto". La que en algunos puntos aborda los requisitos legales necesarios para la constitución de un organismo de certificación; que junto a otros emanados de la Secretaría del Trabajo y Previsión Social, marcan la pauta sobre las formalidades requeridas para la conformación de un organismo de certificación; que son.²³⁶

- o Publicación de convocatoria
- o Establecer un Sistema de Calidad basado en la Normatividad NMX-EC-065-IMNC-2000 "Requisitos generales para organismos que operan sistemas de certificación de producto": el cual debe contar por lo menos con:
 - Una estructura Administrativa.
 - Un consejo directivo

²³⁶ Cfr. http://www.stps.gob.mx/04_sub_prevision/03_dgsht/ser_tra/tra_organismos.html

- Una estructura organizacional
 - Personal técnicamente capacitado, encargado de la certificación.
 - Procedimiento para control de documentos.
 - Sistema de registros.
 - Procedimiento de subcontratación.
 - Procedimiento de certificación.
 - Políticas y procedimientos de confidencialidad.
 - Procedimiento de auditorías Internas y revisión periódica.
 - Procedimiento de vigilancia.
 - Procedimiento para apelaciones, quejas y disputas.
 - Procedimiento para otorgar, mantener, retirar y suspender la certificación.
- Presentar solicitud por escrito a la entidad de acreditación correspondiente.
 - Señalar las normas que pretende evaluar, indicando la materia, sector, rama, campo o actividad respectivos y describir los servicios que pretende prestar y los procedimientos a utilizar.
 - Demostrar que cuenta con la adecuada capacidad técnica, material y humana, en relación con los servicios que pretende prestar, así como, con los procedimientos de aseguramiento de calidad que garanticen el desempeño de sus funciones.
 - Una vez obtenida la acreditación, solicitar la aprobación a la Dirección General de Seguridad y Salud en el Trabajo de esta Secretaría, anexando el oficio de Acreditación otorgado por la Entidad Mexicana de Acreditación

Además de los requisitos legales que debe llenar un organismo de certificación, existen ciertos principios por los que debe de regirse, para que así; su objetivo principal, que es brindar certeza a productos, servicios, procedimientos, empresas, etc. cumpla no solo con requisitos legales, si no también con principios éticos. Algunos de estos principios son:

La aplicación de la imparcialidad en sus criterios; es decir, realizar juicios basados en comparaciones objetivas de la información contenida en los

documentos de referencia, sin verse afectado en ningún momento por opiniones personales.

El uso de la confidencialidad en todas sus operaciones; esto se ve reflejado en un manejo reservado de la información recabada durante sus actividades de certificación.

El ser veraces, en otras palabras, apegarse a las referencias, procedimientos, normas y condiciones instituidas para realizar el proceso de certificación.

Ser equitativo en cualquiera de sus procedimientos. Ya sean los aplicados a productos, organizaciones, procesos, personas o prácticas; debe de quedar claro que en cualquier práctica el criterio a seguir es la igualdad; independientemente de la localización, volumen de trabajo, gama de servicios o cualquier otra característica que lo singularice.

La búsqueda de un no conflicto de intereses en los procedimientos de los organismos certificadores; es decir, evitar verse influenciado por intereses comerciales (o de cualquier otro tipo) que llegasen a influenciar el resultado de la certificación.

Y ante todo, mantener la transparencia en sus procedimientos; con el fin de propósito de que preservar la confiabilidad en todos sus procedimientos.

3.2.3.1. Ejemplos de Organismos Certificadores

3.2.3.1.1. A nivel nacional

En nuestro país existen diversos organismos de certificación reconocidos por la Dirección General de Normas de la Secretaría de Economía y/o acreditados por la Entidad Mexicana de Acreditación (EMA). Los hay tanto para sistemas de calidad, como para empresas, productos, etc. La Dirección General de Normas publica periódicamente una lista de organismos acreditados para certificar determinada norma, de dicha lista seleccionamos a los siguientes como muestra (aunque existen muchos más):

3.2.3.1.1.1. Instituto Mexicano de Normalización y Certificación

El Instituto Mexicano de Normalización y Certificación, A.C. (IMNC, A.C.) una Asociación Civil son fines no lucrativos, multisectorial y de carácter privado, de tercera parte, independiente e imparcial. Se encarga de certificar procesos, productos, sistemas y personas, cuenta con una Unidad de Verificación registrada y reconocida por el Gobierno Mexicano, ha participado en el desarrollo de normas

internacionales como ISO 9000, ISO 14000, ISO 19011 e ISO 17025, cuenta con personal calificado y reconocido a nivel internacional.

3.2.3.1.1.2. Organismo Nacional de Normalización y Certificación de la Construcción y Edificación

Existe también el Organismo Nacional de Normalización y Certificación de la Construcción y Edificación, S.C. (ONNCE) una Sociedad Civil dedicada a la Certificación y Normalización. Fue creada en 1994, en ese mismo año recibió la acreditación como Organismo Nacional de Normalización, y para 1997 es acreditado como Organismo de Certificación "por la Entidad Mexicana de Acreditación, aprobado por la Secretaría de Economía, la Secretaría de Desarrollo Social, la Comisión Nacional de Ahorro de Energía y la Comisión Nacional del Agua y como Organismo de Certificación de Sistemas de Calidad (2000) por la Entidad Mexicana de Acreditación"²³⁷.

Algunos de los objetivos que se plantea esta organización son: la elaboración de normas mexicanas, buscando la armonía y concordancia con las que se manejan a nivel internacional, buscando que respondan a las realidades internas del país. Así como Verificar, Certificar y Dictaminar normas oficiales mexicanas (las denominadas NOM), normas mexicanas de productos (la NMX), normas mexicanas de sistemas de calidad (las NMX-CC/ISO9000), las normas sobre competencia laboral.

3.2.3.1.1.3. Asociación Nacional de Normalización y Certificación del Sector Eléctrico

Otro organismo de Certificación, es la Asociación Nacional de Normalización y Certificación del Sector Eléctrico, A.C. (ANCE). Fundada el 10 de diciembre de 1992; al igual que la IMNC es una institución privada sin fines de lucro, que se encarga de prestar apoyo y servicios de normalización, certificación de sistemas de calidad, laboratorio de pruebas, verificación y certificación de productos.

3.2.3.1.1.4. Consejo para el Fomento de la Calidad de Leche y sus Derivados

Tenemos también al Consejo para el Fomento de la Calidad de Leche y sus Derivados (COFOCALEC), un organismo privado, sin fines lucrativos; cuyo objetivo es promover la calidad de la leche y productos derivados de ésta, en nuestro país; por medio de la "normalización, el fomento y la evaluación de la conformidad, es decir, la determinación del grado de cumplimiento de las normas mexicanas y oficiales mexicanas o internacionales, prescripciones o

²³⁷ <http://www.onnce.org.mx/>

características que aplican a este alimento importante²³⁸. Está conformado por productores de la industria de leche y sus productos, comercializadores y distribuidores, así como representantes de instituciones académicas y de investigación, consumidores, organizaciones relacionados con la leche, así como por representantes del sector público.

3.2.3.1.2. A nivel internacional

El incremento de la actividad comercial a nivel internacional hizo necesario la creación de normas por organismos internacionales. Dichas normas cuentan con la aprobación consensual internacional, que busca una competencia equitativa por medio de la eliminación de barreras técnicas, la creación de un lenguaje común, y el establecimiento de un mínimo de normas a exigir en el comercio mundial.

Nuestro país no es ajeno a los cambios mundiales; ni a las necesidades nacionales; por lo que a través de la Dirección de Asuntos Internacionales de la Secretaría de Economía (Dependiente directa de la subsecretaría de normatividad, inversión extranjera y prácticas comerciales internacionales), busca la integración y participación nacional, en los organismos internacionales y regionales de normalización.

Esto debido a que la Dirección General de Normas de la Secretaría de Economía, es el organismo gubernamental, autorizado para representar a nuestro país en los asuntos y eventos relacionados con la Metrología y Normalización, con forme a lo previsto en el artículo 4° de la Ley de Metrología y Normalización que dice: *"La Secretaría, en coordinación con la Secretaría de Relaciones Exteriores y en los términos de la Ley Orgánica de la Administración Pública Federal, representará al país en todos los eventos o asuntos relacionados con la metrología y normalización a nivel internacional, sin perjuicio de que en dicha representación y conforme a sus atribuciones participen otras dependencias interesadas en razón de su competencia, en coordinación con la propia Secretaría. También podrán participar, previa invitación de la Secretaría, representantes de organismos públicos y privados"*.

Para conseguir este fin, se crearon cuatro comités mexicanos dependientes de la Dirección General de Normas (la presencia y secretariado de cada uno recaen en ésta) para atender a los Organismos Internacionales de Normalización. Estos comités son: la Comisión del CODEX Alimentarius; los Comités Técnicos de la ISO; El Comité Electrotécnico Mexicano (CEM) y Comité Mexicano para la atención de la Comisión Panamericana de Normas Técnicas (COPANT).

²³⁸ <http://cofocalec.org.mx/espanol/Acerca.htm>

La necesidad de que México tenga comisiones en cada uno de estos organismos internacionales de normalización, se debe en gran medida a su importancia mundial, y al amplio rango de actividades que abarcan. Por lo que se hace necesario hablar de cada uno de ellos.

3.2.3.1.2. 1. La Comisión del CODEX Alimentarius (CAC)

Surge como un programa conjunto de la Organización Mundial de la Salud (OMS) y la Organización para la Agricultura y la Alimentación (FAO) en 1963 (año en que tuvo lugar la primera reunión). Actualmente cuenta con 165 países miembros, que representan al 97% de la población mundial. Fue creada con el propósito de lograr un acuerdo sobre normas alimentarias y cuestiones conexas a éstas; para así asegurar la calidad de los productos, proteger al consumidor, reducir las barreras comerciales y facilitar el intercambio comercial de alimentos a nivel mundial.

Para ello, se encarga de la recopilación de Prácticas, Normas y Recomendaciones aprobadas consensualmente por la Comisión del Codex Alimentarios; al día de hoy ha producido "237 normas alimentarias, 41 códigos de prácticas de higiene o tecnológicas, 3274 límites para residuos de plaguicidas, 25 directrices para contaminantes, y se han evaluado, 185 plaguicidas, 1005 aditivos alimentarios, 54 medicamentos veterinarios, de más de 3500 productos, ya sean elaborados, semielaborados o crudos"²³⁹. Actualmente se compone de 28 comités mundiales.

"Cada Comité está representado por un país anfitrión, que actúa como Presidente del mismo y como organizador de los trabajos, preparación y distribución de los documentos, dirección de las reuniones, elaboración de las normas, elaboración de los informes, etc."²⁴⁰.

Nuestro país a pesar de encontrarse agrupado entre las naciones consideradas dentro del tercer mundo (o países en vías de desarrollo), ha ocupado lugares importantes dentro del Comité. En 1987 se le otorgó la presidencia del Comité del Codex sobre Frutas y Hortalizas Frescas; y actualmente es representante regional para América Latina y el Caribe ante el Comité ejecutivo de la Comisión.

Motivado por estas distinciones y otras; nuestro país creó en 1993 el Comité Mexicano para la Atención del CODEX Alimentarius (CMAC), encargado de recibir y enviar las recomendaciones, observaciones o peticiones de nuestro gobierno a la Comisión del Codex.

²³⁹ <http://www.economia.gob.mx>

²⁴⁰ *Ibidem*

3.2.3.1.2. 2. Organización Internacional de Normas (ISO)

Uno de los organismos de certificación más importantes a nivel mundial (el más grande del mundo) es ISO (International Organization for Standardization) o Organización Internacional de Normas. ISO es una red de institutos de estandarización nacionales en 146 países, cuenta con un miembro por cada país, y una Secretaría Central en Ginebra Suiza que coordina el sistema. Es una organización no gubernamental, como en el caso del sistema de las Naciones Unidas, se cuenta con delegaciones de gobiernos nacionales. Sin embargo ISO ocupa una posición especial entre los sectores públicos y privados. Esto debido a que, por una parte muchos de sus institutos miembros son parte de la estructura gubernamental en sus países, o son regulados por sus gobiernos. Y por otro lado, otros miembros tienen sus orígenes únicamente en el sector privado, siendo fundados por socios nacionales de asociaciones industriales.

No obstante, ISO es capaz de actuar como una organización "puente" a través de la cual se pueden alcanzar consensos y soluciones que cumplan los requerimientos comerciales y crecientes necesidades de la sociedad, ya sean simples consumidores y usuarios, o bien corredores de bolsa.

Desde 1947 hasta nuestros días, ISO ha publicado más de 13 700 normas internacionales. Los rangos del programa de trabajo de ISO parten de actividades tradicionales, como la agricultura y la construcción, pasando por la ingeniería mecánica, instrumentos médicos, hasta los más nuevos descubrimientos en tecnología de la información, como la codificación digital de señales audiovisuales para aplicaciones multimedia.

La mayoría de los estándares ISO son altamente específicos, ya que se dedican sólo a un producto, material o proceso. Sin embargo, los estándares que le han ganado más reputación a las familias ISO 9000 y ISO 14000 alrededor del mundo son los llamados "estándares de sistemas de administración genérica". "Genérica" significa que los mismos estándares pueden ser aplicados a cualquier organización, pequeña o grande, cualquiera que sea su producto – incluyendo si su producto está actualmente en servicio – en cualquier sector de la actividad, o si es una empresa privada, de administración pública, o una dependencia de gobierno "Administración de sistemas" se refiere a que hace la organización para administrar sus procesos, o actividades. "Genérica" también significa que no importando que es o hace la organización, si es que quiere establecer una administración de sistemas de calidad o un sistema de administración ambiental, cada uno de estos sistemas contiene ciertas características esenciales que son explicadas en las ya mencionadas normas ISO 9000 y ISO 14000.

Nuestro país reconoce la importancia de ISO a nivel mundial; motivo por el cual, para el 7 de febrero de 1992, se crea el Comité Mexicano para la atención de la Organización Internacional de Normalización (CMISO), dependiente de la DGN

compuesto por expertos técnicos de distintos sectores, dedicados a dar respuesta a los trabajos de ISO, con el propósito de lograr la confluencia de los industriales nacionales en los trabajos de la ISO.

3.2.3.1.2.3. Comisión Electrónica Internacional

En 1906 es creada la Comisión Electrónica Internacional (IEC) con sede en Ginebra, Suiza. Esto debido a que en el Congreso Eléctrico Internacional (celebrado en San Luis, E.U.A.) en 1904 se llegó a la conclusión de que era necesario crear una comisión mundial encargada de desarrollar y publicar normas para el sector eléctrico, electrónico y las tecnologías relativas.

Actualmente cuenta con 57 miembros (cada uno representando a un país), que unidos conforman el 95% de la energía eléctrica a nivel mundial. Su campo de acción abarca desde potencia eléctrica hasta las áreas de electrónica, comunicaciones, conversión de la energía nuclear y la transformación de la energía solar en energía eléctrica. Su misión esencial es la búsqueda de un lenguaje técnico universal, desde "definiciones, símbolos eléctricos y electrónicos o unidades de medición, rangos normalizados, requisitos y métodos de prueba, características de los sistemas como tensión e intensidad y frecuencia, requisitos dimensionales, requisitos de seguridad eléctrica, tolerancias de componentes de equipo eléctrico y electrónico, entre otros"²⁴¹.

Para la consecución de estos fines se auxilia de Comités Técnicos (104 en total), Subcomités y grupos de estudio, encargados de la creación de normas internacionales. Hacia 1997 la Comisión Electrónica Internacional publicó 437 normas internacionales. Cuenta además con vínculos de cooperación y grupos de trabajo con la Organización Internacional de Normalización (ISO) y con la Unión Internacional de Telecomunicaciones (ITU).

Nuestro país atiende a esta importante organización a través del Comité Electrotécnico Mexicano (CEM); creado conforme a lo establecido por la ley General de Normas de Pesas y Medidas, el de febrero de 1981. Siendo reestructurado en dos ocasiones: el 1 de mayo de 1994 y 20 de febrero de 1996)

3.2.3.1.2.4. Comisión Panamericana de Normas Técnicas

La primera vez que se habló de la creación de un organismo americano de normalización; fue en la reunión de la Unión Panamericana de Ingenieros (UPADI) celebrada en 1947, en Brasil. Dos años después (el 12 de julio de 1949) se funda el Comité Panamericano de Normas Técnicas en Sao Paulo, Brasil.

²⁴¹ Ibidem

Tendría que pasar una década para que dicho organismo comenzara a funcionar oficialmente; por lo que es hasta el 2 de abril de 1961, cuando inicia sus labores en la ciudad de Montevideo. Tres años después (19), la Asamblea General del Comité, reunida en la ciudad de Nueva York decide cambiar la denominación del Comité, el cual es rebautizado con el nombre por el que se le conoce hasta nuestros días: Comisión Panamericana de Normas Técnicas (COPANT).

Entre sus finalidades, se plantea: Impulsar su desarrollo industrial, científico y tecnológico y facilitar la cooperación entre los países miembros; así como promover el desarrollo de la normalización técnica y actividades conexas en los países participantes. Pudiendo con esto; elaborar para los países de la región normas que, a pesar de ser de su interés, no hayan sido creadas por Organismos Internacionales reconocidos o que existiendo no correspondan a su interés particular; pudiendo así armonizar las normas técnicas entre los países participantes.

De la atención de este Comité en nuestro país se encarga el Comité Mexicano para la atención de la COPANT; creado el 13 de mayo de 1998 por DGN; para dar respuesta a la documentación enviada por la Comisión Panamericana de Normas Técnicas. Entre los objetivos del comité mexicano para la atención del COPANT están: el difundir y promover el conocimiento de las Normas COPANT; así como el propiciar la cooperación internacional en todos los aspectos y de las necesidades de cada país; y coordinar la participación del Gobierno de México en los trabajos y reuniones de la COPANT a todos los sectores interesados.

3.2.4. Beneficios de la certificación

La certificación es un proceso que no solo auxilia a la seguridad entre empresas, existen otros entes beneficiados por el proceso de certificación; entre ellos tenemos a:

Los gobiernos. Para ellos la certificación, permite asegurar que los servicios y bienes observan los requisitos obligatorios de seguridad, salud, medio ambiente, etc. Es además una forma de controlar las exportaciones e importaciones; así como un importante instrumento para evaluar a los proveedores en las contrataciones que el gobierno establece con empresas; al mismo tiempo que permite verificar que los bienes adjudicados en algún proceso contractual cumplen los requisitos que establece determinado pliego de condiciones.

La industria en general. Hace posible a los industriales demostrar a cualquier interesado, que su empresa cumple cabalmente las obligaciones legales o los acuerdos contractuales; lo que incrementa su buena reputación en el mercado, y por lo tanto su confiabilidad. Llegando al punto que hoy en día algunas empresas exigen determinadas certificaciones a otras compañías para poder negociar con ellas.

El Consumidor. Por medio de los mecanismos de certificación, el consumidor final puede estar seguro que productos, proveedores o servicios cumplen con las normas y lineamientos comerciales; y por lo tanto son confiables.

3.3. Diferencias entre Fe Pública y Certificación

En los apartados anteriores al abordar a la certificación y fe pública, dijimos que éstas pueden ser definidas como:

Fe pública. Conforme a lo expresado por el artículo 44 de la Ley de la Comisión Estatal de Derechos Humanos de Jalisco Fe Pública es "...la facultad de autenticar documentos preexistentes o declaraciones y hechos que tengan lugar o estén aconteciendo en presencia de dichos servidores públicos, sin perjuicio del valor probatorio que se les atribuya, en los términos de este ordenamiento y otras leyes aplicables. Las declaraciones y hechos a que se refiere el párrafo anterior, se harán constar en el acta circunstanciada que al efecto levantará el servidor público correspondiente".

En tanto que doctrinalmente es considerada como: "una presunción legal de verdad; un imperativo jurídico o verdad oficial impuesta por el Estado, vigente mientras no se pruebe su falsedad; la seguridad otorgada por el Estado para afirmar que un acto o hecho es verdadero; el imperativo jurídico o coacción que nos obliga a tener por válidos determinados hechos o acontecimientos sin decir originalmente sobre su verdad objetiva; o más ampliamente como un imperativo jurídico que impone el Estado a un pasivo contingente universal para considerar cierta y verdadera la celebración de un acto o el acaecer de un evento que no percibe este contingente por sus sentidos; también es el contenido del instrumento que lo contiene."²⁴²

Certificación. Mientras que certificación es definida por algunos autores, como una "acción llevada a cabo por una entidad reconocida como independiente de las partes interesadas, mediante la que se manifiesta la conformidad de una empresa, producto, proceso, servicio o persona con los requisitos definidos en normas o especificaciones técnicas"²⁴³

Al tiempo que Ley Federal de Metrología y Normalización en su **artículo 3º** define a la certificación como el: *procedimiento por el cual se asegura que un producto, proceso, sistema o servicio se ajusta a las normas o lineamientos o recomendaciones de organismos dedicados a la normalización nacionales o internacionales.*

²⁴² Cfr. Ríos Hellig, Jorge. *Ob. cit.*, p.46

²⁴³ <http://www.aenor.es/desarrollo/certificacion/quees/queescertificacion.asp>

Del análisis de las definiciones y apartados anteriores del presente capítulo, podemos establecer claramente las diferencias entre certificación y fe pública.

La Fe Pública tiene cuatro características esenciales: Consta documentalmente, proviene del Estado, es un imperativo jurídico, y es oponible a cualquiera (erga omnes). En tanto que la certificación, si bien "puede" constar por escrito (al documento donde consta por escrito se le llama certificado); en ningún momento es imperativa, de hecho una de las características de la certificación es el ser voluntaria, es decir no existe algún elemento coercitivo en su aplicación, por lo tanto no es oponible a terceros; y en todo caso, el aceptarla o no, como válida, dependerá del criterio del particular.

Además de que la fe pública proviene del Estado que enviste a un particular (notario, secretario, funcionario público, etc.) de fe pública; en tanto que la certificación es otorgada por un tercero independiente (organismo de certificación) que no está investido de fe pública y cuya certeza en todo caso radica en el ser aceptado como tal por la confiabilidad, imparcialidad, veracidad y equidad demostrada en otros casos. Simplemente se encargan de brindar certeza sobre determinados productos, procesos, etc. siguiendo determinados lineamientos y requisitos éticos. Si bien, los organismos de certificación son reconocidos y regulados por el ordenamiento jurídico (para este propósito se crearon organismos como la Dirección General de Normas y la Entidad Mexicana de Acreditación), en ningún caso se les otorgan funciones de fedatarios.

En cuanto a las características de la certificación, mencionamos dos: el ser temporal y su carácter voluntario. Ya hablamos de la voluntariedad, y en cuanto a la temporalidad, podemos decir que ésta alude a que la certificación cuenta con cierto tiempo de vigencia, que deberá de ser renovado continuamente; esto es distinto a los criterios adoptados para fe pública, ya que, un instrumento donde conste fe pública será perpetuamente válido, se podrá atacar en todo caso a su autenticidad, pero no a su vigencia, como en el caso de la certificación.

En Conclusión, mientras que la fe pública nace como la necesidad del Estado de investir a ciertos individuos de fe, para así responder a la exigencia social de certidumbre sobre diversos actos. La certificación es un procedimiento autoregulatorio que no es coercitivo (ya que no emana de ninguna entidad investida de fe pública) pero que debido a criterio éticos y consensuales empleados durante el proceso de certificación, es considerada un mecanismo válido para dotar de certeza a diversos procesos donde la figura del fedatario no resulta fundamentalmente necesaria, y por lo tanto puede dejarse el arbitrio de organismos de certificación no gubernamentales.

3.4. La Existencia de la Entidad Certificadora en el marco del Comercio Electrónico como un tercero confiable, más no como un dador de fe pública

A manera de conclusión del presente capítulo e introducción al siguiente; expondremos algunas de las razones jurídicas, del porque una Entidad Certificadora es un tercero confiable, pero no un dador de fe pública. Esto no sólo porque la ley la señala como tal, si no porque existen verdaderas bases jurídicas para considerarla así. Aclarando que éstas son una mera referencia introductoria.

Conforme al artículo 100 del Código de Comercio Vigente, **"...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 puede incluirse información."**

Esta es la razón legal para no considerar a un organismo de certificación, como el prestador de servicios de certificación, un fedatario. Pero esto no tendría sentido sin entender el trasfondo jurídico de tal aseveración; por lo que al respecto pensamos que, el prestador de servicios de certificación en los actos de comercio electrónico embona por muchas causas, en la figura del organismo de certificación en general, expuesta en el presente capítulo, al tiempo que dista mucho de la figura del fedatario (a la que igualmente abordamos en apartados anteriores)

Las razones por las que nos atrevemos a afirmar esto son:

Como dijimos, la certificación; "puede" constar en un documento (recordemos que el documento de acuerdo con las últimas modificaciones al código civil puede asumir otras modalidades además del papel) como la fe pública, a dicho documento se le conoce como certificado (distinto al protocolo notarial u otros documentos de fedatarios). En el caso de los prestadores de servicios de certificación, estos también emiten certificados, esto conforme al artículo 108, del Código de Comercio Vigente que al respecto dice:

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 de Certificado;*
- V. *Periodo de vigencia del Certificado*
- VI. *La fecha y hora de emisión, suspensión y renovación del Certificado;*
- VII. *El alcance de las responsabilidades que asume el Prestador de Servicios de Certificación, y*
- VIII. *La referencia de la tecnología empleada para la creación de la Firma Electrónica.*

Otra de las características de la certificación, es carecer de imperatividad, en todo caso es voluntaria, por lo tanto no es oponible a terceros; por lo que, el aceptarla o no, como válida, dependerá del criterio del particular. Si bien es cierto que nuestro ordenamiento regula al prestador de servicios de certificación por medio de la Secretaría de Economía; el uso o no de éste en las transacciones comerciales, queda a voluntad de las partes; ya que en ningún precepto se habla de una obligatoriedad de uso de entidades de certificación.

Además de que como mencionamos en el apartado anterior la fe pública proviene del Estado que enviste a un particular de ella; al tiempo que la certificación es otorgada por un tercero independiente que no está investido de fe pública; pero aun así es reconocido y regulado por ordenamiento jurídico. Para el caso de los prestadores de servicios de certificación, estos son reconocidos y regulados por diversos artículos (100 –114) del Código Civil Vigente; pero sin dejar de lado al artículo 100, que tajantemente expone: *“La facultad de expedir Certificados no conlleva fe pública por sí misma...”*

Otra de las características de la certificación además del carácter voluntario, es su temporalidad, es decir, que la certificación sólo es válida por un periodo de tiempo que debe de renovarse. Esto lo vemos en Reflejado en los Prestadores de Servicios de Certificación que emiten certificados con una vigencia temporal conforme a los artículos 108 y 109 del Código de Comercio Vigente que dicen:

ARTICULO 108. *Los certificados, para ser considerados validos, 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 emisión, suspensión, y renovación del certificado;

VII. El alcance de las responsabilidades que asume el prestador de servicios de certificación, y

VIII. La referencia de la tecnología empleada para la creación de la firma electrónica.

ARTICULO 109. *Un certificado dejará de surtir efectos para el futuro, en los siguientes casos:*

I. Expiración del periodo de vigencia del certificado, el cual no podrá ser superior a dos años, contados a partir de la fecha en que se hubieren expedido. Ates de que concluya el periodo de vigencia del certificado podrá el firmante renovarlo ante el prestador de servicios de certificación;

II. Revocación por el prestador de servicios de certificación, a solicitud del firmante, o por la persona física o moral representada por este o por un tercero autorizado;

III. Perdida o inutilización por daños del dispositivo en el que se contenga dicho certificado;

IV. Por haberse comprobado que al momento de su expedición, el certificado no cumplió con los requisitos establecidos en la ley, situación que no afecta los derechos de terceros de buena fe, y

V. Resolución judicial o de autoridad competente que lo ordene.

Las anteriores razones nos hacen entender porqué un prestador de servicios de certificación encuadra más en la figura de un tercero certificador que en la otras instituciones jurídicas como el fedatario.

CAPÍTULO CUARTO. ENTIDADES DE CERTIFICACIÓN

4.1. Entidades de Certificación

Este capítulo concluye el presente trabajo, ya que finalmente llegamos al análisis de la naturaleza jurídica del prestador de servicios de certificación (o entidad certificadora). Muchos de los conceptos que trataremos en este capítulo, fueron abordados con más profundidad en apartados anteriores, por lo que no ahondaremos más en ellos; simplemente nos limitaremos a analizar al prestador de servicios de certificación y exponer las razones por las que consideramos que su naturaleza jurídica se acerca más a tal o cual figura.

Para conseguir esto haremos un estudio del prestador de servicios de certificación, desde conceptos y definiciones; hasta aspectos tecnológicos y legales. Con el fin de que el lector entienda la importancia de esta figura, y del porqué un análisis como éste es necesario.

4.1.1. Concepto

Como primer punto para entender la naturaleza del prestador de servicios de certificación (conocido también como entidad certificadora o tercero confiable) mencionaremos los distintos conceptos que de éste existen.

Entre los doctrinarios hay quienes lo definen ya bien como “un tercero imparcial, confiable para ambas partes y para la sociedad toda, dotado de poderes de certificación... autorizado a emitir certificados digitales...”²⁴⁴

Mientras que otros opinan que es “un tercero confiable que acredita el vínculo existente entre una clave y su propietario. Además extiende un certificado de firma electrónica el cual está firmado con su propia clave, para así garantizar la autenticidad de la información”²⁴⁵

Con mayor amplitud, hay quienes dicen de ellos, que son: “personas físicas o jurídicas – empresarialmente hablando y en masa, es más común lo segundo – que expiden certificados electrónicos, y estos son otro tipo de documentos electrónicos caracterizados porque vinculan la clave pública a la privada, cerrándose así el ciclo de acreditación del firmante y comprobándose su identidad. Digamos que son los que garantizan que la realidad digital, contenida en un documento firmado digitalmente, es tal y como ella misma aparenta”²⁴⁶.

Otros autores siendo más técnicos llaman prestadores a aquellos que: “Otorgan y verifican los pares de claves, conservan y archivan información

²⁴⁴ <http://comunidad.derecho.org/jvieg/publicac/firmele2.htm>

²⁴⁵ <http://www.cem.itesm.mx/acs/publicaciones/logos/libros/libros/firma.pdf>

²⁴⁶ <http://www.conocimientosweb.net/portal/article408.html>

adicional o asociada a los usuarios de dichos pares de claves (solo la necesaria). La entidad de certificación tiene como principal función la de hacer corresponder los pares de claves de la firma con su titular. Pero para que funcione el sistema requieren que se realicen funciones de registro de formación y de almacenamiento. El registro de Información coteja los datos y la información del titular con la realidad, comprueba la veracidad de la información y la identidad del solicitante de la firma²⁴⁷.

Aunque parecieran muy distintas las definiciones doctrinales, existen ciertos puntos donde coinciden: En todas ellas se habla de que los prestadores de servicios de certificación, son terceros en la relación; se dice también que están dotados de funciones de certificación; y que por lo tanto expiden certificados. Quizás difieren en atribuir más o menos funciones al prestador de servicios de certificación, pero como hemos visto coinciden en los puntos básicos.

En cuanto a definiciones legales, tenemos la expuesta en la Ley Modelo de UNCITRAL sobre Firma Electrónica del 2001, que en su artículo 2° nos dice lo siguiente: *“Por prestador de servicios de certificación se entenderá la persona que expide certificados y puede prestar otros servicios relacionados con las firmas electrónicas”*

Nuestro Código de Comercio Vigente en el artículo 89 al tratar algunas definiciones adoptó íntegramente ya que dicho artículo reza: *“Para efecto del presente Código, se deberán tomar en cuenta las siguientes definiciones: 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”*.

Las definiciones doctrinales son más amplias y concretas que las definiciones legales; quizás son más fáciles de entender que las legales, pero el hecho de ser tan concretas hace que lo entendido por prestador de servicios de certificación se centre solo en ciertas funciones, a diferencia de las definiciones legales; que aunque escuetas y vagas, dejan abierta la posibilidad de que las actividades de los prestadores de servicios de certificación se pueden incrementar según las necesidades mercantiles y legales.

Por lo que para efectos del presente trabajo adoptaremos la definición dada por el Código de Comercio Vigente, que es lo bastante amplia para adaptarse a nuevas tecnologías, además de que por ser idéntica a la de UNCITRAL hace que de alguna manera sea mundialmente válida.

4.1.2. Protocolos

Recordemos que la función primordial del prestador de servicios de certificación es hacer que las transacciones sean más seguras; pero para que esta

²⁴⁷ <http://www.monografias.com/trabajos13/contelec/contelec.shtml>

seguridad sea posible, se deben establecer ciertos protocolos. Los protocolos se encargan de especificar “las reglas y comportamientos a seguir”

Los protocolos en los que intervienen terceras partes confiables se llaman Tusted Third Party (Tercera Parte Confiable) o TTP por sus siglas en inglés. Algunos de los protocolos TTP más importantes son:

4.1.2.1. Arbitrarios

“En ellos una TPC o Autoridad de Certificación participa en las transacciones para asegurar que ambos lados actúan según las pautas marcadas por el protocolo”²⁴⁸

4.1.2.2. Notariales

Por medio de éste, se garantiza la adecuada operación, también hace posible estimar si las partes involucradas “actuarán por derecho según la evidencia presentada a través de los documentos aportados por los participantes e incluidos dentro del protocolo notarial. En estos casos, se añade la firma (digital) del notario a la transacción, pudiendo éste testificar, posteriormente, en caso de disputa”²⁴⁹.

4.1.2.3. Autoverificables

En ellos ambas partes pueden verificar que se actúe con honestidad durante la transacción. Para esto se valen de la firma digital (elemento básico de este tipo de protocolos) y no necesitan de una Entidad de Certificación para Verificar su autenticidad.

4.1.3. El documento A/CN.9/WG.IV/WP.71 Documento de la Sesión 31ª del Grupo de Trabajo IV, en Materia de Comercio Electrónico

La Secretaría de las Naciones Unidas establece en el párrafo 44 del documento A/CN.9/WG.IV/WP.71 del 31 de diciembre de 1996 los criterios a seguir para el funcionamiento de las entidades de certificación; algunos de estos son²⁵⁰:

1. Independencia (ausencia de interés financiero o de otro tipo en las transacciones subyacentes).

²⁴⁸ Reyes Krafft, Alfredo. *Ob.cit.* p.169

²⁴⁹ http://www.informatica-juridica.com/trabajos/firma_digital.asp

²⁵⁰ <http://www.arrakis.es/~anguiano/artautcert.html>

2. Recursos y capacidad financiera para asumir la responsabilidad por el riesgo de pérdida
3. Experiencia en tecnologías de clave pública y familiaridad con procedimientos de seguridad apropiados.
4. Longevidad (conservación de certificados).
5. Aprobación del equipo y los programas.
6. Mantenimiento de un registro de auditoría y realización de auditorías por una entidad independiente.
7. Existencia de un plan para casos de emergencia.
8. Selección y administración del personal.
9. Disposiciones para proteger su propia clave privada
10. Seguridad interna.
11. Disposiciones para suspender las operaciones, incluida la notificación a los usuarios.
12. Garantías y representaciones.
13. Limitación de la responsabilidad.
14. Seguros.
15. Capacidad para intercambiar datos con otras autoridades certificadoras.
16. Procedimientos de revocación.

Más adelante veremos la forma en que los prestadores de servicios de certificación reconocidos por la ley mexicana observan estos requisitos.

4.1.4. Tipos de Certificación

En el mismo documento A/CN.9/WG.IV/WP.71 de los tipos de certificación que pueden emitir las entidades de certificación, y que a saber son:

4.1.4.1. Identidad

Es el tipo de certificación más popular en nuestros días. En ésta se asocia una clave pública a una identidad digital (equipo, software, etc.) o personal (usuario); se emplea sobre todo para los criptosistemas de clave pública.

4.1.4.2. Autorización o Potestad

Por medio de ésta se certifica a los usuarios, pero en aspectos diferentes a los de identidad.

4.1.4.3. Transaccionales

Para el caso de este tipo de certificación, la certificación versa en "atestiguar que algún hecho o formalidad acaeció o fue presenciado por un tercero"²⁵¹.

4.1.4.4. Tiempo

En estos, por medio de un estampillado digital de tiempo, se certifica que un documento existía en cierto momento.

4.1.5. Requisitos legales para la prestación de servicios de certificación

Los prestadores de servicios de certificación surgen con el propósito de prestar seguridad jurídica en las transacciones vía electrónica; debido a que el medio en el que se desarrollan, al ser tan nuevo es "intangibile", por lo que puede ser objeto de fraudes o errores (como el caso de los hackers).

En un principio eran entidades reconocidas por particulares, pero no así por los ordenamientos jurídicos. Pero dada la creciente importancia y desarrollo del comercio electrónico tanto a nivel mundial, como internacional; los ordenamientos jurídicos de diversos países (entre ellos el nuestro) se vieron en el imperativo de regular a figuras como éstas (nacidas en el seno de los intereses particulares) para responder a las necesidades del mercado. Aunque esto no es extraño para el derecho mercantil, ya que como vimos en el recuento histórico emprendido en el primer capítulo, muchas instituciones mercantiles reconocidas actualmente tuvieron su origen entre los comerciantes (letra de cambio, cheque, pagaré, etc.) para posteriormente ser acogidas por los ordenamientos jurídicos.

Como primer punto para el reconocimiento de los prestadores de servicios de certificación, nuestros legisladores lo abordan y establecen diversos requisitos para éste en el Código de Comercio Vigente, posteriormente la Secretaria de Economía (entidad encargada de la regulación de los prestadores de servicios de certificación) publicó un reglamento y diversas reglas a seguir por los prestadores de servicios de certificación en nuestro país. De esta regulación legal hablaremos en los siguientes apartados.

²⁵¹ Reyes Krafft, Alfredo Alejandro. Ob. Cit. p.171

4.1.5.1. Código de Comercio

Conforme al artículo 100 del Código de Comercio Vigente, las entidades que podrán ser prestadores de servicios de certificación son: *"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"*.

Las entidades referidas deberán de estar acreditadas por la Secretaría de Economía. Para obtener dicha acreditación, deberán cumplir con los requisitos previstos por el artículo 102 del Código de Comercio Vigente que exige:

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;

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.

Obtenida la acreditación, los prestadores de servicios de certificación, deberán notificar a la Secretaría de Economía dentro de los 45 días siguientes al inicio de la prestación de servicios de certificación. Aunque conforme al transitorio tercero debemos tener en cuenta que: *"TERCERO.- En lo que se refiere al artículo 102, dentro de los doce meses siguientes a la entrada en vigor de las reglas generales a que se refiere el artículo anterior, el plazo de 45 días a que se refiere el mismo, será de 90 días"*.

Para el caso de que el prestador de servicios de certificación sea una persona moral de carácter privado (esto conforme al mencionado artículo 100,

fracción II del Código de Comercio). Se exige, según el artículo 101 del citado Código que en su objeto social se estipulen las siguientes actividades:

I. Verificar la identidad de los usuarios y su vinculación con los medios de identificación electrónica;

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 actividad no incompatible con las anteriores.

Asimismo, el Código de Comercio Vigente, nos habla de obligaciones, tanto para el prestador de servicios de certificación, como para el destinatario y la parte que confía. En cuanto al Prestador de Servicios de Certificación, el artículo 104 establece las principales de estas entidades, que entre otras cosas son:

Comprobar la identidad de los solicitantes y otras cuestiones pertinentes para la emisión de certificados; poner a disposición del firmante los dispositivos de generación de los datos de creación y de verificación de la firma electrónica; Dar informes sobre el precio, las condiciones de utilización, las limitaciones de uso y la forma en que se garantiza una posible irresponsabilidad del certificado; Mantener un registro de certificados; guardar confidencialidad sobre la información recibida; en el caso del cese de actividades el prestador deberá comunicar a la Secretaría para así determinar el destino de registros y archivos; establecer medidas para asegurar la confidencialidad y la no alteración de los certificados y datos en el proceso de generación de firma; establecer declaraciones sobre normas y procedimientos; proporcionar los medios de acceso a la parte que confía para que pueda determinar: "a) La identidad del prestador de servicios de certificación; b) que el firmante nombrado en el certificado tenía bajo su control el dispositivo y los datos de creación de firma en el momento en que se expidió el certificado; c) Que los datos de creación de firma eran válidos en la fecha en que se expidió el certificado; d) El método utilizado para identificar al firmante; e) cualquier limitación en los fines o el valor respecto de los cuales puedan utilizarse los datos de creación de la firma o el certificado; f) cualquier limitación en cuanto al ámbito o el alcance de la responsabilidad indicada por el prestador de servicios de certificación; g) Si existe un medio para que el firmante de aviso al prestador de servicios de certificación de que los datos de creación de la firma han sido de alguna manera controvertidos, y h) si se ofrece un servicio de terminación de vigencia del certificado".

De los demás requisitos legales que conforme al Código de Comercio Vigente son necesarios para prestar servicios de certificación, hablaremos en

apartados posteriores, por lo que nos parece innecesario hablar de ellos en el presente apartado.

4.1.5.2. Norma Oficial Mexicana NOM-151-SCFI-2002, Prácticas comerciales-Requisitos que deben observarse para la conservación de mensajes de datos.

Ya hablamos de la estructura de la NOM-151-SCFI-2002, en capítulos anteriores. Dicha norma establece diversos requisitos técnico - legales para el prestador de servicios de certificación. Debido a la tecnicidad de los requisitos exigidos por esta norma, nos parece que citarlas podríamos desviarnos de nuestro tema principal; no obstante a manera de muestra citaremos algunos párrafos del apartado 01. Introducción, que dedica uno de sus subtemas a la "OBTENCION DE LA CONSTANCIA DEL PRESTADOR DE SERVICIOS DE CERTIFICACION" que textualmente dice:

"Para la obtención de la constancia el sistema de conservación deberá usar el protocolo de aplicación descrito en este apéndice para enviar el expediente al prestador de servicios de certificación, 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:

```
<form action="url del programa generador de constancias " method="post"
  enctype="multipart/form-data">
  Expediente: <input type="file" name="expediente">
  <input type="submit" value="Obtener Constancia">
</form>
```

La constancia deberá regresar al cliente como un archivo de tipo mime application/octet-stream²⁵². El prestador de servicios de certificación podrá recibir, si así lo acuerda con sus clientes, medios físicos conteniendo los archivos correspondientes a los expedientes.

FORMACION DE LA CONSTANCIA

El prestador de servicios de certificación 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 prestador

²⁵² Los MIME Types (Multipurpose 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.

de servicios de certificación y (v) su firma digital de acuerdo a la definición correspondiente de esta Norma Oficial Mexicana.

METODO DE VERIFICACION DE AUTENTICIDAD

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 prestador de servicios de certificación en la constancia;*
- 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.*

4.1.5.3. Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación.

El 14 de julio del 2004 aparece el Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación, en él, a lo largo de 29 artículos, se hace un estudio exhaustivo de las normas reglamentarias a las que deben sujetarse los Prestadores de Servicios de Certificación.

Los primeros cuatro artículos establecen disposiciones generales como: el objeto del ordenamiento, para el que las definiciones del artículo 89 del Código de Comercio Vigente, también resultan válidas. La aplicación de los principios de Neutralidad Tecnológica y Compatibilidad Internacional en los ordenamientos sobre materias electrónicas en nuestro país. La obligación de la Secretaría de Economía de llevar una relación actualizada y a disposición de todo el público, 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 Código de Comercio. La relación deberá contener también a las personas físicas que formen parte del personal de los sujetos antes señalados". Así como la obligación de la Secretaría de Economía de integrar un padrón de profesionistas para que auxilien a los prestadores de servicios de certificación.

Le siguen los artículos 5 a 7 que versan sobre los *requisitos de trámite y acreditación* como Prestador de Servicios de Certificación. Nos señala que para el caso de notarios y corredores públicos estos podrán solicitar su acreditación por medio de una persona moral, conforme a la legislación que los regula. Además que se hace mención de los términos dispuestos por la Ley Federal del Procedimiento Administrativo, para el caso del trámite para obtener la acreditación como Prestador de Servicios de Certificación deberán observarse otros requisitos.

Posteriormente se trata a las Operaciones del Prestador de Servicios de Certificación. Sobre el inicio de operaciones tratan los artículos 8° a 14° donde se

hace referencia a la fianza que deberán tener las entidades; y la expedición y registro del certificado por parte de la Secretaría de Economía al interesado, previa verificación de la fianza respectiva, así como otros requisitos de dicha fianza.

Siguiendo lo relativo a operaciones del prestador, están los certificados (15° - 20°) Entre otras cosas mencionan que el prestador está obligado a proporcionar su dirección electrónica a la Secretaría de Economía y a aquellos a los que les otorgue certificados; para fines de validez, suspensión o revocación de los certificados. Así como enviar una copia de cada certificado emitido por ellas, vía electrónica a la Secretaría de Economía para que ésta los resguarde. El artículo 17° reglamenta la fracción III del artículo 108 del Código de Comercio Vigente (del que hablaremos con mayor detenimiento al hacer alusión en apartados posteriores al certificado), donde al hablar de los datos de acreditación ante la Secretaría, que contendrán los Certificados que expidan los Prestadores de Servicios de Certificación se dice que estos deben por incluir al menos:

I. El nombre, denominación o razón social y domicilio del Prestador de Servicios de Certificación;

II. La dirección electrónica donde podrá verificarse la lista de certificados revocados a Prestadores de Servicios de Certificación, y

III. Los demás que, en atención al avance tecnológico, se establezcan en las Reglas Generales que expida la Secretaría”.

También se habla del sello de tiempo a utilizarse para los casos de fecha y hora de emisión de los certificados. Asimismo se establece la obligación de los prestadores de servicios de certificación de emitir, registrar y conservar los certificados en territorio nacional; así como evitar la existencia de elementos de confusión en los certificados. Aunque “La Secretaría podrá autorizar el resguardo de los Datos de Creación de Firma Electrónica del Prestador de Servicios de Certificación fuera del territorio nacional. En este caso, el Prestador de Servicios de Certificación asumirá los costos que impliquen a la Secretaría el traslado de sus servidores públicos para efectuar las visitas de verificación a que se refiere la Sección IV de este Reglamento”.

En cuanto al domicilio, objeto social y estatuto de los prestadores, se nos dice que en caso de cambio en alguno de ellos, los prestadores están obligados a dar aviso a la Secretaría de Economía con 15 días de anticipación para que ésta verifique si se continúa cumpliendo con los requisitos legales.

Sobre las auditorías al prestador de servicios de certificación, nos dice que “Para efecto del artículo 102, inciso A), fracción VI del Código de Comercio, las auditorías que efectúe la Secretaría 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”.

Por último, se nos habla de las sanciones e infracciones para los aplicables al prestador de servicios de certificación. Que se aplicarán, sin perjuicio de las demás responsabilidades en que pueda incurrir el Prestador, y van desde suspensión temporal por diversos periodos de tiempo hasta suspensión definitiva de sus funciones.

4.1.5.4. Reglas generales a las que deberán sujetarse los prestadores de servicios de certificación.

El 4 de agosto de 2004, la Secretaría de Economía publica una serie de reglas, a observar por los prestadores de servicios de certificación; que según el transitorio segundo de las mismas, serán objeto de revisión anual por la Secretaría de Economía.

En dichas reglas, a lo largo de 11 numerales, se describen las formalidades de operación para los prestadores de servicios de certificación. El objetivo de las reglas es dar cabal cumplimiento de lo dispuesto por el Código de Comercio Vigente y en el Reglamento del Código de Comercio en materia de prestadores de servicios de certificación.

Algunas de las especificaciones de las reglas son demasiado técnicas y extensas, por lo que no son realmente importantes para el presente estudio, que se enfoca más a aspectos jurídicos concretos. Por lo que al hablar de las reglas publicadas por la Secretaría de Economía, solo trataremos (y citaremos) algunos aspectos de ellas que nos parecen relevantes para el presente estudio haciendo a un lado cuestiones técnicas. Aclarado esto iniciamos el análisis de las reglas.

Como primer punto, las Reglas Generales nos hablan de los requisitos legales prescritos por el artículo 102 inciso A) fracciones II y III del Código de Comercio Vigente, y 5 fracción III del Reglamento; en este caso, para que la Secretaría de Economía los considere cumplidos, los prestadores de servicios de certificación, deberán observar lo siguiente: en cuanto a elementos humanos. Debe existir un profesional jurídico que deberá: ser licenciado en derecho con título y cédula profesional; y un el profesional informático a éste se le exige: Ser licenciado o ingeniero en área Informática o afin, con título y cédula profesional.

El personal auxiliar del profesional informático, se conformará de: Un Oficial de Seguridad; un administrador de sistemas; un operador de sistemas; un administrador de bases de datos, y un administrador de redes. A quienes de les exige, entre otras cosas: ser técnico, licenciado o ingeniero en área Informática o afin.

En todo caso, el Prestador de Servicios de Certificación cuenta con un plazo no mayor a 6 meses, para notificar a la Secretaría que cuenta con la totalidad del personal auxiliar del profesional informático, salvo el Oficial de Seguridad que deberá estar designado desde el momento de la solicitud de acreditación y podrá ser el propio Profesional Informático. Asimismo, el Prestador de Servicios de Certificación deberá suscribir con el personal que maneje información confidencial un contrato de confidencialidad que se extienda más allá de la vigencia del contrato laboral del empleado o de servicios en caso de una empresa externa.

En cuanto a los elementos materiales y sus procedimientos, se deberá observar lo siguiente: *“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. Las implantaciones de los controles deberán evitar riesgo, daño o pérdida, de los activos, alteración o sustracción de información”*. Los servicios compartidos por otra entidad distinta al Prestador de Servicios de Certificación o por personal de éste no dedicado al servicio de certificación, deberán estar fuera del perímetro de seguridad.

En un documento que se denominará Política de Seguridad Física, se deberá contemplar y desarrollar por lo menos los siguientes aspectos: control de acceso físico; protección y recuperación ante desastres; protecciones contra robo, forzamiento y entrada no autorizada a los espacios físicos; medidas de protección en caso de incendio, contra fallas de servicios eléctricos o de telecomunicaciones, y un procedimiento de actualización para autorización de acceso al personal a las áreas restringidas.

Otro de los documentos que le es exigido al prestador de servicios de certificación es un documento denominado Análisis y Evaluación de Riesgos y Amenazas, en el que desarrollan los siguientes apartados y aspectos: la realización de *“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”*.

Sobre los elementos económicos, las reglas nos hablan de un seguro y la fianza que deberá prestar la entidad certificadora. El monto del primero que será aplicable para cada año lo determinará la Secretaría con base en un análisis de las operaciones comerciales y mercantiles en las que sean utilizados los Certificados, monto que se dará a conocer mediante publicación en el Diario

Oficial de la Federación. Sobre la fianza ésta será conforme a lo siguiente: *“tratándose de un notario o corredor públicos, por un monto equivalente a 5000 veces el salario mínimo general diario vigente en el Distrito Federal; tratándose de personas morales de carácter privado o instituciones públicas, por el monto resultante de multiplicar 5000 el salario mínimo general diario vigente en el Distrito Federal por cada persona física de su personal, o integrante de una persona moral distinta que se contemple para efectos del artículo 104 fracción I del Código dentro de la acreditación para prestar el servicio de certificación en nombre y por cuenta del solicitante conforme al artículo 104 fracción I del Código; Cuando la fianza tenga que ser otorgada por un notario o corredor público, la Secretaría podrá acordar que se otorgue de manera solidaria por parte de los colegios o agrupaciones de notarios o corredores públicos”.*

En cuanto a la Infraestructura Informática, se dice que ésta debe incluir: una Autoridad Certificadora; una Autoridad Registradora; depósitos para: datos de Creación de Firma Electrónica del Prestador de Servicios de Certificación 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; una Declaración de Prácticas de Certificación, y los manuales de operación de las Autoridades Certificadora y Registradora.

Sobre la Política de Seguridad, ésta deberá constar por escrito y cumplir con los siguientes requisitos: *“ser congruente con el objeto del Prestador de Servicios de Certificación; los objetivos de seguridad determinados deberán ser, claros, generales y no técnicos y resultado del Análisis y Evaluación de Riesgos y Amenazas; 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 Declaración de Prácticas de Certificación y con la Política de Certificados”.*

Al mismo tiempo, el Solicitante de Acreditación y el Prestador de Servicios de Certificación deberán elaborar y presentar un plan de continuidad del negocio y recuperación ante desastres, que describa cómo actuará en caso de interrupciones del servicio. Así como también 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. Dicho plan 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; 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 Política de Certificados y la Declaración de Prácticas de Certificación. 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.

En otro punto; las reglas, nos dicen que *"el solicitante de acreditación y el Prestador de Servicios de Certificación 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. Deberá contener también un resumen que incluya: contenido del documento; la historia del posible Prestador de Servicios de Certificación, y Relaciones comerciales con proveedores de insumos o servicios para sus operaciones. Dicho modelo deberá además 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"*.

En la elaboración del Modelo Operacional de la Autoridad Certificadora se deberá considerar la Política de Seguridad de la Información, la Declaración de Prácticas de Certificación, la Política de Certificados, y el Plan de Seguridad de Sistemas por lo que se refiere a la generación de claves. El Modelo Operacional de la Autoridad Certificadora deberá incluir los requerimientos de seguridad física del personal, de las instalaciones y del módulo criptográfico

Así también, el solicitante de acreditación y el Prestador de Servicios de Certificación deberán contar con un 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*. En dicho modelo también se 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. Para esto el

Prestador de Servicios de Certificación 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.

El solicitante de acreditación y el Prestador de Servicios de Certificación deberán contar de igual manera con un Plan de Administración de Claves conforme al cual generará, protegerá y administrará sus claves criptográficas, respecto de los apartados siguientes: 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. Claves de la autoridad certificadora; almacenamiento, respaldo, recuperación y uso de los Datos de Creación de Firma Electrónica de la Autoridad Certificadora del Prestador de Servicios de Certificación.

“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. El Prestador de Servicios de Certificación, su autoridad certificadora y registradoras, utilizarán dispositivos seguros para almacenar sus datos de creación de firma electrónica”.

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 Prestador de Servicios de Certificación o su representante, utilizando cualquiera de los medios admitidos en derecho. El Prestador de Servicios de Certificación 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, a fin de cumplir con el principio de neutralidad tecnológica. Tratándose de la identificación del representante de un Prestador de Servicios de Certificación que sea persona moral privada o institución pública, éste deberá acreditar su personalidad y la legal existencia de su representado a la Secretaría”.*

Sobre la estructura de certificados nos dice que debe ser compatible *“con el estándar ISO/IEC 9594-8; además de contener los datos que aparecen en el artículo 108 del Código de Comercio, para ser considerados como válidos”.* En el caso de las claves 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.

“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”: la fecha y hora en que fue emitida la Lista de Certificados Revocados; el nombre del emisor; la identificación del algoritmo de firma utilizado; La fecha en que emitirá la próxima Lista de Certificados Revocados que no podrá exceder de 24 horas, con independencia de mantener el Protocolo de Estatus de Certificados en Línea (OCSP), número de serie de los certificados revocados por el emisor con fecha y hora de revocación; y la Lista de Certificados Revocados deberá ser firmada por el Prestador de Servicios de Certificación que la haya emitido, con sus Datos de Creación de Firma.

“El solicitante de acreditación y el prestador de servicios de certificación 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, a efecto de garantizar la integridad y disponibilidad de la información ahí contenida. En dicho sitio se incluirá la Política de Certificados y la Declaración de Prácticas de Certificación”. Ahí mismo 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.

“De la misma manera, el solicitante de Acreditación y el Prestador de Servicios de Certificación deberán establecer una Política de Certificados conforme a la cual se establecerá la confianza del usuario en el servicio, que”: permita la interoperabilidad con los Prestadores de Servicios de Certificación ya acreditados y con la Secretaría de Economía; Asegure su concordancia con la Declaración de Prácticas de Certificación y los procedimientos operacionales; 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 firma electrónica avanzada deberá describir la forma en que se precisarán los propósitos, objetivos y alcances del Certificado y sus limitaciones. dé a conocer las medidas de privacidad y de protección de datos que se aplicarán en materia de Firma Electrónica Avanzada. Asimismo, se deberán describir las obligaciones que contrae el Prestador de Servicios de Certificación y el usuario en la emisión y utilización del certificado; la Política de Certificados será pública; deberá establecer bajo qué circunstancias se puede revocar un Certificado y quiénes pueden solicitarlo.

“En la Declaración de Prácticas de Certificación, que deberá elaborar y mantener actualizado el solicitante de acreditación y el Prestador de Servicios de Certificación, determinarán”: las responsabilidades y obligaciones del Prestador de

Servicios de Certificación y de la persona a identificar. Particularmente desarrollará aquellas inherentes a la emisión, revocación y expiración de certificados; los procedimientos de operación para otorgar certificados y el alcance de aplicación de los mismos; la vigencia de los certificados. Y una vez otorgada la acreditación por la Secretaría, la fecha de inicio de operaciones; 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; detalladamente el método de verificación de identidad del usuario que se utilizará para la emisión de los certificados; los procedimientos que se seguirán en los casos de suspensión temporal o definitiva del Prestador de Servicios de Certificación y la forma en que la administración de los certificados emitidos pasarán a la Secretaría o a otro Prestador de Servicios de Certificación, 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.

En tanto que 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 Prestador de Servicios de Certificación, 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 Prestador de Servicios de Certificación en su autoridad certificadora. En el caso que el Prestador de Servicios de Certificación por caso fortuito o de fuerza mayor debidamente comprobado a la Secretaría, no pudiese llevar a cabo el envío, el Prestador de Servicios de Certificación 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 Prestador de Servicios de Certificación 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 Prestador de Servicios de Certificación deberá cerciorarse que la Secretaría recibió la copia de cada certificado.

Mientras que "para los efectos del artículo 108 fracción III del Código y 17 fracción III del Reglamento; los certificados emitidos por el Prestador de Servicios de Certificación 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".

En tanto que *"para los efectos del artículo 108 fracción VI del Código y 18 del Reglamento, la fecha y hora de emisión del Certificado se determinará conforme a lo siguiente: el Prestador de Servicios de Certificación deberá llevar un registro del Sistema de Sello o Estampado de Tiempo que se sincronizará con el de la Secretaría, para asegurar la fecha y la hora de la emisión de los certificados generados por el Prestador de Servicios de Certificación. El Prestador de Servicios de Certificación deberá asegurar en todo momento el enlace del Sistema de Sello o Estampado de Tiempo con el de la Secretaría. El Sistema de Sello o estampado de tiempo podrá ser del propio Prestador de Servicios de Certificación o de una persona física o moral que lo lleve en nombre y por cuenta del Prestador de Servicios de Certificación"*.

Al tiempo que para efectos del artículo *"19 del Reglamento, la Secretaría verificará que los Prestadores de Servicios de Certificación cumplan con la estructura de certificados referida en las presentes Reglas Generales en los apartados 2.4.7. al 2.4.7.4., así como con los estándares internacionales, con el Código de Comercio, el Reglamento y estas Reglas Generales, con el objetivo de asegurar que los certificados emitidos por los Prestadores de Servicios de Certificación, en ningún caso, contengan elementos que puedan generar confusión en la Parte que Confía"*

Siendo que para *"los efectos del artículo 104 fracción IV del Código de Comercio, los casos en que estará a disposición el contenido privado del Registro de Certificados de un Prestador de Servicios de Certificación se sujetarán a lo dispuesto por la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental"*.

Finalmente, *"el Prestador de Servicios de Certificación 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 Reglas Generales"*.

Estas son en general las reglas establecidas para el prestador de servicios de certificación por la Secretaría de Economía. De su lectura podemos entender aun más el funcionamiento del prestador de servicios de certificación.

4.1.6. Autoridades Públicas de Certificación

Ya hablamos de la Infraestructura de Clave Pública en el segundo capítulo al tratar diversos aspectos de la firma electrónica avanzada. Por medio de un esquema, explicamos su funcionamiento. Sin embargo para que algunos de los

conceptos que emplearemos en presente apartado sean comprendidos, debemos retomar a la Infraestructura de Clave Pública.

Como primer punto, debemos decir que toda Infraestructura de Clave Pública debe cumplir con ciertos beneficios básicos para las partes como son: confirmar la privacidad de la información enviada, así como la fuente, destino, integridad y calidad de dicha información.

Mencionamos que para conseguir esto, se vale de mecanismos de seguridad, como la firma electrónica avanzada; así como algunas instituciones como: las Agencias Certificadoras (CA), Agencias de Registro (RA) Protocolos de Administración de Certificados (CMP), Repositorios de Certificados y Servidores Time Stamp.

Sobre las Agencias Certificadoras o Prestadores de Servicios de Certificación, debemos aclarar que el término Tercero Confiable "nos indica aquellas asociaciones que suministran un amplio margen de servicios, frecuentemente asociados con el acceso legal a claves criptográficas"²⁵³. En tanto que la Agencia Certificadora (CA), también llamada prestador de servicios de certificación, es como expusimos en el primer apartado del presente capítulo: *la persona o institución pública que preste servicios relacionados con firmas electrónicas y que expide los certificados, en su caso. A su vez, la Agencia de Registro, es la encargada de registrar, publicar, y en dado caso revocar los certificados*

Como podemos ver, la función principal de la Agencia de Certificación va dirigida a la certificación y todas las cuestiones relativas a ésta; pero para fines prácticos a las funciones de certificación se añaden las de registro. Si bien un Tercero Confiable puede actuar como Agencia Certificadora, para que ésta sea considerada como tal, debe cumplir cabalmente con las siguientes funciones: "Generación y Registro de Claves, Identificación de Peticionarios de Certificados, Emisión de certificado, Almacenamiento en la AC de su clave privada (si así lo autoriza el usuario) Mantenimiento de las claves vigentes y revocadas, y Servicios de Directorio"²⁵⁴

"La estructura y el cuadro de funcionamiento de las autoridades de certificación (public key infrastructure) prevén generalmente una estructura jerarquizada a dos niveles: El nivel superior suele estar ocupado por las autoridades públicas, que es la que certifica a la autoridad subordinada, normalmente privada"²⁵⁵

En nuestro país, conforme a lo dispuesto por el artículo 105 del Código de Comercio Vigente "La Secretaría (de Economía) coordinará y actuará como

²⁵³ http://www.informatica-juridica.com/trabajos/firma_digital.asp

²⁵⁴ Reyes Krafft, Alfredo Alejandro. *Ob. cit.* p.172

²⁵⁵ http://www.informatica-juridica.com/trabajos/firma_digital.asp

autoridad Certificadora, y registradora, respecto de los Prestadores de Servicios de Certificación, previstos en el capítulo”. Es decir, la Secretaría de Economía hará las veces de Autoridad Registradora Central en nuestro país.

Aunque para el caso de las Instituciones financieras, o empresas que prestan servicios relacionados con transferencias de fondos o valores, deben de observar lo dispuesto por artículo 106 del Código de Comercio Vigente, que dice: *“Para la prestación de servicios de certificación, las instituciones financieras y las empresas que les presten servicios auxiliares o complementarios relacionados con transferencias de fondos o valores se sujetarán a las leyes que las regulan, así como a las disposiciones y autorizaciones que emitan las autoridades financieras”* sobre esto, el transitorio cuarto de las reformas hechas en materia de comercio electrónico, mencionan: *“por lo que se refiere al artículo 106, el Banco de México, en el ámbito de su competencia, regulará y coordinará a la autoridad registradora central, registradora y certificadora, de las instituciones financieras y de las empresas mencionadas que presten servicios de certificación”*.

El porque de la distinción entre las autoridades que regulan la prestación de servicios de certificación entre entidades financieras y otro tipo de servicios, es comprensible si miramos al trasfondo histórico²⁵⁶.

Desde 1998 se les permitió a los grandes contribuyentes presentar sus declaraciones al Sistema de Administración Tributaria (SAT) por medios electrónicos a través de un certificado digital proporcionado por el propio SAT. Esta infraestructura era proporcionada al SAT por una empresa proveedora del software y licencias, para hacer las veces de Autoridad Certificadora y Registradora.

Lo anterior para fines jurídicos (sobre todo los procesales) resultaba problemático, ya que el SAT hacía las veces de juez y parte, ya que era la entidad que recibía el documento firmado electrónicamente, pero ella misma emitía el certificado. Para solucionar este problema el SAT se une a el Banco de México, para que éste (o bien alguna nueva sociedad mercantil –previa adecuación de su objeto social-) haga las veces de Agencia Registradora Central.

Esto con el fin de que para el 2001 todos los contribuyentes se vieran en la posibilidad de realizar sus declaraciones vía electrónica; para responder así a diversas modificaciones hechas al Código Fiscal de la Federación en materia de declaraciones vía electrónica.

En cuanto a las instituciones financieras, el Banco de México, ha promovido la creación de una infraestructura de seguridad para el uso de medios de identificación de mensajes electrónicos. Esta infraestructura está basada en el sistema de Infraestructura de Clave Pública (clave pública, clave privada, etc.).

²⁵⁶ Cfr. Reyes Krafft, Alfredo Alejandro, Ob. cit. 203 y s.s.

Es por esto, que el Banco de México ocupa un papel preponderante en las transacciones electrónicas entre instituciones financieras y empresas relacionadas. Y ya que este trabajo se enfoca más a cuestiones mercantiles, los aspectos sobre prestadores de servicios de certificación aquí mencionados corresponden en gran medida a los prestadores de servicios de certificación en general.

Esta es la situación de las Autoridades Públicas de Certificación a nivel nacional; para el caso de otros países nos encontramos con:

En los Estados Unidos, no existe una Autoridad Pública de Certificación, el mercado en gran medida está ocupado por empresas privadas (como verisign), aunque existen iniciativas para la creación de una Autoridad Pública de Certificación.

En España, cuentan con el proyecto CERES, que se desarrolla en conjunto por el Consejo Superior de Informática, el Ministro de Economía y Hacienda y Correos y Telégrafos, y el MAP (Ministerio de Asuntos Públicos); que otorga a la Fabrica Nacional de Moneda y Timbre el papel de entidad encargada de prestar servicios que garanticen la validez y seguridad de la emisión y recepción de documentos y calificaciones por medios telemáticos, electrónicos e informáticos.

“Los servicios que está previsto ofrecer son:

- Primarios.- Emisión de certificados, archivo de certificados, generación de claves, archivo de claves, registro de hechos auditables.
- Interactivos.- Registro de usuarios y entidades, revocación de certificados, publicación de políticas y estándares, publicación de certificados, publicación de listas de revocación y directorio seguro de certificados.
- De certificación de mensajes y transacciones.- Certificación temporal, certificación de contenido, mecanismos de no-repudio: confirmación de envío y confirmación de recepción.
- De confidencialidad.- Soporte de mecanismos de confidencialidad, agente de recuperación de claves y recuperación de datos protegidos²⁵⁷.

Para el caso de Italia, la Atorità per l'informatica nella Pubblica Amministrazione (AIPA) ha sido designada como la autoridad nacional de certificación.

En Perú las entidades de Certificación son supervisadas y controladas por una autoridad administrativa designada por el Poder Ejecutivo.

Venezuela cuenta con un órgano de control denominado “Superintendencia de Servicios de Certificación Electrónica”, dependiente del Ministerio de Ciencia y

²⁵⁷ http://www.informatica-juridica.com/trabajos/firma_digital.asp

Tecnología; es un servicio autónomo con autonomía presupuestaria, administrativa, financiera y de gestión, en las materias de su competencia.

Siguiendo el ejemplo de España, Uruguay en el artículo 2 de la ley 16736 de 1995 establece que: "La Administración Nacional de Correos tendrá a su cargo la prestación de servicios postales, esto es la administración, transporte, o distribución y entrega de envíos de correspondencia, giros postales, y productos postales en general"

"Se entiende la correspondencia electrónica como un tipo especial de correspondencia, ya que la diferencia está en el soporte que contiene la información y en la forma de transferirla, por lo cual la certificación está dentro de sus cometidos. A través de la 'Recomendación de la Comisión Nacional de Informática de fecha 25 de septiembre de 1998':se autoriza a la Administración Nacional de Correos a prestar servicios de Autoridad de Certificación en todo el país"²⁵⁸.

4.1.7. Autoridades Privadas de Certificación

Nuestro ordenamiento habla de la prestación de servicios de certificación por entidades privadas. El multicitado artículo 100 del Código de Comercio Vigente en su fracción II menciona que "*Podrán ser prestadores de servicios de certificación: ... II. Las personas morales de carácter privado*". Pero el mismo Código establece en su artículo 101, que para el caso de personas morales, su objeto social, deberá contener las siguientes actividades:

I. Verificación de la identidad de los usuarios y su vinculación con los medios de identificación electrónica;

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 actividad no compatible con las anteriores.

Estas actividades no abarcan simplemente a las que conforme a los parámetros internacionales corresponderían a un prestador de servicios de certificación (o Autoridad Certificadora) en el sentido tradicional; que serían la certificación y todas las cuestiones relativas a ésta. Si no también hablan de atribuciones que corresponderían a la Agencia Registradora. Por lo que el prestador de servicios de certificación de carácter privado en nuestro país hará

²⁵⁸ <http://comunidad.derecho.org/mjviega/publicac/firmele2.htm>

funciones, no sólo de Autoridad Certificadora, sino también de Agencia Registradora, además de otras funciones de tercero confiable.

La prestación de servicios de certificación por particulares ha sido sumamente importante durante la corta histórica de los sistemas de seguridad en el comercio electrónico. Antes de que existieran los ordenamientos jurídicos en materia de prestadores de servicios de certificación, empresas particulares ya se daban a la tarea de prestar servicios de seguridad, aunque por medio de un contrato entre el titular del certificado digital y el proveedor que lo emitía.

Antes de la regulación jurídica actual; la Firma Electrónica y los Certificados Digitales en nuestro país hasta ese momento habían sido desarrollados por La Asociación Nacional del Notariado Mexicano (ANNM) en conjunción con el Colegio Nacional de Contaduría Pública Mexicana y las empresas SeguriDaTA e Infosel.

Después de las reformas hechas al Código de Comercio en Materia de Comercio Electrónico (entre éstas, las que versan sobre prestadores de servicios de certificación) surgieron varias empresas dedicadas a la prestación de servicios de certificación; una de las primeras fue la constituida por Acertia que en conjunción con diversos Fedatarios Públicos (Notarios y Corredores) provee al mercado nacional de servicios de certificación en materia de comercio electrónico; pero un solo prestador de servicios de certificación para el país resulta insuficiente para el creciente mercado nacional (Acertia sólo cuenta con 34 Agentes Certificadores para el territorio nacional)

Por lo que el surgimiento de nuevas empresas resulta natural. Algunas de las empresas privadas que actualmente se preparan para prestar servicios de certificación en nuestro país son: "Sterling Commerce, proveedor de soluciones de integración empresarial, que se ha aliado con Deloitte & Touche para ofrecer una e-notice, una solución que facilitará la utilización de la Factura Electrónica en México. Así como Advantage Security Systems, representante de Verisign en México, ofrece servicios de certificación con infraestructura de llave pública (PKI); además de la ya mencionada Seguridata"²⁵⁹.

Por lo visto no tienen porque existir problemas entre las entidades públicas que pueden prestar servicios de certificación, tales como: la Secretaría de la Función Pública que puede fungir como prestador de servicios de certificación y autorizar como certificadoras a diversas secretarías de estado; la Secretaría de Economía que puede habilitar a fedatarios, empresas e instituciones públicas como prestadores de servicios de certificación el Banco de México, que está en aptitud de emitir certificados digitales a los clientes de la banca, así como el SAT y Seguro Social (aunque estos por disposición de su propia ley sólo pueden emitir certificados relativos a su ámbito de aplicación); y las empresas privadas en nuestro país; ya que en mayor o menor medida están en las reformas hechas en diversos ordenamientos jurídicos.

²⁵⁹ http://www.netmedia.info/bsecure/articulos.php?id_sec=48&id_art=4819&num_page=21075

Pero existen problemas a nivel técnico entre las entidades privadas y las entidades públicas de certificación, ya que el estándar que actualmente desarrolla el Banco de México no toma en cuenta los requisitos de la industria; ya que la mayoría de los proveedores particulares de certificados digitales operan con un sistema denominado OpenSSL, pero paradójicamente, este sistema no es reconocido por Banco de México.

Esto para el caso de México; pero a nivel internacional, existen autoridades de certificación de amplio reconocimiento, entre las que tenemos:

En España, entre los organismos privados más importantes (dedicados principalmente a la certificación financiera corporativa) está la Agencia de Certificación Electrónica (ACE) conformada por Servicios para Medios de Pago S.A (SERMEPA), Confederación Española de Cajas de Ahorro (CECA) y Sistemas 4By Telefónica. También existen terceros confiables como Banesto y el Banco Bilbao Vizcaya.

Bélgica cuenta con un certificador denominado Système Isabel, que provee de servicios de certificación a socios financieros y comerciales. Además de que la Cámara de Comercio Belga, unida a la empresa VERISIGN ha creado un Tercero de Confianza, por medio del que la Cámara de Comercio hace las funciones de Registro y VERISIGN, actúa como emisor de certificados y técnicas.

El mercado Estadounidense de los prestadores de servicios de certificación, ha estado tradicionalmente ocupado por empresas privadas, entre las más importantes (que incluso llegan a tener filiales en otros países) están: NETSCAPE, que en conjunción con la empresa SUN presta servicios de seguridad de redes (Net Security Systems –NSS-), además de una infraestructura de clave pública denominada I-planet.

Asimismo, existe VERISIGN que tan solo en los Estados Unidos maneja aproximadamente el 30% de todas las transacciones en materia de comercio electrónico; provee de servicios de seguridad a nivel de dirección, es una consultora en materia de seguridad, provee soluciones en materia de autenticación en materia de Infraestructura de Clave Pública, "asimismo ofrece la posibilidad de autenticar en Internet un sitio web o una Intranet, bajo identificación de los servidores SSL"²⁶⁰ o Secure Sockets Layer, una tecnología que codifica los paquetes de información enviados.

Del mismo modo, tenemos a RAS Servicios Profesionales de Seguridad, que entre otras cosas presta los siguientes servicios: autorización (Celar Trusa) para la administración de privilegio de acceso; tecnologías de seguridad sobre Autenticación (Secur ID); así como Infraestructura de Clave Pública (RSA Keon) para el encriptamiento y la administración de certificados (B Safe).

²⁶⁰ Reyes Krafft, Alfredo Aejandro. Ob. cit. p.174

4.1.8. Certificados

Al hablar de la certificación en el capítulo segundo, concluimos que conforme al artículo 3° de la Ley Federal de Metrología y Normalización la certificación es el: *procedimiento por el cual se asegura que un producto, proceso, sistema o servicio se ajusta a las normas o lineamientos o recomendaciones de organismos dedicados a la normalización nacionales o internacionales*. Dicho proceso es verificado por una entidad reconocida como independiente o tercera parte de la relación; que por lo general asegura por escrito su conformidad (con la empresa, producto, proceso, servicio o persona). A este escrito se le conoce como certificado, y constituye una valiosa herramienta para las transacciones comerciales internacionales y nacionales, ya que es un generador de confianza entre las partes.

Los prestadores de servicios de certificación para los actos de comercio electrónico también se valen de certificados para la realización de sus funciones; pero estos, no son estrictamente un medio para asegurar su conformidad con determinada empresa; más bien su principal propósito es ser un documento que atestigüe la validez de la identidad de un individuo o entidad. Aun así, son un elemento primordial del prestador de servicios de certificación, por lo que para poder desentrañar la naturaleza jurídica de esta entidad (propósito del presente estudio) debemos abordar al Certificado Digital emitido por los prestadores de servicios de certificación.

4.1.8.1. Concepto

El Código de Comercio Vigente en su artículo 89 define al Certificado como: *Todo mensaje de datos u otro registro que confirme el vínculo entre un firmante y los datos de creación de firma*

Existen otras definiciones de certificado digital en legislaciones internacionales y doctrinarios del comercio electrónico. Y aunque contamos con una definición dada en nuestro Código, siempre es bueno hacer un recuento de las opiniones de otros doctrinarios o legisladores al respecto.

Entre las legislativas está el concepto de la Ley Modelo UNCITRAL sobre Firma Electrónica, que en inciso b) de su artículo 2, establece: *b) Por "certificado" se entenderá todo mensaje de datos u otro registro que confirme el vínculo entre el firmante y los datos de creación de firma.*

En Chile la ley N° 27269, de firmas y certificados digitales (publicada el 28 de Mayo 2000) lo define en su artículo 6° como *el documento electrónico generado y firmado digitalmente por una entidad de certificación que vincula un par de claves con una persona determinada confirmando su identidad.*

Mientras que en Argentina la ley N°25.506 o Ley de Firma Digital en Argentina, en su artículo 13° dice: *Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular.*

Los doctrinarios lo definen como "un archivo que incorpora la clave pública de un sujeto y la relaciona con su clave privada"²⁶¹.

Existen puntos de discrepancia y de convergencia entre las diferentes definiciones; aunque reina la convergencia y el consenso, llegando al punto en que algunas definiciones, como la dada por nuestro Código de Comercio Vigente y la Ley Modelo UNCITRAL sobre Firma Electrónica, son idénticas debido a la necesidad de un consenso internacional en cuanto a términos de comercio electrónico.

En todo caso, la mayoría de las definiciones coinciden en que el certificado electrónico confirma un vínculo, ya bien entre: El firmante y los datos de creación, un par de claves con una persona, los datos de creación de firma, o bien una clave pública con una privada; frases, que palabras más palabras menos, quieren decir lo mismo. En lo que si discrepan es que en dos de ellas se habla de que el certificado es creado por "entidad de certificación" o "certificador" mientras que en otras se omite este dato ya bien, porque más adelante se ocupan de el prestador de servicios de certificación en particular, o porque se sobreentiende.

Para efectos del presente estudio es de suponerse que emplearemos la definición dada por el artículo 89 del Código de Comercio Vigente.

Si bien la validez de un certificado dependerá por una parte en que el prestador de servicios de certificación verifique la identidad del firmante y de certeza sobre tal información; por otro lado la información contenida en certificado también afectará su validez.

Sobre el contenido del certificado digital, podemos decir que la mayoría de los certificados actuales se basan en el estándar X509 v3, inicialmente publicado por el ITU-T X.509 o ISO/IEC/ITU 9594 – 8 en 1998; al que se hicieron varios cambios, hasta llegar a la versión 3 (de junio de 1996), de dicha versión deriva el documento "RFC2459, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List", en el que se enumeran los campos que debe contener un certificado digital, entre los que tenemos²⁶²:

- Número de serie del Certificado emitido por la Autoridad Certificadora
- Algoritmo usado por la Autoridad Certificadora que valida el Certificado
- Nombre de la autoridad generadora del Certificado

²⁶¹ <http://www.cem.itesm.mx/dacs/publicaciones/ogos/libros/firma.pdf>

²⁶² *Ibidem*

- Validez del Certificado
- Nombre del Propietario del Certificado
- Clave pública del Propietario y Algoritmo usado
- Extensiones Usadas
- Firma Digital de la Autoridad Certificadora
- Algoritmo de Firma Digital que fue usado por la Autoridad Certificadora.

Sobre los contenidos del certificado digital, el Código de Comercio Vigente, en su artículo 108 nos dice:

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 demás 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*
- VIII. La referencia de la tecnología empleada para la creación de la Firma Electrónica.*

Si bien los datos antes expuestos son los que todo certificado emitido por un prestador de servicios de certificación autorizado en México debe contener; en ningún caso es limitativo, por lo que se pueden agregar más datos. Comparado con lo expuesto por el documento "RFC2459, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List" nuestro artículo responde completamente a las exigencias de dicho documento; y hasta podríamos decir que va mas allá con fracciones como la séptima donde se establece que los certificados deben de contener: *El alcance de las responsabilidades que asume el prestador de Servicios de Certificación.*

4 1.8.2. Obligaciones de las partes

En un certificado intervienen principalmente tres entidades: el prestador de servicios de certificación, el firmante y quien confía en el certificado. Cada una de las partes debe de cumplir con ciertas obligaciones para que el certificado funcione y sea considerado válido.

4.1.8.2.1. Obligaciones de los prestadores de servicios de certificación

El prestador de servicios de certificación es de suma importancia, ya que es la entidad encargada de la emisión del certificado. Conforme a lo expuesto por nuestro ordenamiento jurídico, sus obligaciones principales serían²⁶³:

1. Actuar conforme a las declaraciones hechas respecto a sus prácticas y normas. Dicha declaración recibirá el nombre de Declaración de Prácticas de Certificación (que retomaremos más adelante), esta declaración, conforma el límite de responsabilidad frente al firmante y al usuario del prestador de servicios de certificación;
2. Actuar con prontitud para comprobar que todas las declaraciones relevantes hechas por el firmante con respecto al certificado o que estén señaladas en él sean cabales y exactas;
3. Suministrar a la parte que confía en el certificado procedimientos accesibles para que esta pueda determinar por medio del certificado:
 - a) La identidad del prestador de servicios de certificación;
 - b) Que los datos de creación de firma eran válidos en la fecha en que se expidió el certificado o antes de ella;
 - c) Que el firmante nombrado en el certificado tenía bajo su control los datos de creación de firma en el momento en que se expidió el certificado;
4. Suministrar a la parte que confía en el certificado procedimientos accesibles para que cuando esto sea procedente, le permitan determinar:
 - a) El mecanismo empleado para comprobar la identidad del firmante;
 - b) Si la clave privada (datos de creación de firma) es válida;
 - c) Las limitaciones existentes en cuanto a los fines o del valor conforme al cual puede emplearse la clave privada (datos de creación de firma) o el certificado;
 - d) Las limitaciones respecto del grado o alcance de la responsabilidad establecida por el prestador de servicios de certificación;
 - e) El método para que el firmante dé aviso de que la clave privada (datos de creación de firma) no puedan estar o no estén en su poder;
 - f) Si existe algún servicio para la revocación oportuna del certificado;

²⁶³ Cfr. <http://www.cem.itesm.mx/dacs/publicaciones/ogos/libros/firma.pdf>

5. Suministrar un medio para que el firmante dé aviso de que la clave privada (datos de creación de firma) no pueda estar o no esté en su poder y, para el caso de ofrecer servicios de Registro de Certificados cerciorarse de que hay un servicio para revocar el certificado;
6. Emplear para la prestación de sus servicios, procedimientos, sistemas y recursos humanos fiables.

En caso de no cumplir con éstas y otras obligaciones legales, el prestador de servicios de certificación enfrentará las consecuencias legales correspondientes. Esto conforma a lo expuesto por el artículo 110 del Código de Comercio Vigente podría ser:

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.

Aunque el siguiente artículo aclara que a pesar de lo expuesto por el 110, debemos tener en cuenta que:

Artículo 111. – Las sanciones que se señalan en este Capítulo se aplicarán sin perjuicio de la responsabilidad civil o penal y de las penas que correspondan a los delitos en que, en su caso, incurran los infractores.

Existen también diversas sanciones señaladas en el Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación en sus artículos: 23,24,25,26,27,28 y29, que citamos en apartados anteriores.

4.1.8.2.2. Obligaciones del Firmante

Para el caso del firmante, cuando pueda emplearse la clave privada (datos de creación de firma) para crear una firma que tenga efectos jurídicos, cada firmante deberá:

1. Ser lo suficientemente diligente para evitar que los datos de la clave privada (datos de creación de firma) sean utilizados de forma no autorizada;
2. Emplear los procedimientos proporcionados por el prestador de servicios de certificación, o por otra parte hacer un esfuerzo razonable, para dar aviso en cualquiera de las siguientes situaciones:

- a) Cuando el firmante tenga conocimiento de que la clave privada (datos de creación de firma) ha quedado en entre dicho; o
 - b) Las circunstancias de que tiene conocimiento el firmante hacen que exista un riesgo considerable de que la clave privada (datos de creación de firma) ha quedado en entre dicho;
3. El caso de que sea empleado un certificado para refrendar la firma electrónica, ser lo suficientemente diligente para constatar que las declaraciones que haya hecho con respecto al certificado o que deban de considerarse en dicho certificado son cabales y exactas.

4.1.8.2.3. Obligaciones de quien confía

La parte que confía conforme al artículo 107 del Código de Comercio tendría las siguientes obligaciones:

Artículo 107. – Serán responsabilidad del Destinatario y de la Parte que Confía, en su caso, las consecuencias jurídicas que entrañe el hecho de que no hayan tomado medidas razonables para:

- I. Verificar la fiabilidad de la Firma Electrónica, o*
- II. Cuando la Firma Electrónica esté sustentada por un Certificado:*
 - a) *Verificar, incluso en forma inmediata, la validez, suspensión o revocación del Certificado, y*
 - b) *Tener en cuenta cualquier limitación de uso contenida en el certificado.*

4.1.8.3. Administración de Certificados

Entre las funciones del prestador de servicios de certificación están "la generación, producción, distribución, control, seguimiento y destrucción de las llaves públicas o privadas asociadas con los certificados de llave pública"²⁶⁴. Todas estas funciones reciben el nombre de administración de certificados, que se vale de dos elementos básicos para cumplir con sus funciones: la Autoridad Certificadora y el Directorio de Servicios.

De las funciones de la Autoridad Certificadora o Prestador de Servicios de Certificación, hemos hablado a lo largo del presente capítulo. Cayendo en la cuenta que de los prestadores de servicios de certificación en México, realizan funciones que van más allá de las que tradicionalmente corresponden a una autoridad certificadora.

²⁶⁴ Reyes Krafft, Alfredo Alejandro. *Ob. cit.* p.192

En cuanto al directorio de servicios, las reglas generales a las que deberán sujetarse los prestadores de servicios de certificación conforme a lo dispuesto por la Secretaría de Economía nos hablan del Modelo Operacional de la Autoridad Certificadora, que sería equivalente al directorio de servicios de que nos habla la teoría. En éste nos habla de los criterios conforme a los cuales operarán y prestarán sus servicios las autoridades certificadoras a efecto de lograr confiabilidad e interoperabilidad, que se 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. Deberá contener también un resumen que incluya: contenido del documento; la historia del posible Prestador de Servicios de Certificación, y Relaciones comerciales con proveedores de insumos o servicios para sus operaciones. Dicho modelo deberá además 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.

4.1.8.4. Registro de Certificados

Conforme a lo expuesto por el artículo 104 fracción IV del Código de Comercio Vigente; entre las obligaciones del prestador de servicios de certificación tenemos: ... *IV. Mantener un registro de Certificados, en el que quedará constancia de los emitidos y figurarán las circunstancias que afecten a la suspensión, pérdida o terminación de vigencia de sus efectos. A dicho registro podrá accederse por medios electrónicos, ópticos o de cualquier otra tecnología y su contenido público estará a disposición de las personas que lo soliciten. El contenido privado estará a disposición del Destinatario y de las personas que lo soliciten cuando así lo autorice el Firmante, así como en los casos a que se refieran las reglas generales que al efecto establezca la Secretaría; ...*

Sobre esto, el Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación, habla de actividades relacionadas con el Registro de Certificados en diversos artículos como son: El artículo 16° que versa sobre la obligación de los prestadores de servicios de certificación de enviar una copia de cada certificado emitido por ellas, vía electrónica a la Secretaría de Economía para que ésta los resguarde; en tanto que en el artículo 19° se establece la obligación de los prestadores de servicios de certificación de emitir, registrar y conservar los certificados en territorio nacional; así como evitar la existencia de elementos de confusión en los certificados. Aunque el artículo 20° nos dice que *"La Secretaría podrá autorizar el resguardo de los Datos de Creación de Firma Electrónica del Prestador de Servicios de Certificación fuera del territorio nacional. En este caso, el Prestador de Servicios de Certificación asumirá los*

costos que impliquen a la Secretaría el traslado de sus servidores públicos para efectuar las visitas de verificación a que se refiere la Sección IV de este Reglamento”.

Al tiempo que en las Reglas Generales a que deberán sujetarse los prestadores de servicios de certificación, nos mencionan en diferentes ocasiones al Registro de Certificados; al hablar de la Infraestructura Informática, nos dice que ésta debe incluir: una Autoridad Certificadora; una Autoridad Registradora; Depósitos para: Datos de Creación de Firma Electrónica del Prestador de Servicios de Certificación 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; una Declaración de Prácticas de Certificación, y los manuales de operación de las Autoridades Certificadora y Registradora.

Mas adelante, las reglas nos mencionan que el solicitante de acreditación y el Prestador de Servicios de Certificación deberá contar con un 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. En dicho modelo también se 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. Para esto el Prestador de Servicios de Certificación 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. El Modelo Operacional de la Autoridad Registradora deberá comprender de igual forma 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.

Para el cumplimiento de estas funciones que la ley establece, la Entidad Certificadora o Autoridad Certificante se vale de la Agencia Certificadora, que es el agente encargado de autenticar la identidad de los Usuarios de la Autoridad Certificadora, para posteriormente enviar la petición de usuario a la Autoridad Certificadora y la clave pública a la Autoridad Registradora.

La Agencia Certificadora es un si un intermediario entre la Autoridad Certificadora y el Usuario, es por así decirlo un “representante local” de la

Autoridad Certificadora, cuya misión es muy importante, ya que del nivel de la calidad del proceso dependerá, el nivel de confianza de los certificados.

4.1.8.5. Declaración de Prácticas de Certificación

Conforme al artículo 103 del Código de Comercio Vigente: *"Las Responsabilidades de las Entidades Prestadoras de Servicios de Certificación deberán estipularse en el contrato con los firmantes"*. El contrato que contiene éstas y otras especificaciones recibe el nombre de Declaración de Prácticas de Certificación.

Conforme a lo expuesto por las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación; en la Declaración de Prácticas de Certificación, que deberá elaborar y mantener actualizado el solicitante de acreditación y el Prestador de Servicios de Certificación, se determinarán: los procedimientos de operación para otorgar certificados y el alcance de aplicación de los mismos; las responsabilidades y obligaciones del Prestador de Servicios de Certificación 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 Prestador de Servicios de Certificación y la forma en que la administración de los certificados emitidos pasará a la Secretaría o a otro Prestador de Servicios de Certificación, 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 Declaración de Prácticas de Certificación deberá ser compatible por lo menos con el estándar ETSI TS 102 042 y el RFC 3647 o el que le sustituya.

4.1.8.6. Lista de Revocación de Certificados

La lista de revocación de certificados permite determinar la validez de un certificado a través de la condensación en una lista; ya que en ella se incluyen todos los certificados que han sido revocados por alguna razón y a la que los

usuarios pueden acceder fácilmente para comprobar la validez de algún certificado.

Esta lista conforme a las Reglas Generales a que deberán sujetarse los prestadores de servicios de certificación, deberán cumplir con las siguientes especificaciones: 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 24 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 Prestador de Servicios de Certificación que la haya emitido, con sus Datos de Creación de Firma.

4.1.8.7. Dispositivos de Almacenamiento Digitales

Además de los sistemas de seguridad aplicados por los prestadores de servicios de certificación, las claves privadas certificados otorgados a los usuarios deben estar protegidos y asegurados, para así garantizar la integridad de los sistemas de seguridad empleados por la infraestructura de clave pública.

Entre los sistemas empleados actualmente para el almacenamiento de claves tenemos: al Browser, Servidor, la Tarjeta de Microcircuito o Chip Card y las Smart Tokens.

Para el caso del Browser, éste se emplea principalmente para las claves privadas generadas por aplicación (como las creadas por exploradores web); en este caso, la clave se almacena en la máquina local del usuario por medio de la modificación local de la configuración de su Browser; su ventaja radica en ser la forma de almacenamiento de certificados y claves más barata; pero con la desventaja de que el certificado o clave solamente podrá ser utilizado desde la computadora donde está almacenado.

En el caso del servidor, la clave se almacena en un servidor, la ventaja que presenta es que se puede acceder al certificado por medio de la clave a través de cualquier computadora; sus desventajas radican en que se depende totalmente de un solo servidor y que el cliente se puede autenticar sin certificado (que como hemos visto es un mecanismo esencial para generación de confianza en las transacciones vía electrónica)

El método considerado como más seguro es el que emplea la tarjeta de microcircuito, tarjeta inteligente o chip card "es un dispositivo con forma de tarjeta

de crédito con un chip en su interior²⁶⁵ en éste se almacena la clave privada del usuario, realizándose internamente todas las funciones criptográficas, tales como la firma digital y la descripción de claves de sesión. Como dijimos su ventaja radica en ser el dispositivo de almacenamiento más seguro hasta el momento, ya que es pequeño, fácil de transportar y difícil de replicar; pero tiene la desventaja de debido a que requiere de un lector especial para poder hacer uso de él, resulta un dispositivo caro, además de que la tecnología empleada por éste todavía no es accesible a todos los usuarios.

Por último, están las Smart Tokens, que emplean una tecnología idéntica a la empleada por las Smart Cards; pero con una forma e interfase distinta, la llamada USB o Universal Standart Bus (empleada por la mayoría de las computadoras actuales), lo que hace que no sean necesarios lectores adicionales como en el caso de la Chip Card, ya que los dispositivos de almacenamiento se conectan directamente al puerto USB.

De todos los anteriores, actualmente los llamados dispositivos de almacenamiento "Smart" son los más comúnmente empleados y aceptados para integrar las aplicaciones del Infraestructura de Cave Publica, dado que proporcionan una autenticación siempre activa.

En el caso de las Agencias Certificadoras, "existen las tarjetas de almacenamiento de certificados, de tal manera que el certificado se almacena dentro de la tarjeta y no en el disco duro. El certificado digital se respalda en dos "Smart Cards" o "Tokens" de una manera que el certificado se divide dentro de los dispositivos para que el certificado no sea almacenado o custodiado por una sola entidad. Algunas de estas tarjetas cumplen con el Estándar Federal de Proceso de Información (FIPS140 – 1 Nivel 3) el cual elimina cualquier información dentro de la tarjeta en caso de que intente abrir para obtener un certificado digital"²⁶⁶

En cuanto a las disposiciones legales en nuestro país, sobre dispositivos de almacenamiento digitales, las Reglas Generales a que deberán sujetarse los Prestadores de Servicios de Certificación señalan que en el Plan de Administración de Claves se deberá entre otras cosas, emplear para el caso del Prestador de Servicios de Certificación, su autoridad certificadora y registradoras, 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.

²⁶⁵ <http://www.cem.itesm.mx/dacs/publicaciones/ogos/libros/firma.pdf>

²⁶⁶ Ibidem

4.1.8.8. Vigencia de los certificados

Al hablar de certificación en general dijimos que una de sus características es la temporalidad; esta característica está presente en los certificados digitales reconocidos por la legislación de nuestro país; tal es el caso de la fracción V. del artículo 108 del Código de Comercio Vigente que al enumerar los datos que deben de contener los certificados digitales para ser considerados válidos nos habla de: “V. *El periodo de vigencia del Certificado;...*”. Sobre esta fracción el artículo 109 del Código de Comercio Vigente señala:

Artículo 109. – Un certificado dejará de surtir efectos para el futuro en los siguientes casos:

Expiración del periodo de vigencia del Certificado, el cual no podrá ser superior a dos años, contados a partir de la fecha en que se hubieran expedido. Antes de que concluya el periodo de vigencia del Certificado, podrá el Firmante renovarlo ante el Prestador de Servicios de Certificación;

Revocación por el Prestador de Servicios de Certificación, a solicitud del Firmante, o por la persona física o moral representada por éste o por un tercero autorizado;

Pérdida o inutilización por daños del dispositivo en que se contenga dicho Certificado;

Por haberse comprobado que al momento de la expedición, el Certificado no cumplió con los requisitos establecidos en la Ley, situación que no afectará los derechos de terceros de buena fe, y

Resolución judicial o de autoridad competente que lo ordene.

Como podemos ver por lo expuesto en la fracción I, el certificado en nuestro país tiene un periodo de vigencia legal de dos años (que por supuesto puede ser renovado) a partir de su expedición. Claro que este periodo depende de la fecha de emisión, que es regulado en nuestro país por los siguientes artículos:

Como primer punto, el ya mencionado artículo 108 del Código de Comercio Vigente al enumerar los datos que deben de contener *los certificados digitales para ser considerados válidos, en su fracción VI nos dice: “VI. La fecha y hora de*

la emisión, suspensión y renovación del certificado” .En tanto que el Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación en su artículo 18° señala: “La Secretaría determinará en las Reglas Generales que expida, la utilización de un sello de tiempo para asegurar la fecha y hora de la emisión, suspensión y revocación del Certificado”.

Las Reglas Generales a que deberán sujetarse los Prestadores de Servicios de Certificación, nos dicen que: *“para los efectos del artículo 108 fracción VI del Código y 18 del Reglamento, la fecha y hora de emisión del Certificado se determinará conforme a lo siguiente: El Prestador de Servicios de Certificación deberá llevar un registro del Sistema de Sello o Estampado de Tiempo que se sincronizará con el de la Secretaría, para asegurar la fecha y la hora de la emisión de los certificados generados por el Prestador de Servicios de Certificación. El Sistema de Sello o Estampado de Tiempo deberá cumplir por lo menos con el estándar internacional Internet X.509 Public Key Infrastructure Time Stamp y considerar el RFC 3161. El Prestador de Servicios de Certificación deberá asegurar en todo momento el enlace del Sistema de Sello o Estampado de Tiempo con el de la Secretaría. El Sistema de Sello o estampado de tiempo podrá ser del propio Prestador de Servicios de Certificación o de una persona física o moral que lo lleve en nombre y por cuenta del Prestador de Servicios de Certificación”.*

4.1.8.9. Los Certificados Extranjeros

En la actualidad las transacciones son instantáneas, aun en el ámbito internacional; como hemos visto el mundo evolucionó con sistemas que permiten respuestas inmediatas entre puntos geográficos distantes, de alguna manera el mundo se ha hecho más pequeño, por lo que se necesita revisar las viejas estructuras, para adaptarlas a las realidades actuales. Entre ellos el derecho y sus referencias de jurisdicción territorial.

Para el caso de los Prestadores de Servicios de Certificación, documentos tales como el Certificado empleado por ellos, no pueden ser circunscritos a una simple realidad nacional, se deben tomar en cuenta las legislaciones internacionales, así como los instrumentos por ellas empleados, ya que no podemos crear figuras jurídicas (sobre todo mercantiles) que solo se sujeten a una realidad nacional; ya que las realidades internacionales hacen necesarias figuras que no solo respondan a nuestro país, si no al resto del mundo.

Por lo que, así como queremos que las figuras en nuestro país resulten válidas para los contextos internacionales; por correspondencia, debemos de reconocer a las figuras creadas por legislaciones extranjeras. En este afán nuestros legisladores dedican uno de los capítulos del apartado Comercio

Electrónico del Código de Comercio Vigente al reconocimiento de los certificados y firmas electrónicas extranjeras. Es el artículo 114 que nos dice:

Artículo 114.- *Para determinar si un Certificado o Firma Electrónica extranjeros producen efectos jurídicos, o en qué medida los producen, no se tomará en consideración cualquiera de los siguientes supuestos:*

- I. *El lugar en que se haya expedido el Certificado o en que se haya creado o utilizado la Firma Electrónica, y*
- II. *El lugar en que se encuentre el establecimiento del prestador de servicios de certificación o del Firmante.*

Todo Certificado expedido fuera de la República Mexicana producirá los mismos efectos jurídicos en la misma que un Certificado expedido en la República Mexicana si presenta un grado de fiabilidad equivalente a los contemplados por este Título.

Toda Firma Electrónica creada o utilizada fuera de la República Mexicana producirá los mismos efectos jurídicos en la misma que una Firma Electrónica creada o utilizada en la República Mexicana si presenta un grado de fiabilidad equivalente.

A efectos de determinar si un Certificado o una Firma Electrónica presentan un grado de fiabilidad equivalente para los fines de los dos párrafos anteriores, se tomarán en consideración las normas internacionales reconocidas por México y cualquier otro medio de convicción pertinente.

Cuando, sin perjuicio de lo dispuesto en los párrafos anteriores, las partes acuerden entre sí la utilización de determinados tipos de firmas electrónicas y Certificados, se reconocerá que ese acuerdo es suficiente a efectos del reconocimiento transfronterizo, salvo que ese acuerdo no sea válido o eficaz conforme al derecho aplicable.

4.1.9. La naturaleza jurídica de la entidad certificadora

¿Cuál es la naturaleza jurídica del prestador de servicios de certificación? Es la duda que motiva el presente estudio, luego del análisis emprendido en los cuatro capítulos que comprenden la presente tesis, podemos hacer algunas de las siguientes afirmaciones.

Primero, debemos aclarar qué es naturaleza jurídica. La palabra naturaleza tiene connotaciones muy amplias, existen numerosas definiciones y sentidos de ésta. Los diccionarios generales nos dicen que es la "esencia y propiedad característica de cada ser. Virtud calidad o propiedad de las cosas"²⁶⁷. En tanto

²⁶⁷ Raluy Poudevida, Antonio. Ob. cit. p.508

que los diccionarios jurídicos hacen alusión a cuestiones filosóficas para explicar el término, al respecto nos dan diversas definiciones, en una se nos dice que la naturaleza "es el principio que provoca y gobierna el desarrollo de un ser tendiendo a realizar en el cierto tipo"²⁶⁸; a decir de los estudiosos del Derecho, este sentido es propio de los temas relativos al Derecho Natural.

En otro sentido de naturaleza es el de "principio fundamental de todo juicio normativo"²⁶⁹ En tanto que en un tercer sentido naturaleza puede significar "todo lo que es innato, instintivo, espontáneo"²⁷⁰ Aunque también naturaleza significa el "conjunto de propiedades de un género"²⁷¹. O bien un "principio de operación que escapa a la voluntad libre"²⁷²

En todo caso el significado que debemos adoptar, conforme a los teóricos, para definir la naturaleza de una Institución o un acto a la luz del derecho, es decir, la naturaleza jurídica (recordemos que decir que algo es jurídico, hace referencia a que atañe al derecho, se ajusta a él o bien es "relativo al derecho"²⁷³) es la de esencia de un género, es decir, el "conjunto de propiedades de un género"²⁷⁴, género a su vez se definiría como "una clase, es decir como un conjunto de objetos que poseen, todos ellos y solamente ellos, determinados caracteres comunes"²⁷⁵.

Tomando dicho significado como guía, la naturaleza jurídica, sería "el conjunto de propiedades que permiten definir, entre otros objetos, un sector que presenta características comunes (la juridicidad) y al cual llamamos 'lo jurídico'"²⁷⁶. Pero teniendo en cuenta que "como la de cualquier clase de objetos, la naturaleza del derecho (jurídica) se expresa mentalmente en un concepto, y éste se desarrolla mediante la definición correspondiente"²⁷⁷, está claro que nuestra búsqueda se enfocara a la expresión de un concepto y definición de la naturaleza jurídica de la entidad certificadora, donde se expongan las características comunes de juridicidad que la hacen pertenecer a cierta categoría jurídica.

El prestador de servicios de certificación o entidad certificadora, es una figura jurídica mercantil establecida en el artículo 89 el Código de Comercio vigente donde es definida como "*La persona o institución pública que preste servicios relacionados con firmas electrónicas y que expide certificados en su caso*". Surge de la mano de la figura de la firma electrónica avanzada y todas las técnicas criptográficas creadas para preservar la seguridad en las transacciones

²⁶⁸ Enciclopedia Jurídica Omeba. Tomo XX. Driskell S.A. Buenos Aires 1990 p.70

²⁶⁹ Idem p.71

²⁷⁰ Ibidem

²⁷¹ Ibidem

²⁷² idem p. 73

²⁷³ De Pina Vara, Rafael. Ob. cit. p. 339

²⁷⁴ Enciclopedia Jurídica Omeba. Tomo XX. Driskell S.A. Buenos Aires 1990 p.71

²⁷⁵ Ibidem

²⁷⁶ Ibidem

²⁷⁷ Ibidem

informáticas; con el paso del tiempo se descubrió que simples criptogramas que aseguraran fiabilidad no eran suficientes, por lo que la figura de un tercero confiable (como el prestador de servicios de certificación) se hizo necesaria para asegurar aun más las transacciones vía informática. Siendo así que la función primordial de los prestadores de servicios de certificación es hacer las transacciones más seguras (esto se logra a través de protocolos TTP)

El prestador de servicios de certificación es una persona jurídica colectiva (el Código de Comercio la describe como tal), es decir, una persona moral. Las personas morales conforme a nuestra doctrina y ordenamiento jurídico son "una entidad dotada de existencia jurídica, susceptible o capaz de ser titular de derechos subjetivos, facultades, obligaciones y responsabilidades jurídicas"²⁷⁸ Contando con los mismos atributos que las personas físicas (capacidad, patrimonio, denominación o razón social, domicilio y nacionalidad) excepto por el de Estado Civil, además de tener una capacidad jurídica restringida, ya que solo pueden contraer ciertas obligaciones y adquirir determinados derechos. Pero, qué tipo de persona moral es; en principio podríamos afirmar que es la persona moral que presta *servicios relacionados con firmas electrónicas y que expide certificados en su caso*.

Pero la definición dada por el artículo 89 del Código de Comercio nos dice "La persona o *institución pública*..." por lo que es preciso definir el concepto Institución Pública aplicado a la Entidad Certificadora. La palabra Institución tiene numerosos usos en el vocabulario jurídico; en un primer sentido, los juristas entienden por Institución como "los elementos o principios de la ciencia del derecho o de cualquier disciplina jurídica o bien, textos o libros que contienen los principios o aspectos fundamentales del derecho"²⁷⁹ Pero para la sociología jurídica y la teoría del derecho es el "conjunto de reglas, normas, valores y costumbres que rigen un cierto comportamiento social claramente identificado"²⁸⁰.

No obstante los usos más modernos de Institución la ven como: 1. "un conjunto firmemente establecido de prácticas que las normas jurídicas reúnen o agrupan (e.g. la familia)"²⁸¹ y 2. Un "establecimiento, organización (ente público) o instancia (órgano o agencia) dotado de funciones sociales específicas"²⁸². Hasta aquí los sentidos dogmáticos, pero existen definiciones legales al respecto, tal es el caso de la Ley del Trabajo de los Servidores Públicos del Estado y Municipios (del Estado de México), que menciona en su artículo 4º "*Para efectos de esta ley se entiende(...)*III. *Por institución pública, cada uno de los poderes públicos del Estado, los ayuntamientos y los tribunales administrativos, así como los*

²⁷⁸ Tamayo y Salmoran, Rolando. Elementos para una Teoría General del Derecho (Introducción al Estudio de la Ciencia Jurídica) 2ª ed. Temis, México, 1998

²⁷⁹ Instituto de Investigaciones Jurídicas. Diccionario Jurídico Mexicano (I -O) 14ª ed. Editorial Porrúa, México, 2000 p.174

²⁸⁰ *Ibidem*

²⁸¹ *Idem* p. 1747

²⁸² *Ibidem*

organismos auxiliares de carácter estatal y municipal". Esta definición se ajustaría al segundo significado que los dogmáticos dan de Institución, lo que nos llevaría a las siguientes consideraciones sobre las Instituciones Jurídicas.

Siguiendo lo expuesto por la Ley, las Instituciones Públicas al ser figuras relativas a las cuestiones del Estado, entrarían al rubro del Derecho Administrativo, dentro del cual según sus teóricos tendríamos que observar lo siguiente: "Los entes públicos, dentro de los que consideramos al Estado (Federación), las entidades federativas, los municipios, los organismos descentralizados y las demás personas jurídicas colectivas del Derecho Público, tiene ciertas características constantes desde el punto de vista genérico aunque desde el punto de vista específico pueden presentar algunas variaciones. Estas características son(...) 2. La personalidad jurídica distinta de la de sus integrantes. La personalidad jurídica colectiva existe y es distinta de la personalidad individual de cada uno de los integrantes del ente colectivo"²⁸³

El hablar de una personalidad colectiva no es otra cosa que hablar de una persona moral por lo que las Instituciones Públicas serían personas morales, este criterio se ve reforzado por lo expuesto por el artículo 25° del Código Civil para el Distrito Federal Vigente, que en cuanto a personas morales nos dice:

Son personas morales:

- I. La Nación, los Estados y los Municipios;*
- II. Las demás corporaciones de carácter público reconocidas por la Ley;*
- III. Las Sociedades Civiles y Mercantiles;*
- IV. Los sindicatos, las asociaciones profesionales y las demás a que se refiere la fracción XVI del artículo 123 constitucional;*
- V. Las sociedades cooperativas y mutualistas; y*
- VI. Las Asociaciones distintas a las enumeradas que se propongan fines políticos, científicos, artísticos, o cualquier otro fin lícito, siempre que no fueran desconocidas por la ley.*

El propio Código hace mención de Instituciones Públicas haciendo las veces de entidad certificadora; en primer lugar, el artículo 100 del Código de Comercio Vigente, al hacer un listado de las entidades que podrán ser prestadores de servicios de certificación, menciona en su tercer numeral: "*III. Las Instituciones Públicas, conforme a las leyes que les son aplicables*" Posteriormente, los artículos 105 y 106 del mismo Código, nos dicen: artículo 105 "*La Secretaría (de Economía) coordinará y actuará como autoridad certificadora, y registradora, respecto de los prestadores de servicios de certificación previstos en el capítulo*". Artículo 106 "*Para la prestación de servicios de certificación, las instituciones financieras y las empresas que les presten servicios auxiliares o complementarios relacionados con transferencias de fondos o valores se sujetarán a las leyes que las regulan, así como a las disposiciones y autorizaciones que emitan las autoridades financieras*" sobre esto, el transitorio cuarto de las reformas hechas en

²⁸³ Acosta Romero, Miguel. *Compendio de Derecho Administrativo*. 3ª ed. Editorial Porrúa. México 2001 p.55

materia de comercio electrónico menciona: "por lo que se refiere al artículo 106, el Banco de México, en el ámbito de su competencia, regulará y coordinará a la autoridad registradora central, registradora y certificadora, de las instituciones financieras y de las empresas mencionadas que presten servicios de certificación".

Así, ya que la Institución Pública puede ser agrupada en el rubro de las personas morales, para este caso, serían lo mismo. Ahora bien, el hablar de una "Institución Pública" hace referencia a lo público que "por oposición a privado, dicese de todo aquello que atañe o interesa al Estado o a la comunidad (la sociedad)"²⁸⁴. Queda claro que las instituciones que hagan las veces de prestadores de servicios de certificación son públicas, ya que están así contempladas por la ley, además de doctrinalmente ser agrupadas dentro del Derecho Administrativo (rama del Derecho Público). La duda sería si las funciones que realizan son funciones públicas o bien funciones de interés público.

Al respecto se dice que la función pública es una "actividad dirigida en la realización de alguno de los servicios correspondientes al Estado, municipio o, en general, a cualquier organismo público"²⁸⁵ en tanto que interés público es "El conjunto de pretensiones relacionadas con las necesidades colectivas de los miembros de una comunidad y protegidas mediante la intervención directa y permanente del Estado... pretensiones que son compartidas por la sociedad en su conjunto, y cuya satisfacción origina beneficios para todos los integrantes de una colectividad"²⁸⁶

Pensamos que la actividad del prestador de servicios de certificación es una función de interés público, debido a que, si bien las actividades de certificación del prestador (que analizaremos más adelante) son "una necesidad colectiva de la comunidad" no terminan de ser una "actividad dirigida en la realización de alguno de los servicios correspondientes al Estado..." Entendamos que aunque son "pretensiones compartidas por la sociedad en su conjunto, y cuya satisfacción origina beneficios para todos los integrantes de una colectividad"; no son uno de los servicios que estrictamente le corresponderían al Estado (por lo que no son funciones públicas) pero, como en el caso de la regulación jurídica del prestador de servicios de certificación (que era una figura empleada previamente por la práctica) están "protegidas mediante la intervención directa y permanente del Estado".

Siguiendo el orden de la exposición, debemos retomar lo dicho sobre *servicios relacionados con firmas electrónicas y que expide certificados en su caso*. Esta, hace necesario aclarar algunos puntos, como ¿por qué el prestador de servicios de certificación recibe ese nombre?, ¿qué lleva a darle ese calificativo a esta persona moral?

²⁸⁴ De Pina, Rafael. Ob.cit. p.426

²⁸⁵ Idem p.296

²⁸⁶ http://senado.gob.mx/gaceta.php?lg=59lk=31/6_dict_primera/ley_aguas_nacionales.htm

En el capítulo tercero mencionamos que la certificación en general, es definida por la mayoría de los autores, como una “acción llevada a cabo por una entidad reconocida como independiente de las partes interesadas, mediante la que se manifiesta la conformidad de una empresa, producto, proceso, servicio o persona con los requisitos definidos en normas o especificaciones técnicas”²⁸⁷ Esta entidad reconocida como independiente o tercera parte de la relación (certificador), por lo general asegura por escrito su conformidad (con la empresa, producto, proceso, servicio o persona). A este escrito se le conoce como certificado, y constituye una valiosa herramienta para las transacciones comerciales internacionales y nacionales, ya que es un generador de confianza entre las partes.

Los prestadores de servicios de certificación (Entidades de Certificación) se ajustan a esta definición, ya que son terceros confiables que aseguran que la clave pública corresponde a una determinada persona a través de ciertas políticas operativas, el otorgamiento de certificados, mecanismos de seguridad, como la firma electrónica avanzada; así como algunas instituciones como: las Agencias Certificadoras (CA), Agencias de Registro (RA) Protocolos de Administración de Certificados (CMP), Repositorios de Certificados y Servidores Time Stamp, entre otros.

Sobre las Agencias Certificadoras, debemos aclarar que el término Tercero Confiable “nos indica aquellas asociaciones que suministran un amplio margen de servicios, frecuentemente asociados con el acceso legal a claves criptográficas”²⁸⁸. En tanto que la Agencia Certificadora (CA), también llamada prestador de servicios de certificación, es: *la persona o institución pública que preste servicios relacionados con firmas electrónicas y que expide los certificados, en su caso*. A su vez, la Agencia de Registro, es la encargada de registrar, publicar, y en dado caso revocar los certificados.

Siendo que la función principal de la Agencia de Certificación va dirigida a la certificación y todas las cuestiones relativas a ésta; pero para fines prácticos a las funciones de certificación se añaden las de registro. Si bien un Tercero Confiable puede actuar como Agencia Certificadora, para que ésta sea considerada como tal, debe cumplir cabalmente con las siguientes funciones: “Generación y Registro de Claves, Identificación de Peticionarios de Certificados, Emisión de certificado, Almacenamiento en la AC de su clave privada (si así lo autoriza el usuario) Mantenimiento de las claves vigentes y revocadas, y Servicios de Directorio”²⁸⁹

“La estructura y el cuadro de funcionamiento de las autoridades de certificación (public key infrastructure) prevén generalmente una estructura jerarquizada a dos niveles: El nivel superior suele estar ocupado por las

²⁸⁷ <http://www.aenor.es/desarrollo/certificacion/quees/queescertificacion.asp>

²⁸⁸ http://www.informatica-juridica.com/trabajos/firma_digital.asp

²⁸⁹ Reyes Krafft, Alfredo Alejandro. *Ob. cit.* p.172

autoridades públicas, que es la que certifica a la autoridad subordinada, normalmente privada”²⁹⁰

En nuestro país, conforme a lo dispuesto por el artículo 105 del Código de Comercio Vigente *“La Secretaría (de Economía) coordinará y actuará como autoridad Certificadora, y registradora, respecto de los Prestadores de Servicios de Certificación, previstos en el capítulo”*. Es decir, la Secretaría de Economía hará las veces de Autoridad Registradora Central en nuestro país.

Mientras que la prestación de servicios de certificación por entidades privadas, no abarcan simplemente a las que conforme a los parámetros internacionales corresponderían a un prestador de servicios de certificación (o Autoridad Certificadora) en el sentido tradicional; que serían la certificación y todas las cuestiones relativas a ésta. Si no también hablan de atribuciones que corresponderían a la Agencia Registradora. Por lo que el prestador de servicios de certificación de carácter privado en nuestro país hará funciones, no sólo de Autoridad Certificadora, sino también de Agencia Registradora, además de otras funciones de tercero confiable.

Siendo así que entre las obligaciones del prestador de servicios de certificación con respecto a la firma electrónica tendríamos: comprobar la identidad de los solicitantes y otras cuestiones pertinentes para la emisión de certificados; poner a disposición del firmante los dispositivos de generación de los datos de creación y de verificación de la firma electrónica; Dar informes sobre el precio, las condiciones de utilización, las limitaciones de uso y la forma en que se garantiza una posible irresponsabilidad del certificado; mantener un registro de certificados; guardar confidencialidad sobre la información recibida; en el caso del cese de actividades el prestador deberá comunicar a la Secretaría para así determinar el destino de registros y archivos; establecer medidas para asegurar la confidencialidad y la no alteración de los certificados y datos en el proceso de generación de firma; establecer declaraciones sobre normas y procedimientos; proporcionar los medios de acceso a la parte que confía para que pueda determinar (artículo 104 Código de Comercio Vigente): *“a) La identidad del prestador de servicios de certificación; b) que el firmante nombrado en el certificado tenía bajo su control el dispositivo y los datos de creación de firma en el momento en que se expidió el certificado; c) Que los datos de creación de firma eran válidos en la fecha en que se expidió el certificado; d) El método utilizado para identificar al firmante; e) cualquier limitación en los fines o el valor respecto de los cuales puedan utilizarse los datos de creación de la firma o el certificado; f) cualquier limitación en cuanto al ámbito o el alcance de la responsabilidad indicada por el prestador de servicios de certificación; g) Si existe un medio para que el firmante de aviso al prestador de servicios de certificación de que los datos de creación de la firma han sido de alguna manera controvertidos, y h) si se ofrece un servicio de terminación de vigencia del certificado”*.

²⁹⁰ http://www.informatica-juridica.com/trabajos/firma_digital.asp

En cuanto a la función certificadora de los prestadores de servicios de certificación, y los certificados emitidos por éstas, en el capítulo tercero establecimos las diferencias entre certificación y fe pública. La Fe Pública tiene cuatro características esenciales: Consta documentalmente, proviene del Estado, es un imperativo jurídico, y es oponible a cualquiera (erga omnes). En tanto que la certificación, si bien "puede" constar por escrito (al documento donde consta por escrito se le llama certificado); en ningún momento es imperativa, de hecho una de las características de la certificación es el ser voluntaria, es decir no existe algún elemento coercitivo en su aplicación, por lo tanto no es oponible a terceros; y en todo caso, el aceptarla o no, como válida, dependerá del criterio del particular.

Además de que la fe pública proviene del Estado que enviste a un particular (notario, secretario, funcionario público, etc.) de fe pública; en tanto que la certificación es otorgada por un tercero independiente (organismo de certificación) que no está investido de fe pública y cuya certeza en todo caso radica en el ser aceptado como tal por la confiabilidad, imparcialidad, veracidad y equidad demostrada en otros casos. Sólo se encargan de brindar certeza sobre determinados productos, procesos, etc. siguiendo determinados lineamientos y requisitos éticos. Si bien, los organismos de certificación son reconocidos y regulados por el ordenamiento jurídico (para este propósito se crearon organismos como la Dirección General de Normas y la Entidad Mexicana de Acreditación), en ningún caso se les otorgan funciones de fedatarios.

En cuanto a las características de la certificación, mencionamos dos: el ser temporal y su carácter voluntario. Ya hablamos de la voluntariedad, y en cuanto a la temporalidad, podemos decir que ésta alude a que la certificación cuenta con cierto tiempo de vigencia, que deberá de ser renovado continuamente; esto es distinto a los criterios adoptados para fe pública, ya que, un instrumento donde conste fe pública será perpetuamente válido, se podrá atacar en todo caso a su autenticidad, pero no a su vigencia, como en el caso de la certificación.

Las anteriores razones nos hacen entender porqué un prestador de servicios de certificación encuadra más en la figura de un tercero certificador que en la otras instituciones jurídicas como el fedatario. Lo que se reflejará en los efectos jurídicos de un certificado o una certificación, que si bien puede ayudar para fines probatorios y de atribución de firma (recordemos lo establecido por el artículo 93 del Código de Comercio Vigente²⁹¹) siempre será objeto de valoración

²⁹¹ **Artículo 93.** Cuando la ley exija la forma escrita para los actos, convenios o contratos, este supuesto se tendrá por cumplido tratándose del mensaje de datos, 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. Cuando adicionalmente la ley exija la **firma de las partes**, dicho requisito se tendrá por cumplido tratándose de mensajes de datos, siempre que sea **atribuible** a dichas partes.

En los casos en que la ley establezca como requisito que un acto jurídico deba otorgarse en **instrumento ante fedatario público**, este y las partes obligadas podrán, a través del mensaje 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 atribuyen dichos mensajes a las partes y conservar

del juzgador, debido a que si bien la actividad del prestador de servicios de certificación es de carácter público, el documento por él emitido no conlleva fe pública; por lo que, se le podría considerar como un documento privado con un poco más de certidumbre. A más de ser un documento afectado de temporalidad, que solo será válido por un periodo determinado de tiempo, entre otras cuestiones.

Así, ya que la búsqueda de la presente tesis es el "conjunto de propiedades que permiten definir, entre otros objetos, un sector que presenta características comunes (la juridicidad) y al cual llamamos 'lo jurídico'²⁹², es decir, naturaleza jurídica. La suma de todo lo expuesto en el presente apartado sería lo que consideramos como las propiedades y características comunes del prestador de servicios de certificación (entidad certificadora), es decir, su naturaleza jurídica.

Pero en un afán de conceptualizar podríamos decir que la naturaleza jurídica de la entidad certificadora (prestador de servicios de certificación) **Es una persona moral que presta servicios relacionados con firmas electrónicas y que expide certificados en su caso. A la que la ley se refiere también como Institución pública²⁹³, que para el caso de la entidad certificadora es lo mismo que decir persona moral; cuya función principal va dirigida a la certificación y todas las cuestiones relativas a ésta, que en todo caso son funciones de interés público**

4.1.10. La necesidad de la prestadora de servicios de certificación basándose en el criterio de que la confianza es la variable crítica para incentivar el desarrollo del comercio electrónico.

Como vimos en nuestro recuento histórico el comercio surge y se desarrolla casi paralelo a las sociedades humanas. Parte de simples trueques tribales hasta llegar a las complejas transacciones de nuestros días. El comercio es una actividad en constante expansión; hoy en día no conoce de fronteras o límites materiales para su desarrollo. Fenómenos como el comercio electrónico (nacido a raíz de los desarrollos en computadoras y redes), han posibilitado transacciones instantáneas entre lugares distantes, que décadas atrás habrían parecido inimaginables.

El comercio electrónico es el reto presente del comercio; el Derecho Mercantil, que siempre ha auxiliado y se ha retroalimentado de la actividad comercial, debe apoyar el crecimiento de esta nueva modalidad comercial, tal como lo hizo siglos atrás al reconocer figuras como la letra de cambio, cheque o pagaré, que en ese entonces fueron tan novedosas como el comercio electrónico

bajo su resguardo una versión íntegra de los mismos para su ulterior consulta, otorgando dicho documento de conformidad con la legislación aplicable que lo rige.

²⁹² *Ibidem*

²⁹³ Cada uno de los poderes públicos del Estado, los ayuntamientos y los tribunales administrativos, así como los organismos auxiliares de carácter estatal y municipal

de nuestros días. Debe crear un marco legal para el desarrollo de esta nueva modalidad comercial, ya sea mediante el desarrollo de instituciones que auxilien a esta práctica, o bien por medio del reconocimiento de figuras ya empleadas por el medio comercial. El desarrollo o fracaso futuro del comercio electrónico en gran medida dependerá de la habilidad del Derecho de dotar de figuras a esta nueva modalidad comercial.

Aun falta mucho, pero se han hecho algunos avances significativos. A nivel internacional son numerosas las legislaciones que reconocen diversos aspectos y figuras empleadas por el comercio electrónico. En nuestro país se han hecho diversas modificaciones a algunos Códigos (tal es el caso del Código de Comercio) a lo largo del último siglo para reconocer y validar diversos aspectos del comercio electrónico.

Una de las figuras reconocidas en las últimas modificaciones hechas al Código de Comercio, es el prestador de servicios de certificación. Una Persona moral encargada de validar y certificar las cuestiones relativas a la firma electrónica y los certificados digitales. Su importancia radica en brindar certidumbre en las transacciones vía electrónica mediante mecanismos de aseguramiento de personalidad de partes, claves, certificados, etc.

Consideramos que la función del prestador de servicios de certificación es de vital importancia para el desarrollo futuro del comercio electrónico, ya que precisamente, entre las limitantes de éste, están la ausencia de las partes y la incertidumbre de un medio de realidades poco tangibles. Por lo que una institución que otorgue certidumbre en un medio tan intangible e inseguro, puede ser la variable crítica que impulse o aplaste su desarrollo.

Es por esta y otras razones que el prestador de servicios de certificación (entidad certificadora) debe ser una figura amplia y exhaustivamente estudiada y regulada por los juristas y legisladores de nuestro país.

CONCLUSIONES

1. Entre los animales la idea del lucro o intercambio nunca está presente, ya que no son capaces de efectuar las abstracciones intelectuales necesarias para otorgarle valor a los bienes.
2. El Derecho Mercantil es una herramienta valiosa para el desarrollo del tráfico comercial (cualquiera que sea la modalidad que asuma) capaz de cristalizar dentro de sus ordenamientos y codificaciones de Derecho, instituciones que la costumbre comercial utiliza.
3. La rápida transformación histórica del Derecho mercantil, el continuo ensanchamiento del ámbito comercial y la insistente especialización de dicho Derecho, hacen que el intento de dar una definición de que se ajuste a todos los tiempos y circunstancias sea prácticamente imposible
4. En el caso de las transacciones comerciales electrónicas, el contrato se ha perfilado como el más importante de los instrumentos empleados, ya que es capaz de generar vínculos entre las partes; pero además es una figura lo suficientemente flexible para cumplir con las necesidades comerciales particulares de las transacciones electrónicas.
5. El contrato electrónico es igual a cualquier contrato tradicional (por lo que la definición de contrato dada por nuestro Código Civil es válida para éste) sólo cambia la forma de expresión de la voluntad en éste, que en todo caso es por medios electrónicos.
6. En un afán de otorgar seguridad a esta nueva modalidad comercial, y permitir con esto un mejor desarrollo la tecnología ha traído diversas formas de protección de información, como lo son la firma electrónica y los certificados digitales, que el Derecho se ve en la necesidad de regular, por la importancia que han adquirido en los últimos tiempos en el ámbito comercial
7. El principio de equivalencia funcional establecido por los legisladores en las reformas hechas al Código de Comercio en materia de Comercio Electrónico hace que el mensaje de datos, sea equivalentemente funcional a cualquier otro documento jurídico, lo que plantea la posibilidad de que un mensaje de datos pueda ser privado o público, dependiendo de las características legales que éste presente.
8. Los criterios sobre firma electrónica, mensaje de datos, entidad certificadora, y otros relativos al comercio electrónico son casi unánimes a nivel internacional a pesar de lo discrepante de los sistemas legales en nuestro planeta. Muchas de las definiciones adoptadas por nuestros legisladores están basadas en reglas

aceptadas internacionalmente; con el fin de facilitar la tarea a las empresas mexicanas en las transacciones internacionales.

9. La firma electrónica avanzada, hace posible entre otras cosas: la Autenticación (Identifica al usuario que ha enviado el mensaje); la Autorización (el asegurar que es la persona indicada para llevar a cabo la operación concreta); la Privacidad (Garantizar que nadie más verá los mensajes); la Integridad: (Garantiza que no se ha alterado el mensaje) y el No repudio (Nadie excepto el emisor podría haber firmado el documento).
10. Los primeros pasos hacia la seguridad en materia electrónica nos lo dan los sistemas de encriptación asimétrica basados en complejos sistemas matemáticos y tecnológicos. Pero, no son suficientes, para lograr que una firma electrónica avanzada sea lo bastante confiable para las transacciones vía electrónica se necesita de una estructura más compleja. Es para eso que surge la "Open Public Key Infrastructures" (PKI) o Infraestructura de Clave Pública.
11. Las técnicas de seguridad como firma electrónica, certificados digitales, etc. están enfocadas a la modalidad comercial Business to Business, o en todo caso Business to Administration debido a que los costos y estructura necesaria para ser implementados solo pueden ser asumidos por instituciones de este tipo.
12. Para los particulares o consumidores finales existen otro tipo de mecanismos de protección como los Números de identificación personal o NIP bancarios, las tarjetas plásticas con chips, etc. Que quizás no son tan seguros como la firma electrónica, los certificados digitales y otras figuras de seguridad digital; pero son suficientemente seguras para las pequeñas transacciones comerciales y su costo.
13. El desarrollo en tamaño y complejidad de las comunidades; provocó que sus miembros se vieran imposibilitados de presenciar los actos jurídicos de otros conciudadanos; por lo que se creó un sistema que obligara a la colectividad a tener como ciertas algunas afirmaciones; surgiendo así la fe pública como un medio para hacer que los actos celebrados por algunos debieran ser tomados como verdaderos por otros de manera obligatoria.
14. La importancia del organismo de certificación es medular ya que debe ser una entidad lo suficientemente acreditada y confiable para que sus determinaciones y criterios sean reconocidos por las otras partes.
15. Mientras la fe pública nace como la necesidad del Estado de investir a ciertos individuos de la capacidad de otorgarla, para así responder a la exigencia social de certidumbre sobre diversos actos. La certificación es un procedimiento autorregulatorio que no es coercitivo (ya que no emana de ninguna entidad investida de fe pública) pero que debido a criterios éticos y consensuales empleados durante el proceso de certificación, es considerada

un mecanismo válido para dotar de certeza a diversos procesos donde la figura del fedatario no resulta fundamentalmente necesaria, y por lo tanto puede dejarse el arbitro de otros individuos.

16. El prestador de servicios de certificación surge de la mano de la figura de la firma electrónica avanzada, y todas las técnicas criptográficas creadas para preservar la seguridad en las transacciones informáticas. Debido a que los sistemas de seguridad eran muy simples en principio, pero con el paso del tiempo se vio que simples criptogramas que aseguraran fiabilidad no eran suficientes, por lo que la figura de un tercero confiable (como el prestador de servicios de certificación o entidad certificadora) se hizo necesaria para asegurar aun más las transacciones vía informática.
17. La función primordial (a la que se suman otras) de los prestadores de servicios de certificación es hacer que las transacciones electrónicas sean más seguras, pues las entidades de certificación no realizan las transacciones mas seguras, solo hacen que las hechas por otros lo sean.
18. Los sistemas de comunicación actuales hacen que sea instantánea entre puntos geográficos distantes, por lo que documentos como el Certificado emitido por las entidades certificadoras no pueden ser circunscritos a una simple realidad nacional, para su creación, se deben tomar en cuenta las legislaciones internacionales, así como los instrumentos por ellas empleados.
19. Los prestadores de servicios de certificación (Entidades de Certificación) son terceros confiables que aseguran que la clave pública corresponde a una determinada persona a través de ciertas políticas operativas, el otorgamiento de certificados, mecanismos de seguridad, como la firma electrónica avanzada; así como algunas instituciones como: las Agencias Certificadoras (CA), Agencias de Registro (RA) Protocolos de Administración de Certificados (CMP), Repositorios de Certificados y Servidores Time Stamp, entre otros.
20. La naturaleza jurídica de la entidad certificadora (prestador de servicios de certificación) es una persona moral que presta servicios relacionados con firmas electrónicas y que expide certificados en su caso, a la que la ley se refiere también como Institución pública²⁹⁴, decir persona moral, cuya función principal va dirigida a la certificación y todas las cuestiones relativas a ésta, que en todo caso son funciones de interés público

²⁹⁴ Cada uno de los poderes públicos del Estado, los ayuntamientos y los tribunales administrativos, así como los organismos auxiliares de carácter estatal y municipal

GLOSARIO²⁹⁵

ADSL: Abreviación de Asymmetric Digital Subscriber Line, el ADSL es un método de transmisión de datos a través de las líneas telefónicas de cobre tradicionales a velocidad alta. Los datos pueden ser descargados a velocidades de hasta 1.544 Megabits por segundo y cargados a velocidades de hasta 128 Kilobits por segundo. Esa es la razón por la cual se le denomina asimétrico. Esta tecnología es adecuada para el web, ya que es mucho mayor la cantidad de datos que se envían del servidor a un ordenador personal que lo contrario.

ASCII: Abreviación de American Standard Code for Information Interchange, un código de 7-bit que sustituye las letras del alfabeto romano por cifras y otros caracteres informáticos. Los caracteres ASCII permiten comunicar con ordenadores, que utilizan un lenguaje especial llamado binario formados por ceros y unos. Al escribir en el teclado, el ordenador interpreta cada letra escrita en lenguaje binario ASCII, para que puedan ser leídas, manipuladas, almacenadas o recuperadas. Los ficheros ASCII son denominados ficheros de texto.

Base de datos: Una base de datos es un formato estructurado para organizar y mantener informaciones que pueden ser fácilmente recuperadas. Un ejemplo simple de base de datos es una hoja de cálculo.

Bit: Abreviación de binary digit, un bit es la unidad más pequeña de datos que un ordenador puede manejar. Los bits se utilizan en distintas combinaciones para representar distintos tipos de datos. Cada bit tiene un valor 0 ó 1.

Byte: Es una serie de 8 bits. La capacidad de almacenaje de un ordenador se mide en bytes. Un *Kilobyte* (o 1 K) representa 1024 bytes y un *Megabyte* (1 Mb) representa mil "K" bytes, o un millón de bytes.

Byte: Es una serie de 8 bits. La capacidad de almacenaje de un ordenador se mide en bytes. Un *Kilobyte* (o 1 K) representa 1024 bytes y un *Megabyte* (1 Mb) representa mil "K" bytes, o un millón de bytes.

Caché: Cuando se descarga una página web, el dato es "ocultado", lo que significa que es almacenado temporalmente en el ordenador. La próxima vez que se desea esa página, en lugar de pedir el fichero al servidor, el navegador accede a ella a partir del caché, de manera que la página aparezca rápidamente. Pero si la página es actualizada frecuentemente, como lo son las páginas de noticias, de resultados deportivos o de datos financieros, no se verán las informaciones más recientes. Se ha de usar el botón de Recargar del navegador para descargar del servidor los datos más recientes.

CGI: Abreviación de Common Gateway Interface, el CGI es un programa de interfaz que permite al servidor de Internet utilizar programas externos para realizar una función específica. También denominado pasarelas o CGI "scripts", estos programas consisten generalmente de una serie de instrucciones escritas en un lenguaje de programación como C o PERL que procesan la petición de un navegador, ejecutan un programa y formatean los resultados en HTML de manera que puedan ser presentados en el navegador. Se utilizan para añadir interactividad a una página web al permitir a los usuarios rellenar y enviar formularios que podrán ser procesados (como un catálogo en línea), acceder a bases de datos por medio de una búsqueda, y obtener acceso a un sitio protegido escribiendo una contraseña. Los scripts CGI también se usan para introducir una variedad de sistemas de análisis y de tráfico de medida de audiencia de un sitio.

²⁹⁵ <http://www.learnthenet.com/spanish/glossary/adsl.htm>

Conexión por módem: Es un tipo de cuenta para conectarse a Internet. Con este tipo de cuenta, se tiene un sobrenombre o login name y una contraseña que permite acceder a algunos lugares del sistema informático. A través de un proveedor de Internet, ISP, la cuenta permite usar un módem para establecer una conexión con el sistema del proveedor. Una vez que se ha marcado el número del proveedor y que se está conectado, el proveedor conecta al usuario a Internet. Ya se pueden visitar sitios web por medio de un navegador, como si se tuviera una conexión directa a Internet.

Existen distintos tipos de cuenta de conexión por módem. Las cuentas SLIP o PPP permiten navegar en el World Wide Web directamente a partir del sistema operativo Windows o Macintosh. Una cuenta UNIX permite utilizar los comandos UNIX en el sistema del proveedor.

Contraseña: Una contraseña es un código o una palabra que se utiliza para acceder a datos restringidos de un ordenador. Mientras que las contraseñas crean una seguridad contra los usuarios no autorizados, el sistema de seguridad sólo puede confirmar que la contraseña es válida, y no si el usuario está autorizado a utilizar esa contraseña. Esa es la razón por la que es tan importante salvaguardar la contraseña:

No revelar la contraseña.

Diseñar una contraseña que consista de letras, números y símbolos.

Cambiar a menudo de contraseña.

Correo electrónico: También conocido como E-mail, abreviación de electronic mail. Consiste en mensajes, a menudo sólo con texto, enviados de un usuario a otro por medio de una red. El correo electrónico también puede ser enviado automáticamente a varias direcciones.

Dirección IP: Una dirección IP es un código numérico que identifica a un ordenador específico en Internet. Las direcciones de Internet son asignadas por un organismo llamado InterNIC. El registro incluye un nombre (whitehouse.gov), nombre de dominio, y un número (198.137.240.100), dirección o número IP.

FTP: Siglas de File Transfer Protocol. Método muy común para transferir uno o más ficheros de un ordenador a otro. FTP es un medio específico de conexión de un sitio Internet para cargar y descargar ficheros. FTP fue desarrollado durante los comienzos de Internet para copiar ficheros de un ordenador a otro. Con la llegada del World Wide Web, y de los navegadores, ya no se necesitan conocer sus complejos comandos; se puede utilizar FTP escribiendo el URL en la barra de localización que se encuentra en la parte superior de la pantalla del navegador. Por ejemplo, al escribir `ftp://nombre.del.sitio/arpeta/nombredelfichero.zip` se transfiere el fichero nombredelfichero.zip al disco duro del ordenador. Al escribir `ftp://nombre.del.sitio/carpeta/` da una lista con todos los ficheros disponibles en esa carpeta.

Cuando un navegador no está equipado con la función FTP, o si se quiere cargar ficheros en un ordenador remoto, se necesitará utilizar un programa cliente FTP. Para utilizar el FTP, se necesita conocer el nombre del fichero, el ordenador en que reside y la carpeta en la que se encuentra. La mayoría de los ficheros están disponibles a través de "anonymous FTP", lo que significa que se puede entrar en el ordenador con el nombre de usuario "anónimo" y utilizar la dirección de correo electrónico propia como contraseña.

Hacker: Pirata informático. Experto en informática capaz de entrar en sistemas cuyo acceso es restringido. Si sus acciones son malintencionadas, se les denomina crackers.

Host: Un host, literalmente anfitrión, es un ordenador directamente conectado a una red y que efectúa las funciones de un servidor, y alberga servicios, como correo electrónico, grupos de discusión Usenet, FTP, o World Wide Web) accesibles por otros ordenadores de la red.

HTML: Siglas de Hypertext Markup Language. El HTML es el lenguaje informático utilizado para crear documentos hipertexto. El HTML utiliza una lista finita de rótulos, o tags, que describe la estructura general de varios tipos de documentos enlazados entre sí en el World Wide Web.

http: Htp son las siglas de HyperText Transfer Protocol, el método utilizado para transferir ficheros hipertexto por Internet. En el World Wide Web, las páginas escritas en HTML utilizan el hipertexto para enlazar con otros documentos. Al pulsar en un hipertexto, se salta a otra página web, fichero de sonido, o imagen.

La transferencia hipertexto es simplemente la transeferencia de ficheros hipertexto de un ordenador a otro. El protocolo de transferencia hipertexto es el conjunto de reglas utilizadas por los ordenadores para transferir ficheros hipertexto, páginas web, por Internet.

IRC: Siglas de Internet Relay Chat. El IRC es un programa que permite desarrollar conversaciones en línea en tiempo real con gente de todo el mundo escribiendo mensajes por Internet. Se puede participar en grupos o de manera más privada con sólo una persona. El IRC consiste de "canales" que están dedicados a temas específicos. Cualquiera puede crear un "canal" y cualquier mensaje escrito en un canal dado es visto por todos las personas que estén en dicho canal.

ISDN: Siglas de Integrated Services Digital Network. Las líneas ISDN son conexiones realizadas por medio de líneas telefónicas ordinarias para transmitir señales digitales en lugar de analógicas, permitiendo que los datos sean transmitidos más rápidamente que con un módem tradicional.

ISP: Siglas de Internet Servie Provider. Hace referencia al sistema informático remoto al cual se conecta un ordenador personal y a través del cual se accede a Internet.

Java: Java es un lenguaje de programación por objetos creado por Sun Microsystems, Inc. que permite crear programas que funcionan en cualquier tipo de ordenador y sistema operativo. Se usa el Java para crear programas especiales denominados applets, que pueden ser incorporados en páginas web para hacerlas interactivas. Los apliques Java requieren que el navegador utilizado sea compatible con Java.

JavaScript: JavaScript es un lenguaje scripting que permite hacer que las documentos HTML sean dinámicos, por ejemplo haciendo que el relieve de un botón cambie al posicionar el cursor sobre éste.

MIME: Siglas de Multipurpose Internet Mail Extension. Sistema que permite integrar dentro de un mensaje de correo electrónico ficheros binarios (imágenes, sonido, programas ejecutables, etc.).

Módem: Abreviación de Modulator/Demodulator, un módem es un dispositivo que permite que ordenadores remotos comuniquen entre sí, que transmitan y reciban datos utilizando las líneas telefónicas.

NSFNET: National Science Foundation's NETwork. La NSFNET comenzó con una serie de redes dedicadas a la comunicación de la investigación y de la educación. Fue creada por el gobierno de los Estados Unidos, y fue reemplazada por ARPANET como backbone de Internet. Desde entonces ha sido reemplazada por las redes comerciales.

PDF: Siglas de Portable Document Format. El PDF es tipo de fichero creado por Adobe Systems, Inc. que permite la transmisión por Internet de documentos PostScript formateados y de alta resolución, y que estos sean vistos en cualquier ordenador que disponga del software Adobe Acrobat Reader software (que puede ser descargado gratuitamente del sitio web de Adobe).

Los documentos PostScripts son documentos de presentación de gran calidad que pueden contener logos, fotos y elementos gráficos de alta definición, textos con colores, etc. También pueden contener enlaces hipertexto, secuencias animadas de QuickTime y ficheros con sonido. Los ficheros en PDF no necesitan ser convertidos en HTML.

Los ficheros PDF pueden ser incluidos en correos electrónicos, páginas web, CD-ROMs, servicios en línea y en LANs.

POP: Siglas de Point of Presence. Un POP es el punto de acceso a Internet de un usuario.

PPP: Siglas de Point-to-Point Protocol. Es un protocolo de comunicaciones utilizado para transmitir datos de la red a través de las líneas telefónicas. Este tipo de conexión permite comunicar directamente con otros ordenadores de la red por medio de conexiones TCP/IP.

Protocolo: Un protocolo es una serie de reglas que utilizan dos ordenadores para comunicar entre sí. Cualquier producto que utilice un protocolo dado debería poder funcionar con otros productos que utilicen el mismo protocolo.

Script: Un script es un tipo de programa que consiste de una serie de instrucciones que serán utilizadas por otra aplicación.

SLIP: Siglas de Serial Line Internet Protocol. SLIP es un protocolo que permite utilizar el TCP/IP en una línea telefónica por medio de un módem. Tiende a ser reemplazado por el PPP.

SMTP: Siglas de Simple Mail Transfer Protocol. Protocolo utilizado para encaminar el correo electrónico por Internet

SSL: Siglas de Secure Socket Layer. Es un protocolo desarrollado por Netscape Communications Corporation para dar seguridad a la transmisión de datos en transacciones comerciales en Internet. Utilizando la criptografía de llave pública, SSL provee autenticación del servidor, encriptar de datos, e integridad de los datos en las comunicaciones cliente/servidor.

TCP/IP: TCP/IP son las siglas de Transmission Control Protocol/Internet Protocol, el lenguaje que rige todas las comunicaciones entre todos los ordenadores en Internet. TCP/IP es un conjunto de instrucciones que dictan cómo se han de enviar paquetes de información por distintas redes. También tiene una función de verificación de errores para asegurarse que los paquetes llegan a su destino final en el orden apropiado.

IP, Internet Protocol, es la especificación que determina hacia dónde son encaminados los paquetes, en función de su dirección de destino. TCP, o Transmission Control Protocol, se asegura de que los paquetes lleguen correctamente a su destino. Si TCP determina que un paquete no ha sido recibido, intentará volver a enviarlo hasta que sea recibido correctamente.

UNIX: Uno de los sistemas operativos utilizados para hacer funcionar los servidores.

URL: Siglas de Uniform Resource Locator. Es la dirección de un sitio o de una fuente, normalmente un directorio o un fichero, en el World Wide Web y la convención que utilizan los navegadores para encontrar ficheros y otros servicios distantes.

Usenet: Conjunto de grupos de discusión y serie de reglas aceptadas para distribuirlos y mantenerlos. Existen más de 13,000 grupos de discusión en el mundo y la mayoría de ellos hacen parte de Usenet. Sin embargo, un número considerable de grupos de discusión alternativos han nacido al margen de Usenet.

UUCP: Siglas de UNIX to UNIX Copy Program. Se trata de un protocolo para la transferencia de ficheros, noticias, y correo, así como para ejecutar ordenes distantes entre ordenadores.

Virus

Un virus informático es un programa creado especialmente para invadir ordenadores y redes y crear el caos. El daño puede ser mínimo, como que aparezca una imagen o un mensaje en la pantalla, o puede hacer mucho daño alterando o incluso destruyendo ficheros.

World Wide Web: Literalmente "tela de araña mundial", más conocida como web. Existen tres descripciones principales:

Serie de recursos (Gopher, FTP, http, telnet, Usenet, WAIS, y otros) a los que se puede acceder por medio de un navegador.

Serie de ficheros hipertexto disponibles en servidores del web.

Serie de especificaciones (protocolos) que permiten la transmisión de páginas web por Internet.

Se puede considerar el web como una serie de ficheros de texto y multimedia y otros servicios conectados entre sí por medio de un sistema de documentos hipertexto. Http (Hypertext Transfer Protocol) fue creado en 1990, en el CERN, el European Particle Physics Laboratory, en Ginebra, como medio para compartir los datos científicos a nivel mundial, de manera inmediata y barata. Con hipertexto, una palabra o frase puede contener un enlace con otro texto. Para lograr esto, el CERN desarrolló un lenguaje de programación llamado HTML, que permite enlazar fácilmente con otras páginas o servicios en el web.

BIBLIOGRAFIA

Libros:

1. Academia de Estudios Fiscales de Contaduría Pública A.C. Comercio Electrónico – Principios Jurídicos y Marco Fiscal. Dofiscal Editores, México, 2000.
2. Acosta Romero, Miguel. Compendio de Derecho Administrativo. 3ª ed. Porrúa, México 2001
3. Acosta Romero, Miguel. Nuevo Derecho Mercantil. 2ª ed. Porrúa. México. 2003
4. Astudillo Ursúa, Pedro. Elementos de Teoría Económica. 4ª ed. Porrúa. México. 1997.
5. Barrera Graf, Jorge. Instituciones de Derecho Mercantil. 1ª ed. Porrúa, México, 1989.
6. Bejarano Sánchez, Manuel. Obligaciones civiles. 5ª ed. Oxford. México 1999
7. Brom, Juan. Esbozo de Historia Universal. 19ª ed. Grijalbo. México. 1998
8. Carral y de Teresa, Luis. Derecho Notarial y Derecho Registral. 15ª ed. Porrúa, México, 1998.
9. Cervantes Ahumada, Raúl, Derecho Mercantil, 1er curso. Porrúa, 2ª Edición, 2002, México.
10. De J. Tena, Felipe. Derecho Mercantil Mexicano. 19ª ed. Porrúa. México, 2001
11. De Pina Vara, Rafael. Derecho Mercantil Mexicano. 28ª ed. Porrúa. México, 2002.
12. García Rodríguez, Salvador. Derecho Mercantil. 7ª ed. Porrúa. México. 2003.
13. Garrigues, Joaquín. Curso de Derecho Mercantil. Tomo I. 9ª ed. 2ª reimpr. Porrúa. México, 1990.
14. Gómez Lara, Cipriano. Teoría General del Proceso. 9ª ed. Oxford. México, 2000.
15. Gutiérrez y González, Ernesto. Derecho de las obligaciones. 5ª ed. Cajica, S.A. México. 1984

16. Huberman, Leo. Los bienes terrenales del hombre. . 27ª ed. Nuestro Tiempo, México, 1987.
17. Kelsen, Hans. Teoría General del Derecho y del Estado. 2ª ed. UNAM, México, 1983
18. Kent, Peter. Internet ¡Fácil! 3ª ed. Prentice – Hall Hispanoamericana, S.A., México, 1996
19. Mantilla Molina, Roberto L. Derecho Mercantil. 29ª ed. Porrúa. México, 2001
20. Quevedo Coronado, Ignacio. Compendio de Derecho Mercantil Mexicano. 1ª ed. Addison Wesley Longman de México, México, 1998.
21. Quintana Adriano, Elvia Arcelia. Ciencia del Derecho Mercantil. Porrúa. México, 2002
22. Quintano Adriano, Elvia Arcelia. Derecho Mercantil. Mc Graw-Hill/Interamericanas, México, 1997
23. Rábago, José Félix. Introducción a las redes locales. 1ª ed. Anaya Multimedia América. México 1995.
24. Randall, Neil. Trad. Sanchez García, Gabriel. Aprendiendo Internet en 21 días. Prentice Hall Hispanoamericana. México, 1995.
25. Reyes Krafft, Alfredo Alejandro. La firma electrónica y las entidades de certificación. Porrúa, México 2003
26. Ríos Hellig, Jorge. La práctica del Derecho Notarial. 3ª ed. Mc. Graw-Hill, México, 1998. p. 45
27. Smith, Rob, et. al. Trad. Martinez, Miguel Angel. Comercio Electrónico. 1ª ed. Pearson Education. México. 2001.
28. Soriano, Ramón. Compendio de la Teoría General del Derecho. 2ª ed. Ariel, España 1993
29. Tamayo y Salmoral, Rolando. Elementos para una Teoría General del Derecho (Introducción al Estudio de la Ciencia Jurídica) 2ª ed. Temis, México, 1998
30. Tanenbaum, Andrew S. Redes de Ordenadores. 2ª ed. Prentice –Hall Hispanoamericana, S.A. México, 1991.
31. Téllez Valdés, Julio. Derecho Informático.

Obras de Consulta:

1. De Pina Vara, Rafael. Diccionario de Derecho. 24ed. Porrúa, México, 1997.
2. Diccionario Enciclopédico Saber 3. Tomo 2. Fernández Editores. México, 1990.
3. Enciclopedia Microsoft® Encarta® 2002. © 1993-2001 Microsoft Corporation.
4. Enciclopedia Jurídica Omeba. Driskill, S.A., Buenos Aires, 1990
5. Instituto de Investigaciones Jurídicas. UNAM Diccionario Jurídico Mexicano 14ª ed. Porrúa, México, 2000
6. Raluy Poudevida, Antonio. Diccionario Porrúa de la Lengua Española. 48ª ed. Porrúa, México, 2003

Legislación:

1. Constitución Política de los Estados Unidos Mexicanos
2. Código Civil Federal
3. Código Civil para el Distrito Federal
4. Código de Comercio Vigente
5. Código de Procedimientos Civiles para el Distrito Federal
6. Código de Procedimientos Penales para el Distrito Federal
7. Código Federal de Procedimientos Civiles
8. Código Federal de Procedimientos Penales
9. Código Fiscal de la Federación Vigente
10. Código Penal Federal para el Distrito Federal
11. Ley Agraria
12. Ley de Adquisiciones Arrendamientos y Servicios del Sector Público
13. Ley de Instituciones de Crédito
14. Ley de Instituciones de Fianzas
15. Ley de la Comisión Estatal de Derechos Humanos de Jalisco
16. Ley de Navegación
17. Ley de Obras Públicas y Servicios Relacionados con las mismas
18. Ley de Títulos y Operaciones de Crédito
19. Ley del Mercado de Valores
20. Ley del Notariado para el Distrito Federal
21. Ley del Servicios Exterior Mexicano
22. Ley del Trabajo de los Servidores Públicos del Estado y Municipios (del Estado de México)
23. Ley Federal de Correduría Pública
24. Ley Federal de Derecho de Autor
25. Ley Federal de Protección al Consumidor
26. Ley Federal del Trabajo

27. Ley Federal sobre Metrología y Normalización
28. Ley General de Sociedades Mercantiles
29. Ley Orgánica del la Administración Pública para el Distrito Federal.
30. Ley Orgánica del Tribunal Superior de Justicia del Distrito Federal
31. Norma Oficial Mexicana NMX-EC-065-IMNC-2000 "Requisitos generales para organismos que operan sistemas de certificación de producto".
32. Norma Oficial Mexicana NOM-151-SCFI-2002, Sobre Prácticas comerciales - Requisitos que deben observarse para la conservación de mensajes de datos
33. Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación
34. Reglamento del la Ley del Servicio Exterior Mexicano
35. Reglamento del Registro Público de la Propiedad para el Distrito Federal
36. Reglamento Federal de Seguridad, Higiene y Medio Ambiente de Trabajo
37. Reglamento Interno del Registro Agrario Nacional
38. Reglas Generales a que deberán sujetarse los prestadores de servicios de certificación

Cibergrafia:

1. <http://cofocalec.org.mx/espanol/Acerca.htm>
2. <http://comunidad.derecho.org/mjviega/publicac/firmele2.htm>
3. http://es.wikipedia.org/wiki/Derecho_inform%Etico
4. http://v2.vlex.com/es/ppv/doctrina/resultados.asp?query_doc=171892&n_orden=0
5. http://v2.vlex.com/es/ppv/doctrina/resultados.asp?query_doc=178122&n_orden=0&
6. <http://www.aenor.es/desarrollo/certificacion/quees/queescertificacion.asp>
7. <http://www.alfa-redi.org/revista/data/53-7.asp>
8. http://www.amece.org.mx/motor/contenidos/htmls/105_13_12_02.php?acceso
9. <http://www.arrakis.es/~anguiano/artautcert.html>
10. <http://www.businesscol.com/economia/glosaeco/glecon-abc.htm#C>
11. <http://www.cem.itesm.mx/dacs/publicaciones/logos/libros/libros/firma.pdf>
12. <http://www.cimm.com.mx/cimm/clave.html>
13. <http://www.conocimientosweb.net/portal/article408.html>
14. http://www.ebconsultores.com.mx/sol_ebusiness.htm
15. <http://www.economia.gob.mx>
16. http://www.eped.edu.mx/revista/INTRODUCCION_AL_DERECHO_NOTARIAL_PARTE_UNO.htm
17. <http://www.eumed.net/cursecon/dic/C.htm>
18. <http://www.expansiondirecto.com/2000/02/10/tecnologia/5tec.html>
19. <http://www.geocities.com/elplanetamx/introduccion.html>
20. <http://www.hess-cr.com/cursos/diccionario/d.html>
21. http://www.informatica-juridica.com/trabajos/firma_digital.asp
22. <http://www.injef.com/php/index.php?option=content&task=view&id=414&Itemid=35>
23. <http://www.learnthenet.com/spanish/glossary/adsl.htm>

24. <http://www.mecon.gov.ar/comercio/electronico/indirec.htm>
 25. <http://www.monografias.com/trabajos/histocomp/histocomp.shtml>
 26. <http://www.monografias.com/trabajos13/contelec/contelec.shtml>
 27. http://www.netmedia.info/bsecure/articulos.php?id_sec=48&id_art=4819&num_page=21075
 28. <http://www.onncce.org.mx/>
 29. <http://www.ordenjuridico.gob.mx/Congreso/pdf/77.pdf>
 30. <http://www.ordenjuridico.gob.mx/Congreso/pdf/78.pdf>
 31. <http://www.ordenjuridico.gob.mx/Congreso/pdf/79.pdf>
 32. <http://www.prodigyweb.net.mx/bieletto/conclusiones.htm>
 33. <http://www.red.com.mx/scripts/redArticulo.php?idNumero=65&articuloID=7465>
 34. http://www.stps.gob.mx/04_sub_prevision/03_dgsht/ser_tra/tra_organismos.html
 35. <http://www.travel-center.com/Legal/Mexican-Ecommerce-Regulations-Spanish.htm>
 36. <http://www.udem.cl/cyt/derecho/contratacion.html>
 37. <http://comunidad.derecho.org/jviaga/publicac/firmele2.htm>
 39. <http://concytec.gob.pe/fanning/pc/tiempo.htm>
-