UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO.

FACULTAD DE ESTUDIOS SUPERIORES ACATLÁN.

“ANÁLISIS JURÍDICO COMPARATIVO DE LA FIGURA DEL PRESTADOR DE SERVICIOS DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA ENTRE LOS DERECHOS MEXICANO Y ARGENTINO”.

T E S I S

Que para obtener el Título de

LICENCIADO EN DERECHO

PRESENTA

ISRAEL MARIO VILLANUEVA JIMÉNEZ.

Asesor de Tesis.

Lic. José Arturo Espinosa Ramírez.

AGOSTO DE DOS MIL SEIS.

A DIOS, POR PERMITIRME LLEGAR A ESTE MOMENTO Y DARME TODO LO QUE ME RODEA SIN CONDICION ALGUNA.

A LA VIDA, POR REGALARME CADA DÍA PARA DISFRUTARLO COMO SI FUERA EL ÚLTIMO.

A LA UNIVERSIDAD NACIONAL AUTONOMA DE MÉXICO, CON INFINITO AGRADECIMIENTO Y RESPETO POR LA SEGUNDA OPORTUNIDAD QUE ME BRINDÓ PARA REGRESAR A SU SENO.

A LA FACULTAD DE ESTUDIOS SUPERIORES ACATLAN, MI ALMA MATER, POR HABERME PERMITIDO ESTAR EN ELLA TANTO EN LOS MOMENTOS CRITICOS COMO EN SU ACTUAL TRANSICION.

A MI MAMÁ, POR SU GRAN E INCONDICIONAL APOYO Y AMOR, PERO SOBRE TODO LA FE QUE TRATA DE INCULCAR EN MÍ DIA A DIA, NADA ES IMPOSIBLE SI TE LO PROPONES.

A MI PAPÁ, POR EL RESPALDO BRINDADO ANTES Y DURANTE MI DESARROLLO ACADEMICO, SE QUE PODREMOS SUPERAR TODO A PESAR DE LAS DIFERENCIAS LATENTES.

A YURI, QUIEN COMO MI ESPOSA HA SABIDO CAMINAR A MI LADO COMPARTIENDO LOS TRAGOS DULCES Y AMARGOS QUE NOS DA LA VIDA.

A MIS HIJAS MARIANA Y ANDREA, MIS PRINCESITAS QUIENES CON SU ALEGRIA E INOCENCIA ME HAN ENSEÑADO A AMAR Y A DISFRUTAR LOS MEJORES MOMENTOS DE LA VIDA PERO SOBRETODO, QUE LO MAS GRANDE LO ENCONTRAMOS EN LOS DETALLES MAS PEQUEÑOS.

A MIS PROFESORES, QUE CON SU PACIENCIA Y ENTREGA ME INCULCARON EL AMOR A LA CARRERA.

AL LICENCIADO JOSÉ RAFAEL BUSTILLOS CARRILLO, IN MEMORIAN. POR LA GRAN SABIDURÍA Y AMOR A LA UNIVERSIDAD, PERO POR ENCIMA DE TODO, LA HUMILDAD QUE SIEMPRE DEMOSTRÓ A TODOS Y CADA UNO DE SUS ALUMNOS.

A IRMA, SABINA, CATITA, PACHITA, DON PORFIS Y TODOS MIS SERES QUERIDOS QUE SE HAN ADELANTADO EN EL CAMINO. IN MEMORIAM.

A ERIKA, KATHIA Y ANTONIO, PORQUE A PESAR DE LAS DIFERENCIAS, COMO HERMANOS EN LAS BUENAS Y EN LAS MALAS SIEMPRE ESTAREMOS UNIDOS.

A MIS ABUELITOS ANGELITA Y FELIPE, QUIENES ME HAN ENSEÑADO QUE EL VALOR DE LA HONRADEZ VA DE LA MANO DE LA SABIDURIA.

AL CHATO POR SABER TENDERME LA MANO TAN DESINTERESADAMENTE EN ESOS MOMENTOS TAN DIFÍCILES.

A MIS COMPAÑEROS Y AMIGOS POR TODO LO QUE COMPARTIMOS Y EL APOYO QUE EN ELLOS ENCONTRE, ESPECIALMENTE A TANIA, POR HABER COMPARTIDO CONMIGO SUS ALEGRÍAS Y TRISTEZAS.

A MI ASESOR DE TESIS, EL LICENCIADO JOSÉ ARTURO ESPINOSA RAMÍREZ POR EL INTERÉS Y PASION DEMOSTRADO A QUIENES RECURRIMOS A SU CONSEJO.

AL LICENCIADO R. RAFAEL CASTRO REYES, POR SU PACIENCIA Y EL APOYO BRINDADO AL COMPARTIRME SU CONOCIMIENTO Y ENSEÑARME EL DIFICIL ANDAR DE NUESTRA PROFESION.

A TODOS AQUELLOS QUE SABIAN QUE CONSEGUIRÌA LLEGAR A ESTE MOMENTO.

I N D I C E.

I N T R O D U C C I Ó N.

> ***"La acentuada dependencia tecnológica, provocará el pronunciarse por la reflexión."***
> El Correo de la U.N.E.S.C.O. de 1983, Publicación de las Naciones Unidas.

Debido al notable incremento que la tecnología ha sufrido en el ámbito mundial, México al igual que otros países tuvo la imperiosa necesidad de realizar en sus ordenamientos legales y en especial en la materia mercantil, una reforma suficiente y bastante que permitiera obtener una legislación eficaz en materia del comercio electrónico.

Ello atendiendo a que si bien es cierto que nuestro Código de Comercio de 1889 en su tiempo fue una innovación dentro del ámbito jurídico, también lo es que la legislación mercantil nacional ha sido superada en algunos aspectos, principalmente en aquellos donde la tecnología y por supuesto los medios electrónicos, tienen día a día mayor aceptación y empleo, rebasando las expectativas que el código en comento contemplaba.

En consecuencia, frente a la vertiginosa avanzada tecnologica y el auge del comercio electrónico el Derecho en México y en los demás estados del orbe, se fue rezagando dejando al margen toda regulación y protección para el usuario consumidor que realizaba actos de comercio a través de internet.

Ante esta situación, el legislador se dedicó a realizar un proyecto de decreto encaminado a la reforma y adición en diversas disposiciones del Código de Comercio en materia de comercio electrónico, mismas que entrarían en vigor en noviembre del año dos mil tres regulando los temas a tratar en el presente trabajo como lo son la firma electrónica y el prestador de servicios de certificación de firma electrónica.

El comercio electrónico surge como una gran alternativa para realizar cualquier acto de comercio por las grandes ventajas que implica: facilidad en las operaciones, disminución de costos en la comercialización y un amplio mercado donde la oferta se encuentra al alcance del consumidor quien sin tener la necesidad de salir de su domicilio ni de conocer a la parte con quien esta contratando, puede adquirir los mas novedosos productos que internet le ofrece.

Sin embargo, han surgido diversos inconvenientes técnicos y legales para el usuario y consumidor quien se encuentra desprotegido ante la falta de regulación en algunos países y los trastornos informáticos provocados por individuos especializados en informática cuya forma de operar se basa en sabotear u obtener datos confidenciales de los usuarios para realizar toda clase de operaciones sin el consentimiento, mucho menos el conocimiento del usuario y consumidor.

Por ende, resulta esencial tanto crear una firma electrónica que brinde seguridad a su titular al momento de utilizar los medios electrónicos para realizar cualquier tipo de operaciones, como el establecer una institución encargada de salvaguardar todas esas firmas electrónicas cuya existencia la convierta en depositaria de la plena confianza del usuario de sus servicios de certificación.

El presente trabajo tiene como objetivo realizar un análisis jurídico comparativo respecto del Comercio Electrónico y su adopción en las legislaciones mexicana y argentina pero sobre todo, analizar la figura del certificador de firma electrónica, las funciones de certificación que desempeñará así como los posibles efectos que ello conllevará siempre bajo la tutela del organismo público designado por el Poder Ejecutivo de cada Estado, elucidando las posibles ventajas y desventajas de su instauración dentro de la esfera legal mexicana.

En ese orden de ideas, el presente trabajo se apoya en el estudio jurídico comparativo del Comercio Electrónico, la firma electrónica y los prestadores del servicio de certificación de firma electrónica, entre una de las legislaciones

pioneras en la materia como lo es la Ley de Firma Digital emitida bajo el numeral 25.506 en la Nación Argentina y las recientes reformas realizadas en nuestro país al Código de Comercio en materia de Firma Electrónica que se complementan con el Reglamento del Código de Comercio en materia de prestación de servicios de certificación y las Reglas para la acreditación de los prestadores de servicios de certificación de firma electrónica.

En el Capítulo Primero analizaremos la evolución que han tenido los medios de comunicación ante la creciente necesidad del hombre de satisfacer esa ansiedad por ser mejor cada día con el menor esfuerzo, abordando brevemente los avances en materia de computación teniendo a la computadora como protagonista en la revolución informática que ha transformado esencialmente el ritmo actual de vida.

Desde sus orígenes, la computadora ha permanecido en constante evolución desembocando en lo que actualmente la mayoría hemos contactado o escuchado hablar y que hasta éste momento es la máxima expresión de los medios electrónicos de comunicación: internet.

Internet que surgió como un sistema de defensa militar de Estados Unidos y posteriormente se enfocó a un uso académico y de investigación, se ha convertido en la actualidad en la herramienta más poderosa para conseguir no solo información invaluable e infinita, sino también mercancía inimaginable a un bajo costo y con grandes ventajas de consumo.

No fue nada errado el haber asignado a internet el sobrenombre de “la supercarretera de la información”, pues actualmente existen millones de usuarios conectados a la red que en lapsos breves pueden realizar un sinfín de consultas sobre los temas mas variados o simplemente celebrar eficaces transacciones desde la comodidad del hogar sin tener conocimiento de quien es la parte con la que estan contratando.

Dentro del Capítulo Segundo analizaremos la Legislación Argentina en materia de comercio electrónico y la firma electrónica y en particular, al Certificador Licenciado como el legislador argentino denomina al certificador de frima electrónica estableciendo a través de diversos decretos, la pauta para el adecuado desempeño del ente certificador.

Mediante un estudio de los principales ordenamientos legales y sus respectivos preceptos, trataremos de entender la estructura que el legislador argentino brinda al certificador licenciado para convertirlo en el ente depositario de la confianza de los usuarios de los servicios de certificación de firma digital.

Por otra parte, ya en el Capítulo Tercero abordaremos la intensiva reforma que se ha realizado en gran parte de la legislación mexicana, misma que por cuestiones de incompatibilidad de ideologías y tendencias partidistas cuya única aportación es una certeza parcial de lo que se pretende legislar, no ha sido de manera total dejando en un vacio diversos aspectos.

La reforma que entró en vigor en noviembre del dos mil tres, fue el complemento en materia mercantil para regular a una figura mundial tan importante en el medio económico como lo es el comercio electrónico y todo lo que a él viene aparejado como lo son la firma electrónica y el prestador de servicios de certificación de firma electrónica.

Al igual que Argentina, México se guía por la buena fe y el certificador de firma electrónica tendrá la función de ser al igual, un ente depositario de la confianza de los usuarios de sus servicios.

Pero existen marcadas diferencias en torno al complemento que se le brinda a la regulación de las funciones de certificación ya que el legislador mexicano se apoyó en gran medida tanto en las Leyes Modelo emitidas por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (UNCITRAL) como en

las legislaciones de algunos de los Estados que adoptaron dicha figura procurando brindarle un entorno adecuado para no suscitar un vacío legal.

Durante el desarrollo y hasta la total conclusión del presente trabajo de investigación, nos hemos encontrado que las reformas dentro del marco jurídico mexicano han sido intensas, sin que Argentina haya procurado cubrir de certeza el desempeño del ente certificador.

Ya en el Capítulo Cuarto, confrontaremos las legislaciones mexicana y argentina analizando las ventajas y desventajas que pudiera tener nuestro marco jurídico por la adopción del comercio electrónico y su posibles consecuencias en la busqueda de su óptima aplicabilidad empleando la firma electrónica como medio digital de identificación y lo más importante para el presente trabajo: todo aquello que conlleva la instauración del prestador de servicios de certificación de firma electrónica en nuestro país.

CAPÍTULO PRIMERO.

"El desarrollo tecnológico, la evolución de los pensamientos jurídicos, económicos o político-ideológicos, son conceptos cuya unión denota la constante búsqueda del ser humano por una vida mejor o con más facilidades, la cual, en ocasiones, se ve rebasada por el vertiginoso avance de los medios de comunicación. El derecho es una ciencia que busca establecer ciertos parámetros dentro de los cuales debe de caber el correcto comportamiento del individuo en sociedad. Los hechos, actos y factores sociales que influyen al Derecho han evolucionado junto con el hombre a lo largo de la historia además de constituirse en verdaderas condicionantes al momento de crear la norma jurídica."

EDUARDO MARTÍNEZ ALTAMIRANO.

Marco teórico de la firma electrónica.

1.1 Nociones generales de la firma electrónica.

La sociedad mundial actual gira en torno a la información y a la acumulación de conocimientos y la evolución tecnológica de la telemática, entendida ésta como la utilización de la información a través de las telecomunicaciones y el profundo impacto de la informática en la sociedad, han generado profundas transformaciones en todos los ámbitos de la vida social.

Es una constante que para el hombre siempre ha existido la necesidad de cuantificar en forma rápida, precisa y sencilla sus pertenencias, por lo que en un principio empleaba sus manos más al verse limitado al número de sus dedos, requirió de otros medios mecánicos y sistemas numéricos para realizar cuentas a gran escala con la celeridad que los tiempos le iban exigiendo.

A través de la historia, diversos dispositivos han sido creados por el hombre para simplificar todo tipo de operaciones: el ábaco con sus aproximadamente cuatro mil años de edad, las Tablas de logaritmos de John Napier en 1614, la Regla de cálculo en 1630, la Máquina de Blas Pascal en 1642, la tarjeta perforada de Joseph Marie Jacquard en 1804, la Máquina de Charles Babbage en 1834 y el Código de Herman Hollerith en 1880 son los más claros ejemplos.

Siglos de evolución han llevado al hombre a buscar afanosamente comunicarse con sus semejantes en los lugares más recónditos del planeta de las formas más variadas como lo son: el envío de mensajes empleando la estafeta, las diligencias y el correo, el telégrafo, el teléfono y el fax, la radio y la televisión, siendo lógico que todos esos grandes avances en la era de la comunicación tendrían que llegar a un instrumento considerado como la culminación de las comunicaciones y la electrónica aplicada al cálculo: la computadora

Correctamente, Donald H. Sanders refiere que *"el ábaco y la computadora personal son dos pequeños dispositivos para proceso de datos separados por miles de años de historia" (1)*, pues ambos instrumentos han sido de gran utilidad para el ser humano y la computadora desde su aparición y a través de los tiempos, ha demostrado que se trata de un instrumento con un desempeño capaz de realizar en cuestión de segundos operaciones tan precisas cuya resolución tomaría una cantidad inimaginable de tiempo y los resultados no serían del todo confiables.

Es así que desde su aparición como la MARK I o ASCC (Automatic Sequence Controlled Calculator) en 1937, su progreso ha sido constante y de tal magnitud como para culminar en la computadora personal o PC que actualmente empleamos en nuestro trabajo, en el hogar e inclusive, de viaje.

La computadora desató una revolución tecnológica a la que nadie auguraba un desarrollo tan vertiginoso y ni siquiera imaginado los alcances que iba a lograr llegando a un punto tal en la actualidad, que casi todos los individuos tienen contacto con éste instrumento de trabajo tan importante.

Este desarrollo nos lleva al nacimiento de otro auxiliar en cualquier ámbito en el cual uno se interese, un sistema donde la gama de posibilidades es tan infinitamente variada como la cantidad de usuarios que realizan una consulta y que lleva el nombre de Internet.

La red de redes o la supercarretera de la información como popularmente se conoce a internet, es principalmente un servicio de consulta pero también un valioso medio de difusión de información y de celebración de transacciones que permite a un sinfín de individuos acceder a las nuevas tecnologías de la información.

---

(1) H. SANDERS, Donald. "Informática: Presente y futuro". Editorial Mc Graw Hill/Interamericana de México S.A. de C. V., Tercera edición. México, 1990. p. 43.

Frente a éste panorama no es posible concebir a internet sin una computadora, por lo que el desarrollo de ambos ha sido en forma conjunta y continua de tal manera, que no sería nada descabellado el hablar de una globalización en el ámbito de las telecomunicaciones.

Internet nace a finales de la década de los sesentas como parte de un avanzado sistema de defensa militar desarrollado por el Departamento de Defensa de los Estados Unidos de América denominado ARPANET (*Advaced Research Projects Agency Net* o Red de la Agencia de Proyectos de Investigación Avanzada), constando en aquél entonces de solo cuatro computadoras interconectadas entre sí y ubicadas cada una en la Universidad de California (UCLA), en el Instituto de Investigaciones de Stanford (SRI), en la Universidad de California en Santa Bárbara (UCSB) y en la Universidad de UTAH, respectivamente.

Posteriormente y una vez separado internet de las funciones militares, son las universidades las que contribuyen a su crecimiento al permitir su uso para acceder a la red sin importar el lugar de origen, pero con fines académicos, científicos y de investigación.

Poco más tarde y a finales de los ochentas, internet es abierto al sector comercial permitiendo su expansión a nivel internacional, brindando servicio a millones de usuarios en todos los países del orbe y creciendo a un ritmo desenfrenado al grado tal, que aproximadamente cada treinta minutos accede a ésta red un nuevo servidor.

De esa manera es como originalmente desarrollado para el sector militar, en la actualidad gran parte de internet se utiliza para la investigación académica y la actividad comercial, convirtiéndose en un sitio donde los usuarios tienen acceso a artículos científicos y noticias instantáneas, siendo además utilizado ampliamente como red de correo electrónico a nivel mundial logrando dicha conexión a través de múltiples servicios en línea.

Para conocer que es internet, la Maestra Gabriela Barrios-Garrido nos plantea dos conceptos enfocados a puntos de vista distintos, el primero definiéndolo desde un punto de vista técnico como:

"…una red de redes de ámbito mundial comunicadas mediante el protocolo TCP/IP (Transmisión Control Protocol-Internet Protocol), es decir, por un conjunto de pasos, mensajes, formas de los mensajes y secuencias que se utilizan para mover la información de una localización a otra sin errores, fraccionándolos en pequeños paquetes y asegurando su correcta recepción.

*Desde un punto de vista sociológico, internet es un medio de comunicación que une a personas, instituciones, compañías y gobiernos alrededor del mundo, de manera casi instantánea y a través del cual, es posible contactar con un solo individuo, con un grupo amplio de personas interesadas en un tema específico o con el mundo en general". **(2)***

A raíz de la globalización y gran apertura que tiene internet para los usuarios, desde la comodidad de su hogar y contando con una computadora y una clave de acceso a la red, ingresar a éste infinito de transacciones e información es sumamente fácil, pues prácticamente no existe limitante alguna para aquél que se propone cometer ilícitos en perjuicio de los demás usuarios.

*"La transferencia de información y el empleo de los nuevos medios de comunicación trae consigo dificultades jurídicas de una nueva naturaleza las cuales son difíciles de resolver debido a que la utilización de redes no conoce fronteras, situación que requiere la armonización a nivel internacional para alinear las diversas legislaciones nacionales existentes". **(3)***

Significando entonces que Internet se ha convertido en un tema de polémica a nivel internacional debido a la infinidad de usos que puede tener ya como herramienta de acceso a cualquier información, con alcances y contenidos

---

(2) BARRIOS-GARRIDO, Gabriela. "Internet y Derecho en México". Editorial McGraw Hill/Interamericana Editores, S.A. de C. V., Primera Edición. México, 1998. pp 3 y 4.
(3) LUKE, O'CONNOR. "Internet: ¿El medio seguro de la supercarretera de la información?". New Lestter. Lania, Otoño-Invierno 1995, Año 4, Volumen 14.

valiosos y diversos en campos como la cultura, ciencias, artes y desarrollo personal, así como en el abuso en su contenido, dando origen a fraudes, pornografía infantil, sabotajes electrónicos, intromisiones ilegales en sistemas de seguridad, entre otros.

En conclusión, Barrios-Garrido capta en un concepto la más adecuada definición de internet al referir que es *"un sistema internacional de intercambio de comunicación que une personas, instituciones, compañías y gobiernos alrededor del mundo, pudiendo dirigirse a un individuo en particular o a un grupo amplio de personas interesadas en un tema o al mundo en general". **(4)***

Una realidad latente es que la computadora ha dejado de ser solamente un instrumento auxiliar para convertirse en parte esencial de nuestras vidas e internet se ha constituido en el instrumento activo de la globalización cuyo uso continuo experimenta un crecimiento que esta dando lugar a nuevas formas jurídicas producto de las nuevas relaciones con diversas ramas del Derecho.

Por esta y múltiples razones, el Derecho para cumplir con su primordial objetivo de la búsqueda necesaria, pronta y contínua de la justicia y el bien común, debe evolucionar a la par de la tecnología evitando de ésta forma cualquier situación que coloque al usuario de los servicios de la red de redes en un estado de desamparo total.

Asi es como dentro del Derecho surge una rama denominada Derecho Informático a la cual el Doctor Julio Téllez Valdés define como *"una rama de las ciencias jurídicas que contempla a la informática como instrumento (informática jurídica) y como objeto de estudio (derecho de la informática)." **(5)***

---

(4) BARRIOS-GARRIDO, Gabriela. "México ante la nueva normativa global de la tecnología de información: ¿Qué está pasando con el internet?. En el Boletín de Política Informática, México, INEGI, Año XX, Número 2, 199 . p. 56.

(5) TÉLLEZ Valdés, Julio. "Derecho Informático". Editorial McGraw Hill/Interamericana de México, S.A. de C.V., México, 1996. p. 22.

De igual manera, Téllez Valdés define a la Informática Jurídica como *"la técnica interdisciplinaria que tiene por objeto el estudio e investigación de los conocimientos de la informática en general, aplicables a las recuperaciones de información jurídica, así como la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de información jurídica necesarios para lograr dicha recuperación"* y al Derecho de la Informática como *"el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática."* ***(6)***

1.2 Formas de acreditación de la firma electrónica.

En la actualidad las barreras físicas de protección son insuficientes para un sistema de informática y agregando a ello el nivel tan raquítico en el desarrollo computacional que padecen muchos países, la dificultad que les presenta establecer barreras tecnológicas contra los atentados significa altos costos imposibles de solventar.

Dentro del panorama tan vasto que internet ofrece a sus usuarios y consumidores, desafortunadamente también existen condiciones que cubren de incertidumbre cualquier consulta u operación que se realice empleando los medios electrónicos de comunicación.

Estas condiciones son motivadas principalmente por la vasta amplitud que internet brinda y la escasa o nula legislación existente en la materia en algunos estados, lo cual propicia que individuos conocidos como "hackers" y "crackers" se dediquen a sabotear y descifrar las claves de acceso a los sistemas de seguridad de las grandes empresas (principalmente las instituciones bancarias) más aún, entidades gubernamentales donde la mayor de las ocasiones y sin ser detectados, en cuestión de segundos realizan los fraudes y sabotajes más cuantiosos y efectivos, sin que puedan ser localizados.

---

(6) TÉLLEZ Valdés, Julio. op. cit. pp. 26 y 58.

Estos “hackers” y “crackers”, en su mayoría son personas cuyas edades fluctúan principalmente entre los catorce y treinta años de edad y que cuentan con un gran dominio de la informática obtenido por estudios realizados en escuelas especializadas en dicha materia, lo cual significa que para tener un dominio en informática no es necesario contar con una experiencia laboral reflejada en años, sino simplemente tener una estación de trabajo (computadora personal) y conocimientos especiales en computación.

Es por estos motivos que ante dicha perspectiva y el desarrollo tan abierto de internet y el comercio electrónico, fue necesario crear una firma electrónica que brindara seguridad al usuario consumidor que emplea los medios electrónicos para realizar cualquier tipo de operaciones y a la vez, establecer una institución encargada de registrar todas esas firmas electrónicas cuya existencia la convierta en depositaria de la plena confianza del usuario de sus servicios de certificación.

De esta manera, diversos mecanismos de seguridad han surgido en torno al acceso a las redes de comunicación siendo los principales y más usuales: el cifrado, los mecanismos de firma digital, los mecanismos de control de acceso, los mecanismos de integridad de datos y los mecanismos de certificación.

“El cifrado se utiliza para proteger la confidencialidad de las unidades de datos y la información de flujo de tráfico, o para dar soporte o complementar otros mecanismos de seguridad.

Los mecanismos de firma digital se utilizan para proporcionar una analogía electrónica a la firma manuscrita en los documentos electrónicos. De forma similar a las manuscritas, las firmas digitales no deben ser falsificables, los receptores deben ser capaces de verificarlas y el firmante no debe poder rechazarlas posteriormente.

Los mecanismos de control de acceso son las identidades autentificadas de los principales, información sobre dichos principales o capacidades de determinar y reforzar los derechos de acceso. Si un principal intenta utilizar un recurso no autorizado o un recurso autorizado con un mecanismo impropio de acceso, la función de control de

acceso rechazará el intento y podrá además, informar del incidente con el propósito de generar una alarma y guardarla como parte de los informes de auditoría sobre seguridad.

*Los mecanismos de certificación se pueden emplear para asegurarse de ciertas propiedades de los datos que se comunican entre dos o más entidades, como su integridad, origen, tiempo o destino. La certificación la realiza una tercera entidad de confianza, que es la que da testimonio de la autenticidad." **(7)***

De entre todos los mecanismos destinados a satisfacer las necesidades de seguridad y control de la información en los programas de cómputo, la criptografía se configura como el más interesante y eficaz.

Rolf Oppliger menciona que la *"Criptología se refiere a la ciencia de las comunicaciones seguras y comprende tanto la criptografía como el criptoanálisis. La palabra criptología está derivada del griego kryptós, oculto y logos, palabra. En consecuencia, la criptología se puede definir como la ciencia de las palabras ocultas*." ***(8)***

Algunos autores nos mencionan que la criptografía "consiste en codificar los mensajes de forma tal que los intrusos los reciben tergiversados por la magia de los efectos electrónicos implantados", significando tal codificación la transformación de un mensaje en signos inteligibles cuya traducción dependerá de aplicar la clave adecuada.

Considerando que la criptografía (cryptography) es la *"ciencia mediante la cual se preparan mensajes en forma tal que no puedan ser leídos por quienes no conocen los secretos de la forma" **(9)*** y que el cifrar (encipher) o criptografiar es *"convertir*

---

(7) OPPLIGER, Rolf. "Sistemas de autentificación para seguridad en redes". Alfaomega Grupo Editor S.A. de C.V. México, 1998. p. 11.
(8) OPPLIGER, Rolf. op.cit p. 14.
(9) DICCIONARIO DE TERMINOS CIENTÍFICOS Y TÉCNICOS MCGRAW HILL/BOIXAREU. Marcombo Boixareu Editores. Vol 2, Barcelona España. 1981. p. 540.

*un mensaje con texto en lenguaje ordinario en otro de lenguaje ininteligible por medio de un sistema de criptógrafo".**(10)***

De tal modo, nos apegaremos al concepto del Maestro Julio Téllez Valdéz que refiere que la criptografía:

*"...es la ciencia que transcribe las informaciones en forma secreta; forma incomprensible para toda persona que no sea el usuario o destinatario que consiste en "criptar" los programas por un sistema de codificación sofisticado empleando una o varias claves, un conjunto de caracteres que transforman un método general o un algoritmo específico en informaciones codificadas, a efecto de que si el competidor pirata o "enemigo" conoce el algoritmo no le sea de provecho, pues deberá conocer también la clave, la cual podrá ser cambiada y representar consecuentemente un nuevo obstáculo para aquél que quisiera tener acceso al sistema." **(11)***

El cifrado entonces, es utilizar la criptografía con el objeto de codificar datos con propósitos de seguridad para transmisión a través de una red pública y donde el texto original o texto plano se convierte en un equivalente codificado denominado texto cifrado a través de un algoritmo de cifrado. El texto cifrado se codifica en el extremo receptor con el uso de una clave de descifrado.

Para tener una visión acertada de la firma electrónica, es preciso analizar conceptos que de la firma ológrafa nos manejan diversos autores.

La firma es la manifestación expresa de la voluntad, es una condición esencial o el signo inequívoco por el que se reconoce la validez e incluso la existencia de un acto jurídico. Sólo desde el momento en que la firma o en su defecto, la huella dactilar está estampada, debe considerarse que el otorgante ha tenido la intención de hacer suya la declaración contenida en el instrumento.

---

(10) DICCIONARIO DE TERMINOS CIENTÍFICOS Y TÉCNICOS. MCGRAW HILL/BOIXAREU. Marcombo Boixareu Editores. Vol 1, Barcelona España.1981. p. 389.

(11) TELLEZ Valdes, Julio. "La protección jurídica de los programas de computación". Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México. Serie 6. Estudios Doctrinales. Número 124, Segunda edición, México, 1989. p. 54 .

Normalmente, la firma es la manera habitual con que una persona asume tanto derechos como obligaciones inherentes al documento que suscribe.

La Real Academia de la Lengua Española define a la firma (del latín *firmare,* afirmar, dar fuerza), como *"nombre y apellido, o título, de una persona, que ésta pone al pie de un documento escrito de mano propia o ajena, para darle autenticidad o para obligarse a lo que en él se dice y rubrica". **(12)***

Por su parte, el maestro Mantilla Molina define a la firma como *"el conjunto de signos manuscritos estampados por una persona que sabe leer y escribir, con los cuales habitualmente caracteriza los escritos cuyo contenido aprueba". **(13)***

*"La firma es afirmación de individualidad, pero sobre todo de voluntariedad. En el primer aspecto significa que ha sido la persona firmante y no otra quien ha suscrito el documento. En el segundo, que se acepta lo que allí se manifiesta." **(14)***

Y si bien es cierto que la firma manuscrita tiene posibilidades de ser falsificada o alterada, también lo es que cada firma posee ciertos rasgos característicos que la hacen fácilmente distinguible de las demás, los cuales nos dan la certeza de que fue estampada por quien tiene pleno uso de ella.

De acuerdo con lo expuesto, la firma digital no es necesariamente una firma pero si se conformará con rasgos personales inherentes al sujeto, los cuales serán reflejados en los elementos que conforman la clave privada que solamente él conoce.

El creciente empleo de técnicas de autenticación electrónica en sustitución de las firmas manuscritas y de otros procedimientos tradicionales de autenticación, ha

---

(12) DICCIONARIO JURÍDICO MEXICANO. Instituto de Investigaciones Jurídicas, UNAM. Ed. Porrúa, México. 1989. Tercera edición. Tomo II. p. 1453.
(13) MANTILLA MOLINA.L Roberto. "Derecho Mercantil: Introducción y conceptos fundamentales, sociedades". Ed. Porrúa, México. 1992. 2da edición. p. 153.
(14) DICCIONARIO DE DERECHO MERCANTIL. Instituto de Investigaciones Jurídicas, UNAM. Ed. Porrúa. México, 2001. Primera edición. p. 255.

planteado la necesidad de crear un marco jurídico específico para reducir la incertidumbre con respecto a las consecuencias jurídicas que pueden derivarse del empleo de dichas técnicas modernas a las que puede denominarse en general “firmas electrónicas”.

Luego entonces, para trasladar esa firma manuscrita al campo de la informática, es preciso dotarla de ciertos rasgos que se reflejan en un lenguaje binario donde la firma ológrafa es sustituida por un signo electrónico que satisface las funciones de identificación y el cual, el emisor se limita a añadir al mensaje de datos como aceptación de los efectos que en él se consignan.

La firma electrónica es aquella que un firmante coloca en forma digital sobre unos datos, añadiéndola o asociándola lógicamente a los mismos y la utiliza para indicar su aprobación respecto del contenido de esos datos, debiendo generalmente cumplir con los siguientes requisitos:

- Debe estar vinculada únicamente al firmante.
- Debe ser capaz de identificar al firmante.
- Tiene que ser creada utilizando un medio técnico que está bajo el control del firmante.
- Debe estar vinculada a los datos a que se refiere.

Una clase particular de firma electrónica que permite ofrecer mayor seguridad a los usuarios es ”la firma digital asimétrica de clave pública”.

La firma digital asimétrica de clave pública consiste en un criptosistema basado en el uso de un par de claves asociadas: una clave privada que se mantiene en poder de su titular y una clave pública conocida por cualquier persona.

En ésta firma digital o electrónica predominan dos tipos de clave o contraseña, una pública y otra privada, la contraseña pública es aquélla por todos conocida, que obra en manos de las instituciones o de cualquier persona con la cual tendrá

trato el emisor de la firma electrónica; por otra parte, la contraseña privada es conocida única y exclusivamente por el emisor quien la emitirá como aceptación del acto realizado y cuyo manejo será plena responsabilidad del mismo.

Básicamente el procedimiento de la firma digital de clave asimétrica es el siguiente:

- El emisor de un mensaje lo cifra digitalmente utilizando su clave privada.
- El receptor del mensaje puede descifrarlo utilizando la clave pública del emisor.

Como la aplicación de criptografía asimétrica sobre la totalidad del mensaje es muy costosa, en los mensajes de gran extensión suele aplicarse sobre el mismo un algoritmo de resumen que transforma una secuencia de bits ***(15)*** en uno menor, llamada función hash.

Al aplicar esta función se obtiene un resumen del mensaje denominado huella digital cuyas características principales son su irreversibilidad (a partir del hash no puede obtenerse el mensaje completo) y la imposibilidad de obtener un segundo mensaje que produzca el mismo resumen, de forma tal que cualquier cambio en el mensaje produciría un hash diferente.

Una vez aplicada la función hash al mensaje principal, el resumen resultante es cifrado con la clave privada del firmante y es enviado junto al mensaje original, de forma tal que el receptor, para comprobar si el mensaje ha sido firmado por el emisor, debe realizar dos operaciones: descifrar el hash aplicando la clave pública del emisor y aplicar la función hash sobre el mensaje completo obtenido.

---

(15) Bit: (del ing. Bit, acrónimo de binary digit) m Inform. **Unidad de medida de información equivalentea la elección entre dos posibilidades igualmente probables. // 2. Unidad de medida de la capacidad de memoria, equivalente a la posibilidad de almacenar la selección entre dos posibilidades, especialmente usada en los computadores.** ***DICCIONARIO DE LA REAL ACADEMIA DE LA LENGUA ESPAÑOLA. Editorial Espasa Calpe, S.A. Madrid, España. 1992. Vigésima Primera edición. p. 295.***

Si el hash recibido y descifrado y el hash obtenido coinciden, habrá verificado que el mensaje ha sido enviado por quien dijo haberlo hecho y que su contenido no ha sufrido alteraciones.

Estos tipos de sistemas de criptografía asimétrica nos permiten enviar mensajes confidenciales, proporcionando autenticidad, integridad y no repudio por parte del destinatario y de acuerdo al estado del arte actual, alcanzan el nivel de seguridad necesario para poder asimilarlas a la firma escrita en papel.

Si bien hasta el momento la mayoría de las normas dictadas sobre la materia se basan en este tipo de firma, el mejor criterio legislativo será el que adopte una posición abierta que permita el desarrollo de nuevas técnicas y no se limite a exaltar a este sistema en demérito de mejores técnicas futuras.

Aunque el problema más conocido es el de la confidencialidad de los mensajes, con el auge de las comunicaciones electrónicas ha cobrado especial importancia el tema de la autenticidad que también requiere de una aplicación criptográfica.

Para obtener esas claves, existen dos métodos para cifrar datos: *"el método tradicional utiliza una clave secreta como DES, donde tanto el emisor como el receptor comparten la misma clave. Es el método más rápido, pero transmitir la clave secreta al receptor no es seguro.*
El segundo método es la criptografía de clave pública como RSA, que emplea tanto una clave privada como pública. Cada receptor tiene una clave privada que se mantiene en secreto y una clave pública que se da a conocer a todos. El emisor mira la clave pública del receptor y la utiliza para cifrar el mensaje. El receptor emplea una clave privada para descifrarlo.
Si la velocidad es una preocupación, el método de clave pública puede emplearse para enviar la clave secreta seguida por el mensaje que se ha cifrado con dicha clave." ***(16)***

---

(16) FREEDMAN, Alex. "Diccionario de computación bilingüe". Editorial McGraw Hill/Interamericana S.A. Séptima edición. Santa Fe de Bogotá, Colombia. 1996. Vol 1. p. 193.

Los esquemas de autenticación sirven para confirmar tanto la validez del mensaje emitido como la legitimidad del emisor. Intimamente relacionado con este concepto, nos encontramos con la idea de la firma digital, que además asegura que el firmante de un mensaje no puede posteriormente negar haberlo firmado, por ejemplo:

Supongamos que A y B comparten una clave secreta y que A recibe un mensaje cifrado supuestamente por B. En principio y tras la recuperación del mensaje, A no tiene ninguna duda de que dicho mensaje proviene de B (autenticación), pero este esquema no es de firma digital porque B siempre puede repudiar el mensaje alegando que realmente lo produjo A.

Sin embargo este problema se puede resolver fácilmente usando un cifrado de clave pública de la siguiente forma: B envía a A un mensaje cifrado con su clave secreta, A lo descifra con la clave pública de B y guarda la versión cifrada. Así, si B pretende repudiar su firma, A tiene una prueba definitiva: nadie salvo B podría haber generado el mensaje cifrado.

Aunque la firma digital descrita es totalmente válida, no resulta muy práctica dadas las dimensiones de los datos manejados, siendo ahí donde la función hash criptográfica reduce el mensaje de partida a un valor resumen de menor longitud, de forma tal que éste sirve como representación compacta del anterior pudiendo aplicársele el correspondiente cifrado sin problemas de eficiencia en las comunicaciones.

“Para que una función hash sea criptográficamente útil es necesario que verifique las propiedades de "resistencia a las colisiones", las cuales garantizan cierto grado de dificultad para encontrar mensajes distintos con idénticos resúmenes.

Una de las conclusiones que se extraen del estudio de este tipo de ataques es la importancia del parámetro longitud de resumen, ya que la factibilidad de dichos ataques depende directamente de él ("a mayor longitud, mayor seguridad”).

Una vez que se tiene la función hash (basada en claves secretas) productora de resúmenes de una longitud adecuada, se puede combinar con cifrados de clave secreta

*y/o pública, aplicándose éstos sobre mensaje y/o resumen, logrando con ello un esquema de firma digital a la vez práctico y seguro". **(17)***

Es entonces que como principales fines de la firma electrónica, tenemos:

1. Integridad.
2. Autenticación.
3. No repudio.
4. Protección de repetición.

En nuestro país, el Código de Comercio reformado en materia de Firma Electrónica, en su artículo 89 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".*

1.3 Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (UNCITRAL).

Para entrar al estudio de éste tema, es preciso abordar tanto la finalidad de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (UNCITRAL) como de las dos leyes que nos ocupan: la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional sobre Comercio Electrónico y la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional sobre Firmas Electrónicas ***(18)***, cada una con la respectiva guía para su incorporación al derecho interno.

---

(17) CABALLERO GIL, Pino. Artículo publicado en el Boletín electrónico del Criptonomicón en la siguiente dirección de internet: http://www.criptonomicon.com.
(18) La presente información fue obtenida al consultar la siguiente dirección electrónica: http://www.un.or.at

La Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (UNCITRAL), se estableció el 17 de diciembre de 1966 como órgano auxiliar de la Asamblea General de la Organización de las Naciones Unidas, con el mandato expreso de fomentar la armonización y la unificación progresivas del derecho mercantil internacional y de tener presente, el interés de todos los pueblos, en particular el de los países en desarrollo, en el progreso amplio del comercio internacional.

El objetivo de impulsar el desarrollo del derecho internacional privado, promover la uniformidad y armonización de la legislación mercantil, se materializará en cuanto todos los estados del mundo adopten las convenciones y leyes modelo que propone la UNCITRAL.

Toda ley modelo tiene por finalidad orientar a los Estados para adecuar a su derecho interno reglas sobre actos que se desarrollan en el ámbito internacional y que en cierto tiempo, deben ser observadas en sus respectivos ordenamientos jurídicos para evitar que entren en un “aislamiento”, pero permitiendo el libre albedrío de los mismos respecto de la posibilidad de su adopción.

Dicho aislamiento económico surge entonces debido a la inobservancia de ciertas disposiciones del orbe mundial lo cual derivaría en situaciones complejas como falta de inversión extranjera e incluso nacional en un mercado con un futuro incierto ante la falta de garantías para invertir.

Para que una ley modelo sea elevada a obligatoria dentro del ordenamiento jurídico de un Estado, es necesario en primer plano, que exista la necesidad de incorporarla a su orden jurídico, en segundo, que la ley a adoptar no sea contraria a lo que su ordenamiento legal establece y tercero, que su adopción no ocasione un perjuicio mayor al beneficio que ofrezca.

La adopción de un país de un texto emitido por la UNCITRAL tiene un efecto de reconocimiento universal inmediato culminado por las negociaciones realizadas, evitando contradicciones entre el texto en cuestión y el ordenamiento jurídico positivo en el Estado que lo va a adoptar.

Tanto la Ley Modelo de la CNUDMI sobre Comercio Electrónico como la Ley Modelo de la CNUDMI sobre Firmas Electrónicas exaltan la necesidad de que las legislaciones de cada uno de los Estados vayan a la vanguardia, toda vez que la legislación vigente impone o supone restricciones al empleo de los medios modernos de comunicación y la figura del comercio electrónico.

La Asamblea General de la Organización de las Naciones Unidas adopta en la Resolución 51/162 del 16 de diciembre de 1996, la Ley Modelo sobre Comercio Electrónico cuyo principal objetivo es facilitar el uso de medios modernos de comunicación y de almacenamiento de información, basándose en el establecimiento de un equivalente funcional de conceptos conocidos en el tráfico habitualmente operado sobre papel, como serían los conceptos "*escrito, firma* y *original*".

La Ley Modelo de la CNUDMI sobre Comercio Electrónico tiene por finalidad orientar a los Estados para adecuar a su derecho interno reglas sobre los actos de comercio que en las últimas décadas se han llevado a cabo sin el uso tradicional del papel, tales como el correo electrónico y el intercambio electrónico de datos, esto es, induce a la desaparición de las barreras existentes entre un sistema jurídico y otro encaminándose al fenómeno de la globalización.

Esta Ley Modelo proporciona los criterios para apreciar el valor jurídico de los mensajes electrónicos y será muy importante para incrementar y respaldar el uso de las comunicaciones que se realizan sin el uso del papel.

De esta manera, la Ley Modelo en cita y su respectiva Guía para la incorporación al derecho interno se encuentran estructuradas de la siguiente manera:

La Ley Modelo de la CNUDMI sobre Firmas Electrónicas respalda su efectividad en mejorar el entendimiento de este tipo de firmas y reforzar la confianza en determinadas técnicas para su creación en operaciones de suma importancia jurídica, a la vez de ayudar a los Estados a establecer un marco legislativo moderno, armonizado y equitativo para abordar de manera más eficaz las cuestiones relativas a las firmas electrónicas.

Además, al establecer con la flexibilidad conveniente una serie de normas básicas de conducta para las diversas partes que puedan participar en el empleo de firmas electrónicas (firmantes, terceros que actúen confiando en el certificado y terceros prestadores de servicios), la Ley Modelo puede ayudar a configurar prácticas comerciales más armoniosas en el ciberespacio.

Como complemento a la Ley Modelo de la CNUDMI sobre Comercio Electrónico, la Ley Modelo sobre Firmas Electrónicas plantea prácticas normas para comprobar la fiabilidad técnica de estas firmas ofreciendo además, un vínculo entre dicha fiabilidad técnica y la eficacia jurídica que cabe esperar de una firma electrónica determinada.

La Ley Modelo sobre Firmas Electrónicas supone entonces, una contribución importante a la Ley Modelo sobre Comercio Electrónico al adoptar un criterio

conforme al cual puede determinarse previamente la eficacia jurídica de una determinada técnica de creación de una firma electrónica.

Los principales objetivos de ésta Ley Modelo sobre Firmas Electrónicas son el permitir o facilitar el empleo de firmas electrónicas así como brindar una igualdad de trato tanto a los usuarios que cuentan con documentación consignada sobre papel como a los que tienen una información consignada en cualesquiera soporte informático, los cuales son fundamentales para promover la economía y la eficiencia del comercio internacional.

En ese orden de ideas, la Asamblea General de la Organización de las Naciones Unidas adopta en la Resolución 56/80 del 12 de diciembre de 2001 la Ley Modelo de la CNUDMI sobre Firmas Electrónicas y su respectiva guía, mismas que se estructuraron de la siguiente forma:

Primera parte.

Artículo 1 Ámbito de aplicación.
Artículo 2. Definiciones.
Artículo 3. Igualdad de tratamiento de las tecnologías para la firma.
Artículo 4. Interpretación.
Artículo 5. Modificación mediante acuerdo.
Artículo 6. Cumplimiento del requisito de firma.
Artículo 7. Cumplimiento de lo dispuesto en el artículo 6.
Artículo 8. Proceder del firmante.
Artículo 9. Proceder del prestador de servicios de certificación.
Artículo 10. Fiabilidad.
Artículo 11. Proceder de la parte que confía en el certificado.
Artículo 12. Reconocimiento de certificados extranjeros y de firmas electrónicas extranjeras.

Segunda parte

GUÍA PARA LA INCORPORACIÓN DE LA LEY MODELO DE LA CNUDMI PARA LAS FIRMAS ELECTRÓNICAS (2001) AL DERECHO INTERNO.
Finalidad de la presente Guía.
Capítulo I. Introducción a la Ley Modelo.

I. FINALIDAD Y ORIGEN DE LA LEY MODELO.
A. Finalidad.
B. Antecedentes.
C. Historia.

II. LA LEY MODELO COMO INSTRUMENTO DE ARMONIZACIÓN DE LEYES.

III. OBSERVACIONES GENERALES SOBRE LAS FIRMAS ELECTRÓNICAS.
A. Funciones de las firmas.
B. Firmas numéricas y otras firmas electrónicas.

La Comisión de las Naciones Unidas para el Derecho Mercantil Internacional ha afirmado que el propósito de ambas leyes no es restringir o coartar el uso de los medios electrónicos de comunicación sino por el contrario, su finalidad es facilitar y garantizar que las negociaciones así realizadas tengan un reconocimiento y soporte legal suficiente y bastante.

1.4 El comercio en la actualidad. Comercio electrónico y sus ventajas.

En los albores del comercio, los fenicios como expertos navegantes que eran se trasladaban de un lugar a otro llevando consigo las mercancías más diversas y extrañas que pudieran existir en aquélla época teniendo un amplio dominio sobre el resto de los comerciantes quienes tenían que aceptar las condiciones impuestas por quien tenía el control sobre el mercado.

Posteriormente, el Imperio Romano se colocaba a la vanguardia en la actividad comercial pues al tener el control absoluto, Roma hacía valer su jerarquía para con todos los pueblos dominados aplicando imposiciones por demás arbitrarias.

Con el progreso en la navegación, España e Inglaterra en su carrera por el dominio de los mares accidentalmente descubren el Continente Americano y con ello, obtienen un mercado que les proveería de una vasta variedad de materias primas hasta entonces desconocidas en el viejo continente, incrementando así el potencial comercial de éstas naciones; pudiendo mencionar como partícipes de ésta carrera comercial a Portugal y China.

Con la independencia de los países americanos, surge una mayor competencia que no se enfocaba ahora única y exclusivamente al control del comercio marítimo, sino que se traslada a tierra a través de diversos mecanismos los cuales, la mayor de las veces no tenían otro fin más que el de fincar un monopolio evitando con ello el desarrollo armónico y equitativo que sugiere la convivencia mundial.

Así, con los avances tecnológicos y la apertura del comercio mundial, llegamos a un punto determinante y por todos conocido: cualquier conflicto bélico trae aparejada una evolución enfocada en mayor parte al ramo de las telecomunicaciones y el comercio la cual la mayor de las veces, no suele ser equitativa ni para los países en conflicto ni para los demás estados del orbe, teniendo en las dos guerras mundiales una clara muestra de ello.

Ante este panorama, hoy es posible realizar todo tipo de operaciones de una forma tan simple que no podemos imaginar a donde desembocará ésta revolución tecnológica, los beneficios y perjuicios que pudiere traer aparejados y por encima de todo, la seguridad y el respaldo jurídico que protegerán al usuario de los nuevos servicios comerciales.

Por lo anterior y respecto a la problemática que implica la contratación de servicios o adquirir bienes empleando medios electrónicos, es necesario efectuar un breve análisis del contrato así como de sus elementos para encontrarnos en la posibilidad de entender los efectos que la cada vez más frecuente contratación por estos medios tendrá en el ámbito jurídico.

De esa manera, citaré en principio al deber jurídico que se define como *"la necesidad de observar voluntariamente una conducta conforme a lo que prescribe una norma de derecho"* ***(19)***, refiriendo el maestro Gutiérrez y González que el deber jurídico en *stricto sensu "es la necesidad de observar voluntariamente una conducta, conforme a lo que prescribe una norma de derecho, ya a favor de la colectividad, ya de persona determinada"*.

Ahora bien y respecto a la obligación, las Institutas de Justiniano la definen como *"obligation est iuris vinculum quo necesitatem astringimur alicuius solvendae rei secundum nostrae civitatis iura",* o bien, *"la obligación es el vínculo jurídico que nos constriñe con la necesidad de pagar alguna cosa conforme o según a las leyes de nuestra ciudad"*.

Por otra parte, el concepto de obligación en *latu sensu* implica la necesidad jurídica de cumplir voluntariamente con una prestación de carácter patrimonial (pecuniaria o moral), a favor de un sujeto que eventualmente pueda llegar a existir o a favor de un sujeto que ya existe.

---

(19) GUTIERREZ Y GONZÁLEZ, Ernesto. "Derecho de las obligaciones". Editorial Porrúa, Décima Segunda edición. México, 1997. p 42.

En ese mismo orden, es preciso mencionar que para el Maestro Rojina Villegas el contrato se define como *"...un acuerdo de voluntades para crear o transmitir derechos y obligaciones; es una especie dentro del género de los convenios..."*; por otra parte, el convenio *"...es un acuerdo de voluntades para crear, transmitir, modificar o extinguir obligaciones y derechos reales y personales, por lo tanto, el convenio tiene dos funciones: una positiva que es crear o transmitir obligaciones y derechos, y otra negativa: modificarlos o extinguirlos"*. ***(20)***

Luego entonces, un convenio es un acuerdo de voluntades celebrado para modificar o extinguir derechos y obligaciones, mientras tanto, un contrato es el acuerdo de voluntades para crear o transmitir derechos y obligaciones.

Al respecto, es conveniente precisar los conceptos de acto jurídico y hecho jurídico.

Rojina Villegas nos dice que el hecho jurídico *"es un fenómeno de la naturaleza o del hombre que realiza la hipótesis normativa para que se produzcan las consecuencias de derecho"*. ***(21)***

Por otro lado, el Maestro Gutiérrez y González, define al hecho jurídico como *"toda conducta humana o ciertos fenómenos de la naturaleza, que el derecho considera para atribuirles consecuencias jurídicas"*.

En opinión de Rojina Villegas, el acto jurídico es *"una manifestación de voluntad que se realiza con el objeto de producir determinadas consecuencias de derecho"* ***(22).*** Para Gutiérrez y González, el acto jurídico *"es la manifestación exterior de la voluntad que se hace con el objeto de crear, transmitir, modificar o extinguir una obligación o un derecho y que produce el efecto deseado por su autor, porque el derecho sanciona esa voluntad"*. ***(23)***

---

(20) ROJINA VILLEGAS, Rafael. "Compendio de Derecho Civil. Tomo IV. Contratos." Editorial Porrúa, Vigésima Sexta edición. México, 1999. p 7.
(21) GUTIERREZ Y GONZÁLEZ, Ernesto. Op cit. p 157.
(22) ROJINA VILLEGAS. Rafael. Op cit. p 99.
(23) GUTIERREZ Y GONZÁLEZ, Ernesto. Op cit. p 155.

Hecha la distinción anterior entre hechos y actos jurídicos, haremos una breve mención del acto jurídico y sus elementos, pues el presente trabajo tiene una particular relación con la contratación realizada a través de medios electrónicos.

Como elementos de existencia del acto jurídico tendremos al consentimiento y al objeto, como requisitos de validez la capacidad, la forma, la ausencia de vicios de la voluntad y la licitud en el objeto (motivo o fin).

Así pues, el acto jurídico debe tener una serie de elementos que brinden la certeza de que el acto existe y una vez que existe, requiere otra serie de atributos para ser considerado como válido.

Por otra parte, el acto jurídico puede ser existente o inexistente, válido o nulo; donde la inexistencia y la validez no admiten grados por lo que sólo existen actos inexistentes y actos existentes válidos. Por el contrario, la nulidad si admite grados admitiendo la diferenciación entre actos inexistentes afectados de nulidad absoluta y actos inexistentes afectados de nulidad relativa.

El acto inexistente es *"el que no reúne los elementos de hecho que suponen su naturaleza o su objeto, y en ausencia de los cuales es lógicamente imposible concebir su existencia".**(24)* Los actos jurídicos válidos tienen eficacia plena, producen todos los efectos de que son susceptibles, sin embargo, no sucede lo mismo con los actos atacados de invalidez y la suerte de dichos actos no puede determinarse con una palabra como la de los actos válidos.

A su vez, el Maestro Rafael Rojina Villegas nos refiere que *"en la inexistencia falta al acto un elemento esencial. En la nulidad el acto jurídico existe, por cuanto que tiene todos sus elementos esenciales, pero algunos de ellos padecen de un vicio que les resta validez. Este vicio puede ser interno, originando la nulidad relativa o externo, motivando la absoluta". **(25)***

---

(24) BORJA Soriano, Manuel. "Teoría General de las obligaciones". Editorial Porrúa, Décima Octava edición. México, 2001. p 94.
(25) ROJINA Villegas, Rafael. op cit. p 127.

Por cuanto a sus características, la nulidad absoluta: *es imprescriptible, inconfirmable, puede ser invocada por cualquier interesado jurídicamente y generalmente, produce efectos que pueden ser destruidos retroactivamente."*

Resultando entonces que todo acto ejecutado contra lo que mande o prohíba una ley imperativa o prohibitiva, será nulo absolutamente y no podrá ser consentido o adquirir validez invocando el simple transcurso del tiempo.

De esta manera, la nulidad relativa al igual que la absoluta *"…nace en el acto y lo vicia desde su nacimiento, pero la diferencia radica esencialmente en que va en contra de una disposición legal pero establecida a favor de determinadas personas…"*; resultando que para el supuesto de un acto afectado de nulidad relativa, debe ser ratificable, prescriptible, producir efectos y la acción para reclamarla corresponde a la parte afectada.

Respecto al consentimiento, el maestro Rojina Villegas lo define como *"…el acuerdo o concurso de voluntades que tiene por objeto la creación o transmisión de derechos y obligaciones." **(26)***; a su vez, el maestro Gutiérrez y González refiere que el consentimiento *"…es el acuerdo de dos o mas voluntades que tiende a crear, transferir, conservar, modificar o extinguir, efectos de derecho y es necesario que esas voluntades tengan una manifestación exterior". **(27)***

El consentimiento entonces, implica la manifestación de dos o mas voluntades y su acuerdo sobre un punto de interés jurídico componiéndose de dos elementos como lo son la oferta o policitación y la aceptación; elementos independientes que en determinadas circunstancias son susceptibles de producir efectos por si mismos aún cuando no lleguen a conformar el consentimiento.

---

(26) ROJINA Villegas, Rafael. op cit. p 271.
(27) GUTIÉRREZ Y GONZÁLEZ, Ernesto. op cit. p 249.

De tal suerte, el consentimiento puede ser expreso cuando se manifieste por escrito, verbalmente, por medios electrónicos, ópticos o cualquier otra tecnología o ya empleando cualesquiera signos inequívocos; puede ser tácito cuando resulta de hechos o actos que lo presupongan o que autoricen a presumirlo, con la salvedad de los casos en que por ley o por convenio el consentimiento deba manifestarse expresamente.

La oferta como la manifestación unilateral de la voluntad para celebrar un contrato, es el medio a través del cual se da a conocer la materia de la contratación, puede hacerse ya sea a persona determinada o al público en general, bien se trate de persona que se encuentre presente o no en el lugar en que se realice la oferta.

Es en ese momento en que interviene una circunstancia para la formación del consentimiento como lo es el plazo para la aceptación de la oferta, esto es el tiempo que el oferente concede para que su oferta sea aceptada y durante el cual el oferente queda obligado a mantenerse en aptitud de cumplir con lo ofertado, que en términos de lo que el Código Civil Federal en su artículo 1806, será inmediato o por tres días, además del tiempo necesario para la ida y vuelta del correo público o a falta de éste, del que se juzgue necesario, según la facilidad o dificultad de las comunicaciones.

Ahora bien, Gutiérrez y González nos define la aceptación como *"una declaración unilateral de voluntad, mediante la cual se expresa la adhesión a la propuesta, policitación u oferta."**(28)*

Planiol refiere que *"…la aceptación puede revestir como la oferta una forma verbal o escrita; puede también y más frecuentemente que la oferta, ser tácita e inducirse de ciertos hechos que impliquen en su autor la intención de aceptar la proposición que se le ha hecho. Las circunstancias que varían revelan la aceptación no expresa." **(29)***

---

(28) GUTIÉRREZ Y GONZÁLEZ, Ernesto. op cit. p 257.
(29) PLANIOL. Marcel. "Tratado elemental de Derecho Civil, Obligaciones". Traducción de José M. Cajica Jr. Editorial Puebla, México, 1945. p 23.

Luego entonces, la aceptación se trata de una declaración unilateral de la voluntad que puede hacerse de manera tácita o expresa pero contrario a la oferta, la aceptación deberá hacerse a persona determinada, siendo aquella persona a cuya oferta se quiere aceptar, también puede hacerse a persona presente o ausente, con o sin fijación de plazo.

La aceptación debe hacerse lisa y llanamente pues de lo contrario, cualquier modificación implicaría la creación de una nueva oferta, convirtiéndose el oferente en posible aceptante y el posible aceptante de la oferta original se convierte en solicitante.

Tratándose del momento de perfeccionamiento del consentimiento, éste sucede cuando se recibe la aceptación de la propuesta o las condiciones con que la misma se modificó manifestando la adhesión a dichas modificaciones; mas respecto a la contratación a través de medios electrónicos, dicha práctica implica principalmente aceptar que las condiciones son diversas y las instituciones tradicionales tales como la firma y el documento, deben superar los problemas de carácter práctico que pudieran vulnerar la seguridad jurídica de los contratantes.

Aquí es donde entra la figura de la firma electrónica que va a brindar seguridad jurídica a los usuarios de los medios electrónicos y a quienes ofrecen sus productos y servicios empleando dichos medios.

¿E-commerce?, ¿comercio *on-line*?, ¿e-bussiness?, son nuevos términos que la tecnología ha aportado a nuestro léxico ordinario y a la vida del comercio, refiriéndose todos ellos a la nueva forma de hacer comercio: el comercio electrónico.

En términos generales, el comercio electrónico *"…es todo intercambio de datos que se realiza por medios electrónicos, esté o no relacionado estrictamente con la actividad comercial".*

En un sentido más estricto, debe entenderse por comercio electrónico a *"…aquél cuya actividad se circunscribe a las transacciones electrónicas desarrolladas a través de los mecanismos que proporcionan tecnologías tales como el correo electrónico, la web o el EDI"*.

Su principal característica es provocar la transformación de los usuales procesos y mecanismos de transacción basados en papel, en procesos digitales en los que la letra impresa es reemplazada por el lenguaje binario digital (cadenas interminables de unos y ceros combinados con signos).

Contrario a lo que se cree, el comercio electrónico no es un fenómeno nuevo, sino que sus primeras manifestaciones sucedieron en la década de los ochentas, siendo de todas ellas la más consolidada y aún vigente el EDI (Electronic Data Interchange) que consiste en la realización de transacciones comerciales en forma automatizada mediante el intercambio de todo tipo de instrucciones (órdenes de compra, ventas, pagos, transferencias) entre dos computadoras determinadas.

Dicho intercambio se ve sometido a las normas técnicas de estructuración de mensajes de datos, por virtud de las cuales se estandariza un tipo de mensaje que por la frecuencia de su empleo e importancia de su contenido, conviene someter a una forma o formato electrónico riguroso, preciso y facilmente utilizable por los sujetos que intervienen en el tráfico.

Por lo general, el EDI se desarrolla a través de redes cerradas proporcionadas por un proveedor de servicios determinado, entre integrantes de un mismo sector económico (los bancos por ejemplo) que luego de una etapa de conocimiento y negociación logran establecer protocolos compatibles que les permiten realizar transacciones entre sí.

La novedad que trajo Internet a este tipo de formas de realizar transacciones electrónicas es la posibilidad de efectuarlas sin que sea necesario realizar un

acuerdo bilateral previo o sin siquiera conocer a la parte con la cual se está contratando, por tal motivo y a diferencia del EDI, Internet permite que personas y/o empresas hasta entonces desconocidas puedan relacionarse ocasionalmente sin necesidad de contactos previos.

Pero lo antedicho no ha dictado la sentencia de muerte del EDI sino por el contrario, muchas empresas están desarrollando un nuevo navegador de Internet para plataformas EDI que permita conducir el tráfico generado por dicha actividad a través de Internet de una manera más económica, flexible, confiable y accesible que el EDI tradicional.

Con esta nueva modalidad llamada Open EDI, las partes implicadas podrán relacionarse directamente a través de Internet sin acuerdos previos.

Por lo anteriormente expuesto, no es ninguna novedad que el comercio electrónico genere miedo e incertidumbre entre los usuarios de éste servicio, principalmente en aspectos tales como:

- Identificación de las partes.
- Momento de perfeccionamiento del contrato.
- Validez y eficacia de las transacciones electrónicas.
- Prueba del contrato.
- Distribución de responsabilidad entre los contratantes.
- Problemas de inseguridad y confidencialidad en la información.
- Ley aplicable.
- Jurisdicción competente.
- Formas de pago seguras.

“Evidentemente, para que el comercio electrónico pueda desarrollarse se necesita que todos los usuarios involucrados en esta nueva forma de hacer negocios tengan confianza en que sus transacciones no serán interceptadas ni modificadas, que las partes contratantes son las que dicen ser, que los mecanismos de transacción y pago son seguros y que en caso de conflicto, estarán amparados

*por normas y procedimientos eficaces a fin de salvaguardar sus derechos. Hasta que esto no se logre, el comercio electrónico seguirá siendo una realidad para pocos y una utopía para muchos". **(30)***

Significa entonces que, si bien unos cuantos países han adoptado reglas especiales para regular determinados aspectos del comercio, en el orbe aún se advierte la ausencia de un régimen general de tal práctica mercantil en materia electrónica.

De ello puede resultar incertidumbre acerca de la naturaleza jurídica y la validez de la información presentada en otra forma que no sea la de un documento tradicional sobre papel.

Además, la necesidad de un marco legal seguro y de prácticas eficientes se presenta no sólo en aquellos países en los que se está difundiendo el empleo del Intercambio Electrónico de Datos y del Correo Electrónico, sino también en otros muchos países en los que se ha difundido el empleo del fax, el télex (prácticamente en desuso) y otras técnicas de comunicación semejantes.

Aunque las operaciones son seguras tecnológicamente en la firma de confección, las ventas en línea se realizan con riesgos debido a que dada la falta de legislación, la posible reclamación de un cliente que niegue la compra realizada con tarjeta de crédito perjudica en primera instancia al vendedor.

Es cierto que en múltiples legislaciones como la nuestra se ha aceptado que un documento en sentido amplio "es toda manifestación material, destinada e idónea para reproducir una cierta manifestación del pensamiento" ***(31)***, pero en la práctica nuestros jueces y funcionarios difícilmente lograrán concebir la palabra "documento" sin relacionarla con "papel".

---

(30) Esta información se puede consultar en la siguiente página en internet:: http://www.geocities.com
(31) CHIOVENDA, Giusseppe. Principios de Derecho Procesal Civil. Ed. Porrúa, México, 1984. Tomo II. p. 334.

Otro punto esencial es cómo funciona la protección al consumidor en negocios globales, pues puede terminar obligado a recurrir a un tribunal en el extranjero, cosa que muchos de nosotros no haremos, así que lo habitual es que todo negocio que se consume empleando éste medio quede simplemente en manos de la buena fe de las partes (algo sumamente difícil para nuestros tiempos).

La imparable expansión de Internet y el desarrollo del comercio electrónico están transformando la economía y la forma de hacer negocios, por lo tanto, la necesidad de adecuar la legislación a esta nueva realidad parece clara. Ante la reforma aprobada a finales del 2003, resultará interesante estudiar las expectativas y los efectos que tendrá el comercio electrónico en nuestro país.

Otra asignatura pendiente además de la atención al cliente virtual, es la obligación de ofrecer una información lo más clara y completa sobre los productos y servicios ofrecidos para de ésta forma, brindarle al consumidor todas las garantías que le permitan realizar con plena confianza todo tipo de transacción electrónica.

En este aspecto es fundamental una regulación específica y concisa que permita al consumidor saber que producto o servicio exactamente está adquiriendo y cual es su costo (si se incluyen impuestos, gastos de envío, etc.) para así tener un respaldo ante una posible reclamación.

En México, si bien es cierto que la tecnología es accesible para todas las empresas, también es una realidad la falta de desarrollo en la infraestructura de telecomunicaciones que permita un incremento en la accesibilidad a tales tecnologías a un mayor número de empresas y usuarios.

A los problemas técnicos se suma el inconveniente de un marco jurídico confuso donde la transparencia y la credibilidad son dos exigencias que la industria en general tiene hacia las autoridades mexicanas y en donde los empresarios manifiestan que el marco jurídico se encuentra sentado sobre bases correctas pero hace falta rapidez y actualidad en el Derecho Positivo vigente.

Esto quiere decir que en México, la evolución de la tecnología ha rebasado al gobierno y a los legisladores, quienes lejos de mantener al país en una constante actualización, lo han mantenido en la apatía permaneciendo como simples espectadores frente al Comercio Electrónico que se ha erigido como una de las más claras manifestaciones de la globalización mundial.

Por todo lo anteriormente enunciado es necesario mencionar las principales ventajas que ofrece el comercio electrónico cuando se ubica dentro de un adecuado ordenamiento jurídico:

1) Seguridad, facilidad y rapidez en la realización de transacciones,
2) Comodidad para el consumidor,
3) Proyección a nivel internacional de los productos de las empresas (desde las pequeñas hasta las grandes empresas),
4) Reducción de costos de operación y una consiguiente optimización en el manejo de la comercialización de los productos,
5) Un mejor aprovechamiento de la jornada laboral,
6) Minimización de errores,
7) Certeza sobre la competencia de los tribunales que conozcan de una controversia que se suscitare en la materia,
8) Pleno conocimiento de la ley aplicable al caso concreto controvertido,
9) Incremento de las ventas,
10) Eliminación de intermediarios,
11) Disminución del precio final del producto,
12) Surgimiento de nuevas empresas,
13) Una logística infalible,
14) Beneficios para el estado al obtener ingresos mayores por concepto de importación y exportación de productos, y;
15) Desarrollo en la calidad de los productos ofrecidos.

CAPÍTULO SEGUNDO.

"Es indiscutible que las nuevas tecnologías de la información se presentan como una oportunidad inmejorable para que los países menos desarrollados o emergentes puedan achicar la brecha que los separa con los denominados países del primer mundo. La firma digital es un instrumento más que permite la adaptación a este nuevo paradigma socio-económico-cultural, que posibilita la expansión del comercio dentro de esta nueva economía digital globalizada, rediseña las relaciones laborales y la interacción humana y, a su vez, en el ámbito administrativo o gubernamental, optimiza la eficiencia a un bajo costo, con intervención y participación de los administrados (ciudadanos), lo que importa dotar al sistema de una mayor transparencia y obtener la consecuente reducción del gasto público y restablecer la credibilidad en las instituciones democráticas, algo que debe garantizar todo Estado social de Derecho."

DR. HUGO DANIEL CARRION.

Legislación Argentina en materia de Comercio Electrónico.

2.1 Marco jurídico del Comercio Electrónico. *(1)*

Cuando los legisladores presentaron ante el Congreso de la Unión de la Nación Argentina el Anteproyecto de Ley Formato Digital de los Actos Jurídicos referente al Comercio Electrónico, la exposición de motivos fue contundente al manifestar respecto de la carencia de una normatividad jurídica en relación al comercio electrónico y previo al establecimiento dentro del marco jurídico argentino que:

> *"Es por consiguiente necesario, hacer referencia a las situaciones y condiciones existentes y exponer las consideraciones iniciales sobre la forma de concreción de una ley de estas características dado que, la problemática a considerar importa conocer, en primer término, las mecánicas y operatividad representativas de las nuevas tecnologías y su influencia en la sociedad, para considerar luego, los alcances de un marco legal apropiado".*

Lo cual se acentúa en términos de lo siguiente:

> *"En el contexto mundial de referencia, nuestro país se encuentra gravemente desactualizado".*

Por ello, el legislador argentino se enfocó a realizar un análisis detallado de la tendencia mundial encaminada al comercio electrónico el cual ya era objeto de estudio en diversos foros internacionales y nacionales.

Desde el año de 1997 en que el Estado de UTAH en Estados Unidos inició la legislación del comercio electrónico con su "Digital Signature Act" ("Marco para el Comercio Electrónico"), todos los países del orbe se han dedicado a elaborar un ordenamiento jurídico interno que vaya en armonía con lo que la llamada "Sociedad de la Información" demanda.

---

(1) Salvo que se cite otra fuente, la realización del presente Capítulo fue posible al consultar las siguientes direcciones: pki.gov.ar; infoleg.mecon.ar; sfp.gov.ar; itu.ch; itl.nist.gov; smartcardsys.com; rsa.com; ietf.org, y; ftp.isi.edu.

Es innegable que el mundo ha evolucionado vertiginosamente en los últimos años debido a la relación tan íntima existente entre la tecnología informática y las telecomunicaciones y mantenerse al margen de tal revolución tecnológica significaría colocarse en un estado atávico excluyente de la sociedad mundial.

Este fenómeno denominado “Sociedad de la Información” ha tenido como fundamental avance tecnológico la digitalización de la información, lo que deriva en el almacenamiento de grandes cantidades de datos y su desplazamiento en cuestión de segundos, lo cual se refleja en una significativa reducción de costos y de empleo de recursos humanos.

Ante la acometida tecnológica que caracteriza a nuestro tiempo, era imposible quedarse al margen en lo que respecta a la materia de la electrónica, situación que Estados tales como Australia, Estados Unidos, Canadá, Irlanda, Reino Unido, Bermuda, Francia, Alemania, Italia, Dinamarca, España, Portugal, Colombia, Singapur, Hong Kong, Corea, Malasia, India, Chile, Brasil, Ecuador, Perú, Japón y por supuesto Argentina y México entre otros, han tomado en cuenta y adoptado en sus legislaciones o comenzado a contemplar la figura del comercio electrónico y todas las consecuencias y modalidades que trae aparejadas consigo.

Y no podría ser más evidente: la era tecnológica no solamente alienta el desarrollo económico mundial, sino también nos sirve para desarrollar una cultura de transparencia en el manejo de los recursos públicos y el gobierno electrónico o virtual, coloca al gobernador a la vista de cualquier interesado en su desenvolvimiento en un lugar donde sin excusa ni pretexto, será analizado, criticado, descalificado y recriminado por sus errores o falta de previsión en cualquier ámbito que su proceder le haga responsable.

La República Argentina es la que más atención captó para el presente trabajo de investigación por ser una de las primeras naciones de América Latina (junto con Chile) en colocar su gobierno dentro del plano virtual y adoptar en su legislación a

la figura del Comercio Electrónico y en especial a la Firma Digital, así como al ente certificador de ésta: el Prestador de Servicios de Certificación de Firma Electrónica.

El dieciséis de abril de 1998, el legislador argentino emitió el Decreto número 427/98 mediante el cual, estableció el régimen al que se ajustaría el empleo de la firma digital en la instrumentación de los actos internos de la Administración Pública Nacional (entendiendo como tales a aquéllos que no produzcan efectos jurídicos individuales en forma directa), cuyos efectos serían los mismos e inclusive, superiores a los que la firma ológrafa tiene para generar garantía de confianza.

Este Decreto se apoyó en la necesidad de optimizar la actividad del Gobierno adecuando sus sistemas de registro de datos, tendiendo a eliminar el uso del papel y automatizando sus circuitos administrativos; motivo suficiente para que se diera a la tarea de difundir el uso de las nuevas tecnologías, promoviendo el mecanismo de la firma digital considerando principalmente la repercusión positiva que hasta entonces había tenido al ser incorporada en la legislación del sector tanto público como privado de otros países.

Tal postura se apegó a que la firma digital tiene como característica esencial que cumple con la condición de no repudio, la cual significa que sin lugar a dudas una persona efectivamente firmó un documento digital y que dicho documento no fue alterado desde el momento de su firma, siempre y cuando su implementación se haya ajustado a los procedimientos descritos por el Decreto en cita.

Por lo anterior, el legislador argentino consideró como una medida indispensable establecer una Infraestructura de Firma Digital para el Sector Público Nacional con el fin de crear las condiciones de un uso confiable del documento suscrito digitalmente, pues dada su índole, era necesario que la autorización del empleo de la tecnología de la firma digital en el ámbito de este sector se sujetara a un término

de vigencia (dos años) que permitiera evaluar tanto su funcionamiento en las diferentes jurisdicciones como el grado de confiabilidad y seguridad del sistema.

En ese sentido, el Decreto 427/98 en su artículo 3º estableció que:

> *"Las disposiciones del presente Decreto serán de aplicación en todo el ámbito del Sector Público Nacional, dentro del cual se comprende la administración centralizada y la descentralizada, los entes autárquicos, las empresas del Estado, Sociedades del Estado, Sociedades Anónimas con participación estatal mayoritaria, los bancos y entidades financieras oficiales y todo otro ente, cualquiera que sea su denominación o naturaleza jurídica, en que el Estado Nacional o sus organismos descentralizados tengan participación suficiente para la formación de sus decisiones."*

Delegando de esta manera en cada uno de los organismos del Sector Público Nacional el control de los medios que resulten adecuados para extender el empleo de la tecnología de la firma digital, esto en función de los recursos con los que cuenten para realizarlo en el plazo más corto posible.

Así tenemos que en la Subsecretaría de la Gestión Pública dependiente de la Jefatura de Gabinete de Ministros, recae la función de Autoridad de Aplicación del Decreto 427/98 estando facultada además, para dictar los manuales de procedimiento de las Autoridades Certificantes Licenciadas y de los Organismos Auditante y Licenciante, así como los estándares tecnológicos aplicables a las claves mismos que deberán ser definidos en un plazo no mayor de 180 días naturales y cuyos contenidos deberán reflejar el último estado de los avances en la materia (artículo 6º).

Luego entonces, los organismos del Sector Público Nacional deberán informar a la Autoridad de Aplicación y con la periodicidad que ésta establezca, las aplicaciones que concreten de la tecnología autorizada por el presente Decreto.

La Subsecretaria de la Función Pública de la Jefatura de Gabinete de Ministros desempeñaría las funciones de Organismo Licenciante y la Contaduría General de

la Nación, dependiente de la Subsecretaría de Presupuesto de la Secretaría de Hacienda del Ministerio de Economía y Obras y Servicios Públicos, cumpliría con las funciones de Organismo Auditante.

El multicitado Decreto 427/98, en su Anexo I estableció la Infraestructura de Firma Digital para el Sector Público Nacional, delimitando las funciones de los organismos encargados de realizar las funciones necesarias para implementar en el Gobierno el uso de la firma digital, a lo cual me permito transcribir a continuación el referido anexo.

ORGANISMO LICENCIANTE

Funciones:

1. Otorga las licencias habilitantes para acreditar a las autoridades certificantes y emite los correspondientes CERTIFICADOS DE CLAVE PÚBLICA, que permiten VERIFICAR LAS FIRMAS DIGITALES de los CERTIFICADOS que éstas emitan;

2. Deniega las solicitudes de licencias a las autoridades certificantes que no cumplan con los requisitos establecidos para su autorización;

3. Revoca las licencias otorgadas a las AUTORIDADES CERTIFICANTES LICENCIADAS que dejan de cumplir con los requisitos establecidos para su autorización;

4. Verifica que las AUTORIDADES CERTIFICANTES LICENCIADAS utilicen sistemas TECNICAMENTE CONFIABLES;

5. Considera para su aprobación el manual de procedimientos, el plan de seguridad y el de cese de actividades presentados por las autoridades certificantes;

6. Acuerda con el ORGANISMO AUDITANTE el plan de auditoria para las AUTORIDADES CERTIFICANTES LICENCIADAS;

7. Dispone la realización de auditorias de oficio;

8. Resuelve los conflictos individuales que se susciten entre el SUSCRIPTOR de un CERTIFICADO y la AUTORIDAD CERTIFICANTE LICENCIADA emisora del mismo;

9. Resuelve todas aquellas contingencias respecto a la Infraestructura de FIRMA DIGITAL.

Obligaciones:

En su calidad de SUSCRIPTOR de CERTIFICADO y de autoridad certificante, el ORGANISMO LICENCIANTE tiene idénticas obligaciones que las AUTORIDADES CERTIFICANTES LICENCIADAS, y además debe:

1. Abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder bajo ninguna circunstancia, a la CLAVE PRIVADA de cualquier SUSCRIPTOR de los CERTIFICADOS que emita;

2. Mantener el control de su propia CLAVE PRIVADA e impedir su divulgación;

3. Revocar su propio CERTIFICADO DE CLAVE PÚBLICA frente al compromiso de su CLAVE PRIVADA;

4. Permitir el acceso público permanente a los CERTIFICADOS DE CLAVE PÚBLICA que ha emitido en favor de las AUTORIDADES CERTIFICANTES LICENCIADAS, y a la LISTA DE CERTIFICADOS REVOCADOS, por medio de conexiones de telecomunicaciones públicamente accesibles. Esto también se aplica a la información sobre direcciones y números telefónicos de las AUTORIDADES CERTIFICANTES LICENCIADAS;

5. Permitir el Ingreso de los funcionarios autorizados del ORGANISMO AUDITANTE a su local operativo, poner a su disposición toda la información necesaria, y proveer la asistencia del caso;

6. Publicar su propio CERTIFICADO DE CLAVE PÚBLICA en el Boletín Oficial, y en DOS (2) diarios de difusión nacional, durante TRES (3) días consecutivos a partir del día de su emisión;

7. Revocar los CERTIFICADOS emitidos en favor de las AUTORIDADES CERTIFICANTES LICENCIADAS incursas en causales de revocación de licencia, o que han cesado sus actividades;

8. Revocar los CERTIFICADOS emitidos en favor de las AUTORIDADES CERTIFICANTES LICENCIADAS, cuando las CLAVES PÚBLICAS que en ellos figuran dejan de ser TECNICAMENTE CONFIABLES;

9. Supervisar la ejecución del plan de cese de actividades de las AUTORIDADES CERTIFICANTES LICENCIADAS que discontinúan sus funciones;

10. Registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas.

ORGANISMO AUDITANTE

Funciones:
1. Audita periódicamente al ORGANISMO LICENCIANTE y a las AUTORIDADES CERTIFICANTES LICENCIADAS;

2. Audita a las autoridades certificantes previo a la obtención de sus licencias;

3. Acuerda con el ORGANISMO LICENCIANTE el plan de auditoria para las AUTORIDADES CERTIFICANTES LICENCIADAS;

4. Audita a las AUTORIDADES CERTIFICANTES LICENCIADAS a solicitud del ORGANISMO LICENCIANTE:

5. Efectúa las revisiones de cumplimiento de las recomendaciones formuladas en las auditorias.

Obligaciones:
El ORGANISMO AUDITANTE debe:

1. Utilizar técnicas de auditoria apropiadas en sus evaluaciones;

2. Evaluar la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad, y disponibilidad de los datos, como así también el cumplimiento con las especificaciones del manual de procedimientos y el plan de seguridad aprobados por el ORGANISMO LICENCIANTE.

3. Verificar que se utilicen sistemas TECNICAMENTE CONFIABLES;

4. Emitir informes de auditoria con los hallazgos, conclusiones y recomendaciones en cada caso;

5. Realizar revisiones de seguimiento de las auditorias, para determinar si el organismo auditado ha tomado las acciones correctivas que surjan de las recomendaciones;

6. Emitir informes con las conclusiones de las revisiones de seguimiento de auditorias;

7. Intervenir en los simulacros de planes de contingencia;

8. Dar copia de todos los informes de auditoría por él emitidos al ORGANISMO LICENCIANTE.

AUTORIDAD CERTIFICANTE LICENCIADA

Funciones:

1. Emite CERTIFICADOS DE CLAVE PÚBLICA; Para emitir CERTIFICADOS DE CLAVE PÚBLICA, la AUTORIDAD CERTIFICANTE LICENCIADA debe:

a) Recibir del agente requirente una solicitud de EMISION DE CERTIFICADO DE CLAVE PÚBLICA, la cual deberá estar firmada digitalmente con la correspondiente CLAVE PRIVADA;

b) Verificar fehacientemente la información identificatoria del solicitante, la cual deberá estar siempre incluida en el CERTIFICADO, y toda otra información que según lo dispuesto en el manual de procedimientos de la AUTORIDAD CERTIFICANTE LICENCIADA, deba ser objeto de verificación, lo cual deberá realizarse de acuerdo a lo dispuesto en el citado manual;

c) Numerar correlativamente los certificados EMITIDOS;

d) Mantener copia de todos los CERTIFICADOS emitidos, consignando su fecha de emisión.

La AUTORIDAD CERTIFICANTE LICENCIADA puede, opcionalmente, incluir en un CERTIFICADO información no verificada, debiendo indicar claramente tal cualidad.

2. Revoca CERTIFICADOS DE CLAVE PÚBLICA;La AUTORIDAD CERTIFICANTE LICENCIADA revocará los CERTIFICADOS DE CLAVE PÚBLICA por ella emitidos:

a) Por solicitud de su SUSCRIPTOR; o

b) Por solicitud de un TERCERO; o

c) Si llegara a determinar que un CERTIFICADO fue emitido en base a una información falsa, que en el momento de la EMISION hubiera sido objeto de verificación; o

d) Si llegara a determinar que las CLAVES PÚBLICAS contenidas en los CERTIFICADOS dejan de ser TECNICAMENTE CONFIABLES; o

e) Si cesa en sus actividades y no transfiere los CERTIFICADOS emitidos por ella a otra AUTORIDAD CERTIFICANTE LICENCIADA;

La solicitud de REVOCACION DE UN CERTIFICADO debe hacerse en forma personal o por medio de un DOCUMENTO DIGITAL FIRMADO. Si la revocación es solicitada por el SUSCRIPTOR, ésta deberá concretarse de inmediato. Si la revocación es solicitada por un TERCERO, tendrá lugar dentro de los plazos mínimos necesarios para realizar las verificaciones del caso.

La revocación debe indicar el momento desde el cual se aplica y no puede ser retroactiva o a futuro. El CERTIFICADO revocado deberá incluirse inmediatamente en la LISTA DE CERTIFICADOS REVOCADOS, y la lista debe estar firmada por LA AUTORIDAD CERTIFICANTE LICENCIADA. Dicha lista debe hacerse pública en forma permanente, por medio de conexiones de telecomunicaciones públicamente accesibles.

La AUTORIDAD CERTIFICANTE LICENCIADA debe emitir una constancia de la revocación para el solicitante.

3. Provee, opcionalmente, el servicio de SELLADO DIGITAL DE FECHA Y HORA.

Obligaciones:

Adicionalmente a sus obligaciones emergentes como SUSCRIPTORA de su CERTIFICADO emitido por el ORGANISMO LICENCIANTE, la AUTORIDAD CERTIFICANTE LICENCIADA debe:

1. Abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder bajo ninguna circunstancia, a la CLAVE PRIVADA del SUSCRIPTOR;

2. Mantener el control de su CLAVE PRIVADA e impedir su divulgación;

3. Solicitar inmediatamente la REVOCACION DE SU CERTIFICADO, cuando tuviera sospechas fundadas de que su CLAVE PRIVADA ha sido comprometida;

4. Solicitar al ORGANISMO LICENCIANTE la revocación de su CERTIFICADO cuando la CLAVE PÚBLICA en él contenida deje de ser TECNICAMENTE CONFIABLE;

5. Informar inmediatamente al ORGANISMO LICENCIANTE sobre cualquier cambio en los datos contenidos en su CERTIFICADO, o sobre cualquier hecho significativo que pueda afectar la información contenida en el mismo;

6. Operar utilizando un sistema TECNICAMENTE CONFIABLE;

7. Notificar al solicitante sobre las medidas necesarias que éste está obligado a adoptar para crear FIRMAS DIGITALES seguras y para su VERIFICACION confiable; y de las obligaciones que éste asume por cl solo hecho de ser SUSCRIPTOR de un CERTIFICADO DE CLAVE PÚBLICA;

8. Recabar únicamente aquellos datos personales del SUSCRIPTOR del CERTIFICADO que sean necesarios y de utilidad para la emisión del mismo, quedando el solicitante en libertad de proveer información adicional. Toda información así recabada, pero que no figure en el CERTIFICADO, será de trato confidencial por parte de la AUTORIDAD CERTIFICANTE LICENCIADA;

9. Poner a disposición del SUSCRIPTOR de un CERTIFICADO emitido por esta AUTORIDAD CERTIFICANTE LICENCIADA, toda la información relativa a la tramitación del CERTIFICADO;

10. Mantener la documentación respaldatoria de los CERTIFICADOS emitidos por DIEZ (10) años a partir de su fecha de vencimiento o revocación;

11. Permitir el acceso público permanente a los CERTIFICADOS que ha emitido, y a la LISTA DE CERTIFICADOS REVOCADOS, por medio de conexiones de telecomunicaciones públicamente accesibles;

12. Publicar su dirección y sus números telefónicos;

13. Permitir el ingreso de los funcionarios autorizados del ORGANISMO LICENCIANTE o del ORGANISMO AUDITANTE a su local operativo, poner a su disposición toda la información necesaria, y proveer la asistencia del caso;

14. Registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas.

Cese de Actividades:

Los CERTIFICADOS emitidos por una AUTORIDAD CERTIFICANTE LICENCIADA que cesa en sus funciones se revocarán a partir del día y la hora en que cesa su actividad, a menos que sean transferidos a otra AUTORIDAD CERTIFICANTE LICENCIADA. La AUTORIDAD CERTIFICANTE LICENCIADA notificará mediante la publicación por TRES (3) días consecutivos en el Boletín Oficial, la fecha y hora de cese de sus actividades, que no podrá ser anterior a los NOVENTA (90) días corridos contados desde la fecha de la última publicación. La notificación también deberá hacerse individualmente al ORGANISMO LICENCIANTE.

Cuando se hayan emitido CERTIFICADOS a personas ajenas al Sector Público Nacional, la AUTORIDAD CERTIFICANTE LICENCIADA publicará durante TRES (3) días consecutivos en uno o más diarios de difusión nacional, el cese de sus actividades.

La AUTORIDAD CERTIFICANTE LICENCIADA podrá disponer de medios adicionales de comunicación del cese de sus actividades a los SUSCRIPTORES de CERTIFICADOS que son ajenos al Sector Público Nacional.

Si los CERTIFICADOS son transferidos a otra AUTORIDAD CERTIFICANTE LICENCIADA, toda la documentación pertinente también deberá ser transferida a ella.

Requisitos para obtener la licencia de autoridad certificante:

La autoridad certificante que desee obtener una licencia deberá:

1. Presentar una solicitud;

2. Contar con un dictamen favorable emitido por el ORGANISMO AUDITANTE;

3. Someter a aprobación del ORGANISMO LICENCIANTE el manual de procedimientos, el plan de seguridad y el de cese de actividades, así como el detalle de los componentes técnicos a utilizar;

4. Emplear para el ejercicio de las actividades de certificación, personal técnicamente idóneo y que no se encuentre incurso en los supuestos de inhabilitación para desempeñar funciones dentro del Sector Público Nacional;

5. Presentar toda otra información relevante al proceso de otorgamiento de licencias que sea exigida por el ORGANISMO LICENCIANTE.

SUSCRIPTOR DE CERTIFICADO DE CLAVE PÚBLICA

Obligaciones del SUSCRIPTOR:
El SUSCRIPTOR de un CERTIFICADO DE CLAVE PÚBLICA debe:

1. Proveer todos los datos requeridos por la AUTORIDAD CERTIFICANTE LICENCIADA bajo declaración jurada;

2. Mantener el control de su CLAVE PRIVADA e impedir su divulgación;

3. Informar inmediatamente a la AUTORIDAD CERTIFICANTE LICENCIADA, sobre cualquier circunstancia que pueda haber comprometido su CLAVE PRIVADA;

4. Informar inmediatamente a la AUTORIDAD CERTIFICANTE LICENCIADA cuando cambie alguno de los datos contenidos en el CERTIFICADO que hubieran sido objeto de verificación.

CERTIFICADOS DE CLAVE PÚBLICA

Contenido del CERTIFICADO DE CLAVE PÚBLICA:

El CERTIFICADO DE CLAVE PÚBLICA contendrá, como mínimo, los siguientes datos:

1. Nombre del SUSCRIPTOR del CERTIFICADO:

2. Tipo y número de documento del SUSCRIPTOR del CERTIFICADO, o número de licencia, en el caso de CERTIFICADOS emitidos para AUTORIDADES CERTIFICANTES LICENCIADAS;

3. CLAVE PÚBLICA utilizada por el SUSCRIPTOR;

4. Nombre del algoritmo que debe utilizarse con la CLAVE PÚBLICA en el contenida;

5. Número de serie del CERTIFICADO;

6. PERIODO DE VIGENCIA del CERTIFICADO;

7. Nombre de la AUTORIDAD CERTIFICANTE LICENCIADA emisora del CERTIFICADO;

8. FIRMA DIGITAL de la AUTORIDAD CERTIFICANTE LICENCIADA que emite el CERTIFICADO, identificando los algoritmos utilizados;

9. Todo otro dato relevante para la utilización del CERTIFICADO, se explicitará en el manual de procedimientos de la AUTORIDAD CERTIFICANTE LICENCIADA emisora.

Condiciones de Validez del CERTIFICADO DE CLAVE PÚBLICA:

El CERTIFICADO DE CLAVE PÚBLICA es valido únicamente si:

1. ha sido emitido por una AUTORIDAD CERTIFICANTE LICENCIADA;
2. no ha sido revocado;
3. no ha expirado.

Así también, este Decreto dentro de su Anexo II, contempla un Glosario de los términos empleados en la regulación de la firma digital en el sector público:

AUTORIDAD CERTIFICANTE LICENCIADA: Órgano administrativo que emite CERTIFICADOS DE CLAVE PÚBLICA.

CERTIFICADO O CERTIFICADO DE CLAVE PÚBLICA: DOCUMENTO DIGITAL emitido y firmado digitalmente por una AUTORIDAD CERTIFICANTE LICENCIADA, que asocia una CLAVE PÚBLICA con su SUSCRIPTOR durante el PERIODO DE VIGENCIA del CERTIFICADO, y que asimismo hace plena prueba dentro del Sector Público Nacional, de la veracidad de su contenido.

CLAVE PRIVADA: En un CRIPTOSISTEMA ASIMETRICO, es aquella que se utiliza para firmar digitalmente

CLAVE PÚBLICA: En un CRIPTOSISTEMA ASIMETRICO, es aquella que se utiliza para verificar una FIRMA DIGITAL.

COMPUTACIONALMENTE NO FACTIBLE: Dícese de aquellos cálculos matemáticos asistidos por computadora que para ser llevados a cabo requieren de tiempo y recursos informáticos que superan ampliamente a los disponibles en la actualidad.

CORRESPONDER: Con referencia a un cierto PAR DE CLAVES, significa pertenecer a dicho par.

CRIPTOSISTEMA ASIMETRICO: Algoritmo que utiliza un PAR DE CLAVES, una CLAVE PRIVADA para firmar digitalmente y su correspondiente CLAVE PÚBLICA para verificar esa FIRMA DIGITAL. A efectos de este Decreto, se entiende que el CRIPTOSISTEMA ASIMETRICO deberá ser TECNICAMENTE CONFIABLE.

DIGESTO SEGURO (Hash Result): La secuencia de bits de longitud fija producida por una FUNCION DE DIGESTO SEGURO luego de procesar un DOCUMENTO DIGITAL.

DOCUMENTO DIGITAL: Representación digital de actos, hechos o datos jurídicamente relevantes.

DOCUMENTO DIGITAL FIRMADO: DOCUMENTO DIGITAL al cual se le ha aplicado una FIRMA DIGITAL

EMISION DE UN CERTIFICADO: La creación de un CERTIFICADO por parte de una AUTORIDAD CERTIFICANTE LICENCIADA.

ORGANISMO AUDITANTE: Órgano administrativo encargado de auditar la actividad del ORGANISMO LICENCIANTE y de las AUTORIDADES CERTIFICANTES LICENCIADAS.

ORGANISMO LICENCIANTE: Órgano administrativo encargado de otorgar las licencias a las autoridades certificantes y de supervisar la actividad de las AUTORIDADES CERTIFICANTES LICENCIADAS.

FIRMA DIGITAL: Resultado de una transformación de un DOCUMENTO DIGITAL empleando un CRIPTOGRAMA ASIMETRICO y un DIGESTO SEGURO, de forma tal que una persona que posea el DOCUMENTO DIGITAL inicial y la CLAVE PÚBLICA del firmante pueda determinar con certeza:

1. Si la transformación se llevó a cabo utilizando la CLAVE PRIVADA que corresponde a la CLAVE PÚBLICA del firmante;

2. Si el DOCUMENTO DIGITAL ha sido modificado desde que se efectuó la transformación.

La conjunción de los dos requisitos anteriores garantiza su NO REPUDIO y su INTEGRIDAD.

FUNCION DE DIGESTO SEGURO: Es una función matemática que transforma un DOCUMENTO DIGITAL en una secuencia de bits de longitud fija, llamada DIGESTO SEGURO, de forma tal que:

1. Se obtiene la misma secuencia de bits de longitud fija cada vez que se calcula esta función respecto del mismo DOCUMENTO DIGITAL;

2. Es COMPUTACIONALMENTE NO FACTIBLE inferir o reconstituir un DOCUMENTO DIGITAL a partir de su DIGESTO SEGURO;

3. Es COMPUTACIONALMENTE NO FACTIBLE encontrar dos DOCUMENTOS DIGITALES diferentes que produzcan el mismo DIGESTO SEGURO.

INTEGRIDAD: Condición de no alteración de un DOCUMENTO DIGITAL.

LISTA DE CERTIFICADOS REVOCADOS: Es la lista PÚBLICAda por la AUTORIDAD CERTIFICANTE LICENCIADA, de los CERTIFICADOS DE CLAVE PÚBLICA por ella emitidos cuya vigencia ha cesado antes de su fecha de vencimiento, por acto revocatorio.

NO REPUDIO: Cualidad de la FIRMA DIGITAL, por la cual su autor no puede desconocer un DOCUMENTO DIGITAL que el ha firmado digitalmente.

PAR DE CLAVES: CLAVE PRIVADA y su correspondiente CLAVE PÚBLICA en un CRIPTOSISTEMA ASIMETRICO, tal que la CLAVE PÚBLICA puede verificar una FIRMA DIGITAL creada por la CLAVE PRIVADA.

PERIODO DE VIGENCIA (de un CERTIFICADO): Periodo durante el cual el SUSCRIPTOR puede firmar DOCUMENTOS DIGITALES utilizando la CLAVE PRIVADA correspondiente a la CLAVE PÚBLICA contenida en el CERTIFICADO, de modo tal que la FIRMA DIGITAL no sea repudiable.

El PERIODO DE VIGENCIA de un CERTIFICADO comienza en la fecha y hora en que fue emitido por la AUTORIDAD CERTIFICANTE LICENCIADA, o en una fecha y hora posterior si así lo especifica el CERTIFICADO, y termina en la fecha y hora de su vencimiento o revocación.

REVOCACION DE UN CERTIFICADO: Acción de dejar sin efecto en forma permanente un CERTIFICADO a partir de una fecha cierta, incluyéndolo en la LISTA DE CERTIFICADOS REVOCADOS.

SELLADO DIGITAL DE FECHA Y HORA: Acción mediante la cual la AUTORIDAD CERTIFICANTE LICENCIADA adiciona la fecha, hora, minutos y segundos (como mínimo) de su intervención, a un DOCUMENTO DIGITAL o a su DIGESTO SEGURO. La información resultante del proceso antes descrito es firmada digitalmente por la AUTORIDAD CERTIFICANTE LICENCIADA.

SISTEMA CONFIABLE: Equipos de computación, software y procedimientos relacionados que:

1. Sean razonablemente confiables para resguardar contra la posibilidad de intrusión o de uso indebido;

2. Brinden un grado razonable de disponibilidad, confiabilidad, confidencialidad y correcto funcionamiento;

3. Sean razonablemente aptos para el desempeño de sus funciones específicas:

4. Cumplan con los requisitos de seguridad generalmente aceptados.

SUSCRIPTOR: Persona:

1. A cuyo nombre se emite un CERTIFICADO, y

2. Que es titular de la CLAVE PRIVADA correspondiente a la CLAVE PÚBLICA incluida en dicho CERTIFICADO.

TECNICAMENTE CONFIABLE Dícese de los SISTEMAS CONFIABLES que cumplen con los estándares tecnológicos que al efecto dicte la Secretaría de la Función Pública de la Jefatura de Gabinete de Ministros. ADMINISTRACION PÚBLICA NACIONAL.

Este decreto fue el antecedente que el legislador argentino propuso para regular la figura del comercio electrónico, abanderando los principios que a continuación se transcriben para la adopción de la figura del comercio electrónico ***(2)*** y todo lo que ella entraña, teniendo presente su origen internacional y su tendencia hacia la promoción de la uniformidad en el mundo de la información, siendo los siguientes:

a) Promover la compatibilidad con el marco jurídico internacional: Este principio se refiere a la dimensión global o internacional del tema desde el punto de vista legislativo y tecnológico, a fin de permitir el ingreso de Argentina en el mercado mundial del comercio electrónico.

b) Asegurar la neutralidad tecnológica: Este principio se refiere a la flexibilidad que deben tener las normas, es decir, que las mismas no estén condicionadas a un formato, una tecnología, un lenguaje o un medio de transmisión específicos, sino que contemplen el entorno para dar una igualdad de trato a las demás tecnologías, lo que derivaría en una compatibilidad extraterritorial.

c) Garantizar la igualdad en el tratamiento jurídico del uso de las nuevas tecnologías de procesamiento de la información: Este principio permite la equiparación del documento y firma electrónica a sus equivalentes tradicionales, tanto en sus efectos como en el régimen jurídico aplicable. Se sigue así la tendencia internacional a la homologación de regímenes. En particular esto se expresa en dos consecuencias: la igualdad en el ámbito de aplicación de los documentos en formato papel y los documentos electrónicos, salvo excepciones legales expresamente señaladas y la aplicación del sistema a todo tipo de actos y transacciones.

d) Facilitar el comercio electrónico interno e internacional.

e) Fomentar y estimular la aplicación de nuevas tecnologías de la información en la celebración de relaciones jurídicas: la adopción de estos últimos

---

(2) Anteproyecto de Ley Formato Digital de los Actos Jurídicos.

principios permitirá la modernización de las prácticas jurídicas y comerciales en el ámbito nacional e internacional.

f) Respetar la observancia de la buena fe en las relaciones jurídicas instrumentadas según esta ley: Esta es la reafirmación del criterio que opera como soporte filosófico del derecho argentino: la buena fe.

2.1.2 De la Firma Digital.

Al adoptar el uso del formato digital para la celebración de los actos jurídicos se eliminan las barreras reglamentarias para la realización de transacciones por vías electrónicas y en el marco de la legislación nacional argentina, el principio de libertad contractual permite a las partes contrayentes convenir entre ellas la modalidad de sus transacciones, es decir, si ellas aceptan o no las firmas digitales.

Consciente de la importancia que en el entorno del comercio electrónico tiene la manifestación del consentimiento de las partes contratantes al momento de estampar la firma en el contrato celebrado y trasladándonos al campo digital, la figura de la firma digital cubre con las expectativas planteadas para su adopción con la reducción que en costos y en tiempo impone la actualidad.

El legislador argentino tomó en cuenta la intención de la comunidad internacional respecto del trato de las nuevas tecnologías en el campo del comercio, misma que quedara plasmada en las Leyes Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional tanto sobre Comercio Electrónico como sobre Firmas Electrónicas, cada una con la respectiva guía para su incorporación al derecho interno de cada Nación.

Al realizar la inclusión de tales normas internacionales en su ordenamiento interno, la Nación Argentina aceptó que el reconocimiento jurídico de firmas digitales debe reposar sobre criterios objetivos, transparentes, no discriminatorios y proporcionales, los cuales no deben ser condicionados a ninguna autorización o licenciamiento del prestatario del servicio respectivo.

Por tanto, las exigencias comunes aplicables a los prestatarios de servicios de certificación deben permitir el reconocimiento internacional de firmas y certificados para los países integrantes del Mercosur y del mundo que cuentan con un marco normativo compatible para permitir otorgarle a las firmas digitales emitidas por un ente argentino, el carácter de extraterritorialidad que la tecnología actualmente exige, siempre rigiéndose en el ejercicio de sus funciones por los principios de objetividad, transparencia y no discriminación.

Respecto a la materia de la responsabilidad y tomando en consideración los principios enunciados en el párrafo anterior, las reglas comunes deben contribuir a originar y mantener la confianza de los usuarios, de los suscriptores y de las organizaciones, para que confíen plenamente tanto en los certificados emitidos, como en los prestatarios de servicios de certificación y así conseguir una amplia difusión de las firmas digitales.

Las contrataciones comprendidas en el régimen digital, podrán realizarse en formato digital firmado digitalmente, utilizando los procedimientos de selección y las modalidades que correspondan, lo cual significa que el legislador no deja tanto al libre albedrío de las partes el determinar el formato de dichas contrataciones, sino que previamente ha establecido un criterio que se considera el más aceptable tanto en la legislación nacional, como en la que rige a cada provincia argentina.

De esta manera, las jurisdicciones y entidades estarán obligadas a aceptar el envío de ofertas, la presentación de informes, documentos, comunicaciones, impugnaciones y recursos relativos a los procedimientos de contratación celebrados en formato digital y firmados digitalmente, conforme lo establezca la reglamentación.

Con lo que se refiere a los efectos que pudiera producir su publicidad, se considerarán válidas las notificaciones en formato digital firmado digitalmente siempre y cuando cumplan con los requisitos que enuncia el artículo 8° de la Ley 19.549.

Los documentos digitales firmados digitalmente tendrán el mismo valor legal que los documentos en soporte papel con firma manuscrita y serán considerados como medio de prueba de la información contenida en ellos retomando con ello el principio del "equivalente funcional" plasmado en la legislación internacional. ***(3)***

Así es como el día once de diciembre de dos mil uno, el Senado y la Cámara de Diputados de la Nación Argentina reunidos en Congreso, sancionaron con fuerza de ley la Ley de Firma Digital bajo el numeral 25.506 ***(4)***, misma que se estructuró de la siguiente manera:

Consideraciones generales.
Certificados digitales.
Certificador licenciado.
Titular de un certificado digital.
Organización institucional.
Autoridad de aplicación.
Sistema de auditoría.
Comisión Asesora para la Infraestructura de Firma Digital.
Responsabilidad.
Sanciones.
Disposiciones Complementarias

Pero la firma digital no sería nada sin el respaldo de una adecuada infraestructura legal especializada en materia digital, por lo que el artículo 6º de la ley en estudio define que:

> *"…se entiende por documento digital a la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo. Un documento digital también satisface el requerimiento de escritura..."*

---

(3) op.cit. Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil en materia de Firma Electrónica.
(4) La Ley 25.506 se compulsa en su totalidad en el Anexo A del presente trabajo.

Esto significa que el documento digital va a ser el traslado del característico documento de papel y sus respectivos signos, a la representación numérica necesaria y suficiente para ser plenamente identificada a través de los medios electrónicos e inclusive, consentida por quienes van a plasmar su voluntad.

Aunado a lo expuesto en el primer capítulo, se establece que dicha información digital tendrá un respaldo o almacenamiento temporal de 10 años contados a partir de su celebración e incluso, posterior a la misma que será suficiente para otorgar plena certeza a los actos celebrados por éste medio.

El mencionado resguardo es de gran utilidad para el caso de una posterior consulta y verificación de la autenticidad del contenido de los documentos digitales y también, será un importante apoyo probatorio frente a la calidad que las leyes le atribuyan a los mensajes revestidos de la tecnología digital.

No menos importante es toda la protección que la legislación argentina brinda a la creación de una firma digital colocando diversos “candados“ de seguridad para evitar la duplicidad y mal uso de las firmas en perjuicio de su titular.

Desde la circulación del documento digital firmado por el remitente autorizado, hasta que es verificado por el receptor y aceptado en todas y cada una de sus condiciones, la Ley de Firma Digital le brinda la protección necesaria que otorga confiabilidad en el manejo de este servicio de transacción electrónica.

En su artículo 2º, la Ley de firma Digital refiere que:

> *”…se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma. Los procedimientos de firma y verificación a ser utilizados para tales fines serán los*

determinados por la Autoridad de Aplicación en consonancia con estándares tecnológicos internacionales vigentes…".

Si atendemos a los orígenes del vocablo digital, en la forma más simple se refiere a dactilar, de los dedos, a las huellas dactilares o digitales, en cambio, se ha asociado el término digital a los dígitos entendiendo como tales a los números, letras y símbolos que de manera individual se van agrupando en forma sucesiva y ordenada para conformar un sistema de comunicación electrónica que solamente puede ser interpretado a través de fórmulas matemáticas a fin de identificar plenamente al emisor.

Esto quiere decir que para optimizar el manejo de información empleando medios electrónicos, se creó un sistema binario capaz de procesar información y compactarla en un reducido espacio, lo cual devenga en el flujo de grandes cantidades de datos en un mínimo lapso de tiempo acortando con ello los procesos y costos de comunicación acorde a la revolución tecnológica actual.

Resultando que tal procesamiento de datos aplicado a la firma digital, no es más que el sustituto binario de la firma ológrafa con sus mismos rasgos característicos los que una vez trasladados al campo de la informática, adquieren la misma fuerza de aceptación y validez de los actos celebrados en los medios tradicionales (llámese papel).

Si la firma digital además de los rasgos infalsificables que la estructuran se apoya en un respaldo y en el manejo exclusivo que de ella haga su titular, serán plena responsabilidad del mismo sus consecuencias y el reclamo posterior sobre algún acto consentido y aceptado en el que conste su firma digital, no podrá ser repudiado por él.

Por todo lo anterior y a efecto de brindar un adecuado respaldo a la firma digital, el legislador argentino creó la Jefatura del Gabinete de Ministros cuya principal

función será el mantener bajo control tanto al ente licenciante conocido como Oficina Nacional de Tecnologías de Información de la Subsecretaría de la Función Pública dependiente de la referida jefatura, como a los certificadores de la firma digital, estableciendo las diversas normas que regirán su funcionamiento para obtener y conservar la confianza de los usuarios de los servicios de certificación de firma electrónica.

Más aún, con el objetivo de mantener vigente a la legislación argentina en el ámbito digital y en pleno uso de las facultades conferidas por el artículo 99, inciso 1 de la Constitución Nacional de la Nación Argentina, la Jefatura del Gabinete de Ministros emitió el once de noviembre del dos mil tres, el Decreto 1028/2003 ***(5)*** por medio del cual, es disuelto el Ente Administrador de Firma Digital creado por el Decreto 2628/2002 emitido el diecinueve de diciembre de dos mil dos.

Esta disolución tuvo como objetivo primordial reordenar y racionalizar los recursos que dicho ente recibía como órgano técnico administrativo encargado de otorgar las licencias a los certificadores, además de supervisar su actividad y dictar las normas tendientes a asegurar el régimen de libre competencia en el mercado de los prestadores de servicios de certificación y la protección a los usuarios de la Firma Digital, recayendo ahora tales funciones en la Oficina Nacional de Tecnologías de Información de la Subsecretaría de la Gestión Pública de la Jefatura del Gabinete de Ministros.

De la misma forma y colocándose en un nivel donde las obligaciones son paralelas, tanto la Oficina Nacional de Tecnologías de Información de la Subsecretaría de la Gestión Pública como los Certificadores Licenciados se obligan a mantener un secreto absoluto en el desempeño de las funciones de certificación.

---

(5) La presente información puede ser consultada en la siguiente dirección electrónica: http://www.pki.gov.ar

Pero a manera de establecer un control neutral, se configura la práctica de auditorias a dichas autoridades mismas que no solamente quedarán contempladas en el ámbito de las funciones gubernamentales, sino que en su mayoría podrán ser realizadas por un organismo auditante denominado Contaduría General de la Nación, que será dependiente de la Subsecretaría de Presupuesto de la Secretaría de Hacienda del Ministerio de Economía y Obras y Servicios Públicos, el cual se integrará principalmente por representantes de instituciones de educación superior especializadas en la materia.

Tales auditorias tienen como objetivo evaluar a través de diversos y complejos lineamientos de verificación, la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y disponibilidad de los datos, así como el cumplimiento de las especificaciones del manual de procedimientos y los planes de seguridad y de contingencia aprobados por el ente licenciante.

La Ley de Firma Digital, en su artículo 35 establece la Comisión Asesora para la Infraestructura de Firma Digital como autoridad encargada de emitir todos los lineamentos necesarios para evitar un posible rezago tecnológico, la cual funcionará en forma colegiada y estará integrada multidisciplinariamente por expertos en la materia, quienes deberán contar con una reconocida trayectoria y que provendrán tanto de Organismos del Estado como de Universidades Nacionales y Provinciales e inclusive, de Cámaras, Colegios u otras asociaciones profesionales siendo designados por el Poder Ejecutivo para cumplir sus funciones por un período de cinco años renovables por una sola vez.

Es entonces que en la Comisión Asesora para la Infraestructura de Firma Digital, recae no tanto que la legislación nacional permanezca a la vanguardia a nivel mundial en el comercio electrónico, sino que se mantenga constantemente actualizada dentro del plano que esta forma de practicar el comercio en el mundo demanda.

También se establece una Infraestructura de Firma Digital que no solamente ofrecerá autenticación y garantía de integridad para los documentos digitales o electrónicos, sino también constituirá la base tecnológica que permitirá otorgarles validez jurídica, todo ello coordinado con la tarea de regular el funcionamiento de los certificadores licenciados de manera tal que se garantice la adecuada prestación de los servicios de certificación.

No menos importante es mencionar que el legislador argentino no deja a la deriva a la Ley de Firma Digital, sino que la complementa con su respectiva Reglamentación emitida bajo el Decreto número 2.628/2002. ***(6)***

Dicho reglamento apoya a la Ley de Firma Digital en el cumplimiento de los fines de reconocer tanto el empleo de la firma digital y de la firma electrónica, como su eficacia jurídica para otorgar seguridad a los usuarios de dichos servicios en las transacciones electrónicas que celebren, promoviendo un comercio electrónico seguro para permitir tener una constancia y certeza para las partes contratantes.

A la vez, la sanción de la Ley 25.506 otorga un decisivo impulso para la progresiva despapelización del Estado, contribuyendo a mejorar su gestión, facilitar el acceso de la comunidad a la información pública y posibilitar la realización de trámites por Internet en forma segura.

Es necesario recalcar que la Ley 25.506 en su numeral 5º establece una diferencia entre la firma digital y la firma electrónica en los siguientes términos:

> *1.- Firma Electrónica: Se entiende por firma electrónica al 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 algunos de los requisitos legales para ser considerada firma digital. En*

---

(6) El referido Decreto No. 2.628/2002 emitido como la Reglamentación de la Ley de Firma Digital fue publicado en el Boletín Oficial el 20 de diciembre del año 2002 y se compulsa en su totalidad como Anexo B del presente trabajo.

caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez.

2.- Firma digital: Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital, posterior a su firma. Los procedimientos de firma y verificación a ser utilizados para tales fines serán los determinados por la Autoridad de Aplicación en consonancia con estándares tecnológicos internacionales vigentes".

Este criterio general resulta precisado en función de que el legislador argentino le otorga a la firma digital, en cuanto a su alcance, un grado de confiabilidad superior al de la firma electrónica, procurando mantener aquellas formalidades consagradas en el derecho argentino para la celebración de determinados actos.

2.1.3 Del Certificador Licenciado.

El certificador licenciado es la persona en la cual recae la confianza del titular de la firma electrónica, siendo un tercero ajeno a las relaciones comerciales existentes entre el emisor de la firma digital y el receptor del mensaje de datos que se convierte en responsable del seguro resguardo del registro de tales rúbricas, cuya actividad realizará con estricto apego a los principios de objetividad, transparencia y no discriminación.

El artículo 17 de la Ley de Firma Digital establece que:

"*Se entiende por certificador licenciado a toda persona de existencia ideal, registro público de contratos u organismo público que expide certificados, presta otros servicios en relación con la firma digital y cuenta con una licencia para ello, otorgada por el ente licenciante. La actividad de los certificadores licenciados no pertenecientes al sector público se prestará en régimen de competencia. El*

arancel de los servicios prestados por los certificadores licenciados será establecido libremente por éstos."

Dicho prestador de servicios, podrá ser una persona física o moral de carácter público o privado, que tendrá como responsabilidad verificar la emisión, autenticidad y resguardo de los certificados digitales y que para obtener licencia como ente certificador, deberá cubrir con los requisitos establecidos para el otorgamiento del licenciamiento, debiendo manifestar además los fines para los cuales requiere su autorización.

El trámite de obtención de licencia de certificador inicia con la presentación de la solicitud debidamente firmada ya sea por el interesado o su representante legal, cuando se trate de persona física o moral, o bien, por la máxima autoridad de la autoridad o jurisdicción cuando sea una entidad pública.

A esta solicitud deberán anexarse los documentos que se refieren en la Sección 1 de los Requisitos para el licenciamiento de Certificadores, mismos que serán sometidos a estrictos controles legales y técnicos, a la vez que se efectuarán auditorías en las instalaciones del solicitante por parte del organismo licenciante como actos previos al otorgamiento o negativa de licenciamiento correspondiente.

Quiere decir que no se otorgará la autorización a cualquier persona sin antes tener la plena certeza sobre su existencia, pues no habrá lugar al registro y funcionamiento de prestadores de servicios de certificación que actúen en forma fraudulenta, donde para el supuesto de solicitarles que respondan de su responsabilidad, la autoridad auditante encuentre que dicho prestador nunca existió.

Además, el solicitante del otorgamiento de licenciamiento deberá cubrir el pago del arancel que dicho procedimiento genere, mismo que al igual que las multas que se llegarán a imponer como sanción, será abonado en la Coordinación de Tesorería dependiente de la Dirección General Técnico Administrativa de la Jefatura del

Gabinete de Ministros, constituyendo también un seguro de caución a efecto de garantizar el cumplimiento de las obligaciones derivadas del ejercicio de sus funciones.

Por cuanto a los Certificadores Licenciados pertenecientes a entidades y jurisdicciones del sector público, estos estarán exentos del pago del arancel para el trámite del licenciamiento de certificación más no de la obligación de constituir el seguro de caución corerspondiente.

La Oficina Nacional de Tecnologías de Información de la Subsecretaría de la Gestión Pública dependiente de la Jefatura del Gabinete de Ministros como ente licenciante, deberá realizar el análisis exhaustivo de la documentación presentada para el trámite del licenciamiento y para el supuesto de encontrar alguna irregularidad, notificará al interesado que tendrá un plazo de diez días para subsanar o aclarar cualquier omisión que presente la solicitud o los documentos presentados y en caso de no desahogar la prevención ordenada, su solicitud será desechada de plano.

Una vez transcurrido el plazo de sesenta días, el organismo licenciante emitirá un dictamen legal y técnico que determinará la aptitud para el ejercicio de las funciones y obligaciones inherentes al licenciamiento y para el supuesto de que el solicitante no cumpliera con los lineamientos para el licenciamiento, emitirá una resolución desfavorable debidamente fundada y motivada sin que el monto depositado por concepto del arancel generado por dicho trámite sea

El ente licenciante referido lo tenemos en la Oficina Nacional de Tecnologías de Información de la Subsecretaría de la Gestión Pública dependiente de la Jefatura del Gabinete de Ministros y será el organismo encargado tanto de otorgar las licencias a los certificadores, como de supervisar su actividad y de dictar las normas tendientes a asegurar el régimen de libre competencia en el mercado de los prestadores particulares y la protección de los usuarios de la Firma Digital.

Dentro del marco de sus funciones, el Certificador Licenciado no solo tendrá a su cargo la prestación del servicio de certificación de las firmas digitales que los usuarios le soliciten, sino también se obliga a coadyuvar a la autoridad judicial en todas aquéllas actividades que se le requiera, como por ejemplo para el supuesto de una controversia que se ventile ante los tribunales, aporte los elementos necesarios que apoyen al juzgador para obtener certeza sobre la litis planteada.

En el desempeño de sus funciones y durante los cinco años de vigencia de su respectiva licencia la cual podrá ser renovada, los Certificadores Licenciados ya sean públicos o particulares, se regirán por las disposiciones de la Ley de Firma Digital y su correspondiente reglamento y en la mayor de las veces, el cobro por la prestación de sus servicios lo realizarán sujetando sus respectivos aranceles a lo que determine el mercado.

A la vez, el artículo 13 de la ley en cita define al certificado digital disponiendo que:

> *"Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular*."

De tal manera y atendiendo al concepto que establece la ley en comento, tenemos que un documento digital es la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo, el cual debe satisfacer el requerimiento de escritura, pues tal y como se establece en los considerandos del Decreto 2.628, la sanción de la Ley 25.506 otorga un decisivo impulso para la progresiva despapelización del Estado, contribuyendo a mejorar su gestión, facilitar el acceso de la comunidad a la información pública y posibilitar la realización de trámites por Internet en forma segura y rápida.

Esto quiere decir que el documento digital tendrá las características de aquél que se plasma en papel obteniendo una validez similar, con la gran ventaja de que su respectivo acuse se archivará en un espacio menor y podrá ser consultado en su resguardo en la misma forma en que fue plasmado, evitando con ello el consiguiente traspapeleo y la pérdida de tiempo, dinero y esfuerzo para encontrar la información requerida.

En lo referente al formato, codificación, contenido e interpretación de los certificados digitales y listas de certificados revocados, el certificado digital será expedido por el certificador licenciado cubriendo con los estándares tecnológicos de emisión establecidos en el Anexo III de la Infraestructura de Firma Digital, concretamente en el estándar ITU-T X.509 (ISO/IEC 9594-8), siendo que estos certificados serán emitidos en conjunto con los tratados internacionales sobre la materia para otorgarle una validez no solo provincial o nacional, obteniendo así una validez basada en la reciprocidad internacional que los cubre de certeza extraterritorial.

En dicho certificado, el certificador hará constar los datos de identificación individual tanto del titular de la firma digital como del mismo certificador que lo expidió de modo tal que pueda ser posteriormente consultado y ante la existencia de una posible alteración, permita determinar la probable responsabilidad ya del signatario o bien del certificador.

La Ley 25.506 no establece un periodo de vigencia único para todos los certificados digitales, sino que permite tanto al titular como al certificador fijarlo a su libre albedrío pero debiendo constar éste en el certificado emitido, siendo su titular el único responsable de los efectos y consecuencias que produzca durante la vigencia del mismo, debiendo por ende, hacer el uso conforme a lo solicitado.

Durante el periodo referido, tanto el titular del certificado como el certificador licenciado, serán responsables del manejo y resguardo de la firma digital y la Oficina Nacional de Tecnologías de Información de la Subsecretaría de la Gestión Pública, dependiente de la Jefatura del Gabinete de Ministros, será la encargada de supervisar la actividad del certificador de firmas y de dictar las normas tendientes a asegurar tanto el régimen de libre competencia en el mercado de los prestadores como la protección de los usuarios de firma digital.

Pero a la vez que la Ley 25.506 en su artículo 38 establece una responsabilidad entre el certificador y el titular de la firma, también delimita la responsabilidad del certificador licenciado ante terceros, la cual abarca los daños y perjuicios que provoque por incumplimiento a las previsiones de la ley en comento, por los errores u omisiones que presenten los certificados digitales que expida, por no revocarlos dentro de los términos establecidos para ello y por las consecuencias imputables a la inobservancia de los procedimientos de certificación exigibles.

Por consiguiente e interpretando lo establecido en la ley en cita, corresponderá al prestador del servicio de certificación demostrar que actuó con la debida diligencia y que los daños y perjuicios ocasionados al titular del certificado, fueron ocasionados por causas imputables al usuario y no a él cuando haya dado debido cumplimiento a los estándares técnicos y parámetros de seguridad en la emisión, publicación y resguardo de los certificados emitidos.

2.2 Actualidad y efectividad de la Ley de Firma Digital.

La tendencia mundial en la era de la globalización permite sostener que el comercio electrónico en Argentina está produciendo una verdadera revolución en las transacciones comerciales que se celebran en dicho país, dado que importa un significativo parteaguas tanto en la negociación como en los sistemas de contrataciones, a la vez que trae aparejado un profundo cambio cultural.

Esta revolución digital significa una profunda redefinición en el ámbito del Derecho, principalmente en lo que se refiere a las tradicionales nociones de jurisdicción, competencia, ámbitos de validez espacial y temporal, entre otras, dado que son conceptualmente inadecuadas con relación a la proyección de extraterritorialidad que envuelve al ciberespacio y la globalización tan exacerbada que la sociedad de la información plantea.

Por otra parte, dentro del ámbito político y social, la revolución digital impulsa una reestructuración del papel que juegan el Estado y el protagonismo privado, pues como lo enuncié anteriormente, el gobierno virtual es una figura vanguardista impulsora de la cultura de transparencia en la administración pública.

A través del profundo análisis que el legislador realizó a las diversas normas que en materia de comercio electrónico ha adoptado el ordenamiento jurídico de la nación Argentina, es importante señalar lo manifestado en el cuerpo del Anteproyecto de Ley Formato Digital de los actos jurídicos referente al Comercio Electrónico al citar las diversas normas adoptadas en el marco jurídico de aquél país:

> "*Esta breve reseña muestra que hoy nuestro país no está en condiciones de decir que tiene respuestas jurídicas apropiadas para las necesidades que requieren los sistemas de implementación del comercio electrónico y las tecnologías vinculadas"*.

Tal manifestación denota la gran preocupación que en la Nación Argentina existe a raíz de la severa crisis económica que predomina en aquél país sudamericano y el hecho de pensar en la existencia de un ente depositario de la confianza de los usuarios de sus servicios que no fuera lo suficientemente controlado por el Estado, fue motivo suficiente para realizar un intenso análisis de las propuestas y contrapropuestas que pudieran vertirse respecto de la materia del comercio electrónico.

Por ello, el certificador licenciado promete ser una figura eficaz, puesto que el Estado Argentino le ha creado un entorno de certeza tan amplio, que los usuarios de los servicios de certificación de firma digital confían plenamente en los servicios ofrecidos por dicho ente.

CAPÍTULO TERCERO.

"Los seres humanos, por más diversos que parezcan sus caracteres y sus temperamentos, por más disímiles sus fines particulares, por más contrarias sus actitudes, coinciden en un punto fundamental: en una genérica aspiración de obtener su felicidad, que se traduce en una situación subjetiva consciente de bienestar duradero, que no es otra cosa que una satisfacción íntima permanente."

IGNACIO BURGOA ORIHUELA.

Legislación Mexicana en materia de Comercio Electrónico.

3.1 Derecho vigente. *(1)*

Aproximadamente desde el año de 1996, en nuestro país se han realizado diversos foros de discusión y análisis sobre la figura del comercio electrónico en los cuales se ha dado relevante importancia a la materia, más ello no había sido suficiente como para llegar a los oídos de los legisladores.

Durante los meses de septiembre y octubre de ese mismo año, se llevó a cabo en diversas sedes del país el Foro de Consulta sobre Derecho e Informática, organizado en forma conjunta por el Instituto Nacional de Estadística, Geografía e Informática y la H. Cámara de Diputados, con la finalidad de revisar el marco jurídico inherente a la informática. *(2)*

En el marco de los diversos eventos a los cuales acudieron notables personalidades políticas, juristas y economistas, se escucharon comentarios excelentes sobre la adopción de la materia digital dentro del ordenamiento legal mexicano.

Por ejemplo, durante el Tercer Evento celebrado en la Ciudad de Monterrey, Nuevo León el 25 de septiembre de 1996, el Dr. Alfredo Bustos y de la Tijera se refirió al impacto de la tecnología informática cuya evolución hace necesaria la revisión de temas relativos a la aplicación del derecho y su relación con esta tecnología.

---

(1) Salvo que se cite otra fuente, el presente capítulo se realizó al consultar las siguientes páginas de internet: economia.gob.mx; sat.gob.mx; sii.cl; jurídicas.unam.mx; sii.cl; biblioweb.dgsca.unam.mx; geocities.com; it-cenit.org.ar; derecho-internet.org; arkhaios.com; comunidad.derecho.org; senado.gob.mx; enterate.unam.mx; ecertchile.cl; firmadigital.gob.mx.

(2) En la Ciudad de Boca del Río, Veracruz, el 18 de septiembre de 1996 se realizó el Primer Evento del Foro de Consulta sobre Derecho e Informática; en la Ciudad de Guadalajara, Jalisco, el 20 se celebró el Segundo evento; en la Ciudad de Monterrey, Nuevo León, el 25 tuvo lugar el Tercer Evento; en la Ciudad de Tijuana, Baja California, el 27 se realizó el Cuarto Evento y para el 4 de octubre se clausuró el foro en la Ciudad de México, Distrito Federal con el Quinto Evento.

Comentó que el Plan Nacional de Desarrollo propuesto para ese año, señala en forma explícita las directrices para promover el desarrollo de las tecnologías de la información en nuestro país y a partir de lo cual, se integró el Programa de Desarrollo Informático que plantea como objetivo general el promover el adecuado uso y aprovechamiento de la informática en los diferentes sectores del país, para tal efecto, este programa contempla como una de sus acciones la de revisar y adecuar el marco jurídico aplicable.

Al igual que en ocasiones anteriores, es tan sorprendente el hecho que no se haya brindado la importancia debida a un tema tan importante a nivel mundial como lo es el comercio electrónico y que apenas hacia el año 1999 se comenzara a asumir la regulación en la legislación nacional de dicha figura.

En el capítulo de exposición de motivos de la iniciativa presentada el 30 de abril de 1999, el legislador proponente manifestó que

> *"Ante el rápido desarrollo de los sistemas informáticos y de comunicación, el hombre se ha visto obligado a buscar maneras más rápidas, prácticas y eficientes de llevar a cabo la actividad comercial y los medios electrónicos modernos han contribuido considerablemente a acortar las distancias entre los sujetos participantes en toda actividad comercial".*

Dicha iniciativa destaca que la legislación comercial y la *lex mercatoria* han sido rebasadas en el contexto internacional, debido principalmente a "lagunas legales" nacionales que se han constituido en barreras insalvables para el comercio, al exigir que para la validez de los actos y contratos mercantiles se utilice el papel.

Éste punto es el que principalmente se buscó vencer a través del reconocimiento de la contratación por vía electrónica con lo cual, la principal pretensión global, es que los actos así celebrados sean igualmente válidos que aquellos plasmados en papel.

Por tal motivo, el legislador mexicano tomó como base jurídica la Ley Modelo en materia de Comercio Electrónico de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) respaldándola con un intensivo análisis del contexto, la legislación vigente y la actual práctica comercial nacional e internacional, a fin de conseguir que dicha Ley Modelo se adaptara de manera precisa a la realidad nacional sin ser lesiva al momento de su adopción.

Asimismo, se precisó que el régimen jurídico mexicano sobre comercio electrónico debería ser compatible con el derecho internacional de la materia, concretando así el principal objetivo como lo es el brindar seguridad y certeza en las transacciones electrónicas tanto nacionales como internacionales.

La actualización legislativa pretendida con dicha iniciativa toma en cuenta el principio de "neutralidad del medio" y por lo mismo no hace referencia ni se compromete con ninguna tecnología en particular, precisamente para obtener la validez extraterritorial que a la certificación de firma electrónica otorga el derecho internacional.

De ahí que la importancia de estas reformas emana de una realidad consistente en el hecho de que los modernos medios de comunicación (internet, videoconferencias, comunicación celular, etc.) han difundido su uso con gran rapidez en las operaciones comerciales tanto nacionales como internacionales, realidad que hace presumir que este tipo de comunicación es y será preponderante en el presente así como en el futuro próximo.

Dado que la actividad comercial es vital para el desarrollo económico nacional y mundial, era más que esencial una correcta actualización de la legislación mexicana sobre la materia, más aún, tomando en cuenta que la Ley Modelo que sirvió de base a la reforma aprobada ha sido exitosamente adoptada en diversos países del orbe para sustituir e incluso, eliminar diversas trabas que la legislación

nacional imponía por el excesivo manejo de los actos tradicionalmente plasmados en papel.

Así, se buscó facilitar el comercio electrónico dando igualdad de trato a los contratos que tengan soporte informático con relación a aquellos que sean soportados en documentación consignada en papel.

Este es el principio conocido por la Ley Modelo como "criterio del equivalente funcional", mismo que esta basado en un análisis de los objetivos y funciones del requisito tradicional de la presentación de un escrito consignado sobre papel con miras a determinar la manera de satisfacer sus objetivos y funciones con técnicas empleadas en el comercio electrónico.

Anterior a la publicación en el Diario Oficial de la Federación del 29 de mayo de 2000 del Decreto por el que se reforman y adicionan diversas disposiciones del Código Civil para el Distrito federal en Materia Común y para toda la República en Materia Federal, del Código Federal de Procedimientos Civiles, del Código de Comercio y de la Ley de Protección al Consumidor, la regulación existente en México respecto de las transacciones electrónicas era mínima al respecto del reconocimiento y la validez de las firmas otorgadas a través de los medios electrónicos. ***(3)***

Con la referida reforma, se incorpora en el artículo 1803 del Código Civil Federal el concepto jurídico *"mensaje de datos"*, que implica el consentimiento otorgado por medios electrónicos.

Al igual que se reconoce la validez de la oferta y la aceptación o rechazo de la misma, realizadas a través de un mensaje de datos, también se reconoce que el mensaje de datos electrónico tiene la misma validez y cumple el requisito de la

---

(3) La presente información se puede consultar en la siguiente página de internet: http://www.natlaw.com

forma escrita que se exige para el contrato y demás documentos legales que deben ser firmados por las partes.

Asimismo, por una parte se reconoce que tanto la forma escrita como la firma original, tienen cumplidos los requisitos legales para la validez de las transacciones, tratándose de un mensaje de datos acompañado de la firma electrónica y por otra parte, se atiende igualmente al reconocimiento de los requisitos de autenticidad, integridad y confiabilidad de la información, generada, comunicada o archivada a través de un mensaje de datos.

Respecto a la celebración de contratos entre no presentes, el Derecho Mexicano se colocaba en una rigorista postura para evitar los posibles fraudes que se suscitaren en esta contratación entre no presentes y exceptuando al teléfono, las partes contratantes debían celebrar un contrato normativo previo a la celebración del acto en cuestión y estipulando por escrito la manera de contratar.

Hacia el 6 de octubre del 2000, se publicó en la Segunda Sección del Diario Oficial de la Federación el “Convenio de colaboración para establecer los mecanismos de emisión y administración de los Certificados Digitales, que se utilizarán para acceder al Registro Público de Comercio y para realizar transacciones comerciales”, que celebraran la Secretaría de Comercio y Fomento Industrial (actualmente Secretaría de Economía), la Asociación Nacional del Notariado Mexicano, A.C. y el Colegio de Corredores Públicos.

El referido convenio fue celebrado con el objetivo de establecer los mecanismos de emisión y administración de los certificados digitales para realizar transacciones comerciales y establecer los lineamientos para el registro de los notarios y corredores públicos que soliciten su acreditación como certificadores de firma electrónica.

En otras palabras, significa que mediante certificaciones hechas por notarios y corredores públicos, será posible celebrar contratos por medios electrónicos con lo cual se da un paso adicional muy importante en el proceso de brindar seguridad jurídica al comercio electrónico en México.

Estos certificados digitales junto con las firmas digitales, son las tecnologías más utilizadas a nivel mundial para "firmar" documentos electrónicos y las reformas reconocen que los documentos firmados electrónicamente tienen los mismos efectos legales que un papel firmado "por escrito".

El tema de las firmas digitales es sumamente interesante y puede llegar a ser técnicamente complejo como lo hemos mencionado en el desarrollo del presente trabajo, pero en ocasiones es en esa misma complejidad donde radica su propia seguridad, pues al establecerse diversos "candados" se hace casi infranqueable la muralla que electrónicamente envuelve a los mensajes de datos.

Actualmente, existe gente que se pregunta porqué esa necesidad de firmar un documento en el que conste como suprema manifestación de lo que el mismo consigna su rúbrica, siendo la misma práctica la que nos plantea la respuesta a esa incógnitas:

> *1.- "Por exigencia legal. Diversas leyes exigen que las partes firmen un contrato como manifestación expresa de su consentimiento y una de las reformas al Código de Comercio establece que cuando la ley exija que un contrato sea por escrito y firmado estos requisitos se tendrán por cumplidos cuando el mensaje de datos (que es la manera con la que las reformas se refieren a cualquier comunicación electrónica) cumpla con las condiciones que el mismo ordenamiento legal señala.*
>
> *2.- Para autenticar el mensaje. Es decir, para mostrar claramente nuestra voluntad de contratar, manifestar la aceptación de una oferta y/o acusar de recibido un mensaje de datos no hay manifestación superior del consentimiento que la firma". **(4)***

---

(4) Esta información puede ser consultada en la dirección electrónica: http://www.bakerinfo.com.

Y si bien la legislación puede ayudar a eliminar barreras legales (que aún son bastantes), es necesario cuidar que en lugar de conformar una labor facilitadora, se convierta en un agente que inhiba el hasta ahora acelerado desarrollo del comercio electrónico en nuestro país.

Previo a las reformas del 2000, los medios de comunicación más avanzados en materia de comunicaciones y de transferencias que contemplaba la legislación mexicana se limitaban al telégrafo y al fax, medios electrónicos mundialmente "prehistóricos" comparados con la computadora.

En la iniciativa del 22 de marzo de 2000, el legislador dejó muy clara su postura ante la revolución tecnológica que actualmente afrontamos, donde importantes avances en la electrónica han transformando la forma en que las sociedades trabajan, aprenden y se comunican entre sí.

Además y tomando en consideración que las redes de información no sólo han transformando los hábitos de las sociedades, sino también la forma en que operan las empresas y que cada vez es más evidente el cómo las tecnologías de la información contribuyen a mejorar la productividad de las empresas, el legislador nacional comprendió que no era posible permanecer con los ojos cerrados y los brazos cruzados ante tan vertiginosa evolución.

Por tal motivo, consideró al comercio electrónico como un elemento que permitirá al sector productivo de nuestro país aprovechar la revolución informática actual, pues representa una poderosa estrategia para impulsar la competitividad y eficiencia de las empresas mexicanas de cualquier sector y nivel económico; sin embargo, también constituye un enorme reto para el sector empresarial mexicano el competir exitosamente en el mercado mundial utilizando las herramientas tecnológicas actuales.

Ante tal panorama, el empresario mexicano ha comprendido la tendencia mundial actual y las empresas nacionales han comenzado a modernizarse, prueba de ello es que actualmente el 70% de las operaciones de comercio electrónico en el segmento empresa-empresa en México, se realizan con éxito celebrando gran cantidad de transacciones a través de medios electrónicos.

Por su parte, el gobierno juega un papel importante en la tarea de promoción y desarrollo en el uso de la informática para mejorar el servicio a los usuarios de los medios electrónicos, tomando en cuenta que el empleo de sistemas informáticos que hagan más eficientes las relaciones entre gobierno, empresas y ciudadanía en general tiene un impacto positivo en la economía del país.

Es entonces que para llevar a México al ámbito de la sociedad digital, la Secretaría de la Contraloría y Desarrollo Administrativo (SECODAM), creó un sistema electrónico denominado COMPRANET cuyo principal objetivo es permitir la utilización de internet en los procesos de adquisiciones gubernamentales de obras y servicios, esto para efectos de lograr la eficiencia, rapidez y transparencia en las adquisiciones gubernamentales. ***(5)***

Asimismo, en fecha 30 de mayo de 2000 se publicó una reforma a la Ley Federal del Procedimiento Administrativo a través de la cual se crea TRAMITANET como un sistema que permite el intercambio de mensajes a través de medios de comunicación electrónica, precisando que para las comunicaciones oficiales entre particulares y autoridades, se emplearán medios de identificación electrónica en sustitución de la firma electrónica y los documentos presentados por estos medios, producirán los mismos efectos que las leyes otorgan a los documentos firmados autógrafamente, teniendo en consecuencia, el mismo valor probatorio que las disposiciones legales otorgan a éstos.

---

(5) BACA CARDOSO, Silvia Elizabeth. "Necesidades Informativas en materia de Comercio Electrónico", Tesis Profesional. UNAM. ENEP Acatlán. p. 109.

A nivel internacional y reiterando lo mencionado con antelación, se han realizado importantes esfuerzos en el ámbito jurídico mundial para regular al comercio electrónico y prueba de ello, son las Leyes Modelo sobre Comercio Electrónico y sobre la Firma Electrónica con sus respectivas guías que la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (UNCITRAL) ha propuesto a todos los Estados como guía para establecer o fortalecer la legislación que rige el uso de métodos de comunicación y almacenamiento de información sustitutos del papel y con ello, dar valor jurídico a la utilización de estos medios digitales.

El año 2003 fue crucial para la legislación nacional y en especial para la materia mercantil pues en ese año se complementan las reformas a diversas normas nacionales.

En virtud de lo anterior, las reformas que se consideraron para el sistema jurídico mexicano, debían contemplar las menciones necesarias para aprovechar los avances logrados no sólo en el ámbito comercial sino también en otros ámbitos para así poder obtener una interacción total y armónica entre ellos, considerándolos como un todo y no de una manera individual y aislada, siempre con el primordial objetivo de atender a la figura especial del comercio electrónico.

Mas no se trataba únicamente de brindar al comercio electrónico un panorama legislativo adecuado en materia mercantil, sino también era necesario otorgar valor probatorio suficiente en los procesos administrativos y judiciales al uso de medios electrónicos y a los mensajes de datos, evitando que quedara al arbitrio del juez considerar o no su eficacia probatoria en caso de controversia.

Pero la revolución tecnológica mundial alcanzó al Derecho Mexicano y con las Reformas al Código de Comercio en materia de Firma Electrónica publicadas el 29 de agosto de 2003 en el Diario Oficial de la Federación, México se coloca dentro de la esfera mundial de las transferencias electrónicas.

3.2 Actualidad y efectividad de la Legislación Mexicana.

Por lo anteriormente expuesto, se consideró conveniente adecuar en forma general el marco jurídico mexicano, resultando elemental reconocer la posibilidad de que las partes puedan externar su voluntad o solicitar algún bien o servicio a través del uso de medios electrónicos e incluso, dar validez jurídica al uso de medios de identificación electrónica.

De esa manera, el Gobierno de México, reconociendo la importancia que ha tenido internet en la sociedad mundial y en las relaciones comerciales de nuestro país con el resto del mundo, estableció políticas para el desarrollo del comercio electrónico adoptando diversas acciones para modernizar el marco legislativo a efecto de adecuarlo a la realidad de la práctica comercial sin el soporte en papel, es decir, empleando los medios electrónicos y permitiendo su uso con plena seguridad jurídica.

Tratándose de la Constitución Política de los Estados Unidos Mexicanos como ley suprema de nuestro país, el artículo 6 hace mención respecto al derecho que tienen los ciudadanos para acceder a la información con que cuenta el gobierno, dando con ello pauta para la creación de la Ley Federal de Acceso a la Información Pública publicada en el Diario Oficial de la Federación el 11 de junio de 2002, como un aliciente a la política gubernamental de transparentar el manejo de los recursos públicos.

Respecto al manejo seguro de la información estadística y geográfica nacional, se reformó la Ley de Información, Estadística y Geográfica con el objeto de brindar confidencialidad a la información proporcionada con tales fines estableciendo además las posibles sanciones a los funcionarios públicos que incurrieran en la manipulación de dicha información. ***(6)***

---

(6) ***Ley de Información,Estadística y Geográfica.*** ***Artículo 37.*** *Los informantes, en su caso, podrán exigir que sean rectificados los datos que les conciernan, al demostrar que son inexactos, incompletos, equívocos u obsoletos, y denunciar ante las autoridades administrativas y judiciales todo hecho o circunstancia que*

Por su parte, el Código Penal Federal también se sometió a una intensiva reforma, con el principal objetivo de salvaguardar el patrimonio tanto público como privado ante los constantes ataques de sabotaje y sustracción de datos confidenciales e inclusive, protegiendo los derechos de autor tan severamente castigados en nuestro país, estableciendo en su Título Noveno, el Capítulo II denominado Acceso ilícito a sistemas y equipo de informática. ***(7)***

---

demuestre que se ha desconocido el principio de confidencialidad de los datos o la reserva establecida por disposición expresa, en el ejercicio de las facultades que esta Ley confiere a las unidades que integran los sistemas nacionales

Para proteger los intereses del solicitante, cuando proceda, deberá entregársele un documento en donde se certifique el registro de la modificación o corrección. Las solicitudes correspondientes se presentarán ante la misma autoridad que captó la información registrada.

Artículo 38. *Los datos e informes que los particulares proporcionen para fines estadísticos o provengan de registros administrativos o civiles, serán manejados, para efectos de esta Ley, bajo la observancia de los principios de confidencialidad y reserva y no podrán comunicarse, en ningún caso, en forma nominativa o individualizada, ni harán prueba ante autoridad administrativa o fiscal, ni en juicio o fuera de él.*

Cuando se deba divulgar la información estadística, ésta no podrá referirse, en ningún caso, a datos relacionados con menos de tres unidades de observación y deberá estar integrada de tal manera, que se preserve el anonimato de los informantes.

En el caso de informantes a los que se refiere la fracción II del artículo 36, sólo podrá difundirse información respecto de tres o más unidades de observación localizadas dentro de una misma rama o actividad económica, entidad federativa, municipio, nivel de ingreso o de cualquier otro indicador estratificado.

Artículo 39. *Las personas a quienes se les requieran datos estadísticos o geográficos deberán ser informadas de:*

I.- *El carácter obligatorio o potestativo de sus respuestas;*

II.- *Las consecuencias de la falsedad en sus respuestas a los cuestionarios que se les apliquen;*

III.- *La posibilidad del ejercicio del derecho de rectificación;*

IV.- *La confidencialidad en la administración de la información estadística que proporcionen, y*

V.- *La forma en que será divulgada o suministrada la información;*

VI.- *El plazo para proporcionar la información, que deberá fijarse conforme a la naturaleza y características de la información a rendir.*

Las anteriores previsiones deberán aparecer en los cuestionarios y documentos que se utilicen para recopilar datos estadísticos, o se harán del conocimiento de los informantes, al captar la información estadística o geográfica.

(7) <u>Código Penal Federal.</u> TÍTULO NOVENO. CAPÍTULO II. ACCESO ILÍCITO A SISTEMAS Y EQUIPO DE INFORMÁTICA.

Artículo 211 Bis. *A quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.*

Artículo 211 bis 1*. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.*

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

Artículo 211 bis 2. *Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.*

Asimismo, la Ley Federal contra la Delincuencia Organizada procura también por la protección a las comunicaciones privadas, mismas que serán intervenidas solamente cuando se funde la necesidad de tal medida, así como delimitar la obligación tanto de los servidores públicos competentes como de los proveedores de los servicios de comunicación para cooperar en estos supuestos. ***(8)***

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Artículo 211 bis 3. *Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.*

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

Artículo 211 bis 4*. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.*

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Artículo 211 bis 5. *Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.*

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

Artículo 211 bis 6. *Para los efectos de los artículos 211 Bis 4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código.*

Artículo 211 bis 7. *Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.*

Artículo 424 bis. *Se impondrá prisión de tres a diez años y de dos mil a veinte mil días multa:*

. .II. A quien fabrique con fin de lucro un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación..

(8) <u>Ley Federal contra la Delincuencia Organizada.</u>

Artículo 16. *Cuando en la averiguación previa de alguno de los delitos a que se refiere esta Ley o durante el proceso respectivo, el Procurador General de la República o el titular de la unidad especializada a que se refiere el artículo 8o. anterior, consideren necesaria la intervención de comunicaciones privadas, lo solicitarán por escrito al juez de distrito, expresando el objeto y necesidad de la intervención, los indicios que hagan presumir fundadamente que en los delitos investigados participa algún miembro de la delincuencia organizada; así como los hechos, circunstancias, datos y demás elementos que se pretenda probar.*

Artículo 26. *Los concesionarios, permisionarios y demás titulares de los medios o sistemas susceptibles de intervención en los términos del presente capítulo, deberán colaborar eficientemente con la autoridad competente para el desahogo de dichas diligencias, de conformidad con la normatividad aplicable y la orden judicial correspondiente.*

Dentro de ese orden, resultaba necesario actualizar los alcances de la legislación Civil Federal vigente, principalmente en lo relativo a los actos que requieren de la forma escrita otorgada ante un fedatario público y que pueden conservar e incluso, fortalecer la seguridad jurídica en beneficio de los obligados si se utilizan medios electrónicos, ópticos o cualquier otra tecnología, conforme a un procedimiento claro y particularmente descriptivo, que acredite la atribución de información a una persona y asegure que ésta será susceptible de una posterior consulta.

Es por ello que se incorporaron los mismos principios que en materia mercantil, por cuanto al comercio electrónico y las obligaciones que la celebración a través de los medios electrónicos trae aparejadas consigo, precisando la validez jurídica que tendrá el consentimiento expresado en esta materia. ***(9)***

Tratándose del Código Federal de Procedimientos Civiles, se propuso una adición con el fin de conceder tanto efectos jurídicos como validez y fuerza probatoria a la

---

Artículo 27. *Los servidores públicos de la unidad especializada a que se refiere el artículo 8o. de esta Ley, así como cualquier otro servidor público, que intervengan comunicaciones privadas sin la autorización judicial correspondiente, o que la realicen en términos distintos de los autorizados, serán sancionados con prisión de seis a doce años, de quinientos a mil días multa, así como con destitución e inhabilitación para desempeñar otro empleo, cargo o comisión públicos, por el mismo plazo de la pena de prisión impuesta.*

Artículo 28. *Quienes participen en alguna intervención de comunicaciones privadas deberán guardar reserva sobre el contenido de las mismas.*

Los servidores públicos de la unidad especializada prevista en el artículo 8o. de esta Ley, así como cualquier otro servidor público o los servidores públicos del Poder Judicial Federal, que participen en algún proceso de los delitos a que se refiere esta Ley, que revelen, divulguen o utilicen en forma indebida o en perjuicio de otro la información o imágenes obtenidas en el curso de una intervención de comunicaciones privadas, autorizada o no, serán sancionados con prisión de seis a doce años, de quinientos a mil días multa, así como con la destitución e inhabilitación para desempeñar otro empleo, cargo o comisión públicos, por el mismo plazo que la pena de prisión impuesta.

La misma pena se impondrá a quienes con motivo de su empleo, cargo o comisión público tengan conocimiento de la existencia de una solicitud o autorización de intervención de comunicaciones privadas y revelen su existencia o contenido.

(9) <u>Código Civil Federal.</u>

Artículo 1803. *El consentimiento puede ser expreso o tácito, para ello se estará a lo siguiente:*

I.- Será expreso cuando la voluntad se manifiesta verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos, y

II.- El tácito resultará de hechos o de actos que lo presupongan o que autoricen a presumirlo, excepto en los casos en que por ley o por convenio la voluntad deba manifestarse expresamente.

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

información que conste en medios electrónicos y con ello reconocer efectos jurídicos a las obligaciones que de conformidad con el Código Civil Federal contraigan las partes mediante el uso de medios electrónicos. ***(10)***

Tal prueba deberá valorarse conforme al sistema legal, por lo que el propio legislador establece las reglas a seguir para determinar la fuerza probatoria de la información generada a través de medios electrónicos, considerando primordialmente dos aspectos: la fiabilidad del método utilizado y la atribuibilidad de la información a su emisor.

En lo referente al Código de Comercio, con la iniciativa presentada el legislador se propuso hacer una amplia reforma al texto vigente con lo cual se conseguiría una legislación mercantil innovadora, eficaz y actualizada en materia informática brindando la posibilidad de que los comerciantes puedan ofertar bienes o servicios a través de medios electrónicos y que los usuarios recurran a dicha prestación con toda la confianza posible.

Por otra parte, si bien se reconoce la necesidad de contar con un marco jurídico nacional que acepte el uso de medios electrónicos, también se enfatiza en que dicho marco no debe olvidar brindar la protección basta y suficiente al consumidor usuario de esos medios.

En tal virtud, la iniciativa de reforma propuso también la adecuación de la Ley Federal de Protección al Consumidor, ordenamiento que en nuestro país tiene por

---

(10) <u>Código Federal de Procedimientos Civiles.</u>
Artículo 210 A. *Se reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier tecnología.*
Para valorar la fuerza probatoria de la información a que se refiere el párrafo anterior, se estrimará primordialmente la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas obligadas el contenido de la información relativa y ser accesible para su ulterior consulta.
Cuando una ley requiera que un documento sea conservado o presentado en su forma original, este requisito quedará satisfecho si se acredita que la información generadoa, comunicada,recibida o archivada por medios electrónicos, ópticos o de cualquier tecnología, se ha mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y ésta pueda ser accesible para su ulterior consulta.

objeto promover y proteger los derechos del consumidor, para incorporar las disposiciones mínimas que aseguren los derechos básicos del consumidor en las operaciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología. ***(11)***

La Ley en comento establece las obligaciones de los proveedores en este tipo de transacciones, a efecto de garantizar de manera íntegra la protección de los derechos de los consumidores procurando la equidad y la seguridad jurídica entre las partes contratantes.

---

(11) <u>Ley Federal de Protección al Consumidor.</u>

Artículo 1. *La presente ley es de orden público e interés social y de observancia en toda la República. Sus disposiciones son irrenunciables y contra su observancia no podrán alegarse costumbres, usos, prácticas o estipulaciones en contrario.*

El objeto de esta ley es promover y proteger los derechos de los consumidores y procurar la equidad y seguridad jurídica entre los proveedores y consumidores.

Son principios básicos de las relaciones de consumo:

...VIII. La efectiva protección a los consumidores en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología y la adecuada utilización de los datos apropiados.

Arículo 24.*La Procuraduría tiene las siguientes atribuciones:*

...IX bis. Promover en coordinación con la Secretaría la formulación, difusión y uso de códigos de ética, por parte de los proveedores que incorporen los principios previstos por esta ley respecto de las transacciones que celebren con consumidoresa través del uso de medios electrónicos, ópticos o de cualquier otra tecnología

Artículo 76 bis. *Las disposiciones del presente Capítulo aplican a las relaciones entre proveedores y consumidores efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología. En la celebración de dichas transacciones se cumpliira´con lo siguiente:*

I. El proveedor utilizará la información proporcionada por el consumidor en forma confidencial, por lo que no podrá difundirla o transmitirla a otros proveedores ajenos a la transacción, salvo autorización expresa del propio consumidor o por requerimiento de autoridad competente;

II. El proveedor utilizará alguno de los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por el consumidor e informará a éste, previamente a la celebración de la transacción, de las características generales de dichos elementos;

III. El proveedor deberá proporcionar al consumidor, antes de la celebración de la transacción, su domicilio físico, números telefónicos y demás medios a los que pueda acudir el propio consumidor para presentarle sus reclamaciones o solicitarle aclaraciones;

IV.El proveedor evitará las prácticas comerciales engañosas respecto de las características de los productos, por lo que deberá cumplir con las decisiones relativas a la información y publicidad de los bienes y servicios que ofrezca, señaladas en esta Ley y demás disposiciones que se deriven de ella;

V.El consumidor tendrá derecho a conocer toda la información sobre los términos, condiciones, costos, cargos adicionales, en su caso, formas de pago de los bienes y servicios ofrecidos por el proveedor;

VI.El proveedor respetará la decisión del consumidor en cuanto a la cantidad y calidad de los productos que desea recibir, así como la de no recibir avisos comerciales, y;

VII.El proveedor deberá de abstenerse de no usar estrategias de venta o pulbicitarias que no proporcionen al consumidor información clara y suficiente sobre los servicios ofrecidos y cuidará las prácticas de mercadotecnia dirigidas a la población vulnerable, como niños, ancianos y enfermos, proporcionando mecanismos que adviertan cuando la información no sea apta para esa población.

Por cuanto a la Ley Orgánica de la Administración Pública Federal y como lo he referido con antelación, la Secretaría de la Contraloría y Desarrollo Administrativo, a efecto de acercar al Gobierno a la era digital del internet, creó los sistemas de COMPRANET y TRAMITANET.

En materia fiscal, se han venido introduciendo diversas reformas tanto al Código Fiscal de la Federación como a la Ley del Servicio de Administración Tributaria al crear el sistema DECLARANET, cuyo pricipal objetivo es el permitir a los contribuyentes presentar sus declaraciones fiscales y efectuar el pago de impuestos a través de los medios electrónicos, empleando la firma electrónica avanzada como medio de identificación tanto de los contribuyentes como de las propias autoridades fiscales. ***(12)***

De igual manera y para mantener un pleno control y vigilancia respecto a las incidencias que se llegaran a suscitar en la red, la Policia Federal Preventiva creó la unidad especializada en medios electrónicos denominada “Unidad de Policía Cibernética”, cuya principal función es salvaguardar la integridad de los usuarios de internet detectando la posible comisión de actos delictivos en perjuicio de individuos e instituciones privadas y públicas. ***(13)***

Dentro de ese ámbito, fue reformada la Ley Federal de Derechos de Autor para proteger los derechos patrimoniales que sobre los programas de computación tienen sus autores e inclusive, cuando se trata de compilaciones de carácter

---

(12) <u>Ley del Servicio de Adminisración Tributaria.</u>
Artículo 2o. *El Servicio de Administración Tributaria tiene la responsabilidad de aplicar la legislación fiscal y aduanera con el fin de que las personas fisicas y morales contribuyan proporcional y equitativamente al gasto público, de fiscalizar a los contribuyentes para que cumplan con las disposiciones tributarias y aduaneras, de facilitar e incentivar el cumplimiento voluntario de dichas disposiciones, y de generar y proporcionar la información necesaria para el diseño y la evaluación de la política tributaria.*
El Servicio de Administración Tributaria implantará programas y proyectos para reducir su costo de operación por peso recaudado y el costo de cumplimiento de las obligaciones por parte de los contribuyentes. Cuando en el texto de esta Ley se haga referencia a contribuciones, se entenderán comprendidos los aprovechamientos federales.
(13) Esta información fue obtenida de la siguiente dirección electrónica: http://www.ssp.gob.mx

intelectual, aportando los conceptos elementales para una adecuada interpretación. ***(14)***

---

(14) ***<u>Ley Federal de Derechos de Autor</u>. Artículo 13.-*** *Los derechos de autor a que se refiere esta Ley se reconocen respecto de las obras de las siguientes ramas:*
…XI. *Programas de cómputo;*

Artículo 101.. *Se entiende por programa de computación la expresión original en cualquier forma, lenguaje o código, de un conjunto de instrucciones que, con una secuencia, estructura y organización determinada, tiene como propósito que una computadora o dispositivo realice una tarea o función específica.*

Artículo 102. *Los programas de computación se protegen en los mismos términos que las obras literarias. Dicha protección se extiende tanto a los programas operativos como a los programas aplicativos, ya sea en forma de código fuente o de código objeto. Se exceptúan aquellos programas de cómputo que tengan por objeto causar efectos nocivos a otros programas o equipos.*

Artículo 103. *Salvo pacto en contrario, los derechos patrimoniales sobre un programa de computación y su documentación, cuando hayan sido creados por uno o varios empleados en el ejercicio de sus funciones o siguiendo las instrucciones del empleador, corresponden a éste.*
Como excepción a lo previsto por el artículo 33 de la presente Ley, el plazo de la cesión de derechos en materia de programas de computación no está sujeto a limitación alguna.

Artículo 104. *Como excepción a lo previsto en el artículo 27 fracción IV, el titular de los derechos de autor sobre un programa de computación o sobre una base de datos conservará, aún después de la venta de ejemplares de los mismos, el derecho de autorizar o prohibir el arrendamiento de dichos ejemplares. Este precepto no se aplicará cuando el ejemplar del programa de computación no constituya en sí mismo un objeto esencial de la licencia de uso.*

Artículo 105. *El usuario legítimo de un programa de computación podrá realizar el número de copias que le autorice la licencia concedida por el titular de los derechos de autor, o una sola copia de dicho programa siempre y cuando:*
I. *Sea indispensable para la utilización del programa, o*
II. *Sea destinada exclusivamente como resguardo para sustituir la copia legítimamente adquirida, cuando ésta no pueda utilizarse por daño o pérdida. La copia de respaldo deberá ser destruida cuando cese el derecho del usuario para utilizar el programa de computación.*

Artículo 106. *El derecho patrimonial sobre un programa de computación comprende la facultad de autorizar o prohibir:*
I. *La reproducción permanente o provisional del programa en todo o en parte, por cualquier medio y forma;*
II. *La traducción, la adaptación, el arreglo o cualquier otra modificación de un programa y la reproducción del programa resultante;*
III. *Cualquier forma de distribución del programa o de una copia del mismo, incluido el alquiler, y*
IV. *La decompilación, los procesos para revertir la ingeniería de un programa de computación y el desensamblaje.*

Artículo 107. *Las bases de datos o de otros materiales legibles por medio de máquinas o en otra forma, que por razones de selección y disposición de su contenido constituyan creaciones intelectuales, quedarán protegidas como compilaciones. Dicha protección no se extenderá a los datos y materiales en sí mismos.*

Artículo 231. *Constituyen infracciones en materia de comercio las siguientes conductas cuando sean realizadas con fines de lucro directo o indirecto:*
I. *Comunicar o utilizar públicamente una obra protegida por cualquier medio, y de cualquier forma sin la autorización previa y expresa del autor, de sus legítimos herederos o del titular del derecho patrimonial de autor;*
II. *Utilizar la imagen de una persona sin su autorización o la de sus causahabientes;*
III. *Producir, reproducir, almacenar, distribuir, transportar o comercializar copias de obras, fonogramas, videogramas o libros, protegidos por los derechos de autor o por los derechos conexos, sin la autorización de los respectivos titulares en los términos de esta ley;*

3.3 Proyecto de Decreto que Reforma y Adiciona diversas disposiciones del Código de Comercio en materia de Firma Electrónica.

Ante la andanada de voces que se hicieron escuchar en el mundo y a pesar de los constantes desacuerdos en derredor de la función legislativa nacional, el legislador se enfocó a plasmar en la legislación mexicana ese clamor cada vez mayor que pedía atención a la materia electrónica.

Por ello es que hacia el 30 de octubre del año dos mil dos, el Senado de la República durante el Primer Periodo Ordinario de Sesiones en su Tercer año de Ejercicio, recibió de la Cámara de Diputados del Honorable Congreso de la Unión la Minuta del Proyecto de Decreto por el que se Reforman y Adicionan diversas disposiciones del Código de Comercio en Materia de Firma Electrónica.

Después de diversas discusiones en torno a la conveniencia de reformar la legislación mercantil que por su propia vigencia se encaminaba a quedar obsoleta, no es sino hasta el 29 de agosto del 2003 cuando se culmina con la actualización de la legislación nacional, pues se publica en el Diario Oficial de la Federación una importante reforma a diversas disposiciones del Código de Comercio en Materia de Firma Electrónica. ***(15)***

IV. *Ofrecer en venta, almacenar, transportar o poner en circulación obras protegidas por esta Ley que hayan sido deformadas, modificadas o mutiladas sin autorización del titular del derecho de autor;*
V. *Importar, vender, arrendar o realizar cualquier acto que permita tener un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación;*
VI. *Retransmitir, fijar, reproducir y difundir al público emisiones de organismos de radiodifusión y sin la autorización debida;*
VII. *Usar, reproducir o explotar una reserva de derechos protegida o un programa de cómputo sin el consentimiento del titular;*
VIII. *Usar o explotar un nombre, título, denominación, características físicas o psicológicas, o características de operación de tal forma que induzcan a error o confusión con una reserva de derechos protegida;*
IX. *Utilizar las obras literarias y artísticas protegidas por el capítulo III, del Título VII de la presente Ley en contravención a lo dispuesto por el artículo 158 de la misma, y*
X. *Las demás infracciones a las disposiciones de la Ley que impliquen conducta a escala comercial o industrial relacionada con obras protegidas por esta Ley.*

(15) La presente información se puede consultar en la página de internet: http://www.gobernación.gob.mx

Más entrando en materia del presente trabajo, es necesario desglosar las reformas respecto al establecimiento de la figura del Prestador de Servicios de Certificación de Firma Electrónica haciendo un análisis del entorno que en materia mercantil rodea a ésta figura.

Como lo he referido con anterioridad, de manera neutral y adecuada el legislador mexicano no se comprometió con ninguna tecnología de emisión de firma electrónica tomando en cuenta el principio del equivalente funcional y la reciprocidad internacional pretendidos por la figura del comercio electrónico y retoma tal criterio al redactar el segundo párrafo del artículo 89 reformado:

> *"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 medios no electrónicos y de la Firma Electrónica en relación con la firma autógrafa".*

A su vez y dentro del artículo en cita, el legislador establece diversos conceptos para lograr el enfoque adecuado de la ley a la realidad, de entre los cuales es preciso citar los siguientes:

*"**Certificado:** Todo Mensaje de Datos u otro registro que confirme el vínculo entre un Firmante y los datos de creación de Firma Electrónica"* ; entendiendo por mensaje de datos a "*la información generada, enviada, recibida, archivada o comunicada a través de medios electrónicos, ópticos o cualquier otra tecnología, cuyo contenido estará conformado de manera tal que no haya lugar a dudas respecto de su autoría."*

Dicho certificado deberá contener como requisitos esenciales y conforme al artículo 108 del Código de Comercio reformado: la indicación de ser un certificado, su código de identificación exclusivo, los datos de identificación del certificador que lo emitió, nombre del titular del certificado, el periodo de su vigencia (que será como máximo de dos años), la fecha y hora de su emisión, suspensión o renovación, el alcance de las responsabilidades que asume el Prestador de

Servicios de Certificación y la referencia de la tecnología empleada para la creación de la Firma Electrónica.

*"**Firma Electrónica:** Los datos en forma electrónica consignados en un Mensaje de Datos, o adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al Firmante en relación con el Mensaje de Datos e indicar que el Firmante aprueba la información contenida en el Mensaje de Datos, y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio"*;

Lo que significa que la firma electrónica estará conformada por todos aquellos elementos comprendidos como rasgos característicos y exclusivos que su titular emplea y el que obre agregada al mensaje de datos no implica que carezca de validez jurídica, sino por el contrario, tendrá la misma validez que si se hubiere consignado en papel.

El 20 de marzo de 2002, se publica en el Diario Oficial de la Federación la Norma Oficial Mexicana NOM-151-SCFI-2002, referente a las Prácticas comerciales y los requisitos que deben observarse para la conservación de mensajes de datos y si bien la Reforma al Código de Comercio no establece diferencia alguna entre la Firma Electrónica y la Firma Digital, en ésta norma encontramos las siguientes definiciones:

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

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

Ambas definiciones nos enfocan al concepto de la firma como conjunto de rasgos que caracterizan a cada uno de los titulares de ella, pero la diferencia estriba en

que la firma digital es una especie de la firma electrónica teniendo en aquélla el rasgo personalísimo que el titular infunde en su creación y en la firma electrónica la aceptación de emisión del mensaje enviado.

Un concepto más que la reforma emplea es el de la Firma Electrónica Avanzada o Fiable que será aquella firma electrónica que cumpla con los requisitos contemplados en las fracciones I a IV del artículo 97 de la Ley en cita. ***(16)***

De la misma manera, el legislador proporciona los elementos necesarios para adecuar al mensaje de datos en el marco de seguridad que el usuario o firmante requiere para realizar toda clase de transacciones electrónicas, pues solamente él tendrá el manejo personalísimo de la firma digital, con la que acepte la responsabilidad plena sobre los mensajes que envíe sin posibilidad de repudiarlos y en caso de que exista una evidente alteración, tenga el firmante los elementos necesarios para respaldar su negativa a aceptar el mensaje controvertido como propio.

Salvo prueba en contrario y sin perjuicio del uso de cualquier otro método de verificación de la identidad del emisor, se presumirá que se actuó con la debida diligencia si el método que usó 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.

Pero en la creación de la firma electrónica que el firmante utilizará para expresar su conformidad empleando medios electrónicos, el Prestador de Servicios de Certificación de Firma Electrónica determinará y hará del conocimiento de los

---

(***16***) ***Código de Comercio.***

Artículo 97. *La Firma Electrónica se considerará Avanzada o Fiable si cumple por lo menos los siguientes requisitos: I.Los Datos de Creación de la 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 de ésta hecha después del momento de la firma.*

usuarios si las Firmas Electrónicas Avanzadas o Fiables que ofrece cumplen o no con los requerimientos dispuestos en las fracciones I a IV del artículo 97, conforme a lo que establece el artículo 98 del Código de Comercio reformado.

Más aún, con base en la reciprocidad internacional, la determinación que se haga con arreglo al párrafo anterior, deberá ser compatible con las normas y criterios internacionales reconocidos, sin perjuicio de la aplicación de las normas del derecho internacional privado.

En el Código de Comercio, con la reforma se introduce dentro del Capítulo III titulado De los Prestadores de Servicios de Certificación, tema medular del presente trabajo de investigación.

Dicho capítulo encierra esta figura que propone ventajas y seguridad a los usuarios de los servicios que los medios electrónicos de comunicación estan ofreciendo donde la mayor de las veces, se ha superado a la legislación vigente y su acelerado e incluso descontrolado crecimiento, pudiera desembocar en un caos en los sistemas financieros a nivel mundial.

El Prestador de Servicios de Certificación de Firma Electrónica será el tercero ajeno a las relaciones comerciales entre el emisor y el receptor cuyo principal fin será el brindar la exclusividad necesaria sobre la firma electrónica al titular del certificado que emita teniendo en él a *"la persona o institución pública que preste servicios relacionados con Firmas Electrónicas y que expide los Certificados, en su caso, comprendiendo entonces que el certificador será considerado un funcionario público en desempeño de sus funciones"*.

Para comprender la función de dicho ente es necesario abordar los antecedentes de la función de la Certificación.

El diccionario de la lengua española define que la certificación “es el acto por medio del cual una persona asegura o da fe de un hecho del que tiene exacto conocimiento. La certificación es el documento en el que, bajo la fe y la palabra de la persona que lo autoriza con su firma, se hace constar un hecho, acto o cualidad, a fin de que pueda surtir los correspondientes efectos jurídicos. La palabra certificación viene del latín *certificatio*, acción y efecto de certificar; para otros procede del latin *certificare*, de *certus*, cierto, y *facere*, hacer; hacer cierta una cosa por medio de instrumento público.” ***(17)***

Tenemos entonces, que la certificación es producir una presunción de certeza de lo que en la misma se hace constar, la cual se afirma obteniendo una fuerza probatoria que será respaldada por la autoridad que la emite.

De tal manera, el Reglamento del Código de Comercio en materia de Prestadores de Servicios de Certificación, en su artículo 4º establece el trámite para la acreditación como prestador de servicios de certificación en la forma y términos siguientes:

> *“I. El solicitante deberá acreditar que se encuentra en alguno de los supuestos a que se refiere el artículo 100 del Código:”*

Es pertinente hacer mención que el artículo 100 reformado establece quienes podrán ser Prestadores de Servicios de Certificación debidamente acreditados por la Secretaría de Economía, quien por conducto de la Subsecretaría de Normatividad, Inversión Extranjera y Prácticas Comerciales Internacionales, ha tenido a bien designar como Unidad Administrativa responsable del trámite para el otorgamiento de la acreditación como prestador de servicios de certificación a la Dirección General de Normatividad Mercantil ***(18)***, organismo que va a actuar con estricto apego a lo establecido en los artículos 102 inciso A del Código de

---

(17) <u>ENCICLOPEDIA JURÍDICA OMEBA.</u> Editorial Bibliográfica Omeba. Buenos Aires, Argentina, 1976. Tomo II. p.949.

(18) Esta información se obtuvo de la siguiente dirección electrónica: http://www.cofemertramites.gob.mx

Comercio reformado y 7, 8 y 9 del Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación.

Esta Dirección General de Normatividad Mercantil será la autoridad encargada de efectuar los trámites administrativos necesarios para la obtención de la acreditación de referencia, mismos que iniciarán con una “Solicitud para autorización de la procedencia para la acreditación de prestadores de servicios de certificación de firma electrónica”, para lo cual, el interesado a través de un escrito libre en el que hará una exposición del o los motivos por los cuales pretende obtener la acreditación como prestador del servicio de certificación de firma electrónica, deberá aportar los siguientes datos de información para comprobar plenamente su identidad o la de su representante:

1. Lugar y fecha de emisión del escrito;
2. Órgano administrativo al que se dirige (para el supuesto que nos ocupa lo es la Dirección General de Normatividad Mercantil);
3. Nombre completo del solicitante;
4. Nombre del representante legal (en caso de que éste aparezca en el certificado);
5. Domicilio para recibir notificaciones así como teléfono y correo electrónico e inclusive, el nombre de la o las personas autorizadas para recibirlas;
6. Petición expresa de solicitar la acreditación y emisión de su certificado, y;
7. Firma del solicitante.

La Dirección General de Normatividad Mercantil contará con un plazo máximo de treinta días hábiles para requerir al particular la información faltante. Una vez que la solicitud ha sido ingresada, cuenta con un plazo de NOVENTA DÍAS hábiles para emitir su resolución misma que puede ser ya otorgando la acreditación y generando el certificado como prestador de servicios de certificación de firma electrónica, o bien rechazando dicha solicitud cuando encuentre que alguno de los elementos requeridos no fueron oportunamente aportados por el solicitante.

La determinación emitida será publicada en el Diario Oficial de la Federación dentro de los treinta diás siguientes a su resolución.

Concluído el trámite de “Solicitud para autorización de la procedencia para la acreditación de prestador de servicios de certificación de firma electrónica”, el interesado tendrá un plazo de CUARENTA Y CINCO DÍAS para presentar el trámite de Acreditación como Prestador de Servicios de Certificación y una vez obtenida la resolución favorable del dictamen de procedencia de acreditación deberá presentar la siguiente documentación:

1. La póliza de la fianza será expedida a favor de la Tesorería de la Federación por el monto equivalente a 5,000 veces el salario mínimo general diario vigente en el Distrito Federal (para el caso de ser Notario o Corredor Público), debiendo cumplir con lo establecido en el apartado 3.1.1 de las Reglas Generales.
Tratándose de las personas morales de carácter privado o de las instituciones públicas certificadoras de firma electrónica, se fijó la fianza a otorgar por un monto similar al de los fedatarios públicos pero esta cantidad será aplicada por cada persona física que directamente o como integrante de una persona moral distinta, se pretenda contemplar dentro de la acreditación para prestar el servicio de certificación en nombre y por cuenta del solicitante, esto de conformidad al artículo 104 fracción I del Código mercantil reformado. En caso de no haber obtenido la póliza de fianza no se generará el certificado.

2. En su caso la Identificación Oficial del Representante Legal para el supuesto de que los datos de éste sean los que aparezcan en el Certificado que expedirá la Secretaría de Economía.

3. Comprobante del pago de derechos por concepto de la Acreditación como Prestador de Servicios de Certificación de Firma Electrónica en el formato 5 de la Secretaría de Hacienda y Crédito Público que ampare la cantidad de $139,300.00 (CIENTO TREINTA Y NUEVE MIL TRESCIENTOS PESOS 00/100 M.N.).

Para la resolución del trámite de acreditación, la Dirección General de Normatividad Mercantil tomará en cuenta los siguientes criterios:

1) Que la Fianza haya sido obtenida conforme al apartado 3.1.1 de las Reglas Generales para la Acreditación de los Prestadores de Servicios de Certificación de Firma Electrónica.
2) En caso de que el solicitante no haya obtenido la póliza de fianza en términos del artículo 8 del Reglamento del Código de Comercio en Materia de prestadores de Servicios de Certificación de Firma Electrónica, no se generará el certificado. La Secretaría de Economía establecerá en las Reglas Generales las condiciones a que se sujetará la fianza que otorgarán los interesados que obtengan su acreditación, previo al inicio de su operaciones, quienes contarán con un plazo de diez días contados a partir de que se haya autorizado la procedencia de la acreditación, para obtener de compañía debidamente autorizada la fianza que deberán de presentar.
3) Se comprobará la identidad del solicitante o su representante en los términos del artículo 10 del Reglamento del Código de Comercio en Materia de prestadores de Servicios de Certificación de Firma Electrónica y del apartado 4 de las Reglas Generales. Siendo entonces que la Secretaría de Economía como autoridad certificadora y registradora a través de sus servidores públicos y empleando cualquiera de los medios admitidos por el derecho, deberá comprobar la identidad del Prestador de Servicios de Certificación de Firma Electrónica o de su representante, para que éste pueda generar sus Datos de Creación de Firma Electrónica, sujetándose a lo dispuesto por los artículos 104 fracción IV y 105 del Código de Comercio.
4) El solicitante o su representante legal deberá presentarse con sus Datos de Creación de Firma Electrónica para la generación de su certificado, de conformidad con el apartado 4.2 de las Reglas Generales para la Acreditación de los Prestadores de Servicios de Certificación de Firma Electrónica. Luego entonces, 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, siempre bajo la supervisión de la Secretaría de Economía. En dicha generación se podrá utilizar cualquier tecnología por lo que el procedimiento técnico variará de acuerdo a la que sea utilizada, lo anterior a fin de cumplir con el principio de la neutralidad tecnológica.

Partiendo de los posibles candidatos a Prestadores de Servicios de Certificación de Firma Electrónica que dicho precepto establece, tenemos en primer plano a los Notarios Públicos y Corredores Públicos, fedatarios que tanto en su acreditación como en el desempeño de sus funciones tienen características similares, aunque el corredor preponderantemente se constituye para certificar actos de comercio y el notario a actividades civiles principalmente.

> *"…Tratándose de notarios o corredores públicos, a través de copia certificada de la patente, título de habilitación o documento que en términos de la legislación de la materia les acredite estar en ejercicio de la fe pública, y…"*

De esta forma, el legislador en su reforma los coloca como primeros en la lista de certificadores, pero es prudente señalar ha sido omiso en reformar sus respectivas legislaciones: la Ley Federal de Correduría Pública y las Leyes del Notariado de cada Entidad Federativa.

En entrevista celebrada con el Licenciado Andrés Jiménez Cruz, Notario Público Número 178 del Distrito Federal, en apoyo al presente trabajo y con el propósito de obtener un punto de vista profesional de alguien que se encuentra cercano a la instauración de la figura del Prestador de Servicios de Certificación de Firma Electrónica en nuestro país, tuvimos diversas cuestiones que plantear.

De las respuestas proporcionadas llegamos a la conclusión de que en efecto, a pesar de haberse celebrado el Convenio de colaboración para establecer los mecanismos de emisión y administración de los Certificados Digitales, que se utilizarán para acceder al Registro Público de Comercio y para realizar transacciones comerciales, celebrado entre la Secretaría de Comercio y Fomento Industrial (actualmente la Secretaría de Economía) y la Asociación Nacional del Notariado Mexicano, A.C, y el Colegio de Corredores Públicos, su respectivas leyes no se han actualizado por lo que no es posible determinar el alcance de las funciones que dichos fedatarios tendrán en su desempeño como certificadores de firma electrónica.

Inclusive, la reforma a los códigos civiles y procesales de cada entidad se encuentra a la expectativa para introducir la figura del comercio electrónico exaltando los elementos probatorios que se puedan aportar en materia procesal.

A efecto de garantizar el debido desempeño de las funciones del Prestador de Servicios de Certificación de Firma Electrónica en el Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación ***(19)***, se fijó una fianza la cual será consignada ante la Secretaría de Economía en una póliza de fianza expedida a favor de la Tesorería de la Federación.

El Licenciado Andrés Jiménez Cruz comentó además, que la fianza que otorgan los Notarios y Corredores Públicos conforme a la Ley del Notariado y la Ley Federal de Correduría Pública servirá también para garantizar su desempeño como autoridades certificadoras. Como lo he referido con antelación, el monto de dicha fianza fue fijado en 5,000 veces el salario mínimo general diario vigente en el Distrito Federal tratándose de un Corredor o Notario Público (aproximadamente doscientos cincuenta mil pesos).

> *"…b) Tratándose de las personas a que se refiere la fracción II del artículo 100 del Código, se requerirá de copia certificada del acta, póliza u otro instrumento público, que acredite su constitución de acuerdo con las leyes mexicanas y que su objeto social es el establecido en el artículo 101 del Código;…"*

Por otra parte y en tratándose de las personas morales de carácter privado o de las instituciones públicas certificadoras de firma electrónica, se fijó la fianza a otorgar por un monto similar al de los fedatarios públicos pero esta cantidad será aplicada por cada persona física que directamente o como integrante de una persona moral distinta, se pretenda contemplar dentro de la acreditación para prestar el servicio de certificación en nombre y por cuenta del solicitante, esto de conformidad al artículo 104 fracción I del Código mercantil reformado.

---

(19) Reglamento del Código de Comercio en materia de Prestadores de Servicios de Certificación. Artículo 6º. El referido reglamento se compulsa en su totalidad como Anexo C al presente trabajo.

Pero la función de certificación de firma electrónica que realicen los Notarios y Corredores Públicos no conllevará fe pública por sí misma, de manera tal que podrán llevar a cabo certificaciones que la impliquen o no, ya sea en documentos en papel, archivos electrónicos o en cualquier otro medio o sustancia en el que pueda incluirse información.

> *"…II. Dentro de los cinco días siguientes a la recepción de la solicitud, difundirá en los medios electrónicos con que cuente para tal efecto, el nombre, actividad profesional, domicilio del solicitante y los de las personas físicas que, tratándose de personas morales, le representen y aquellas que pretendan brindar el servicio de certificación;…"*

Siendo que la Dirección General de Normatividad Mercantil, deberá poner en conocimiento del dominio público las referencias más precisas del solicitante de la acreditación como prestador de servicios de certificación para que el usuario de sus servicios tenga la confianza para acudir a él, e inclusive, para transparentar las funciones que desempeñará.

> *"…III. Remitirá para consulta los datos indicados en el inciso anterior a las secretarías de la Función Pública, de Gobernación, de Comunicaciones y Transportes, y de Relaciones Exteriores así como a la Procuraduría General de la República, para que en el ámbito de su competencia evalúen dicha información y, en su caso, manifiesten lo que a sus atribuciones corresponda;…"*

Requisito indispensable para que el Prestador de Servicios de Certificación de Firma Electrónica acredite que no cuenta con impedimento legal alguno para el ejercicio de sus funciones, que en éste caso lo son el no encontrarse inhabilitado para desempeñar un cargo de índole público, además de no estar sujeto a proceso penal alguno e inclusive, que cuenta copn los elementos tecnológicos suficientes y bastantes para el desempeño de la función certificadora más aún, que se encuentra constituido conforme a las leyes mexicanas ya sea como persona física o moral.

"…IV. Dentro de los veinte días siguientes a la recepción de la solicitud, revisará y evaluará de manera preliminar la información y documentación recibida. Cuando derivado de la revisión, detecte la falta de cualquiera de los requisitos señalados en el Código, este Reglamento o las Reglas Generales, deberá prevenir al interesado por escrito por única vez, para que subsane la omisión dentro del término de 20 días contados a partir de su notificación. Transcurrido dicho plazo sin que sea desahogada la prevención, se desechará el trámite;…"

La Dirección General de Normatividad Mercantil a efecto de que el solicitante subsane la falta de alguna documentación o información, tiene la facultad para prevenirlo para que en un plazo razonable aporte los elementos necesarios que resultaron faltantes para dar curso a su solicitud, de lo contrario, le será desechado de plano el tramite iniciado.

"…V. La Secretaria realizará dentro de los 25 días siguientes a la fecha de presentación de la solicitud, una visita de verificación en el domicilio que señale el solicitante, a efecto de comprobar que sus instalaciones cumplen con los requisitos humanos, materiales, económicos y tecnológicos que precisa este Reglamento y las Reglas Generales, así como constatar la funcionalidad, operatividad y viabilidad de la prestación del servicio por el solicitante, y el cumplimiento con las normas y criterios internacionales, cuando no sean materia de una evaluación de la conformidad en términos de la Ley Federal sobre Metrología y Normalización, y…"

Tal procedimiento de verificación será realizado de conformidad con el procedimiento establecido en la Ley Federal sobre Metrología y Normalización, mismo que llevará a cabo una dependencia competente en materia de prestación de servicios de certificación de firma electrónica, atendiendo a los lineamientos que emita la Comisión Nacional de Normalización. ***(20)***

---

(20) Ley Federal sobre Metrología y Normalización.
Artículo 58. *Se instituye la Comisión Nacional de Normalización con el fin de coadyuvar en la política de normalización y permite la coordinación de actividades que en esta materia corresponda realizar a las distintas dependencias y entidades de la administración pública federal.*
Artículo59. *Integrarán la Comisión Nacional de Normalización:*

I. Los subsecretarios correspondientes de las Secretarías de Desarrollo Social; Medio Ambiente, Recursos Naturales y Pesca; Energía; Comercio y Fomento Industrial (actualmente de Economía); Agricultura, Ganadería y Desarrollo Rural; Comunicaciones y Transporte, Salud; Trabajo y Previsión Social, y Turismo;
II. Los subsecretarios correspondientes de las Secretarías de Hacienda y Crédito Público; Desarrollo Social; Energía, Minas e Industria Paraestatal; Comercio y Fomento Industrial (Economía); Agricultura y Recursos Hidráulicos; Comunicaciones y Transportes; Salud, Trabajo y Previsión Social,Turismo y Pesca;
III. Sendos representantes de la Asociación Nacional de Universidades e Institutos de Enseñanza Superior; de las cámaras y asociaciones de industriales y comerciales del país que determinen las dependencias; organismos nacionales de normalización y organismos del sector social productivo; y
IV. Los titulares de las subsecretarías correspondientes de las Secretarías de Hacienda y Crédito Público, de la Contsrloría y Desarrollo Administrativo, y de Educación Pública, así como del Consejo Nacional de Ciencia y Tecnología; del Centro Nacional de Metrología; del Insituto Nacional de Ecología; de la Procuraduría Federal del Consumidor; del Instituto Mexicano del Transporte, del Instituto Nacional de Pesca, y de los institutos de investigación o entidades relacionadas con la materia que se consideren pertinentes.
Por cada propietario podrá designarse un suplente para cubrir las ausencias temporales de aquél exclusivamente.
Asimismo podrá invitarse a participar en las sesiones de la Comisión a representantes de otras dependencias, de las entidades federativas, organismos públicos y privados, organizaciones de trabajadores, consumidores y profesionales e instituciones científicas y tecnológicas, cuando se traten temas de su competencia, especialidad o interés.
La Comisión será presidida rotativamente durante un año por los subsecretarios en el orden establecido en la fracción I de este artículo.
Para el desempeño de sus funciones, la Comisión contará con un secretariado técnico a cargo de la Secretaría y un Consejo Técnico.
***Artículo 60.** La Comisión tendrá las siguientes funciones:*
I. Aprobar anualmente el Programa Nacional de Normalización y vigilar su cumplimiento;
II.Establecer reglas de coordinación entre las dependencias y entidades de la administración pública federal y organizaciones privadas para la elaboración y difusión de normas y su cumplimiento;
III. Recomendar a las dependencias la elaboración, modificación, cancelación de normas oficiales mexicanas, o su expedición conjunta;
IV. Resolver las discrepancias que puedan presentarse en los trabajos de los comités consultivos nacionales de normalización;
V. Opinar, cuando se requiera, sobre el registro de organismos nacionales de normalización;
VI. Proponer la integración de grupos de trabajo para el estudio e investigación de materias específicas;
VII. Proponer las medidas que se estimen oportunas para el fomento de la normalización, así como aquéllas necesarias para resolver las quejas que presenten los interesados sobre aspectos relacionados con la apliacción de la presente Ley;
VII. Dictar los linamientos necesarios para la organización de los comités consultivos nacionales de normalización y opinar respecto de aquéllos aplicables a los comités de evaluación, y
IX. Todas aquéllas que sean necesarias para la realización de las funciones señaladas.
El reglamento interior de la Comisión determinará la manera conformela cual se realizarán estas funciones.
***Artículo 62.** Los comités consultivos nacionales de normalización son órganos para la elaboración de normas oficiales mexicanas y la promoción de su cumplimiento.*
Estarán integradas por personal técnico de las dependencias competentes, según la materia que corresponda al comité, organizaciones de industriales, prestadores de servicios, comerciantes, productores agropecuarios, forestales o pesqueros; centros de investicgación científica o tecnológica, colegios de profesionales y consumidores.
Las dependencias competentes, en coordinación con el secretariado técnico de la Comisión Nacional de Normalización, determinarán que organizaciones de las mencionadas en el párrafo anterior, deberán integrar el comité consultivo de que se trate, así como en el caso de los comités que deban constituirse para participar en actividades de normalización internacional.
***Artículo 63.** Las dependencias competentes, de acuerdo con los lineamientos que dicte la Comisión Nacional de Normalización, organizarán los comités consultivos nacionales de normalización y fijarán las reglas para*

"…VI. Una vez realizada la visita y dentro de los 45 días siguientes a la presentación de la solicitud, la Secretaría resolverá sobre la procedencia o no de la acreditación…".

Como lo he mencionado en párrafos que anteceden, la Secretaría de Economía por conducto de la Dirección General de Normatividad Mercantil emitirá la resolución del dictamen de procedencia de acreditación, hecho lo anterior, el Prestador de Srvicios de Certificación de Firma Electrónica procederá a la presentación de los documentos que avalen el pago de la fianza como de la acreditación para el desempeño de sus funciones.

Ahora bien y tratándose del artículo 5 del Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación, una vez que se ha cumplido con todos y cada uno de los requisitos a que se refiere el Código de Comercio, la Secretaría otorgará la acreditación como Prestador de Servicios de Certificación, expedirá el certificado respectivo y lo registrará, teniendo dicho certificado una vigencia de diez años.

La acreditación será publicada en el Diario Oficial de la Federación dentro de los treinta días siguientes a la resolución que determine su procedencia.

Reiterando que para la expedición del certificado, previamente la Secretaria de Economía comprobará la identidad del Prestador de Servicios de Certificación o su representante, para que éste conforme al procedimiento que determinen las Reglas Generales, acuda a generar los Datos de Creación de Firma Electrónica.

Ningún Prestador podrá tener más de una acreditación simultáneamente.

---

su operación. La dependencia que regule el mayor número de actividades del proceso de un bien o servicio dentro de cada comité, tendrá la presidencia correspondiente.
Los mismos se organizarán por materias o sectores a nivel nacional y no podrá existir más de un comité por dependencia, salvo en los casos debidamente justificados ante la Comisión.
***Artículo 79.** Para operar como organismo de certificación, será necesario contar con el acreditamiento de la Secretaría en los términos del artículo 69, mismos que se otorgará siempre que se cumpla con lo siguiente:*
I. Solicitar por escrito

Entrando al análisis del Artículo 101 el cual establece las principales actividades que contendrá el objeto social de las personas morales privadas e instituciones públicas constituidas como Prestadores de Servicios de Certificación, tenemos las siguientes:

> ***"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."*

De igual manera, queda establecido en el artículo 4 del Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación que las personas morales autorizadas para desempeñar funciones de certificación, tendrán que constituirse conforme a lo que establece el artículo 2º, fracción I, inciso a) de las Reglas generales para la acreditación de los Prestadores de Servicios de Certificación de Firma Electrónica ***(21)*** en los siguientes términos:

"...Para las personas a que se refiere la fracción II del citado artículo, se requerirá de copia certificada del Acta Constitutiva, en su caso el acta de asamblea extraordinaria, u otro instrumento, en donde conste:

i) Que se encuentren constituidas como sociedades mercantiles de acuerdo con las leyes mexicanas;..."

De acuerdo a lo que reconoce la Ley General de Sociedades Mercantiles en su artículo 1º, tenemos como sociedades mercantiles a: la sociedad en nombre colectivo, la sociedad en comandita simple, la sociedad de responsabilidad limitada, la sociedad anónima, la sociedad en comandita por acciones y la sociedad cooperativa, mismas que deberán constituirse conforme a las disposiciones de la Ley en cita.

---

(21) La presente información fue obtenida de la página en internet http://www:firmadigital.gob.mx

“ii) que el objeto de la persona moral es el requerido en el artículo 101 del Código de Comercio;...”

Esto es, que se constituyan para desempeñar las funciones de certificación de firma electrónica.

“iii) que el asiento principal de sus negocios se encuentre en el territorio nacional;”

Lo cual bien podría significar cumplir con lo que el artículo 1º de las Reglas generales en comento proponen con su establecimiento:

“...asegurar la existencia de un sistema de certificación de firma electrónica avanzada y confiable, que confirme su continuidad en el tiempo y que sirva de base para el desarrollo comercial y tecnológico del país.”

Puesto que sería ilógico que los certificadores de firma electrónica que se van a desempeñar conforme a la legislación mexicana para impulsar la economía nacional se establecieran en el extranjero, ya que las experiencias anteriores han dejado un amargo sabor de boca en la población en general que no tan fácilmente va a depositar toda su confianza y patrimonio en manos de un tercero extranjero.

Ello apartándonos de cualquier tendencia xenofóbica, tiene sustento en que un extranjero velará por obtener beneficio en primer término para si mismo y no le interesaría en grandes proporciones la economía de una nación que no es la propia.

Además, el Certificador puede establecer una o más plazas certificadoras dentro del territorio nacional siempre y cuando cuente con la autorización para ello por parte de la Secretaría de Economía y satisfaga los requisitos que refiere el artículo 2º de las Reglas para la acreditación de los Prestadores de Servicios de Certificación de Firma Electrónica.

Más aún, que los elementos técnicos empleados en la generación de una firma electrónica, garanticen tanto la exclusividad del titular como la compatibilidad en el manejo con los estándares internacionales fijados en cierto tiempo.

". . iv) los datos de inscripción en el Registro Público de Comercio; y . ."

Teniendo en el Registro Público del Comercio a la autoridad encargada de inscribir los actos mercantiles así como los que se relacionan con los comerciantes, cuya operación estará a cargo de la Secretaría de Economía a través de la Dirección General de Normatividad Mercantil.

". . v) la personalidad de su representante con facultades para Actos de Administración o poder especial para este acto, debidamente inscrita en el mencionado Registro Público de Comercio; . ."

Así, la representación de la persona moral certificadora recaerá en persona debidamente acreditada conforme a los lineamientos que determine el Registro Público de Comercio.

"...si se trata de las personas a que se refiere la fracción tercera, se requerirá de copia simple del decreto por el que se crean y, en su caso al mismo, con la fecha de publicación en el Diario Oficial de la Federación, así como el fundamento de la competencia de quien firma la solicitud en representación de la Institución Pública..."

Estas personas son las instituciones públicas que conforme a la reglamentación interna de cada una de ellas, tendrán la capacidad de designar persona con las facultades de representación suficientes para el desempeño de la actividad asignada.

Posterior a la solicitud que se dirija a la Secretaría de Economía, ésta asignará personal suficiente y calificado para realizar una visita de verificación directamente en las instalaciones del Prestador de Servicios de Certificación.

En dicha visita, se supervisará el debido cumplimiento de los elementos humanos, materiales, económicos y tecnológicos elementales así como el plan de trabajo y

de atención a las posibles contingencias que estarán diseñados y debidamente integrados para el óptimo desempeño de la actividad de certificación a efecto de garantizar la seguridad de la información y la confidencialidad en su manejo, de conformidad a lo que el artículo 3º del Reglamento del Código de Comercio en materia de Prestación de Servicios de Certificación establece **(ANEXO C)**.

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

Algo que parece interesante es lo que menciona el artículo 102 en su inciso B) "*Si la Secretaría no ha resuelto respecto a la petición del solicitante, para ser acreditado conforme al artículo 100 anterior, dentro de los 45 días siguientes a la presentación de la solicitud, se tendrá por concedida la acreditación."*, teniendo entonces que la afirmativa ficta operará respecto a la omisión de respuesta de la autoridad competente a la solicitud realizada dentro del término que para ello se le concedió.

Durante el periodo de vigencia del certificado de inscripción del certificador que tendrá como máximo diez años con opción de renovación, la Secretaría de Economía realizará funciones de autoridad certificadora y registradora de los Prestadores de Servicios de Certificación así como de vigilancia en el desempeño de sus funciones determinando los alcances de la responsabilidad del certificador y del titular del certificado.

Por último, cabe mencionar que en el caso de que un Prestador de Servicios de Certificación sea suspendido, inhabilitado o cancelado en su ejercicio, el registro y los certificados que haya expedido pasarán, para su administración, a otro

Prestador de Servicios de Certificación que para tal efecto señale la Secretaría mediante reglas generales, de lo que se deduce que no operará la figura del interinato en la certificación, pues el certificador no puede delegar las funciones que le fueron conferidas y de las cuales es el pleno responsable.

CAPÍTULO CUARTO.

"Libertas est naturalis facultas eius, quod cuique facere libet, nisi si qud vi, aut iure prohibetur."

(La libertad es una facultad natural de hacer aquello que a cada uno le agrada, si no está prohibido por alguna ley o lo impida la violencia)

FLORENTINO.

<u>Comparación entre lo establecido en la Legislación Argentina y en la Legislación Mexicana.</u>

4.1 La Ley de Firma Digital frente al Proyecto de Decreto que Reforma y Adiciona diversas disposiciones del Código de Comercio en materia de Firma Electrónica.

En éste capítulo, analizaremos las principales semejanzas y diferencias que existen entre la Ley de firma Digital que la Nación Argentina establece bajo el numeral 25.506 y las reformas efectuadas al Código de Comercio en materia de Firma Electrónica mismas que en el mes de noviembre del año 2003 iniciaran su vigencia dentro del marco de la legislación mexicana.

En primer término, es de suma importancia resaltar que la legislación argentina establece una ley que regula exclusivamente a la firma digital como lo es la Ley 25.506, a diferencia de la legislación mexicana que incluye a la referida firma y al comercio electrónico en el Código de Comercio, sin embargo, ambas legislaciones respaldan a cada Ley con una reglamentación adecuada.

Pese a ello, debería considerarse la regulación de la firma electrónica en México, en un formato similar a la legislación argentina.

Por otra parte, la legislación argentina brinda la posibilidad de que la función de emisión de certificados digitales, pueda ser realizada por Certificadores no licenciados y que los certificados que emitan tengan los mismos efectos jurídicos conforme a la Ley 25.506 de Firma Digital. ***(1)***

---

(1) op cit. <u>REGLAMENTACIÓN DE LA LEY DE FIRMA DIGITAL. DECRETO Nº 2.628/02. Artículo 2.</u>

Esto significa que el Certificador licenciado no necesariamente deberá contar con una instrucción profesional, sino que le bastará con satisfacer los requisitos que la propia Ley y su Reglamentación han establecido.

Situación que nuestro país no contempla, puesto que se han establecido como requisitos para la acreditación como Prestador de Servicios de Certificación el contar con un nivel profesional de educación mínimo como Ingeniero en Computación o su equivalente con certificación y/o experiencia de al menos 5 años en el ámbito de la seguridad informática, debiendo contar además con un abogado o Licenciado en Derecho experto en comercio electrónico.

En lo que se refiere al plazo de la vigencia de la licencia o autorización para ejercer funciones de prestador de servicios de certificación de firma electrónica, la Ley 25.506 en su artículo 26 establece que será de cinco años, pudiendo ser renovada cuando su titular realice una declaración jurada en la que conste el cumplimiento de la Ley en cita y con pleno conocimiento de que durante ese periodo estará sometido a la práctica auditorías anuales.

Por su parte, el legislador mexicano estableció una vigencia de diez años para dicha licencia siendo renovable al igual, dando debido cumplimiento a las disposiciones que se establecieron para el desempeño de sus funciones y que durante la vigencia de su licencia no haya incurrido en alguna de las causales que señala el Reglamento del Código de Comercio en materia de Prestación de Servicios de Certificación en los siguientes términos:

> ***"Artículo 14.*** *La Secretaría sancionará con suspensión temporal de uno hasta dos meses en el ejercicio de sus funciones al Prestador de Servicios de Certificación que:*
> ***I.*** *Omita determinar y hacer del conocimiento de los usuarios si las Firmas Electrónicas Avanzadas o Fiables que les ofrecen cumplen o no los requerimientos dispuestos en las fracciones I a IV del artículo 97 del Código;*
> ***II.*** *Deje de cumplir con alguno de los requisitos que establece el Código para el otorgamiento de la acreditación;*
> ***III****. Actúe en contravención de los procedimientos definidos y específicos para la tramitación de un Certificado;*

IV. *No permitir que se efectúe la consulta inmediata sobre la validez, suspensión o revocación de los certificados que emita, o*
V. *No informe, antes de la emisión de un Certificado, a la persona que solicite sus servicios, de su precio, de las condiciones precisas para la utilización del Certificado, de sus limitaciones de uso y, en su caso, de la forma en que garantiza su posible responsabilidad.*

Artículo 15 *La Secretaría sancionará con suspensión temporal de tres meses y hasta cuatro meses en el ejercicio de sus funciones al Prestador de Servicios de Certificación que:*
I. *Reincida en cualquiera de las conductas u omisiones a que se refiere el artículo anterior;*
II. *Modifique su objeto social sin dar aviso previo a la Secretaría;*
III. *No notifique a la Secretaría la iniciación de la prestación de servicios de certificación dentro de los 45 días naturales siguientes al comienzo de dicha actividad;*
IV. *No cuente con los elementos requeridos para garantizar la seguridad de la información y su confidencialidad;*
V. *Omita remitir a la Secretaría una copia de cada certificado por él generado;*
VI. *No ponga a disposición del Firmante los dispositivos de generación de los Datos de Creación y de verificación de la Firma Electrónica, o*
VII. *No proporcione los medios de acceso que permitan a la Parte que Confía en el certificado determinar los aspectos a que se refiere el artículo 104 fracción IX.*

Artículo 16 *La Secretaría sancionará con suspensión temporal de cinco y hasta seis meses en el ejercicio de sus funciones, al Prestador de Servicios de Certificación que:*
I. *Reincida en cualquiera de las conductas a que se refiere el artículo anterior;*
II. *No cuente con fianza vigente por el monto y condiciones que se determinan en forma general en este Reglamento y en las Reglas Generales;*
III. *Provoque a causa de su negligencia, imprudencia o dolo en la expedición de un certificado la nulidad de un acto jurídico, o*
IV. *Cambie de domicilio sin la autorización de la Secretaría.*

Artículo 17 *La Secretaría sancionará con suspensión definitiva en el ejercicio de sus funciones al Prestador de Servicios de Certificación que:*
I. *Reincida en cualquiera de las conductas a que se refiere el artículo anterior;*
II. *No compruebe la identidad de los solicitantes y cualesquiera circunstancias pertinentes para la emisión de un certificado los términos establecidos por el Código y este Reglamento;*
III. *Proporcione documentación o información falsa para obtener la acreditación como Prestador de Servicios de Certificación;*
IV. *Altere, modifique o destruya los certificados que emita sin que medie resolución de la Secretaría o de autoridad judicial que lo justifique;*
V. *Emita, registre o conserve los certificados que expida fuera del territorio nacional;*
V. *Impida a la Secretaría efectuar las auditorias a que se refiere el Código y éste Reglamento;*
VII. *Revele los Datos de Creación de Firma Electrónica que correspondan a su propio certificado, y*
VIII. *No guarde confidencialidad respecto a la información que haya recibido para la prestación del servicio de certificación.”*

Argentina por su parte, establece como autoridad emisora o licenciante a la Oficina Nacional de Tecnologías de Información de la Subsecretaría de la Gestión Pública dependiente de la Jefatura de Gabinete de Ministros, misma que será el organismo encargado tanto de otorgar las licencias a los certificadores como de dictar las normas tendientes a asegurar el régimen de libre competencia en el mercado de los prestadores particulares e inclusive, de velar por la protección a los usuarios de la firma digital.

A efecto de cumplir con este cometido, el Ente licenciante se auxiliará de la Contaduría General de la Nación dependiente de la Subsecretaría de Presupuesto de la Secretaría de Hacienda del Ministerior de Economía y Obras y Servicios Públicos para supervisar las actividades de dicho ente y del Certificador Licenciado.

De tal manera, el legislador argentino designa a la Comisión Asesora para la Infraestructura de Firma Digital como el órgano emisor de lineamientos tendientes a evitar el rezago tecnológico en la aplicación de las normas emitidas en la materia del comercio electrónico y como organismo auxiliar de las actividades de verificación establece a las Entidades de Auditoría que se integrarán de manera colegiada principalmente por representantes de las instituciones de educación superior especializadas en la materia.

En México, las reformas al Código de Comercio en materia de Firma Electrónica reconocen a la Secretaría de Economía como única autoridad registradora que realizará dicha función a través del Registro Público del Comercio dependiente de las Dirección General de Normatividad Mercantil.

A la vez y al igual que su homólogo argentino, el legislador mexicano establece como autoridad verificadora de las funciones del Prestador de Servicios de Certificación de Firma Electrónica a las Entidades Supervisoras que se integrarán de manera colegiada por miebros distinguidos de Instituciones de Educación

Superior que se hayan destacado en la materia de la electrónica, lo cual permite establecer el órgano auxiliar encargado de asumir el control y responsabilidad directa sobre los prestadores de los servicios de certificación.

Respecto al otorgamiento de la fianza que como garantía para el desempeño de las funciones de certificación de firma electrónica se establece, en la Nación Argentina ni la Ley 25.506 ni su correspondiente reglamentación que lo es el Decreto 2.628/02, refieren nada al respecto, limitandose a manifestar que el certificador licenciado deberá contar con los elementos humanos, tecnológicos y económicos suficientes para su buen desempeño.

La legislación mexicana representada por el Código de Comercio además de establecer como fianza la cantidad que resulte de cinco mil veces el salario mínimo general diario vigente en el Distrito Federal, exige la contratación de un seguro de responsabilidad civil contra daños y/o pérdidas de terceros por un monto mínimo de quinientos mil pesos, tratándose de cualquier error u omisión por parte del certificador.

De igual manera y en tratándose de las personas físicas o morales que actúen en nombre y por cuenta del certificador para comprobar la identidad del usuario y cualesquiera otras circunstancias referentes a la emisión de los certificados así como las que desempeñen funciones como autoridad registradora, se deberá contratar un seguro por responsabilidad civil contra daños y/o pérdidas de terceros producidas por un monto mínimo de cuatrocientos mil pesos.

La respectiva Póliza de Fianza deberá remitirse a la Secretaría de Economía dentro del plazo de los 20 días siguientes al inicio de las funciones del prestador de servicios de certificación y el seguro deberá mantenerse vigente mientras el certificador permanezca en el ejercicio de sus funciones e inclusive, durante todo el año siguiente a aquél en que haya dejado de ejercer en forma definitiva, siempre y cuando no se haya interpuesto acción de responsabilidad en su contra,

en cuyo caso deberá mantenerse vigente hasta que concluya el proceso respectivo.

Sobre la responsabilidad civil y penal que cada legislación establece para el certificador de firma electrónica y las sanciones que serán aplicadas en caso de incurrir en alguna falta, las mismas pueden abarcar desde una sanción económica, hasta llegar a la suspensión e inhabilitación temporal o definitiva de las funciones de certificación e inclusive, a ser privativas de la libertad.

Cabe hacer mención que para el otorgamiento del Certificado al Prestador de Servicios de Certificación, se requiere haber cubierto el pago de derechos por la cantidad de $125,000.00 (CIENTO VEINTICINCO MIL PESOS 00/100 .M.N.) además de haber satisfecho plenamente los requisitos establecidos en

La Reglamentación de la Ley de Firma Digital Decreto 2.628/02, en su artículo 31 determina que *"en ningún caso, la responsabilidad que pueda emanar de una certificación efectuada por un certificador licenciado, público o privado, comprometerá la responsabilidad pecuniaria del Estado en su calidad de Ente Administrador de la Infraestructura de Firma Digital"*, dejando por demás claro que en ningún momento el Estado será responsable solidario respecto de las funciones que el Certificador Licenciado tenga que desempeñar.

Asimismo, la Ley 25.506 en sus artículos 37, 38 y 39 comprendidos en el Capítulo IX intitulado *"Responsabilidad"*, nos refiere:

> *"Artículo 37. Convenio de partes. La relación entre el certificador licenciado que emita un certificado digital y el titular de ese certificado se rige por el contrato que celebren entre ellos, sin perjuicio de las previsiones de la presente ley, y demás legislación vigente"*.

Queriendo decir que para que exista la relación entre el Certificador Licenciado y el titular del certificado, es necesario celebrar un contrato en el cual se establecerán las condiciones en que cada una de las partes determinará el

alcance de sus respectivas responsabilidades y no se deje al libre albedrío del certificador la emisión o el uso del certificado a su titular responsable.

> *"Artículo 38. Responsabilidad de los certificadores licenciados ante terceros. El certificador que emita un certificado digital o lo reconozca en los términos del artículo 16 de la presente ley, es responsable por los daños y perjuicios que provoque, por los incumplimientos a las previsiones de ésta, por los errores u omisiones que presenten los certificados digitales que expida, por no revocarlos, en legal tiempo y forma cuando así correspondiere y por las consecuencias imputables a la inobservancia de procedimientos de certificación exigibles. Corresponderá al prestador del servicio demostrar que actuó con la debida diligencia"*.

Esto es, que el certificador reconozca un certificado emitido en el extranjero con estricto apego a la reciprocidad internacional, debiendo verificar que cumpla con los requisitos tanto del Estado en que fue emitido como con los que la Ley de Firma Digital señala, o para el caso de que falte alguno de los requisitos esenciales para el certificado, no lo haya revocado en el término que se le otorga para tales efectos.

En dichos supuestos, la carga de la prueba recaerá en el Certificador y no en el titular, pues deberá demostrar que los daños y perjuicios que ocasionó el certificado digital emitido en el desempeño de sus funciones, fueron por causas inimputables al certificador derivadas únicamente del manejo irracional que del mismo realizó su titular.

> *"Artículo 39. Limitaciones de responsabilidad. Los certificadores licenciados no son responsables en los siguientes casos:*
> *a) Por los casos que se excluyan taxativamente en las condiciones de emisión y utilización de sus certificados y que no estén expresamente previstos en la ley;*
> *b) Por los daños y perjuicios que resulten del uso no autorizado de un certificado digital, si en las correspondientes condiciones de emisión y utilización de sus certificados constan las restricciones de su utilización;*
> *c) Por eventuales inexactitudes en el certificado que resulten de la información facilitada por el titular que, según lo dispuesto en las normas y en los manuales*

de procedimientos respectivos, deba ser objeto de verificación, siempre que el certificador pueda demostrar que ha tomado todas las medidas razonables".

Redundando en lo anteriormente expuesto y en los límites de su desempeño, no puede ser posible extender la responsabilidad del Certificador Licenciado como emisor del certificado, a un punto tal que abarque el uso indebido que el titular del certificado emitido pueda darle o por omisiones en su manejo.

En México, el Código de Comercio establece en el artículo 110 que:

"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".

Motivo por el cual y en términos de lo referido, el Prestador de Servicios de Certificación podrá hacer las manifestaciones que a su derecho convengan con el objeto delimitar su responsabilidad frente a terceros y al titular del certificado que emitió, esto con estricto apego a la garantía de audiencia que la Constitución Política de los Estados Unidos Mexicanos establece.

Dependiendo de la gravedad de la falta en que haya incurrido y de su posible reincidencia, el certificador será sancionado con suspensión de manera temporal o definitiva de sus funciones, debiendo cubrir además una multa que será fijada tomando en cuenta la infracción cometida.

La Ley Federal del Procedimiento Administrativo como Ley aplicable para el procedimiento de imposición de sanciones al Certificador de Firma Electrónica, en su artículo 72 dispone para estos supuestos que en primer lugar, se deberá notificar al infractor que se encuentra sujeto a un proceso administrativo a efecto

de que se encuentre en posibilidad de aportar los medios que considere suficientes para demostrar lo que a su derecho convenga.

Resultando que tal y como lo establece el artículo 74 de la Ley en cita, una vez oído el infractor y desahogadas las pruebas ofrecidas y admitidas, se procederá a emitir la resolución procedente, misma que en virtud del artículo 73 de la misma Ley, deberá estar debidamente fundada y motivada tomando en consideración:

> *"I. Los daños que se hubieren producido o puedan producirse;*
> *II. El carácter intencional o no de la acción u omisión constitutiva de la infracción;*
> *III. La gravedad de la infracción; y*
> *IV. La reincidencia del infractor".*

A su vez, el artículo 111 de la multicitada Ley dispone:

> *"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".*

En Argentina existe ya la regulación a la figura de los delitos informáticos en el Código Penal denominado Ley 11.179, que en su artículo 78 bis refiere: *"Los términos firma y suscripción comprenden la firma digital, la creación de una firma digital o firmar digitalmente. Los términos documento, instrumento privado y certificado comprenden el documento digital firmado digitalmente.";* ubicando a tal figura, dentro del marco de los Delitos contra la Propiedad y contra la Fé Pública. ***(2)***

---

(2) Ley 11.179. CODIGO PENAL DE LA NACION ARGENTINA. Capítulo IV. Estafas y otras defraudaciones
ARTICULO 172. *Será reprimido con prisión de un mes a seis años, el que defraudare a otro con nombre supuesto, calidad simulada, falsos títulos, influencia mentida, abuso de confianza o aparentando bienes, crédito, comisión, empresa o negociación o valiéndose de cualquier otro ardid o engaño.*
ARTICULO 173. *Sin perjuicio de la disposición general del artículo precedente, se considerarán casos especiales de defraudación y sufrirán la pena que él establece:*
1. El que defraudare a otro en la substancia, calidad o cantidad de las cosas que le entregue en virtud de contrato o de un título obligatorio;
2. El que con perjuicio de otro se negare a restituir o no restituyere a su debido tiempo, dinero, efectos o cualquier otra cosa mueble que se le haya dado en depósito, comisión, administración u otro título que produzca obligación de entregar o devolver;

Durante la elaboración del presente trabajo y como lo he referido en el Capítulo Segundo, el legislador mexicano ha tenido a bien realizar una profunda reforma al marco jurídico nacional que contempla a la figura de los delitos cometidos empleando medios electrónicos, haciendo a un lado la posibilidad de un posible descontrol en el campo mercantil electrónico, sin embargo, continúan generándose vacios legales que solamente se lograrán llenar con una reforma armónica de las leyes nacionales.

Un acierto del Código de Comercio al contrario de la Ley de Firma Digital de la Nación Argentina, es que tiene respaldo en dos excelentes complementos como lo son el Reglamento del Código de Comercio en materia de Prestación de Servicios de Certificación y las Reglas para la acreditación de los Prestadores de Servicios de Certificación de Firma Electrónica, mismos que en su conjunto brindan la pauta para determinar los requisitos mínimos para el desempeño de las funciones del Prestador de Servicios de Certificación de Firma Electrónica

Es de esta manera que en las Reglas para la Acreditación de los Prestadores de Servicios de Certificación de Firma Electrónica (mismas que se compulsan en su totalidad con sus respectivos anexos como Anexo D), se establecen diversas disposiciones en complemento al Código de Comercio siendo en el inciso c) de la fracción I, del artículo 2 donde se encuentra la parte medular del desempeño de las funciones del Prestador de Servicios de Certificación, quien deberá contrar entre otros, con los siguientes elementos:

---

3. El que defraudare, haciendo suscribir con engaño algún documento;
4. El que cometiere alguna defraudación abusando de firma en blanco, extendiendo con ella algún documento en perjuicio del mismo que la dio o de tercero; . . . .
TITULO XII. DELITOS CONTRA LA FE PUBLICA. Capítulo I. Falsificación de moneda, billetes de banco, títulos al portador y documentos de crédito.
ARTICULO 289. *Será reprimido con prisión de seis meses a tres años:*
1. El que falsificare marcas, contraseñas o firmas oficialmente usadas o legalmente requeridas para contrastar pesas o medidas, identificar cualquier objeto o certificar su calidad, cantidad o contenido, y el que las aplicare a objetos distintos de aquellos a que debían ser aplicados.
2. El que falsificare billetes de empresas públicas de transporte.
3. El que falsificare, alterare o suprimiere la numeración de un objeto registrada de acuerdo con la ley.

*"**Elementos Humanos:** Un Director de Autoridad Certificadora, un Oficial de Seguridad, un Responsable de la entidad acreditadora y un Responsable de la autoridad registradora, los cuales deberán cubrir los perfiles y exámenes a que se refiere el Anexo 2 de las presentes reglas, y presentar el requerimiento de la letra "e" de la presente fracción. Asimismo, deberán contar con un abogado o licenciado en derecho, experto en comercio electrónico que cubra con el perfil que el PSC estipule, mismo que será aprobado por la Secretaría.*

***Elementos Materiales:** Los PSC deberán contar con todos los recursos materiales para ejercer sus funciones, incluyendo de manera enunciativa más no limitativa: con el hardware y software necesarios, los elementos materiales necesarios para lograr un plan de continuidad de negocio, la plataforma tecnológica, seguridad física, la operación de las Autoridades Certificadora y Registradora; así como para resguardar la confidencialidad de la información.*

***Elementos Económicos: i)** Contar con un seguro de responsabilidad civil contra daños y/o pérdidas de terceros, producidas como consecuencia de cualquier error u omisión del PSC, sus equipos o empleados, y del solicitante, por un monto mínimo de quinientos mil pesos, moneda nacional. El seguro deberá mantenerse vigente mientras el PSC permanezca en actividad, e inclusive durante todo el año siguiente a aquél en que haya dejado de ejercer en forma definitiva, siempre y cuando no se haya interpuesto acción de responsabilidad en su contra, en cuyo caso deberá mantenerse vigente hasta que concluya el proceso respectivo. **ii)** En caso de que el PSC sea de los que refiere la fracción II del artículo 100 del Código de Comercio, deberá contar cuando menos con un capital social y prueba de financiamiento por un millón de pesos moneda nacional, combinados si fuera el caso, entre capital fijo y variable.*

***Elementos Tecnológicos:** Una plataforma tecnológica que observe los requerimientos de seguridad física, el Plan de seguridad de sistemas, Plan de administración de llaves, la Política de certificados de firma avanzada, la declaración de prácticas de certificación y los modelos operacionales de las autoridades certificadora y registradora, de acuerdo con el Anexo 2 de las presentes reglas, en el entendido de que los certificados deberán ser generados y almacenados en el territorio nacional".*

4.2 La aplicabilidad del comercio electrónico.

En la actualidad, la influencia de los medios electrónicos de comunicación en nuestra agitada y cotidiana forma de vida es mas que evidente.

La evolución de la computadora como principal pilar de la revolución tecnológica fue tan acelerada de aproximadamente unos diez años a la fecha, que hoy día tiene una gran intervención en todos los ámbitos no solamente de la comunicación, sino también en los campos de la salud, el entretenimiento, la educación y la ciencia con resultados asombrosos en su precisión, más su vertiginoso avance se ha visto momentáneamente contenido.

La economía no podría quedarse al margen y gran parte de sus actuales actividades dependen de un parpadeo o un “click”, ya sea para sufrir un severo trastorno o tener el aliciente necesario para que los mercados bursátiles ya incrementen sus inversiones, impulsando la economía de un Estado o bien, sufran severos trastornos que consecuentemente lo coloquen en una severa recesión.

Es por estas y otras múltiples razones, que a nivel internacional el comercio electrónico ha dejado muy claro que su eficiencia va acorde con las exigencias actuales en relación a los costos de operación y la consiguiente supresión de algunos innecesarios trámites corporativos y administrativos, lo cual desemboca en una disminución drástica de la intervención del factor humano en el entorno de la globalización económica, con logros casi perfectos y con un alto grado de aprovechamiento.

La Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (UNCITRAL) se ha encargado de proporcionar las bases para legislar al comercio electrónico y hasta el momento, los resultados obtenidos en aquéllos estados que han adoptado la Ley Modelo que emitiera en materia de comercio electrónico, son

más que alentadores y ejemplares para que otros estados se encaminen a adoptarlo en su ordenamiento interno.

A pesar de las dificultades tecnológicas, ideológicas, educativas, políticas y en mayor grado, económicas, se ha prestado importancia aunque no la debida, al comercio electrónico y cada día son más los países que se adhieren a esta modalidad del mercado mundial, atraídos por las evidentes ventajas que ofrece mismas que han sido mencionadas en el desarrollo del presente trabajo de investigación.

Tanto Argentina como México, adoptaron en sus legislaciones a la figura del comercio electrónico contemplando los logros conseguidos en otros países del orbe, evitando que su adopción fuera lesiva para los intereses nacionales y procurando sobretodo la compatibilidad de dicha figura con su marco legal.

4.3 Efectividad de la firma electrónica.

Cuando la UNCITRAL emitió la Ley Modelo en materia de Firma Electrónica, lo hizo con el objetivo primordial de aportar a los Estados un lineamiento lo suficientemente adecuado para adoptar en sus ordenamientos legales a ésta figura.

Con las desventajas que ofrece la firma electrónica al igual que la firma autógrafa, con sus posibles alteraciones y consiguientes consecuencias, también presenta enormes ventajas, principalmente en lo que se refiere a la contratación entre no presentes, situación que los legisladores argentinos y mexicanos tomaron muy en cuenta al momento de integrar la firma electrónica o digital en su respectivo ordenamiento interno.

Algo contundentemente cierto es que su manejo es más fácil, preciso y seguro, pues solamente dependerá del titular el uso que haga de ella y las consecuencias

de los actos que celebre y consienta al momento de agregar su firma digital, se tendrán como jurídicamente válidas.

El National Institute of Standards and Technology (NIST) creado por el Congreso de Estados Unidos para apoyar a la industria en el desarrollo de las tecnologías necesarias para mejorar la calidad de los productos, modernizar sus procesos de fabricación, asegurar su confiabilidad y facilitar su rápida comercialización en base a los últimos avances científicos, se dió a la tarea de plantear diversos mecanismos de almacenamiento de datos entre los cuales los más interesantes son:

> *"**1) Diskette:** presenta características que lo hacen el medio más práctico y económico ya que se puede leer en todas las computadoras, es fácilmente transportable y permite almacenar un gran volumen de información. Sin embargo no es un medio confiable ya que su uso intensivo puede causar pérdida de información por ello, se recomienda realizar copias de resguardo de la clave privada del titular.*
>
> ***2) Disco rígido o duro:** al igual que el diskette se encuentra en todos los equipos aunque es más confiable con respecto al mantenimiento de la información, sin embargo cuenta con las desventajas de que en primera, no es transportable, lo que implica que el usuario sólo puede utilizar su clave privada desde una sola estación de trabajo; y en segunda, la mayoría de los equipos no cuentan actualmente con un Sistema Operativo que impida el acceso de usuarios no habilitados a los archivos donde se almacene la clave privada la cual aunque se encuentra protegida por un sistema criptográfico que restringe su uso al titular de la misma, no puede evitarse su destrucción voluntaria o involuntariamente.*
> *Por lo anterior, es recomendable contar con una política de seguridad para los equipos, no sólo a nivel de red, si se desea utilizar este tipo de dispositivos. Los discos rígidos removibles solucionan el problema de la seguridad, pero igualmente deben ser utilizados personalmente.*
>
> ***3) Smart Cards:** o llamadas tarjetas inteligentes, son los dispositivos mejor considerados para esta tarea ya que cuentan con varias características que*

hacen apropiado su uso para almacenar las claves privadas: son fácilmente transportables y seguras e incluso es posible incorporar en ellas los algoritmos necesarios para la generación del par de claves, la firma y la verificación de manera tal de proteger la clave privada de todo acceso externo. El inconveniente actual es la poca disponibilidad de lectores instalados sobre el parque actual de computadoras personales y una opción es que pueden ser incorporados a las computadoras de manera externa o interna y a manera de ejemplo es posible el uso de un dispositivo dentro del lector de diskette.

4) Tarjetas de memoria: *permiten solamente almacenar información, sin ninguna capacidad criptográfica, sin embargo, cuenta con las mismas limitaciones que las Smart Cards en lo que respecta a los lectores y al almacenamiento seguro de la información, motivo por el cual, es recomendable el uso de Smart Cards en lugar de estos dispositivos.*

5) Módulos Criptográficos en hardware: *permiten almacenar la clave privada y realizar todos los cálculos criptográficos dentro del mismo. Su capacidad, tanto en seguridad como en velocidad de cálculo es superior a una implementación y ejecución por software, lo que los hacen apropiados para aplicaciones críticas de máxima seguridad donde se requiera dicha capacidad. Sin embargo, no son apropiados para almacenar las claves privadas de los usuarios ya que no son transportables."* **(*3*)**

Es por todo lo anteriormente expuesto que no es tan sencilla la implementación de la figura de la firma electrónica en las formas habituales de hacer comercio, ya que es menester el establecimiento de un adecuado sistema de detección de posibles sabotajes (cracking) o intrusión ilegal (hacking) en los sistemas de manejo de la información consignada en los mensajes de datos respaldada en los archivos electrónicos a cargo de los Prestadores de Servicios de Certificación de Firma Electrónica.

A su vez, dichos certificadores y de conformidad a lo que disponen el Código de Comercio, el Reglamento del Código de Comercio en materia de Prestación de

---

(3) La presente información se puede consultar en la siguiente página de internet: http://www.itl.nist.gov

Servicios de Certificación y las Reglas para la acreditación de los Prestadores de Servicios de Certificación de Firma Electrónica, necesitan tener bien definidas y establecidas sus instalaciones físicas, eléctricas, electrónicas y así como un control del personal en el lugar donde establecerán su centro de operaciones de certificación, a efecto de evitar un acceso no autorizado a los archivos en los cuales el certificador resguardará las operaciones que realice.

Además, deberán de contar con un plan de contingencias eficiente y probado periódicamente para salvaguardar dicha información tanto de los ataques informáticos (como los "virus"), accesos no autorizados o sabotajes, como de los que por inclemencias del tiempo (apagones, inundaciones) o por disturbios sociales (mítines, motines, etc.) se llegaren a suscitar.

4.4 Funcionalidad del Prestador de Servicios de Certificación de Firma Electrónica. (*4*)

Al cabo del desarrollo del presente trabajo de investigación, nos hemos formulado constantemente una pregunta: ¿es realmente necesaria la función e instauración en nuestro país de un certificador de firma electrónica?.
La respuesta es obvia, pues la necesidad de su instauración estriba en brindar ese respaldo que como tercero ajeno a las transacciones comerciales que las partes celebren tiene al no perseguir interés alguno en el negocio cual juzgador en una controversia, por lo cual, se obliga a conducirse con total apego a la imparcialidad y profesionalismo que su actividad le demande.

Su función también es necesaria toda vez que al certificar una firma electrónica, le da al titular de la misma el pleno dominio sobre ella, misma que frente a terceros será la forma expresa de manifestar su consentimiento al igual que si lo realizará

---

(4) Salvo que se cite otra fuente, esta información se obtuvo al consultar la página internet http://www.pscworld.com

en el medio tradicional de reconocer las obligaciones contraídas como lo es el papel.

Para ello, se han establecido tres tipos de certificado a emitir que deberán cumplir en proporcionar los tres factores de seguridad mas importantes como son privacidad, autentificación e integridad en los mensajes, estos certificados serán:

a) **Certificado de servidor:** tendrá como única finalidad asegurar la existencia y denominación de una entidad en internet. Estos certificados serán utilizados a través de aplicaciones en servidores con el protocolo SSL (Secure Sockets Layer), el cual fue diseñado por Netscape Communications para habilitar las comunicaciones de manera encriptada y autenticada a través de internet siendo usado principalmente en comunicaciones entre navegadores y servidores web. Para soportar la encriptación, se emitirán este tipo de certificados de hasta 128 bits utilizando tecnología de Codificación Controlada por el Servidor (SGC por sus siglas en inglés Served-Gated Cryptography).
b) **Certificado de representación:** su única finalidad será asegurar la existencia y denominación del signatario del certificado. Serán emitidos a personas físicas o morales con actividad empresarial para garantizar frente a terceros su identidad, autenticidad e integridad de sus mensajes, así como que el representante legal de una empresa o persona física manifieste que su representada se encuentra capacitada legalmente para la celebración del acto y acreditar que la personalidad que ostenta y las facultades con que cuenta no le han sido limitadas, modificadas o revocadas. Este tipo de certificados se emitirá con una longitud en su llave de 1024 bits.
c) **Certificado personal:** Tendrá como única finalidad asegurar la existencia y denominación del signatario del certificado. Estos certificados serán emitidos a personas físicas para garantizar frente a terceros su identidad,

autenticidad e integridad de sus mensajes. La longitud de su llave será igual de 1024 bits.

El Prestador de Servicios de Certificación de Firma Electrónica realizará funciones de certificación de los actos que ante él se celebren sin que se deduzca que los actos certificados serán cubiertos con la fé pública de un Notario, un Corredor o cualquiera otro servidor público en ejercicio de sus funciones, por tanto, los certificados que emitan podrán ser de dos tipos.

a) **Sin fé pública.** Los que se efectúen ante un agente certificador con un costo variable de los $2,000.00 (DOS MIL PESOS 00/100 M.N.) a $1,000.00 (MIL PESOS 00/100 M.N.) aproximadamente.
b) **Con fé pública.** Los que realiza un Fedatario Público (Notario o Corredor) acreditado como Agente Certificador o bien, cuando lo emite un agente certificador y se registran con Ratificación de Firma, siendo por tanto, instrumentos públicos en términos de los artículos 1237 y 1391 fracción II del Código de Comercio. El costo será determinado por la **Lista de Precios de los Certificados sin fe Pública** más los servicios del Fedatario Público que se trate, el cual varía entre $2,700.00 (DOS MIL SETECIENTOS PESOS 00/100 M.N.) a $7,000.00 (SIETE MIL PESOS 00/100 M.N.) aproximadamente.

Por cuanto al precio para la emisión de cada certificado, se tomará en cuenta el tipo de acreditación y los precios citados serán por concepto de su emisión y la renovación por año de hasta un 70% del precio publicado.

Siendo entonces que la Acreditación como Prestador de Servicios de Certificación de Firma Electrónica se regirá por los aranceles que establezca la Secretaría de Economía, en tanto que el costo de los certificados que expidan será determinado por la libre competencia.

Si bien es cierto que en un principio el monto de la fianza establecida y los demás requisitos económicos exigidos para el desempeño de las funciones de certificación me parecieron un tanto excesivos y limitantes para con las personas fisicas y morales de carácter privado, también es cierto que al entrar al análisis de las reformas suscitadas en nuestra legislación mercantil he llegado a considerar que dichos requisitos económicos fueron establecidos para ser suficientes y bastos a modo de garantizar la prestación de los servicios del certificador.

Al acudir a una entrevista con la Licenciada Rosa María Guevara Ibarra, Jefa del Departamento de Creditación de la Dirección General de Normatividad Mercantil, perteneciente a la Subsecretaría de Normatividad, Inversión Extranjera y Prácticas Comerciales Internacionales dependiente de la Secretaría de Economía, me hizo referencia que al ser la responsable de dar el seguimiento a todos y cada uno de los trámites de acreditación de Certificadores de Firma electrónica en nuestro país, ha encontrado que tanto Fedatarios Públicos como personas físicas y morales de carácter público o privado han mostrado interés en obtener su acreditación como autoridad certificadora, sin embargo, no registran su correspondiente tramitación ante el panorama tan complicado que les presenta la exigencia de los requisitos humános, físicos y técnicos aunados al costo de la acreditación como del trámite de revisión de documentos y otorgamiento de fianzas que les significaría una derrama económica mínima de $1,000,000.00 (UN MILLÓN DE PESOS 00/100 M.N.).

De tal suerte que hasta el momento se cuenta con dos Prestadores Servicios de Certificación de Firma electrónica acreditados debidamente ante la Secretaría de Economía y que se encuentran en ejercicio de sus funciones siendo los siguientes:

1. **Advantage Security, S. de R.L. de C.V.** Con fecha 13 de diciembre de 2005, se publica en el Diario Oficial de la Federación el Acuerdo por el cual el Director General de Normatividad Mercantil Hugo

Ricardo de la Rosa Guzmán le otorgó la acreditación como Prestador de Servicios de Certificación **(*5*)**.

2. **PSC World, S. DE R.L. de C.V.** El 15 de diciembre de 2005, fue publicada en el Diario Oficial de la Federación la resolución en que fuera otorgada su acreditación como PSCFE **(*6*)**.

Cada certificador ha tenido a bien determinar el costo de cada tipo de certificado que emitan y el segundo de ellos incluso, se ha asociado con dos fedatarios públicos para el supuesto de la expedición de un certificado de firma electrónica con fé pública.

Así también y dentro del marco que conforma sus estructuras, los certificadores en cita se han fijado como objetivo primordial para el desempeño de sus funciones la implementación de los Servicios de Seguridad Administrado para la Infraestructura de Llave Pública (PKI), a partir de una revisión metodológica acorde las mejores prácticas internacionales en materia de Seguridad de la Información y la aplicación de las leyes y normativas existentes en nuestro país.

Lo anterior esperando despejar la duda latente que surge en relación a la seguridad que brindaría el que los principales certificadores sean extranjeros, aunada al hecho de que si será suficiente que se reconozca al Prestador de Servicios de Certificación de Firma Electrónica representado en una persona moral o física de carácter privado, el haberse constituído conforme a las leyes mexicanas relativas a las sociedades sin importar su nacionalidad, capital social extranjero o establecimiento de sucursales en el territorio nacional.

Abundando en lo expuesto en el desarrollo del presente trabajo, nos encontramos que la vigilancia de la Secretaría de Economía y los organos designados auxiliares sobre las funciones de certificación, resguardo, registro, vigilancia y control de los

---

(5) Esta información fue obtenida de la dirección electrónica http://www.advantage-security.com
(6) op.cit. http://www.pscworld.com

prestadores de servicios de certificación de firma electrónica hasta el momento se encuentra en un estado aceptable, aunado al resguardo que el propio Registro Público de Comercio realizará respecto de los certificados emitidos.

Sin embargo, la actual infraestructura de las redes de comunicación electrónica aún es débil por lo cual, no tenemos la certeza de hasta que punto podrá ser capaz de soportar los diversos ataques que los saboteadores (crackers) e intrusos (hackers) enfilen hacia las transmisiones de los mensajes de datos, pues las pérdidas económicas podrían ser estratosféricas incluso a nivel nacional.

Su debilidad se manifiesta con las constantes averías que sufre el sistema de telefonía celular o la saturación de las líneas telefónicas, incluso a nivel satelital, lo que nos obliga a pensar en el supuesto de una transmisión masiva de mensajes de datos y su acertada recepción que en tiempos actuales y a futuro, no se puede permitir un error que de suscitarse, significaría pérdidas insospechadas para las partes contratantes y para la Nación.

Aunado a lo anterior, necesitamos conocer si los grandes servidores o buscadores en internet como Yahoo, Altavista, AOL, Google, entre otros, aceptarán los términos y condiciones que la Secretaría de Economía les imponga cumplir para la realización de auditorias o para preinstalar sus bases.

Ello porque la Secretaría de Economía va a funcionar como archivo central donde se resguardarán los certificados de firma digital así como los actos que certifiquen los prestadores de servicios de certificación y necesariamente tiene que contar tanto con un acceso electrónico adecuado para soportar los envíos de información de los certificadores, como con un sistema eficiente y confiable en materia de seguridad informática.

Por otra parte, es necesario determinar si la Secretaría de Economía será capaz de cumplir con los requisitos que en materia de certificación de calidad impongan

los servidores para permitir el uso de sus servicios, pues además de las tarifas que cobran por ello, necesitan cumplir con ciertos estándares establecidos por los demás servidores y organismos para mantener un orden informático (por ejemplo el límite de almacenamiento de datos).

4.5 Conveniencia de la instauración en la Legislación Mexicana de un Prestador de Servicios de Certificación de Firma Electrónica.

Incipiente e incompleto es como en lo personal considero al marco jurídico nacional frente a la competencia mundial en materia del comercio electrónico.

Incipiente porque a pesar de tener antecedentes que datan desde los años ochentas, no se había tomado con la debida seriedad el incorporarlo a la legislación nacional y no es sino hasta el año dos mil que se comienza a configurar el entorno informático necesario para su desarrollo, e incompleto por los motivos que expongo en los párrafos subsecuentes.

Estados Unidos, España, Francia, Tailandia y Malasia por mencionar a los mas importantes, son Estados que se enfocaron para competir a nivel mundial en materia mercantil y los resultados obtenidos han sido satisfactorios hasta el momento, pues en ellos el prestador de servicios de certificación de firma electrónica juega un primordial papel al funcionar como ente depositario de la confianza de los usuarios de los servicios electrónicos de contratación.

Las reformas que se suscitaron en nuestro país toman en cuenta las directrices que el orbe estableció y el planteamiento propuesto es adecuado, siendo necesario complementarlo con las reformas que se realicen a la Ley Federal de Correduría Pública debidamente respaldada por cada Entidad Federativa en sus respectivas leyes del Notariado y sus códigos adjetivos y sustantivos tanto civiles como penales, esto por cuanto al valor y eficacia probatoria que se le brinde a un documento digital.

Hasta ahora es abismal el atraso que la mayoría de los empresarios nacionales tienen en materia de informática, pues los recursos humanos, financieros, administrativos y materiales son limitados y la falta de difusión y confiabilidad en el ordenamiento legal mexicano cuenta con vacios que hasta el momento han hecho dificil la práctica del comercio electrónico.

Probablemente debido a una falta de previsión o una severa laguna legal, la situación imperante en la Nación Argentina pudo ser originada en parte y no totalmente por haber errado en la delegación de dicha facultad certificadora hacia entes certificadores no licenciados que en el desempeño de sus funciones, no contaban con la suficiente experiencia profesional y elementos técnicos y económicos para hacer frente al tráfico electrónico mundial.

Es por todo lo mencionado en el presente trabajo y apoyándonos en las experiencias anteriores, que resulta un tanto complicado determinar el grado de confiabilidad y efectividad que tendrá la figura del prestador de servicios de certificación de firma electrónica en México, pues aunque sus esquemas de funcionamiento queden perfectamente delimitados en el ordenamiento legal, la duda se hace presente en si la autoridad certificadora será lo suficientemente capaz de corresponder a la confianza depositada por los usuarios de sus servicios más aún, si estará plenamente respaldada por la Secretaría de Economía en el cumplimiento de sus funciones certificadoras.

Pero también es importante resaltar que la necesidad de establecer al prestador de servicios de certificación de firma electrónica en México, estriba en la capacidad que tenga el comerciante nacional de enfrentarse a las imposiciones que la globalización impone hoy día en materia mercantil, respaldándolo tanto con una legislación acorde a la competencia mundial que cada vez se vuelve más impositiva, como con un ente dedicado exclusivamente a resguardar los actos electrónicamente celebrados otorgándoles la validez que la reciprocidad internacional les demanda.

C O N C L U S I O N E S.

1) Nuestra actual forma de vida exige una participación intensiva donde la preparación es la constante ante los cambios vertiginosos que la evolución en las tecnologías de la información ha desencadenado.

2) Después de una escalada impresionante, la evolución informática continúa y quienes han adquirido lo más moderno en equipo de cómputo, en un lapso breve de tiempo tienen que actualizar o desechar su equipo, pues los procesadores y los programas se desarrollan aceleradamente brindando no solamente facilidad en su manejo, sino también una mayor capacidad de almacenaje de datos y rapidez en la respuesta.

3) Internet es la máxima expresión de la revolución tecnológica que actualmente ha superado todas las expectativas generadas desde su aparición, convirtiéndose en algo más que un servicio de búsqueda de información y comunicaciones, siendo hoy por hoy el medio más eficaz para realizar las transacciones mas inusuales pero a la vez, también se encuentra a la deriva en materia de seguridad, resultando por ello esencial crear una cultura de ética en los usuarios que día a día acceden a la red, fomentando en todo momento el respeto a los derechos fundamentales de los cibernautas que confían en los servicios que ofrece.

4) Es necesario establecer pero sobretodo difundir entre las naciones la figura de un organismo que controle y vigile cercanamente los movimientos de la red de redes hacia su interior en el ámbito de validez tanto nacional como internacional, que proteja a todos los usuarios que abanderan la buena fe y la moral, evitando con ello la comisión de excesos en perjuicio de cualquier persona que cuente con su computadora personal y una conexión a internet.

5) Por lo anterior, es primordial que el Derecho ante el desmesurado desarrollo tecnológico, reestructure su visión del mundo contemporáneo para evitar dejar en un estado de indefensión a los usuarios de los servicios de contratación a través de medios electrónicos.

6) En el ámbito internacional, la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (UNCITRAL por sus siglas en inglés), ha propuesto a las naciones Leyes Modelo cada una con sus respectivas reglas, con el principal objetivo de unificar criterios para no convertir las materias del comercio electrónico y la firma electrónica en temas de trato únicamente nacional, sino que su adopción sea acorde con la práctica comercial convencional a nivel mundial.

7) En la actualidad, el comercio demanda un mínimo grado de dificultad, una rapidez constante y un mínimo de errores e inclusive, la inexistencia de riesgos en la inversión que como consecuencia, le permitan obtener grandes ganancias y beneficios, motivos por los cuales el comercio electrónico es práctica constante en la sociedad mundial.

8) El comercio electrónico como protagonista de la actual revolución informática, sociológica y económica, permitirá que el sector productivo de nuestro país impulse la competitividad y eficiencia de las empresas nacionales de cualquier sector y nivel económico pero a la vez, se constituye en un enorme reto que el sector empresarial mexicano enfrentará en el mercado mundial.

9) La firma electrónica se presenta como la manifestación contemporánea de la voluntad plasmada en medios electrónicos sin dejar de satisfacer los requisitos de la firma autógrafa, pues cuenta con los mismos rasgos que caracterizan a ésta mismos que hacen posible detectar cualquier alteración o uso indebido por persona ajena a su titular, rasgos que transformados en

algoritmos, se integran individualmente hasta conformarse en una cadena o serie de bits que solamente el titular podrá manejar o delegar bajo su más estricta responsabilidad.

10) El consentimiento como elemento de existencia de los contratos, exige la existencia de normas específicas en materia de comercio electrónico, toda vez que la contratación a través de medios electrónicos es una forma diversa de contratar que no se encuentra contemplada ni en el supuesto de la contratación entre presentes, ni en la contratación entre ausentes.

11) En el empleo de los medios electrónicos, el momento del envío y de la recepción de un mensaje de datos resultan trascendentales en materia del consentimiento, toda vez que su incidencia es esencial en la formación del mismo y para la contratación a través de los medios electrónicos, la exteriorización de la declaración de la voluntad se encuentra plasmada en la firma electrónica.

12)Tal exteriorización de la voluntad se puede hacer a través de los medios electrónicos, siempre que sea legalmente atribuible al firmante para que surta efectos la función identificativa de la misma para brindar certeza de que es el firmante y no un tercero quien asume la obligación.

13) Los sistemas de seguridad en materia informática creados con el fin de salvaguardar las comunicaciones consignadas en un mensaje de datos desde su emisión hasta su resguardo, se configuran como el blindaje más confiable que en materia de telecomunicaciones se ha conseguido establecer, resultando de entre todos el encriptado y la firma digital los de mayor difusión principalmente por su confiabilidad, bajo costo y alto desempeño.

14) Tanto Argentina como México, procuran brindarle al usuario consumidor que emplea los medios electrónicos, el respaldo legal necesario para efectuar operaciones mercantiles tomando a la buena fe como la esencia en sus respectivas legislaciones.

15) El prestador de servicios de certificación de firma electrónica como ente depositario de la confianza de las partes que realicen transacciones electrónicas, en todo momento deberá acreditar cumplir con requisitos tan variados como complicados en su conjunto pero justificables entre sí, en primera por la importancia en el desempeño de las funciones que el certificador va a realizar y en segunda, por las circunstancias plagadas de escepticismo que actualmente rodean el constante actuar de las autoridades.

16) Las reformas a la legislación nacional y en especial al Código de Comercio en nuestro país, han plasmado perfectamente la intención de las leyes modelo y la realidad mundial, sin embargo, es necesario realizar una profunda reforma tanto a la Ley Federal de Correduría Pública como a las Leyes y códigos de cada Entidad (principalmente a las Leyes del Notariado) para así, conseguir una adecuada coordinación legislativa y evitar la aparición de lagunas legales, esto con el principal objetivo de mantener la confianza del usuario de los servicios ofrecidos a través de los medios electrónicos.

17) Asimismo, la Secretaría de Economía deberá de comprobar su capacidad para mantener el orden respecto de los certificadores y los actos que realicen así como su manejo, difusión y resguardo para su posterior consulta, todo de manera coordinada y responsable constituyéndose en un ente capaz y suficiente para atender el reclamo que la actividad certificadora demande a cada momento.

18) Luego entonces, la Secretaría de Economía no debe limitarse solamente a una actividad de vigilancia y sanción en el plano nacional, sino también aplicarse en el plano internacional obligándose a atender la intervención que tengan los extranjeros en las funciones de certificación y sobretodo, al momento de reconocer los efectos jurídicos que los certificados extranjeros puedan tener en México.

19) Por lo que respecta al Gobierno Mexicano en todos sus niveles, se encuentra obligado a difundir y vigilar la promoción de las nuevas tecnologías en materia de comunicación para desarrollar servicios que sean aptos para atender al usuario y a la vez, prevenir y solventar cualquier eventualidad que pudiera acarrear consigo una severa crisis económica.

20) El Prestador de los servicios de certificación de firma electrónica, tiene bases sólidas tanto en la Nación Argentina como en nuestro país, sin embargo y ante la constante evolución de las tecnologías, es prioridad de cada uno de los Estados procurar por el respaldo legal que brinde certeza jurídica nacional e internacional a sus funciones y responsabilidades.

21) Tanto Argentina como México, pugnan por una despapelización tanto en el sector público como en el privado, procurando en todo momento el impulso a sus respectivas economías y el consiguiente beneficio para sus habitantes enfocándose a comprender el movimiento tan acelerado de la economía mundial, para de esa manera, evitar entrar en desventaja y otorgando concesiones perjudiciales para la salud económica, jurídica y social de todos los países partícipes de esta nueva tendencia comercial.

BIBLIOGRAFÍA.

1. **ACOSTA ROMERO, Miguel. "Compendio de Derecho Administrativo. Parte General". Editorial Porrúa. México, 2000.**
2. **ALTAMARK, Daniel Ricardo. "Informática y Derecho". Editorial Desalma. Buenos Aires, Argentina, 1987.**
3. **BACA CARDOSO, Silvia Elizabeth. "Necesidades Informativas en materia de Comercio Electrónico". Tesis Profesional. UNAM. ENEP Acatlán.**
4. **BARRIOS GARRIDO, Gabriela. "Internet y Derecho en México". Editorial McGraw/Hill Interamericana Editores, Sociedad Anónima de Capital Variable. México, 1998.**
5. **BARRIOS GARRIDO, Gabriela. "México ante la nueva normativa global de la tecnología de información: ¿Qué está pasando con el internet?". En Boletín de Política Informática, México, INEGI, Año XX, Número 2, 1997.**
6. **BARRIOS-GARRIDO, Gabriela. "Internet y Derecho en México". Editorial McGraw/Hill Interamericana Editores, Sociedad Anónima de Capital Variable. México, 1998.**
7. **BELTRAMONE, GUILLERMO-ZAVALE, Ezequiel. "El Derecho en la Era Digital". Editorial Juris.**
8. **BURGOA Orihuela, Ignacio. "Las garantías individuales". 20a edición, Editorial Porrúa, México, 1986.**
9. **CABALLERO GIL, Pino. Artículo publicado en el Boletín del Criptonomicón #32.**
10. **CARRION, Hugo Daniel. "Ponencia presentada por el autor en el Auditorio León de Greiff de la Universidad Nacional de Colombia el 7 de mayo de 1999".**
11. **CASTELLS, Manuel. "Globalización, sociedad y política en la era de la información".**
12. **CERVANTES AHUMADA, Raúl. "Derecho Mercantil Primer Curso". Editorial Porrúa. México, 2000.**
13. **CERVANTES AHUMADA, Raúl. "Títulos y Operaciones de Crédito". Décimocuarta Edición. Editorial Porrúa. México, 1999.**
14. **CHIOVENDA, Giusseppe. "Principios de Derecho Procesal Civil". Tomo II. Editorial Porrúa, México, 1984.**
15. **DEL POZO, Luz María. "Informática en el Derecho". Editorial Trillas. México, 1992**
16. **DICCIONARIO DE TERMINOS CIENTÍFICOS Y TÉCNICOS. MC GRAW HILL / BOIXAREU. Marcombo Boixareu Editores. Vol 1, Barcelona España. 1981.**
17. **DICCIONARIO DE TERMINOS CIENTÍFICOS Y TÉCNICOS. MC GRAW HILL / BOIXAREU. Marcombo Boixareu Editores. Vol 2, Barcelona España. 1981.**
18. **ENCICLOPEDIA JURÍDICA OMEBA. Editorial Bibliográfica Omeba. Buenos aires, Argentina, 1976. Tomo II.**
19. **FARREL, Christopher A. "A Day Trade online". Jhon Wiley. Nueva York, 1999.**
20. **FREEDMAN, Alex. "Diccionario de Computación Bilingüe". 7ª edición.Editorial Mc Graw Hill / Interamericana S.A. Santa Fe de Bogotá, Colombia. 1996. Vol 1.**

21. **GARCÍA MAINEZ, Eduardo. "Introducción al Estudio del Derecho". Editorial Porrúa, México, 1994.**
22. **GUTIERREZ Y GONZÁLEZ, Ernesto. Derecho de las obligaciones. Treceava Edición. Editorial Porrúa. México, 2001.**
23. **H. SANDERS, Donald. "Informática: Presente y futuro". Tercera edición. Editorial Mc Graw Hill / Interamericana de México S.A. de C. V. México, 1990.**
24. **INSTITUTO DE INVESTIGACIONES JURÍDICAS, UNAM. "Diccionario de Derecho Mercantil". Ed. Porrúa. México, 2001.**
25. **INSTITUTO DE INVESTIGACIONES JURÍDICAS, UNAM. "Diccionario Jurídico Mexicano". 3era edición. Ed. Porrúa, México. 1989. Tomo II.**
26. **INSTITUTO DE INVESTIGACIONES JURÍDICAS. "Diálogo sobre la Informática Jurídica". Editado por la Universidad Nacional Autónoma de México, Serie: E Varios, número 45. México, 1989.**
27. **LUKE, O'CONNOR. "Internet: ¿El medio seguro de la supercarretera de la información?". En New Lestter. Lania, Otoño-Invierno 1995, Año 4, Volumen 14.**
28. **MANTILLA MOLINA, Roberto L. "Derecho Mercantil: Introducción y conceptos fundamentales, sociedades". Ed. Porrúa, México. 1992. 2da edición. p. 153.**
29. **MARTÍNEZ ALTAMIRANO, Eduardo. "Derecho a la intimidad: Desarrollo, tutelación y perspectiva comparativa". Revista jurídica ABC Información y análisis jurídicos, Madrid, Segunda Epoca, dic 2000, Número 126.**
30. **NUEVA ENCICLOPEDIA TEMÁTICA. Trigésima Edición. Editorial Cumbre, Sociedad Anónima. México, 1983.**
31. **OPPLIGER, Rolf. "Sistemas de autentificación para seguridad en redes". Alfaomega Grupo Editor S.A. de C.V. México, 1998.**
32. **ORGANIZACIÓN DE LAS NACIONES UNIDAS. "El correo de la U.N.E.S.C.O. de 1983".**
33. **PEREZNIETO CASTRO, Leonel. "Derecho Internacional Privado". Sexta Edición. Editorial Harla, Sociedad Anónima de Capital Variable. México, 1995.**
34. **RIBAS ALEJANDRO, Javier. "Aspectos Jurídicos del Comercio Electrónico en internet". Aranzadi Editorial. Pamplona, España, 1999.**
35. **RIOS ESTAVILLO, J. José. "Derecho Informático en México: Informática Jurídica y derecho de la informática". Instituto de Investigaciones Jurídicas. Universidad Nacional Autónoma de México. México, 1997.**
36. **ROJINA VILLEGAS, Rafael. "Derecho Civil Mexicano: Introducción y personas". Décima Edición. Editorial Porrúa. México, 2001.**
37. **SEARA VÁZQUEZ, Modesto. "Derecho Internacional Público". Décimo Segunda Edición. Editorial Porrúa, Sociedad Anónima de Capital Variable. México, 1988.**
38. **SENADO DE LA REPUBLICA. "Gaceta Parlamentaria". Año 2002 No. 81. Jueves 28 de noviembre de 2002.**
39. **SERRA ROJAS, Andrés. "Derecho Administrativo Doctrina, Legislación y Jurisprudencia". Décimo Octava Edición. Editorial Porrúa. México, 1997.**
40. **SHURETY, Samantha. e-business with Net.Commerce. Editorial Prentice Hall. Upper Sadle River, New Jersey. 1999.**
41. **TELLEZ VALDÉS, Julio. "Contratos Informáticos". Editado por el Instituto de Investigaciones Jurídicas de la Universidad Nacional**

Autónoma de México. Serie G: Estudios Doctrinales, número 117, México. 1988.
42. TELLEZ VALDÉS, Julio. "La protección jurídica de los programas de computación". Segunda Edición. Editado por el Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México. Serie 6: Estudios Doctrinales, número 124. México. 1989.
43. TÉLLEZ VALDÉS, Julio. "Derecho Informático". Editorial Mc Graw Hill / Interamericana de México, S.A. de C.V., México, 1996.
44. TELLEZ VALDÉS, Julio. "Derecho Informático". Segunda Edición. Editorial Mc Graw Hill/Interamericana Editores, Sociedad Anónima de Capital Variable. México, 1996.
45. TOFFLER, Alvin y Heidi. "La nueva economía apenas comienza". Editorial La Nación. 9 de mayo de 2001.
46. VILLORO TORANZO, Miguel. "Introducción al Estudio del Derecho". Décima Edición. Editorial Porrúa. México, 1993.
47. WESTLAND, J Christopher. "Global Electronic Commerce: theory and case studies". MIT (Massachusetts Institut Tecnology). Cambridge, Massachusetts. 1999.

L E G I S L A C I Ó N.

1. Anteproyecto de Ley Firma Digital de los Actos Jurídicos referente al Comercio Electrónico. Argentina.
2. Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil en materia de Comercio Electrónico.
3. Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil en materia de Firma Electrónica.
4. Ley de firma digital No. 25.506.
5. Constitución Nacional de la Nación Argentina, 2003.
6. Decreto 1028/2003.
7. Decreto 2.628/2002. Reglamentación de la Ley de Firma Digital, 2002.
8. Código de Comercio. 2003/2005.
9. Norma Oficial Mexicana NOM-151-SCFI-2002, referente a las Prácticas comerciales y los requisitos que deben observarse para la conservación de mensajes de datos, 2003.
10. Ley General de Sociedades Mercantiles, 2003.
11. Reglamento Interior de la Secretaría de Economía, 2003.
12. Ley Federal del Procedimiento Administrativo, 2003.
13. Reglamento del Código de Comercio en materia de Prestación de Servicios de Certificación, 2003.
14. Reglas para la Acreditación de los Prestadores de Servicios de Certificación de Firma Electrónica, 2003.
15. Ley del Notariado del Distrito Federal, 2003.
16. Ley Federal de Correduría Pública, 2003.

DIRECCIONES ELECTRÓNICAS EN INTERNET.

1. **http://www.pscworld.com**
2. **http://www.advantage-security.com**
3. **http://www.derecho-internet.org**
4. **http://www.cofemertramites.gob.mx**
5. **http://www.geocities.com**
6. **http://www.it-cenit.org.ar**
7. **http://www.arkhaios.com**
8. **http://www.bakerinfo.com**
9. **http://www.biblioweb.dgsca.unam.mx**
10. **http://www.comunidad.derecho.org**
11. **http://www.criptonomicon.com**
12. **http://www.ctv.es**
13. **http://www.ecertchile.cl**
14. **http://www.economia.gob.mx**
15. **http://www.enterate.unam.mx**
16. **http://www.firmadigital.gob.mx**
17. **http://www.gobernación.gob.mx**
18. **http://www.infoleg.mecon.gov.ar**
19. **http://www.internet.org**
20. **http://www.jurídicas.unam.mx**
21. **http://www.leydigital.com**
22. **http://www.llrx.com**
23. **http://www.natlaw.com**
24. **http://www.nic.ar**
25. **http://www.notariadomexicano.org.mx**
26. **http://www.pki.gov.ar**
27. **http://www.sat.gob.mx**
28. **http://www.senado.gob.mx**
29. **http://www.sii.cl**
30. **http://www.un.or.at**
31. **http://www.uncitral.org**
32. **http.//www.itl.nist.gov**
33. **http.//www.sfp,gov,ar**
34. **http.//www.ito.ch**
35. **http.//www.smartcardsys,com**
36. **http.//www.rsa.com**
37. **http.//www.ietf.or**
38. **http.//www.ftp.isi.edu**

ANEXO A. LEY DE FIRMA DIGITAL. Ley 25.506

Consideraciones generales. Certificados digitales. Certificador licenciado. Titular de un certificado digital. Organización institucional. Autoridad de aplicación. Sistema de auditoría. Comisión Asesora para la Infraestructura de Firma Digital. Responsabilidad. Sanciones. Disposiciones Complementarias.
Sancionada: Noviembre 14 de 2001.
Promulgada de Hecho: Diciembre 11 de 2001.
El Senado y Cámara de Diputados de la Nación Argentina reunidos en Congreso, etc. sancionan con fuerza de Ley:

LEY DE FIRMA DIGITAL

CAPITULO I
Consideraciones generales

ARTICULO 1º — Objeto. Se reconoce el empleo de la firma electrónica y de la firma digital y su eficacia jurídica en las condiciones que establece la presente ley.

ARTICULO 2º — Firma Digital. Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma. Los procedimientos de firma y verificación a ser utilizados para tales fines serán los determinados por la Autoridad de Aplicación en consonancia con estándares tecnológicos internacionales vigentes.

ARTICULO 3º — Del requerimiento de firma. Cuando la ley requiera una firma manuscrita, esa exigencia también queda satisfecha por una firma digital. Este principio es aplicable a los casos en que la ley establece la obligación de firmar o prescribe consecuencias para su ausencia.

ARTICULO 4º — Exclusiones. Las disposiciones de esta ley no son aplicables:
a) A las disposiciones por causa de muerte;
b) A los actos jurídicos del derecho de familia;
c) A los actos personalísimos en general;
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 disposiciones legales o acuerdo de partes.

ARTICULO 5º — Firma electrónica. Se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez.

ARTICULO 6º — Documento digital. Se entiende por documento digital a la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo. Un documento digital también satisface el requerimiento de escritura.

ARTICULO 7º — Presunción de autoría. Se presume, salvo prueba en contrario, que toda firma digital pertenece al titular del certificado digital que permite la verificación de dicha firma.

ARTICULO 8º — Presunción de integridad. Si el resultado de un procedimiento de verificación de una firma digital aplicado a un documento digital es verdadero, se presume, salvo prueba en contrario, que este documento digital no ha sido modificado desde el momento de su firma.

ARTICULO 9º — Validez. Una firma digital es válida si cumple con los siguientes requisitos:
a) Haber sido creada durante el período de vigencia del certificado digital válido del firmante;
b) Ser debidamente verificada por la referencia a los datos de verificación de firma digital indicados en dicho certificado según el procedimiento de verificación correspondiente;
c) Que dicho certificado haya sido emitido o reconocido, según el artículo 16 de la presente, por un certificador licenciado.

ARTICULO 10. — Remitente. Presunción. Cuando un documento digital sea enviado en forma automática por un dispositivo programado y lleve la firma digital del remitente se presumirá, salvo prueba en contrario, que el documento firmado proviene del remitente.

ARTICULO 11. — Original. Los documentos electrónicos firmados digitalmente y los reproducidos en formato digital firmados digitalmente a partir de originales de primera generación en cualquier otro soporte, también serán considerados originales y poseen, como consecuencia de ello, valor probatorio como tales, según los procedimientos que determine la reglamentación.

ARTICULO 12. — Conservación. La exigencia legal de conservar documentos, registros o datos, también queda satisfecha con la conservación de los correspondientes documentos digitales firmados digitalmente, según los procedimientos que determine la reglamentación, siempre que sean accesibles para su posterior consulta y permitan determinar fehacientemente el origen, destino, fecha y hora de su generación, envío y/o recepción.

CAPITULO II
De los certificados digitales

ARTICULO 13. — Certificado digital. Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular.

ARTICULO 14. — Requisitos de validez de los certificados digitales. Los certificados digitales para ser válidos deben:
a) Ser emitidos por un certificador licenciado por el ente licenciante;
b) Responder a formatos estándares reconocidos internacionalmente, fijados por la autoridad de aplicación, y contener, como mínimo, los datos que permitan:
1. Identificar indubitablemente a su titular y al certificador licenciado que lo emitió, indicando su período de vigencia y los datos que permitan su identificación única;
2. Ser susceptible de verificación respecto de su estado de revocación;
3. Diferenciar claramente la información verificada de la no verificada incluidas en el certificado;
4. Contemplar la información necesaria para la verificación de la firma;
5. Identificar la política de certificación bajo la cual fue emitido.

ARTICULO 15. — Período de vigencia del certificado digital. A los efectos de esta ley, el certificado digital es válido únicamente dentro del período de vigencia, que comienza en la fecha de inicio y finaliza en su fecha de vencimiento, debiendo ambas ser indicadas en el certificado digital, o su revocación si fuere revocado.
La fecha de vencimiento del certificado digital referido en el párrafo anterior en ningún caso puede ser posterior a la del vencimiento del certificado digital del certificador licenciado que lo emitió.
La Autoridad de Aplicación podrá establecer mayores exigencias respecto de la determinación exacta del momento de emisión, revocación y vencimiento de los certificados digitales.

ARTICULO 16. — Reconocimiento de certificados extranjeros. Los certificados digitales emitidos por certificadores extranjeros podrán ser reconocidos en los mismos términos y condiciones exigidos en la ley y sus normas reglamentarias cuando:

a) Reúnan las condiciones que establece la presente ley y la reglamentación correspondiente para los certificados emitidos por certificadores nacionales y se encuentre vigente un acuerdo de reciprocidad firmado por la República Argentina y el país de origen del certificador extranjero, o
b) Tales certificados sean reconocidos por un certificador licenciado en el país, que garantice su validez y vigencia conforme a la presente ley. A fin de tener efectos, este reconocimiento deberá ser validado por la autoridad de aplicación.

CAPITULO III
Del certificador licenciado

ARTICULO 17. — Del certificador licenciado. Se entiende por certificador licenciado a toda persona de existencia ideal, registro público de contratos u organismo público que expide certificados, presta otros servicios en relación con la firma digital y cuenta con una licencia para ello, otorgada por el ente licenciante.
La actividad de los certificadores licenciados no pertenecientes al sector público se prestará en régimen de competencia. El arancel de los servicios prestados por los certificadores licenciados será establecido libremente por éstos.

ARTICULO 18. — Certificados por profesión. Las entidades que controlan la matrícula, en relación a la prestación de servicios profesionales, podrán emitir certificados digitales en lo referido a esta función, con igual validez y alcance jurídico que las firmas efectuadas en forma manuscrita. A ese efecto deberán cumplir los requisitos para ser certificador licenciado.

ARTICULO 19. — Funciones. El certificador licenciado tiene las siguientes funciones:
a) Recibir una solicitud de emisión de certificado digital, firmada digitalmente con los correspondientes datos de verificación de firma digital del solicitante;
b) Emitir certificados digitales de acuerdo a lo establecido en sus políticas de certificación, y a las condiciones que la autoridad de aplicación indique en la reglamentación de la presente ley;
c) Identificar inequívocamente los certificados digitales emitidos;
d) Mantener copia de todos los certificados digitales emitidos, consignando su fecha de emisión y de vencimiento si correspondiere, y de sus correspondientes solicitudes de emisión;
e) Revocar los certificados digitales por él emitidos en los siguientes casos, entre otros que serán determinados por la reglamentación:
1) A solicitud del titular del certificado digital.
2) Si determinara que un certificado digital fue emitido en base a una información falsa, que en el momento de la emisión hubiera sido objeto de verificación.
3) Si determinara que los procedimientos de emisión y/o verificación han dejado de ser seguros.
4) Por condiciones especiales definidas en su política de certificación.
5) Por resolución judicial o de la autoridad de aplicación.
f) Informar públicamente el estado de los certificados digitales por él emitidos. Los certificados digitales revocados deben ser incluidos en una lista de certificados revocados indicando fecha y hora de la revocación. La validez y autoría de dicha lista de certificados revocados deben ser garantizadas.

ARTICULO 20. — Licencia. Para obtener una licencia el certificador debe cumplir con los requisitos establecidos por la ley y tramitar la solicitud respectiva ante el ente licenciante, el que otorgará la licencia previo dictamen legal y técnico que acredite la aptitud para cumplir con sus funciones y obligaciones. Estas licencias son intransferibles.

ARTICULO 21. — Obligaciones. Son obligaciones del certificador licenciado:
a) Informar a quien solicita un certificado con carácter previo a su emisión y utilizando un medio de comunicación las condiciones precisas de utilización del certificado digital, sus características y efectos, la existencia de un sistema de licenciamiento y los procedimientos, forma que garantiza su posible responsabilidad patrimonial y los efectos de la revocación de su propio certificado digital y

de la licencia que le otorga el ente licenciante. Esa información deberá estar libremente accesible en lenguaje fácilmente comprensible. La parte pertinente de dicha información estará también disponible para terceros;
b) Abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder bajo ninguna circunstancia, a los datos de creación de firma digital de los titulares de certificados digitales por él emitidos;
c) Mantener el control exclusivo de sus propios datos de creación de firma digital e impedir su divulgación;
d) Operar utilizando un sistema técnicamente confiable de acuerdo con lo que determine la autoridad de aplicación;
e) Notificar al solicitante las medidas que está obligado a adoptar para crear firmas digitales seguras y para su verificación confiable, y las obligaciones que asume por el solo hecho de ser titular de un certificado digital;
f) Recabar únicamente aquellos datos personales del titular del certificado digital que sean necesarios para su emisión, quedando el solicitante en libertad de proveer información adicional;
g) Mantener la confidencialidad de toda información que no figure en el certificado digital;
h) Poner a disposición del solicitante de un certificado digital toda la información relativa a su tramitación;
i) Mantener la documentación respaldatoria de los certificados digitales emitidos, por diez (10) años a partir de su fecha de vencimiento o revocación;
j) Incorporar en su política de certificación los efectos de la revocación de su propio certificado digital y/o de la licencia que le otorgara la autoridad de aplicación;
k) Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, la lista de certificados digitales revocados, las políticas de certificación, la información relevante de los informes de la última auditoría de que hubiera sido objeto, su manual de procedimientos y toda información que determine la autoridad de aplicación;
l) Publicar en el Boletín Oficial aquellos datos que la autoridad de aplicación determine;
m) Registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas;
n) Informar en las políticas de certificación si los certificados digitales por él emitidos requieren la verificación de la identidad del titular;
o) Verificar, de acuerdo con lo dispuesto en su manual de procedimientos, toda otra información que deba ser objeto de verificación, la que debe figurar en las políticas de certificación y en los certificados digitales;
p) Solicitar inmediatamente al ente licenciante la revocación de su certificado, o informarle la revocación del mismo, cuando existieren indicios de que los datos de creación de firma digital que utiliza hubiesen sido comprometidos o cuando el uso de los procedimientos de aplicación de los datos de verificación de firma digital en él contenidos hayan dejado de ser seguros;
q) Informar inmediatamente al ente licenciante sobre cualquier cambio en los datos relativos a su licencia;
r) Permitir el ingreso de los funcionarios autorizados de la autoridad de aplicación, del ente licenciante o de los auditores a su local operativo, poner a su disposición toda la información necesaria y proveer la asistencia del caso;
s) Emplear personal idóneo que tenga los conocimientos específicos, la experiencia necesaria para proveer los servicios ofrecidos y en particular, competencia en materia de gestión, conocimientos técnicos en el ámbito de la firma digital y experiencia adecuada en los procedimientos de seguridad pertinentes;
t) Someter a aprobación del ente licenciante el manual de procedimientos, el plan de seguridad y el de cese de actividades, así como el detalle de los componentes técnicos a utilizar;
u) Constituir domicilio legal en la República Argentina;

v) Disponer de recursos humanos y tecnológicos suficientes para operar de acuerdo a las exigencias establecidas en la presente ley y su reglamentación;
w) Cumplir con toda otra obligación emergente de su calidad de titular de la licencia adjudicada por el ente licenciante.

ARTICULO 22. — Cese del certificador. El certificador licenciado cesa en tal calidad:
a) Por decisión unilateral comunicada al ente licenciante;
b) Por cancelación de su personería jurídica;
c) Por cancelación de su licencia dispuesta por el ente licenciante.
La autoridad de aplicación determinará los procedimientos de revocación aplicables en estos casos.

ARTICULO 23. — Desconocimiento de la validez de un certificado digital. Un certificado digital no es válido si es utilizado:
a) Para alguna finalidad diferente a los fines para los cuales fue extendido;
b) Para operaciones que superen el valor máximo autorizado cuando corresponda;
c) Una vez revocado.

CAPITULO IV
Del titular de un certificado digital

ARTICULO 24. — Derechos del titular de un certificado digital. El titular de un certificado digital tiene los siguientes derechos:
a) A ser informado por el certificador licenciado, con carácter previo a la emisión del certificado digital, y utilizando un medio de comunicación sobre las condiciones precisas de utilización del certificado digital, sus características y efectos, la existencia de este sistema de licenciamiento y los procedimientos asociados. Esa información deberá darse por escrito en un lenguaje fácilmente comprensible. La parte pertinente de dicha información estará también disponible para terceros;
b) A que el certificador licenciado emplee los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por él, y a ser informado sobre ello;
c) A ser informado, previamente a la emisión del certificado, del precio de los servicios de certificación, incluyendo cargos adicionales y formas de pago;
d) A que el certificador licenciado le informe sobre su domicilio en la República Argentina, y sobre los medios a los que puede acudir para solicitar aclaraciones, dar cuenta del mal funcionamiento del sistema, o presentar sus reclamos;
e) A que el certificador licenciado proporcione los servicios pactados, y a no recibir publicidad comercial de ningún tipo por intermedio del certificador licenciado.

ARTICULO 25. — Obligaciones del titular del certificado digital. Son obligaciones del titular de un certificado digital:
a) Mantener el control exclusivo de sus datos de creación de firma digital, no compartirlos, e impedir su divulgación;
b) Utilizar un dispositivo de creación de firma digital técnicamente confiable;
c) Solicitar la revocación de su certificado al certificador licenciado ante cualquier circunstancia que pueda haber comprometido la privacidad de sus datos de creación de firma;
d) Informar sin demora al certificador licenciado el cambio de alguno de los datos contenidos en el certificado digital que hubiera sido objeto de verificación.

CAPITULO V
De la organización institucional

ARTICULO 26. — Infraestructura de Firma Digital. Los certificados digitales regulados por esta ley deben ser emitidos o reconocidos, según lo establecido por el artículo 16, por un certificador licenciado.

ARTICULO 27. — Sistema de Auditoría. La autoridad de aplicación, con el concurso de la Comisión Asesora para la Infraestructura de Firma Digital, diseñará un sistema de auditoría para evaluar la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y disponibilidad de los datos, así como también el cumplimiento de las especificaciones del manual de procedimientos y los planes de seguridad y de contingencia aprobados por el ente licenciante.

ARTICULO 28. — Comisión Asesora para la Infraestructura de Firma Digital. Créase en el ámbito jurisdiccional de la Autoridad de Aplicación, la Comisión Asesora para la Infraestructura de Firma Digital.

CAPITULO VI
De la autoridad de aplicación

ARTICULO 29. — Autoridad de Aplicación. La autoridad de aplicación de la presente ley será la Jefatura de Gabinete de Ministros.

ARTICULO 30. — Funciones. La autoridad de aplicación tiene las siguientes funciones:
a) Dictar las normas reglamentarias y de aplicación de la presente;
b) Establecer, previa recomendación de la Comisión Asesora para la Infraestructura de la Firma Digital, los estándares tecnológicos y operativos de la Infraestructura de Firma Digital;
c) Determinar los efectos de la revocación de los certificados de los certificadores licenciados o del ente licenciante;
d) Instrumentar acuerdos nacionales e internacionales a fin de otorgar validez jurídica a las firmas digitales creadas sobre la base de certificados emitidos por certificadores de otros países;
e) Determinar las pautas de auditoría, incluyendo los dictámenes tipo que deban emitirse como conclusión de las revisiones;
f) Actualizar los valores monetarios previstos en el régimen de sanciones de la presente ley;
g) Determinar los niveles de licenciamiento;
h) Otorgar o revocar las licencias a los certificadores licenciados y supervisar su actividad, según las exigencias instituidas por la reglamentación;
i) Fiscalizar el cumplimiento de las normas legales y reglamentarias en lo referente a la actividad de los certificadores licenciados;
j) Homologar los dispositivos de creación y verificación de firmas digitales, con ajuste a las normas y procedimientos establecidos por la reglamentación;
k) Aplicar las sanciones previstas en la presente ley.

ARTICULO 31. — Obligaciones. En su calidad de titular de certificado digital, la autoridad de aplicación tiene las mismas obligaciones que los titulares de certificados y que los certificadores licenciados. En especial y en particular debe:
a) Abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder, bajo ninguna circunstancia, a los datos utilizados para generar la firma digital de los certificadores licenciados;
b) Mantener el control exclusivo de los datos utilizados para generar su propia firma digital e impedir su divulgación;
c) Revocar su propio certificado frente al compromiso de la privacidad de los datos de creación de firma digital;
d) Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, los domicilios, números telefónicos y direcciones de Internet tanto de los certificadores licenciados como los propios y su certificado digital;
e) Supervisar la ejecución del plan de cese de actividades de los certificadores licenciados que discontinúan sus funciones.

ARTICULO 32. — Arancelamiento. La autoridad de aplicación podrá cobrar un arancel de licenciamiento para cubrir su costo operativo y el de las auditorías realizadas por sí o por terceros contratados a tal efecto.

CAPITULO VII
Del sistema de auditoría

ARTICULO 33. — Sujetos a auditar. El ente licenciante y los certificadores licenciados, deben ser auditados periódicamente, de acuerdo al sistema de auditoría que diseñe y apruebe la autoridad de aplicación.
La autoridad de aplicación podrá implementar el sistema de auditoría por sí o por terceros habilitados a tal efecto. Las auditorías deben como mínimo evaluar la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y, disponibilidad de los datos, así como también el cumplimiento de las especificaciones del manual de procedimientos y los planes de seguridad y, de contingencia aprobados por el ente licenciante.

ARTICULO 34. — Requisitos de habilitación. Podrán ser terceros habilitados para efectuar las auditorías las Universidades y organismos científicos y/o tecnológicos nacionales o provinciales, los Colegios y Consejos profesionales que acrediten experiencia profesional acorde en la materia.

CAPITULO VIII
De la Comisión Asesora para la Infraestructura de Firma Digital

ARTICULO 35.— Integración y funcionamiento. La Comisión Asesora para la Infraestructura de Firma Digital estará integrada multidisciplinariamente por un máximo de 7 (siete) profesionales de carreras afines a la actividad de reconocida trayectoria y experiencia, provenientes de Organismos del Estado nacional, Universidades Nacionales y Provinciales, Cámaras, Colegios u otros entes representativos de profesionales.
Los integrantes serán designados por el Poder Ejecutivo por un período de cinco (5) años renovables por única vez.
Se reunirá como mínimo trimestralmente. Deberá expedirse prontamente a solicitud de la autoridad de aplicación y sus recomendaciones y disidencias se incluirán en las actas de la Comisión.
Consultará periódicamente mediante audiencias públicas con las cámaras empresarias, los usuarios y las asociaciones de consumidores y mantendrá a la autoridad de aplicación regularmente informada de los resultados de dichas consultas.

ARTICULO 36. — Funciones. La Comisión debe emitir recomendaciones por iniciativa propia o a solicitud de la autoridad de aplicación, sobre los siguientes aspectos:
a) Estándares tecnológicos;
b) Sistema de registro de toda la información relativa a la emisión de certificados digitales;
c) Requisitos mínimos de información que se debe suministrar a los potenciales titulares de certificados digitales de los términos de las políticas de certificación;
d) Metodología y requerimiento del resguardo físico de la información;
e) Otros que le sean requeridos por la autoridad de aplicación.

CAPITULO IX
Responsabilidad

ARTICULO 37. — Convenio de partes. La relación entre el certificador licenciado que emita un certificado digital y el titular de ese certificado se rige por el contrato que celebren entre ellos, sin perjuicio de las previsiones de la presente ley, y demás legislación vigente.

ARTICULO 38. — Responsabilidad de los certificadores licenciados ante terceros.
El certificador que emita un certificado digital o lo reconozca en los términos del artículo 16 de la presente ley, es responsable por los daños y perjuicios que provoque, por los incumplimientos a las

previsiones de ésta, por los errores u omisiones que presenten los certificados digitales que expida, por no revocarlos, en legal tiempo y forma cuando así correspondiere y por las consecuencias imputables a la inobservancia de procedimientos de certificación exigibles. Corresponderá al prestador del servicio demostrar que actuó con la debida diligencia.

ARTICULO 39. — Limitaciones de responsabilidad. Los certificadores licenciados no son responsables en los siguientes casos:
a) Por los casos que se excluyan taxativamente en las condiciones de emisión y utilización de sus certificados y que no estén expresamente previstos en la ley;
b) Por los daños y perjuicios que resulten del uso no autorizado de un certificado digital, si en las correspondientes condiciones de emisión y utilización de sus certificados constan las restricciones de su utilización;
c) Por eventuales inexactitudes en el certificado que resulten de la información facilitada por el titular que, según lo dispuesto en las normas y en los manuales de procedimientos respectivos, deba ser objeto de verificación, siempre que el certificador pueda demostrar que ha tomado todas las medidas razonables.

CAPITULO X
Sanciones

ARTICULO 40. — Procedimiento. La instrucción sumarial y la aplicación de sanciones por violación a disposiciones de la presente ley serán realizadas por el ente licenciante. Es aplicable la Ley de Procedimientos Administrativos 19.549 y sus normas reglamentarias.

ARTICULO 41. — Sanciones. El incumplimiento de las obligaciones establecidas en la presente ley para los certificadores licenciados dará lugar a la aplicación de las siguientes sanciones:
a) Apercibimiento;
b) Multa de pesos diez mil ($ 10.000) a pesos quinientos mil ($ 500.000);
c) Caducidad de la licencia.
Su gradación según reincidencia y/u oportunidad serán establecidas por la reglamentación.
El pago de la sanción que aplique el ente licenciante no relevará al certificador licenciado de eventuales reclamos por daños y perjuicios causados a terceros y/o bienes de propiedad de éstos, como consecuencia de la ejecución del contrato que celebren y/o por el incumplimiento de las obligaciones asumidas conforme al mismo y/o la prestación del servicio.

ARTICULO 42. — Apercibimiento. Podrá aplicarse sanción de apercibimiento en los siguientes casos:
a) Emisión de certificados sin contar con la totalidad de los datos requeridos, cuando su omisión no invalidare el certificado;
b) No facilitar los datos requeridos por el ente licenciante en ejercicio de sus funciones;
c) Cualquier otra infracción a la presente ley que no tenga una sanción mayor.

ARTICULO 43. — Multa. Podrá aplicarse sanción de multa en los siguientes casos:
a) Incumplimiento de las obligaciones previstas en el artículo 21;
b) Si la emisión de certificados se realizare sin cumplimentar las políticas de certificación comprometida y causare perjuicios a los usuarios, signatarios o terceros, o se afectare gravemente la seguridad de los servicios de certificación;
c) Omisión de llevar el registro de los certificados expedidos;
d) Omisión de revocar en forma o tiempo oportuno un certificado cuando así correspondiere;
e) Cualquier impedimento u obstrucción a la realización de inspecciones o auditorías por parte de la autoridad de aplicación y del ente licenciante;
f) Incumplimiento de las normas dictadas por la autoridad de aplicación;
g) Reincidencia en la comisión de infracciones que dieran lugar a la sanción de apercibimiento.

ARTICULO 44. — Caducidad. Podrá aplicarse la sanción de caducidad de la licencia en caso de:

a) No tomar los debidos recaudos de seguridad en los servicios de certificación;
b) Expedición de certificados falsos;
c) Transferencia no autorizada o fraude en la titularidad de la licencia;
d) Reincidencia en la comisión de infracciones que dieran lugar a la sanción de multa;
e) Quiebra del titular.
La sanción de caducidad inhabilita a la titular sancionada y a los integrantes de órganos directivos por el término de 10 años para ser titular de licencias.

ARTICULO 45. — Recurribilidad. Las sanciones aplicadas podrán ser recurridas ante los Tribunales Federales con competencia en lo Contencioso Administrativo correspondientes al domicilio de la entidad, una vez agotada la vía administrativa pertinente.
La interposición de los recursos previstos en este capítulo tendrá efecto devolutivo.

ARTICULO 46. — Jurisdicción. En los conflictos entre particulares y certificadores licenciados es competente la Justicia en lo Civil y Comercial Federal. En los conflictos en que sea parte un organismo público certificador licenciado, es competente la Justicia en lo Contencioso-administrativo Federal.

CAPITULO XI
Disposiciones Complementarias

ARTICULO 47. — Utilización por el Estado Nacional. El Estado nacional utilizará las tecnologías y previsiones de la presente ley en su ámbito interno y en relación con los administrados de acuerdo con las condiciones que se fijen reglamentariamente en cada uno de sus poderes.

ARTICULO 48. — Implementación. El Estado nacional, dentro de las jurisdicciones y entidades comprendidas en el artículo 8º de la Ley 24.156, promoverá el uso masivo de la firma digital de tal forma que posibilite el trámite de los expedientes por vías simultáneas, búsquedas automáticas de la información y seguimiento y control por parte del interesado, propendiendo a la progresiva despapelización.
En un plazo máximo de 5 (cinco) años contados a partir de la entrada en vigencia de la presente ley, se aplicará la tecnología de firma digital a la totalidad de las leyes, decretos, decisiones administrativas, resoluciones y sentencias emanados de las jurisdicciones y entidades comprendidas en el artículo 8º de la Ley 24.156.

ARTICULO 49. — Reglamentación. El Poder Ejecutivo deberá reglamentar esta ley en un plazo no mayor a los 180 (ciento ochenta) días de su publicación en el Boletín Oficial de la Nación.

ARTICULO 50. — Invitación. Invítase a las jurisdicciones provinciales a dictar los instrumentos legales pertinentes para adherir a la presente ley.

ARTICULO 51. — Equiparación a los efectos del derecho penal. Incorpórase el siguiente texto como artículo 78 (bis) del Código Penal:
Los términos firma y suscripción comprenden la firma digital, la creación de una firma digital o firmar digitalmente. Los términos documento, instrumento privado y certificado comprenden el documento digital firmado digitalmente.

ARTICULO 52. — Autorización al Poder Ejecutivo. Autorízase al Poder Ejecutivo para que por la vía del artículo 99, inciso 2, de la Constitución Nacional actualice los contenidos del Anexo de la presente ley a fin de evitar su obsolescencia.

ARTICULO 53. — Comuníquese al Poder Ejecutivo.
DADA EN LA SALA DE SESIONES DEL CONGRESO ARGENTINO, EN BUENOS AIRES, A LOS CATORCE DIAS DEL MES DE NOVIEMBRE DEL AÑO DOS MIL UNO.
— REGISTRADA BAJO EL Nº 25.506 —
RAFAEL PASCUAL. — EDUARDO MENEM. — Guillermo Aramburu. — Juan C. Oyarzún.

ANEXO

Información: conocimiento adquirido acerca de algo o alguien.

Procedimiento de verificación: proceso utilizado para determinar la validez de una firma digital. Dicho proceso debe considerar al menos:

a) que dicha firma digital ha sido creada durante el período de validez del certificado digital del firmante;

b) que dicha firma digital ha sido creada utilizando los datos de creación de firma digital correspondientes a los datos de verificación de firma digital indicados en el certificado del firmante;

c) la verificación de la autenticidad y la validez de los certificados involucrados.

Datos de creación de firma digital: datos únicos, tales como códigos o claves criptográficas privadas, que el firmante utiliza para crear su firma digital.

Datos de verificación de firma digital: datos únicos, tales como códigos o claves criptográficas públicas, que se utilizan para verificar la firma digital, la integridad del documento digital y la identidad del firmante.

Dispositivo de creación de firma digital: dispositivo de hardware o software técnicamente confiable que permite firmar digitalmente.

Dispositivo de verificación de firma digital: dispositivo de hardware o software técnicamente confiable que permite verificar la integridad del documento digital y la identidad del firmante.

Políticas de certificación: reglas en las que se establecen los criterios de emisión y utilización de los certificados digitales.

Técnicamente confiable: cualidad del conjunto de equipos de computación, software, protocolos de comunicación y de seguridad y procedimientos administrativos relacionados que cumplan los siguientes requisitos:

1. Resguardar contra la posibilidad de intrusión y/o uso no autorizado;

2. Asegurar la disponibilidad, confiabilidad, confidencialidad y correcto funcionamiento;

3. Ser apto para el desempeño de sus funciones específicas;

4. Cumplir las normas de seguridad apropiadas, acordes a estándares internacionales en la materia;

5. Cumplir con los estándares técnicos y de auditoría que establezca la Autoridad de Aplicación.

Clave criptográfica privada: En un criptosistema asimétrico es aquella que se utiliza para firmar digitalmente.

Clave criptográfica pública: En un criptosistema asimétrico es aquella que se utiliza para verificar una firma digital.

Integridad: Condición que permite verificar que una información no ha sido alterada por medios desconocidos o no autorizados.

Criptosistema asimétrico: Algoritmo que utiliza un par de claves, una clave privada para firmar digitalmente y su correspondiente clave pública para verificar dicha firma digital.

Anexo B Decreto Nº 2.628/02. Reglamentación de la Ley de Firma Digital.
(Publicado en el Boletín Oficial el 20/12/2002).

Bs. As., 19/12/2002

VISTO la Ley N° 25.506, el Decreto N° 427 del 16 de abril de 1998, el Decreto N° 78 del 10 de enero de 2002, el Decreto N° 333 del 19 de febrero de 1985 y sus modificatorios y la Resolución N° 194 del 27 de noviembre de 1998 de la ex SECRETARIA DE LA FUNCION PUBLICA, y

CONSIDERANDO:
Que la sanción de la Ley N° 25.506 de firma digital representa un avance significativo para la inserción, de nuestro país en la sociedad de la información y en la economía digital, brindando una oportunidad para el desarrollo del sector productivo vinculado a las nuevas tecnologías.
Que otros países ya han normado sobre la materia, con positiva repercusión tanto en el ámbito privado como público.
Que con la sanción de la citada Ley N° 25.506, de firma digital se reconoce el empleo de la firma, digital y de la firma electrónica y su eficacia jurídica en las condiciones que la misma ley establece.
Que dicho reconocimiento constituye un elemento esencial para otorgar seguridad a las transacciones electrónicas, promoviendo el comercio electrónico seguro, de modo de permitir la identificación en forma fehaciente de las personas que realicen transacciones electrónicas.
Que asimismo, la sanción de la Ley N° 25.506 otorga un decisivo impulso para la progresiva despapelización del Estado, contribuyendo a mejorar su gestión, facilitar el acceso de la comunidad a la información pública y posibilitar la realización de trámites por Internet en forma segura.
Que la reglamentación de la Ley N° 25.506 permitirá establecer una Infraestructura de Firma Digital que ofrezca autenticación, y garantía de integridad para los documentos digitales o electrónicos y constituir la base tecnológica que permita otorgarles validez jurídica.
Que debe regularse el funcionamiento de los certificadores licenciados de manera de garantizar la adecuada prestación de los servicios de certificación.
Que resulta necesario crear un Ente Administrador de Firma Digital, encargado de otorgar las licencias a los certificadores, supervisar su actividad y dictar las normas tendientes a asegurar el régimen de libre competencia en el mercado de los prestadores y protección de los usuarios de Firma Digital.
Que la citada Ley contempla la creación de una Comisión Asesora para la Infraestructura de Firma Digital, conformada por un equipo multidisciplinario de especialistas en la materia, con el fin de asesorar y recomendar a la Autoridad de Aplicación estándares tecnológicos, y otros aspectos que hacen al funcionamiento de la mencionada Infraestructura, por lo cual deben establecerse las bases para su formación y adecuado funcionamiento.
Que el Decreto N° 427 del 16 de abril de 1998 ha sido una de las normas pioneras a nivel nacional e internacional en reconocer la validez jurídica de la firma digital, para lo cual creó una Infraestructura de Firma Digital para el Sector Público Nacional bajo la dependencia de la JEFATURA DE GABINETE DE MINISTROS.
Que esta experiencia ha sido un antecedente fundamental para la incorporación de la tecnología en la gestión pública, constituyendo una fuente de consulta para distintas jurisdicciones nacionales y provinciales.
Que dado que la Ley N° 25.506 establece una Infraestructura de Firma Digital de alcance federal, a fin de optimizar el aprovechamiento de los recursos y las experiencias desarrolladas, resulta conveniente subsumir la mencionada Infraestructura del Sector Público Nacional dentro de la creada a nivel federal por la Ley citada.

Que a tal fin, corresponde derogar el Decreto N° 427/98, por el cual se reconoce el empleo de la firma digital en el ámbito de la Administración Pública Nacional, ya que la Ley N° 25.506 cubre los objetivos y el alcance del mencionado Decreto.
Que ha tomado intervención el servicio jurídico competente.
Que la presente medida se dicta en virtud lo dispuesto por el artículo 49 de la Ley N° 25.506, y por el artículo 99, inciso 2, de la Constitución de la Nación Argentina.
Por ello,

EL PRESIDENTE DE LA NACIÓN ARGENTINA DECRETA:

CAPITULO I
CONSIDERACIONES GENERALES

Artículo 1° *— Objeto. La presente reglamentación regula el empleo de la firma electrónica y de la firma digital y su eficacia jurídica.*
En los casos contemplados por los artículos 3°, 4° y 5° de la Ley N° 25.506 podrán utilizarse los siguientes sistemas de comprobación de autoría e integridad:
a) Firma electrónica,
b) Firma digital basada en certificados digitales emitidos por certificadores no licenciados en el marco de la presente reglamentación,
c) Firma digital basada en certificados digitales emitidos por certificadores licenciados en el marco de la presente reglamentación,
d) Firma digital basada en certificados digitales emitidos por certificadores extranjeros que hayan sido reconocidos en los siguientes casos:
1. En virtud de la existencia de acuerdos de reciprocidad entre la República Argentina y el país de origen del certificador extranjero.
2. Por un certificador licenciado en el país en el marco de la presente reglamentación y validado por la Autoridad de Aplicación.

Art. 2° *— Validez de los certificados, digitales emitidos por certificadores no licenciados. Los certificados digitales emitidos por certificadores no licenciados serán válidos para producir los efectos jurídicos que la ley otorga a la firma electrónica.*

Art. 3° *— Certificados digitales emitidos por certificadores licenciados. Los certificados digitales contemplados, en el artículo 13 de la Ley N° 25.506 son aquellos cuya utilización permite disponer de una firma digital amparada por las presunciones de autoría e integridad establecidas en los artículos 7° y 8° de la ley citada.*

CAPITULO II
DE LA AUTORIDAD DE APLICACIÓN

Art. 4° *— Normas técnicas. Facúltase a la JEFATURA DE GABINETE DE MINISTROS, a determinar las normas y los procedimientos técnicos para la generación, comunicación, archivo y conservación del documento digital o electrónico, según lo previsto en los artículos 11 y 12 de la Ley N° 25.506.*

Art. 5° *— Conservación. El cumplimiento de la exigencia legal de conservar documentos, registros o datos, conforme a la legislación vigente a la materia, podrá quedar satisfecha con la conservación de los correspondientes, documentos digitales firmados digitalmente. Los documentos, registros o datos electrónicos, deberán ser almacenados por los intervinientes o por terceros confiables aceptados por los intervinientes, durante los plazos establecidos en las normas específicas.*
Se podrán obtener copias autenticadas a partir de los originales en formato digital firmado digitalmente. La certificación de autenticidad se hará de conformidad a los procedimientos legales, vigentes para el acto de que se trate, identificando el soporte que procede la copia.

Art. 6° *— Regulación. Facúltase a la JEFATURA DE GABINETE DE MINISTROS a establecer:*
a) Los estándares tecnológicos y de seguridad aplicables en consonancia con estándares internacionales.
b) Los procedimientos de firma y verificación en consonancia con los estándares tecnológicos definidos conforme el inciso precedente.
c) Las condiciones mínimas de emisión de certificados digitales.
d) Los casos en los cuales deben revocarse los certificados digitales.
e) Los datos considerados públicos contenidos en los certificados digitales.
f) Los mecanismos que garantizarán la validez y autoría de las listas de certificados revocados.
g) La información que los certificadores licenciados deberán publicar por Internet.
h) La información que los certificadores licenciados deberán publicar en el Boletín Oficial.
i) Los procedimientos mínimos de revocación de certificados digitales cualquiera que sea la fuente de emisión, y los procedimientos mínimos de conservación de la documentación de respaldo de la operatoria de los certificadores licenciados, en el caso que éstos cesen su actividad.
j) El sistema de auditoría, incluyendo las modalidades de difusión de los informes de auditoría y los requisitos de habilitación para efectuar auditorías.
k) Las condiciones y procedimientos para el otorgamiento y revocación de las licencias.
l) Las normas y procedimientos para la homologación de los dispositivos de creación y verificación de firmas digitales.
m) El reglamento de funcionamiento de la Comisión Asesora para la Infraestructura de Firma Digital.
n) El procedimiento de instrucción sumarial y la gradación de sanciones previstas en la Ley N° 25.506, en virtud de reincidencia y/u oportunidad.
o) Los procedimientos aplicables para el reconocimiento de certificados extranjeros.
p) Las condiciones de aplicación de la presente ley en el Sector Público Nacional, incluyendo la autorización para prestar servicios de certificación
digital para las entidades y jurisdicciones de la Administración Pública Nacional.
q) Los contenidos mínimos de las políticas de certificación de acuerdo con los estándares nacionales e internacionales y las condiciones mínimas que deberán cumplirse en el caso de cese de actividades de un certificador licenciado.
r) Los niveles de licenciamiento.
s) Reglamentar el uso y los alcances de los certificados de firma digital emitidos por los Registros Públicos de Contratos.
t) Exigir las garantías y seguros necesarios para prestar el servicio previsto.
u) Las condiciones de prestación de otros servicios en relación con la firma digital y otros temas cubiertos en la ley.

CAPITULO III
DE LA COMISION ASESORA PARA LA INFRAESTRUCTURA DE FIRMA DIGITAL

Art. 7° *— Comisión Asesora para la Infraestructura de Firma Digital. En el ámbito de la JEFATURA DE GABINETE DE MINISTROS funcionará la Comisión Asesora para la Infraestructura de Firma Digital, que se constituirá de acuerdo a lo dispuesto por el artículo 35 de la Ley N° 25.506.*

Art. 8° *— Integración. La Comisión Asesora para la Infraestructura de Firma Digital estará integrada multidisciplinariamente por profesionales de carreras afines a la actividad, de reconocida trayectoria y experiencia, provenientes de organismos del Estado Nacional, Universidades, Cámaras, Colegios u otros entes representativos profesionales. Para integrar la Comisión Asesora para la Infraestructura de Firma Digital se deberán reunir los siguientes requisitos:*

a) Poseer título universitario, expedido por Universidad Nacional o privada reconocida por el Estado, correspondiente a carrera profesional de duración no inferior a CUATRO (4) años, con incumbencias relacionadas con la materia.
b) Antecedentes académicos y/o profesionales o laborales en la materia.

***Art. 9°** — Ejercicio de funciones. El ejercicio de las funciones como miembro de la Comisión Asesora para la Infraestructura de Firma Digital será ad honorem.*

***Art. 10.** — Consulta Pública. La Comisión Asesora para la Infraestructura de Firma Digital establecerá los mecanismos que permitan mantener un intercambio de información fluido con organismos públicos, Cámaras, usuarios y asociaciones de consumidores sobre los temas que se están tratando a los efectos de recibir aportes y opiniones. Para cumplir con este cometido podrá implementar consultas públicas presenciales, por escrito o mediante foros virtuales, abiertos e indiscriminados, o cualquier otro medio que la Comisión considere conveniente o necesario.*

CAPITULO IV
DEL ENTE ADMINISTRADOR DE FIRMA DIGITAL

***Art. 11.** — Ente Administrador de Firma Digital. Créase el Ente Administrador de Firma Digital dependiente de la JEFATURA DE GABINETE DE MINISTROS, como órgano técnico, administrativo encargado de otorgar las licencias a los certificadores y de supervisar su actividad, según las exigencias instituidas por el presente decreto y las normas reglamentarias, modificatorias o de aplicación que se dicten en el futuro y de dictar las normas tendientes a asegurar el régimen de libre competencia, equilibrio de participación en el mercado de los prestadores y protección de los usuarios.*

***Art. 12.** — Autoridades del Ente Administrador de Firma Digital. El Ente Administrador de Firma Digital será conducido por un Directorio integrado por TRES (3) miembros, designados por el JEFE DE GABINETE DE MINISTROS, previo concurso. Hasta tanto, sea realizado el concurso el JEFE DE GABINETE DE MINISTROS designará a los integrantes del Directorio, uno de los cuales ocupará el cargo de Presidente del Ente. El gerenciamiento del Ente estará a cargo del Coordinador Ejecutivo designado por el JEFE DE GABINETE DE MINISTROS.*

***Art. 13.** — Funciones del Ente Administrador.*
Son funciones del Ente Administrador:
a) Otorgar las licencias habilitantes para acreditar a los certificadores en las condiciones que fijen el presente decreto y las normas reglamentarias, modificatorias o de aplicación que se dicten en el futuro.
b) Fiscalizar el cumplimiento de las normas legales y reglamentarias en lo referente a la actividad de los certificadores licenciados.
c) Denegar las solicitudes de licencia a los prestadores de servicios de certificación que no cumplan con los requisitos establecidos, para su licenciamiento.
d) Revocar las licencias otorgadas a los Certificadores licenciados que dejen de cumplir con los requisitos establecidos para su licenciamiento.
e) Aprobar las políticas de certificación, el manual de procedimiento, el plan de seguridad, de cese de actividades y el plan de contingencia, presentado por los certificadores solicitantes de la licencia o licenciados.
f) Solicitar los informes de auditoría en los casos que correspondiere.
g) Realizar inspecciones a los certificadores licenciados por sí o por terceros.
h) Homologar los dispositivos de creación y verificación de firmas digitales, con ajuste a las normas y procedimientos establecidos por la presente reglamentación.
i) Disponer la instrucción sumarial, la aplicación de sanciones e inhabilitar en forma temporal o permanente a todo certificador o licenciado que no respetare o incumpliere los requerimientos y disposiciones de la Ley N° 25.506, el presente decreto y las normas complementarias.

j) Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, los domicilios, números telefónicos, direcciones de Internet y certificados digitales de los certificadores licenciados.
k) Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, los domicilios, los números telefónicos, direcciones de Internet y certificados digitales de los certificadores cuyas licencias han sido revocadas.
I) Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, el domicilio, números telefónicos, direcciones de Internet y certificados digitales del Ente Administrador.
m) Administrar los recursos generados de acuerdo con lo dispuesto por el artículo 16 de la presente reglamentación, provenientes de las distintas fuentes de financiamiento.
n) Fijar el concepto y los importes de todo tipo de aranceles y multas previstos en la Ley N° 25.506 y en el artículo 16 de la presente reglamentación.
o) Solicitar la ampliación o aclaración sobre la documentación presentada por el certificador.
p) Dictar las normas tendientes a asegurar el régimen de libre competencia, equilibrio de participación en el mercado de los prestadores y protección de los usuarios.

Art. 14. *— Obligaciones del Ente Administrador.*
El Ente Administrador tiene idénticas obligaciones que los titulares, de certificados y que los Certificadores Licenciados, en su caso, y además debe:
a) Permitir el acceso público permanente a la nómina actualizada de certificadores licenciados con los datos correspondientes.
b) Supervisar la ejecución del plan de cese de actividades de los Certificadores licenciados que discontinúan sus funciones;
c) Registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas.
d) Supervisar la ejecución de planes de contingencia de los certificadores licenciados.
e) Efectuar las tareas de control del cumplimiento de las recomendaciones formuladas por el Ente Administrador para determinar si se han tomado las acciones correctivas correspondientes.
f) Recibir, evaluar y resolver los reclamos de los usuarios de certificados digitales relativos a la prestación del servicio por parte de certificadores licenciados.

Art. 15. *— Organización del Ente Administrador. Dentro del plazo de SESENTA (60) días corridos de la fecha de constitución del Directorio, el ENTE ADMINISTRADOR DE FIRMA DIGITAL elevará para su consideración al JEFE DE GABINETE DE MINISTROS la propuesta de su estructura organizativa y de su reglamento de funcionamiento.*

Art. 16. *— Recursos del Ente Administrador. El Ente Administrador podrá arancelar los servicios que preste para cubrir total o parcialmente sus costos. Los recursos propios del Ente Administrador se integrarán con:*
a) Los importes provenientes de los aranceles que se abonen por la provisión de los siguientes servicios:
1.- Servicios de certificación digital,
2.- Servicios de certificación digital de fecha y hora,
3.- Servicios de almacenamiento seguro de documentos electrónicos,
4.- Servicios prestados por autoridades de registro,
5. - Servicios prestados por terceras partees confiables,
6. - Servicios de certificación de documenttos electrónicos firmados digitalmente
7.- Otros servicios o actividades relacionados a la firma digital.
b) Los importes provenientes de los aranceles de homologación de dispositivos de creación y verificación de firmas digitales.
c) Los importes provenientes de los aranceles de certificación de sistemas que utilizan firma digital.

d) Los importes provenientes de los aranceles de administración del sistema de auditoría y las auditorías que el organismo realice por sí o por terceros.
e) Los subsidios, herencias, legados, donaciones o transferencias bajo cualquier título que reciba.
f) El producido de multas.
g) Los importes que se le asignen en el cálculo de recursos de la respectiva ley de presupuesto para la administración nacional.
h) Los demás fondos, bienes, o recursos que puedan serle asignados en virtud de las leyes y reglamentaciones aplicables.

***Art. 17.** — Financiamiento del Ente Administrador. Instrúyese a la JEFATURA DE GABINETE DE MINISTROS para que proceda a incluir en su presupuesto los fondos necesarios para que el Ente Administrador pueda cumplir adecuadamente sus funciones.*
Transitoriamente, desde la entrada en vigencia de la presente reglamentación y hasta que se incluyan las partidas necesarias en el Presupuesto Nacional los costos de financiamiento del Ente Administrador serán afrontados con el crédito presupuestario correspondiente a la JEFATURA DE GABINETE DE MINISTROS.

CAPITULO V
DEL SISTEMA DE AUDITORIA

***Art. 18.** — Precalificación de entidades de auditoria. La JEFATURA DE GABINETE DE MINISTROS convocará a concurso público para la precalificación de entidades de auditoria entre las universidades y organismos científicos y/o tecnológicos nacionales o provinciales, los Colegios y Consejos profesionales, que acrediten experiencia profesional acorde en la materia, interesadas en prestar el servicio de auditoria de entidades prestadoras de servicios de certificación digital. A tal fin, elaborará un Pliego Estándar de Precalificación de Entidades de Auditoria, y determinará la periodicidad de la convocatoria.*

***Art. 19.** — Informe de auditoria. El informe de auditoria evaluará los sistemas utilizados por el certificador de acuerdo con los requerimientos de la Ley N° 25.506, el presente decreto y las normas complementarias.*

***Art. 20.** — Conflicto de intereses. Para garantizar la objetividad e imparcialidad de la actividad de auditoria no podrán desempeñarse en la prestación de servicios de auditoria aquellas entidades o personas vinculadas con prestadores de servicios de certificación, lo que será establecido en el Pliego Estándar de Precalificación de Entidades de Auditoria previsto en el artículo 18 del presente decreto.*

***Art. 21.** — Deber de confidencialidad. Las entidades auditantes y las personas que efectúen las auditorias deben mantener la confidencialidad sobre la información considerada amparada bajo normas de confidencialidad por el Certificado Licenciado.*

CAPITULO VI
DE LOS ESTÁNDARES TECNOLÓGICOS

***Art. 22.** — Aplicación provisoria de los estándares vigentes. Hasta tanto la JEFATURA DE GABINETE DE MINISTROS apruebe los Estándares Tecnológicos de Infraestructura de Firma Digital en consonancia con estándares tecnológicos internacionales, mantendrán su vigencia los establecidos en la Resolución N° 194/98 de la ex Secretaría de la Función Publica.*

CAPITULO VII
DE LA REVOCACIÓN DE CERTIFICADOS DIGITALES

***Art. 23.** — Revocación de certificados. Se deberán revocar los certificados digitales emitidos en los siguientes casos:*
a) A solicitud del titular del certificado digital

b) Si se determina que un certificado digital fue emitido en base a una información falsa que en el momento de la emisión hubiera sido objeto de verificación.
c) Si se determina que los procedimientos de emisión y/o verificación han dejado de ser seguros.
d) Por condiciones especiales definidas en las Políticas de Certificación.
e) Por Resolución Judicial o de la Autoridad de Aplicación debidamente fundada.
f) Por fallecimiento del titular.
g) Por declaración judicial de ausencia con presunción de fallecimiento del titular.
h) Por declaración judicial de incapacidad del titular.
i) Si se determina que la información contenida en el certificado ha dejado de ser válida.
j) Por el cese de la relación de representación respecto de una persona.

CAPITULO VIII
DE LOS CERTIFICADORES LICENCIADOS

Art. 24. *— Obtención de la licencia. Para obtener una licencia, los proveedores de servicios de certificación deberán particularizar las actividades para las cuales requieren la licencia y acreditar por los medios que este determine ante el Ente Administrador de Firma Digital:*
a) Documentación que demuestre:
1.- En el caso de personas jurídicas, su personería.
2.- En el caso de registro público de contratos, tal condición
3.- En el caso de organización pública, la autorización de su máxima autoridad para iniciar el proceso de licenciamiento y la correspondiente aprobación de la JEFATURA DE GABINETE DE MINISTROS, de acuerdo con lo dispuesto en el artículo 41 de la presente reglamentación.
b) El cumplimiento de las condiciones establecidas en la ley; este decreto y las normas complementarias.
c) Las políticas de certificación para las cuales solicita licencia que respaldan la emisión de sus certificados, Manual de Procedimientos, Plan de Seguridad, Plan de Cese de Actividades y Plan de Contingencia satisfactorias de acuerdo con las normas reglamentarias.
d) Toda aquella información o requerimiento, que demande la Autoridad de Aplicación.

Art. 25. *— Efectos del licenciamiento. El otorgamiento de la licencia no implica que el Ente Administrador de la Infraestructura de Firma Digital, la JEFATURA DE GABINETE DE MINISTROS, las entidades auditantes o cualquier organismo del Estado garantice la provisión de los servicios de certificación o los productos provistos por el Certificador Licenciado.*

Art. 26. *— Duración de la licencia. Las licencias tendrán un plazo de duración de CINCO (5) años y podrán ser renovadas.*
Los certificadores licenciados deberán efectuar anualmente una declaración jurada en la cual conste el cumplimiento de las normas establecidas en la Ley N° 25.506, en el presente decreto y en las normas complementarias.
Los certificadores licenciados serán sometidos a auditorias anuales.

Art. 27. *— Causales de caducidad de la licencia. El Ente Administrador podrá disponer de oficio, y en forma preventiva la caducidad de la licencia en los siguientes casos:*
a) Falta de presentación de la declaración jurada anual.
b) Falsedad de los datos contenidos en la declaración jurada anual.
c) Dictamen desfavorable de auditoria basado en causales graves.
d) Informe de la inspección dispuesta por el Ente Administrador desfavorable basado, en causales graves.
e) Cuando el certificador licenciado no permita la realización de auditorias o inspecciones dispuestas por el Ente Administrador.

Art. 28. *— Reconocimiento de certificados extranjeros. De acuerdo a lo establecido en el artículo 6° de la presente reglamentación, facúltase a la JEFATURA DE GABINETE DE MINISTROS a*

elaborar y firmar acuerdos de reciprocidad con gobiernos de países extranjeros, a fin de otorgar validez, en sus respectivos territorios, a los certificados digitales emitidos por certificadores de ambos países, en tanto se verifique el cumplimiento de las condiciones establecidas por la Ley N° 25.506 y su reglamentación para los certificados emitidos por certificadores nacionales.
Los certificadores licenciados no podrán reconocer certificaciones emitidas por certificadores extranjeros correspondientes a personas con domicilio o residencia en la República Argentina. El Ente Administrador de Firma Digital establecerá las relaciones que los certificadores licenciados deberán guardar entre los certificados emitidos en la República Argentina y los certificados reconocidos de certificadores extranjeros.

Art. 29. *— Políticas de Certificación. La JEFATURA DE GABINETE DE MINISTROS definirá el contenido, mínimo de las políticas de certificación de acuerdo con los estándares nacionales e internacionales vigentes, las que deberán contener al menos la siguiente información:*
a) Identificación del certificador licenciado.
b) Política de administración de los certificados y detalles de los servicios arancelados.
c) Obligaciones de la entidad y de los suscriptores de los certificados.
d) Tratamiento de la información suministrada por los suscriptores, y resguardo de la confidencialidad en su caso.
e) Garantías que ofrece para el cumplimiento de las obligaciones que se deriven de sus actividades.

Art. 30. *— Seguros. El certificador licenciado debe contar con seguros vigentes acordes con las responsabilidades asumidas, que cumplan con los siguientes requisitos.*
a) Ser expedidos por una entidad aseguradora autorizada para operar en la República Argentina.
b) Establecer la obligación de la entidad aseguradora de informar previamente al Ente Administrador de la Infraestructura de Firma Digital la terminación del contrato o las modificaciones que reduzcan el alcance o monto de la cobertura.
Los certificadores licenciados pertenecientes a entidades y jurisdicciones del sector público quedarán exentos de la obligación de constituir el seguro previsto en el presente artículo.

Art. 31. *— Responsabilidad de los certificadores licenciados. En ningún caso, la responsabilidad que pueda emanar de una certificación efectuada por un certificador licenciado, público o privado, comprometerá la responsabilidad pecuniaria del Estado en su calidad de Ente Administrador de la Infraestructura de Firma Digital.*

Art. 32. *— Recursos de los certificadores licenciados. Para el desarrollo adecuado de las actividades de certificación, el certificador deberá acreditar que cuenta con un equipo de profesionales, infraestructura física tecnológica y recursos financieros, como así también procedimientos y sistemas de seguridad que permitan:*
a) Generar en un ambiente seguro las firmas digitales propias y todos los servicios para los cuales solicite licencia.
b) Cumplir con lo previsto en sus políticas y procedimientos de certificación.
c) Garantizar la confiabilidad de los sistemas de acuerdo con los estándares aprobados por la Autoridad de Aplicación.
d) Expedir certificados que cumplan con:
1.- Lo previsto en los artículos 13 y 14 de la Ley N° 25.506.
2.- Los estándares tecnológicos aprobados por la JEFATURA DE GABINETE DE MINISTROS.
e) Garantizar la existencia de sistemas de seguridad física y lógica que cumplimenten las normativas vigentes.
f) Proteger el manejo de la clave privada de la entidad mediante un procedimiento de seguridad que impida el acceso a la misma a personal no autorizado.
g) Proteger el acceso y el uso de la clave privada mediante procedimientos que exijan la participación de más de una persona.

h) Registrar las transacciones realizadas, a fin de identificar el autor y el momento de cada una de las operaciones.
i) Utilizar con exclusividad los sistemas que cumplan las funciones de certificación con ese propósito, sin que se les asigne ninguna otra función.
j) Proteger a todos los sistemas utilizados directa o indirectamente en la función de certificación con procedimientos de autenticación y seguridad de alto nivel de protección, que deban ser actualizados de acuerdo a los avances tecnológicos para garantizar la correcta prestación de los servicios de certificación.
k) Garantizar la continuidad de las operaciones mediante un Plan de Contingencia actualizado y aprobado.
l) Disponer de los recursos financieros adecuados al tipo de actividad de certificación que desarrolla, acorde con los niveles de responsabilidad derivados de la misma.

Art. 33. *— Servicios de Terceros. En los casos en que el certificador licenciado requiera o utilice los servicios de infraestructura tecnológicos prestados por un tercero, deberá prever dentro de su Plan de Contingencia los procedimientos a seguir en caso de interrupción de estos servicios, de modo tal que permita continuar prestando sus servicios de certificación sin ningún perjuicio para los suscriptores.*
Los contratos entre el certificador licenciado y los proveedores de servicios o infraestructura deberán garantizar la ejecución de los procedimientos contemplados en el Plan de Cese de actividades aprobado por el Ente Licenciante. El certificador licenciado o en proceso de licenciamiento deberá facilitar al Ente Licenciante toda aquella información obrante en los contratos vinculada a la prestación de servicios de certificación y a la implementación del Plan de Cese de actividades y el Plan de Contingencia.
La contratación de servicios o infraestructura no exime al prestador de la presentación de los informes de auditoria, los cuales deberán incluir los sistemas y seguridades del prestador contratado.

Art. 34. *— Obligaciones del certificador licenciado. Además de lo previsto en el artículo 21 de la Ley N° 25.506, los certificadores licenciados deberán:*
a) Comprobar por sí o por medio de una Autoridad de Registro que actúe en nombre y por cuenta suya, la identidad y cualquier otro dato de los solicitantes considerado relevante para los procedimientos de verificación de identidad previos a la emisión del certificado digital, según la Política de Certificación bajo la cual se solicita.
b) Mantener a disposición permanente del público las Políticas de Certificación y el Manual de Procedimientos correspondiente.
c) Cumplir cabalmente con las políticas de certificación acordadas con el titular y con su Manual de Procedimientos.
d) Garantizar la prestación establecida según los niveles definidos en el acuerdo de servicios pactados con sus usuarios, relativo a los servicios para los cuales solicitó el licenciamiento.
e) Informar al solicitante de un certificado digital, en un lenguaje claro y accesible, en idioma nacional, respecto de las características del certificado solicitado, las limitaciones a la responsabilidad, si las hubiere, los precios de los servicios de certificación, uso, administración y otros asociados, incluyendo cargos adicionales y formas de pago, los niveles de servicio al proveer, las obligaciones que el suscriptor asume como usuario del servicio de certificación, su domicilio en la República Argentina y los medios a los que el suscriptor puede acudir para solicitar aclaraciones, dar cuenta del mal funcionamiento del sistema o presentar sus reclamos.
f) Disponer de un servicio de atención a titulares y terceros, que permita evacuar las consultas y la pronta solicitud de revocación de certificados.
g) Garantizar el acceso permanente, eficiente y gratuito de los titulares y terceros al repositorio de certificados revocados.

h) Mantener actualizados los repositorios de certificados revocados por el período establecido por el Ente Administrador.
i) Abstenerse de generar, exigir, tomar conocimiento o acceder bajo ninguna circunstancia a la clave privada del suscriptor.
j) Informar al Ente Administrador de modo inmediato la ocurrencia de cualquier evento que comprometa la correcta prestación del servicio.
k) Respetar el derecho del titular del certificado digital a no recibir publicidad de ningún tipo por su intermedio, salvo consentimiento expreso de éste.
l) Publicar en el Boletín Oficial durante UN (1) día, el certificado de clave pública correspondiente a la política para la cual obtuvo licenciamiento;
m) Cumplir las normas y recaudos establecidos para la protección de datos personales.
n) En los casos de revocación de certificados contemplados en el apartado 3 del inciso e) del artículo 19 de la Ley N° 25.506, deberá sustituir en forma gratuita aquel certificado digital que ha dejado de ser seguro por otro que sí cumpla con estos requisitos.
El Ente Administrador deberá establecer el proceso de reemplazo de certificados en estos casos. En los casos en los que un certificado digital haya dejado de ser seguro por razones atribuibles a su titular, el certificador licenciado no estará obligado a sustituir el certificado digital.
o) Enviar periódicamente al Ente Administrador, informes de estado de operaciones con carácter de declaración jurada.
p) Contar con personal idóneo y confiable, con antecedentes profesionales acordes a la función desempeñada.
q) Responder a los pedidos de informes por parte de un tercero respecto de la validez y alcance de un certificado digital emitido por él.

CAPITULO IX
DE LAS AUTORIDADES DE REGISTRO

Art. 35. — *Funciones de las Autoridades de Registro. Los Certificadores Licenciados podrán delegar en Autoridades de Registro las funciones de validación de identidad y otros datos de los suscriptores de certificados y de registro de las presentaciones y trámites que les sean formuladas, bajo la responsabilidad del Certificador Licenciado, cumpliendo las normas y procedimientos establecidos por la presente reglamentación.*
Una autoridad de Registro es una entidad responsable de las siguientes funciones:
a) La recepción de las solicitudes de emisión de certificados.
b) La validación de la identidad y autenticación de los datos de los titulares de certificados.
c) La validación de otros datos de los titulares de certificados que se presenten ante ella cuya verificación delegue el Certificador Licenciado.
d) La remisión de las solicitudes aprobadas al Certificador Licenciado con la que se encuentre operativamente vinculada.
e) La recepción y validación de las solicitudes de revocación de certificados; y su direccionamiento al Certificador Licenciado con el que se vinculen.
f) La identificación y autenticación de los solicitantes de revocación de certificados.
g) El archivo y la conservación de toda la documentación respaldatoria del proceso de validación de identidad, de acuerdo con los procedimientos establecidos por el certificador licenciado.
h) El cumplimiento de las normas y recaudos establecidos para la protección de datos personales.
i) El cumplimiento de las disposiciones que establezca la Política de Certificación y el Manual de Procedimientos del Certificador Licenciado con el que se encuentre vinculada, en la parte que resulte aplicable.

Art. 36. *— Responsabilidad del certificador licenciado respecto de la Autoridad de Registro. Una Autoridad de Registro puede constituirse como una única unidad o con varias unidades dependientes jerárquicamente entre sí, pudiendo, delegar su operatoria en otras autoridades de registro, siempre que medie la aprobación del Certificador Licenciado. El Certificador, Licenciado*

es responsable con los alcances establecidos en la Ley N° 25.506, aún en el caso de que delegue parte de su operatoria en Autoridades de Registro, sin perjuicio del derecho del certificador de reclamar a la Autoridad de Registro las indemnizaciones por los daños y perjuicios que aquél sufriera como consecuencia de los actos y/u omisiones de ésta.

CAPITULO X
DISPOSICIONES PARA LA ADMINISTRACIÓN PÚBLICA NACIONAL

Art. 37. *— Despapelización del Estado. Sin perjuicio de la aplicación directa de la ley en lo relativo a la validez jurídica de la firma electrónica, de la firma digital y de los documentos digitales, la implementación de las disposiciones de la ley y del presente decreto para la digitalización de procedimientos y trámites internos de la Administración Pública Nacional, de las Administraciones Públicas Provinciales, y de los Poderes Legislativos y Judiciales del orden nacional y provincial, así como los vinculados a la relación de las mencionadas jurisdicciones y entidades con los administrados, se hará de acuerdo a lo que fijen reglamentariamente cada uno de los Poderes y Administraciones.*

Art. 38. *— Aplicaciones en organismos de la Administración Pública Nacional. Los organismos de la Administración Pública Nacional que para la tramitación de documentos digitales o la implementación de aplicaciones requieran firma digital, solamente aceptarán certificados digitales emitidos por Certificadores, Licenciados, o certificados digitales emitidos por certificadores extranjeros reconocidos por acuerdos internacionales o por certificadores licenciados del país.*
Las entidades y jurisdicciones pertenecientes al sector público podrán ser certificadores licenciados y emitir certificados para agentes y funcionarios públicos destinados a las aplicaciones de gestión interna de los organismos públicos a que éstos pertenecieran. Cuando razones de orden público o de interés social lo ameriten y cuenten con la autorización de la JEFATURA DE GABINETE DE MINISTROS podrán emitir certificados a particulares.
En aquellas aplicaciones en las que el Estado interactúe con la comunidad, se deberá admitir la recepción de documentos digitales firmados digitalmente utilizando certificados digitales emitidos por certificadores licenciados privados o públicos, indistintamente.

Art. 39. *— Autoridades de Registro pertenecientes a la Administración Pública Nacional. En las entidades y jurisdicciones pertenecientes a la Administración Pública Nacional, las áreas de recursos humanos cumplirán las funciones de Autoridades de Registro para los agentes y funcionarios de su jurisdicción. En el caso, y si las aplicaciones de que se trate lo requieren, la máxima autoridad del organismo podrá asignar, adicionalmente, a otra unidad las funciones de Autoridad de Registro.*

Art. 40. *— Agentes y funcionarios. La Autoridad de Aplicación podrá requerir para el cumplimiento de lo establecido en la presente reglamentación la adscripción de agentes y funcionarios pertenecientes a las entidades y jurisdicciones comprendidas en el artículo 8° de la Ley N° 24.156 y sus modificatorias.*

Art. 41. *— Utilización por las entidades y jurisdicciones de la Administración Pública Nacional. La JEFATURA DE GABINETE DE MINISTROS, establecerá las normas de aplicación de la presente reglamentación en la Administración Pública Nacional, que deberán contemplar:*
a) Las acciones tendientes a promover el uso masivo de la firma digital con el fin de posibilitar el trámite de los expedientes en forma simultánea, búsquedas automáticas de información, seguimiento y control por parte de los interesados.
b) Las acciones tendientes a implementar la progresiva despapelización del Estado, a fin de contar en un plazo de CINCO (5) años con la totalidad de la documentación administrativa en formato digital.
c) La interoperabilidad entre aplicaciones.

d) La autorización para solicitar el licenciamiento como certificador ante el Ente Administrador de la Infraestructura de Firma Digital para las entidades y jurisdicciones de la Administración Pública Nacional.
e) La participación del Cuerpo de Administradores Gubernamentales a los fines de difundir el uso de la firma digital y facilitar los procesos de despapelización.

Art. 42. *— Presentación de documentos electrónicos. Los organismos de la Administración Pública Nacional deberán establecer mecanismos que garanticen la opción de remisión, recepción, mantenimiento y publicación de información electrónica, siempre que esto sea aplicable, tanto para la gestión de documentos entre organismos como para con los ciudadanos.*

Art. 43. *— Normas para la elaboración y redacción de la documentación administrativa. Lo dispuesto en la presente reglamentación constituye una alternativa a lo establecido por el Decreto N° 333/85 y sus modificatorios.*

Art. 44. *— Glosario. Apruébase el glosario que obra como Anexo I del presente Decreto.*

Art. 45. *— Derogación. Derógase el Decreto N° 427/98.*

Art. 46. *— Comuníquese, publíquese, dése a la Dirección Nacional del Registro Oficial y archívese. — DUHALDE. — Alfredo N. Atanasof. — Juan J. Álvarez.*

ANEXO I
GLOSARIO

1.- Firma Electrónica: Se entiende por firma electrónica al 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 algunos de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez (artículo 5°, Ley N° 25.506).

2.- Firma digital: Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital, posterior a su firma.
Los procedimientos de firma y verificación a ser utilizados para tales fines serán los determinados por la Autoridad de Aplicación en consonancia con estándares tecnológicos internacionales vigentes (artículo 2°, Ley N° 25.506).

3.- Documento Digital o Electrónico: Se entiende por documento digital a la representación digital de actos o hechos, con independencia del soporte: utilizado para su fijación, almacenamiento archivo. Un documento digital también satisface el requerimiento de escritura (artículo 6°, Ley N° 25.506).

4.- Certificado Digital: Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular (artículo 13, Ley N° 25.506).

5.- Certificador Licenciado: Se entiende por certificador licenciado a toda persona de existencia ideal, registro público de contratos u organismo público que expide certificados, presta otros servicios en relación con la firma digital y cuenta con una licencia para ello, otorgada por el ente licenciante.
La actividad de los certificadores licenciados no pertenecientes al sector público se prestará en régimen de competencia. El arancel de los servicios prestados por los certificadores licenciados será establecido libremente por éstos (artículo 17, Ley N° 25.506).

6.- Política de Certificación: Conjunto de criterios que indican la aplicabilidad de un certificado a un grupo de usuarios en particular o a un conjunto de aplicaciones con similares requerimientos de seguridad. En inglés Certification Policy (CP).

7.- Manual de Procedimientos: Conjunto de prácticas utilizadas por el certificador licenciado en la remisión y administración de los certificados. En inglés Certification Practice Statement (CPS).

8.- Plan de Seguridad: Conjunto de políticas, prácticas y procedimientos destinados a la protección; de los recursos del certificador licenciado.

9.- Plan de Cese de Actividades: conjunto de actividades a desarrollar por el certificador licenciado en caso de finalizar la prestación de sus servicios.

10.- Plan de Contingencias: Conjunto de procedimientos a seguir por el certificador licenciado ante situaciones de ocurrencia no previstas que comprometan la continuidad de sus operaciones.

11.- Lista de certificados revocados: Lista de certificados que han sido dejados sin efecto en forma permanente por el Certificador Licenciado, la cual ha sido firmada digitalmente y publicada por el mismo. En inglés Certificate Revocation List (CRL).

12.- Certificación digital de fecha y hora: Indicación de la fecha y hora cierta, asignada a un documento o registro electrónico por una tercera parte confiable y firmada digitalmente por ella.

13.- Terceras partes confiables: Entidades independientes que otorgan seguridad y confiabilidad al manejo de la información.

14.- Proveedor de servicios de certificación digital: Entidad que provee el servicio de emisión y administración de certificados digitales.

15.- Homologación de dispositivos de creación y verificación de firmas digitales: Proceso de comprobación efectuado para establecer la adecuación de los dispositivos a requerimientos mínimos establecidos.

16.- Certificación de sistemas que utilizan firma digital: Proceso de comprobación efectuado para establecer la adecuación de un sistema o aplicación a requerimientos mínimos establecidos.

17.- Suscriptor o Titular de certificado digital: Persona a cuyo nombre se emite un certificado y posee una clave privada que se corresponde con la clave pública contenida en el mismo.

Anexo C <u>Reglamento del Código de Comercio en materia de Prestadores de Servicios de Certificación.</u>

CAPÍTULO I

DISPOSICIONES GENERALES

ARTÍCULO 1o.- *El presente ordenamiento establece las normas reglamentarias a que se sujetarán los servicios relacionados con firmas electrónicas y la expedición de certificados para actos de comercio, a través de prestadores de servicios de certificación.*
Para efecto de este Reglamento se estará a las definiciones a que se refiere el artículo 89 del Código de Comercio así como a las siguientes:
I. *Código, al Código de Comercio, y*
II. *Reglas Generales: a las Reglas Generales que deberá publicar la Secretaría, en términos de los artículos 102 inciso A) fracción V, 104 fracciones IV y VI y 113 del Código, en el Diario Oficial de la Federación.*

ARTÍCULO 2o.- *Para los efectos de la acreditación de un Prestador de Servicios de Certificación, la Secretaría aceptará cualquier método o sistema para crear una firma electrónica, firma electrónica avanzada o certificado, y promoverá que éstos puedan concurrir o funcionar con diferentes equipos y programas de cómputo, conforme a los principios de neutralidad tecnológica y compatibilidad internacional, en tanto se satisfagan los requisitos que establece el Código, este Reglamento y las Reglas Generales.*

CAPÍTULO II
DE LA ACREDITACIÓN

ARTÍCULO 3o.- *Para efectos de lo dispuesto por el artículo 102, inciso A), fracción II, la Secretaría detallará en las Reglas Generales los requerimientos humanos, materiales, económicos y tecnológicos a que se refiere dicho artículo, con base en las obligaciones que deben cumplir los Prestadores de Servicios de Certificación en términos del artículo 104 del Código, para ello:*

I. *Los elementos humanos deberán incluir al menos un profesionista jurídico y otro informático, que acrediten el grado académico y los cursos que determinen las Reglas Generales, responsables de aprobar el plan de continuidad del negocio que presente el solicitante. Las personas a que se refiere el artículo 104 fracción I del Código, en todo caso deberán ser licenciados en derecho que comprueben conocer la operación como usuarios de los sistemas informáticos que habrá de utilizar el solicitante;*
II. *Respecto de los elementos materiales, se considerará el dinamismo del avance tecnológico y la necesidad de preservar la seguridad física y lógica en la prestación del servicio de certificación, por lo que se referirán al equipo y programas de cómputo e infraestructura mínima para su operatividad;*
III. *Los elementos económicos comprenderán al menos un capital equivalente a un tanto igual a la inversión realizada para cumplir con los elementos humanos, tecnológicos y materiales, así como un seguro de responsabilidad civil contra daños y/o pérdidas de terceros, producidas por el Prestador de Servicios de Certificación o sus empleados, por un monto equivalente a treinta veces el salario mínimo general diario vigente en el Distrito Federal correspondiente a un año, y*
IV. *Los elementos Tecnológicos garantizarán la continuidad del servicio, por lo que referirán la declaración de prácticas de certificación y los modelos operacionales que utilizará el solicitante y que deberán ser compatibles con las normas y criterios internacionales. En todo caso los certificados deberán ser generados en el territorio nacional.*

Artículo 4o.- *El trámite para la acreditación como Prestador de Servicios de Certificación se desahogará en términos de lo dispuesto por la Ley Federal de Procedimiento Administrativo, para lo cual Secretaría estará a lo siguiente:*

I. *El solicitante deberá acreditar que se encuentra en alguno de los supuestos a que se refiere el artículo 100 del Código:*
a) *Tratándose de notarios o corredores públicos, a través de copia certificada de la patente, título de habilitación o documento que en términos de la legislación de la materia les acredite estar en ejercicio de la fe pública, y*
b) *Tratándose de las personas a que se refiere la fracción II del artículo 100 del Código, se requerirá de copia certificada del acta, póliza u otro instrumento público, que acredite su constitución de acuerdo con las leyes mexicanas y que su objeto social es el establecido en el artículo 101 del Código;*
II. *Dentro de los cinco días siguientes a la recepción de la solicitud, difundirá en los medios electrónicos con que cuente para tal efecto, el nombre, actividad profesional, domicilio del solicitante y los de las personas físicas que, tratándose de personas morales, le representen y aquellas que pretendan brindar el servicio de certificación;*
III. *Remitirá para consulta los datos indicados en el inciso anterior a las secretarías de la Función Pública, de Gobernación, de Comunicaciones y Transportes, y de Relaciones Exteriores así como a la Procuraduría General de la República, para que en el ámbito de su competencia evalúen dicha información y, en su caso, manifiesten lo que a sus atribuciones corresponda;*
IV. *Dentro de los veinte días siguientes a la recepción de la solicitud, revisará y evaluará de manera preliminar la información y documentación recibida. Cuando derivado de la revisión, detecte la falta de cualquiera de los requisitos señalados en el Código, este Reglamento o las Reglas Generales, deberá prevenir al interesado por escrito por única vez, para que subsane la omisión dentro del término de 20 días contados a partir de su notificación. Transcurrido dicho plazo sin que sea desahogada la prevención, se desechará el trámite;*
V. *La Secretaria realizará dentro de los 25 días siguientes a la fecha de presentación de la solicitud, una visita de verificación en el domicilio que señale el solicitante, a efecto de comprobar que sus instalaciones cumplen con los requisitos humanos, materiales, económicos y tecnológicos que precisa este Reglamento y las Reglas Generales, así como constatar la funcionalidad, operatividad y viabilidad de la prestación del servicio por el solicitante, y el cumplimiento con las normas y criterios internacionales, cuando no sean materia de una evaluación de la conformidad en términos de la Ley Federal sobre Metrología y Normalización, y*
VI. *Una vez realizada la visita y dentro de los 45 días siguientes a la presentación de la solicitud, la Secretaría resolverá sobre la procedencia o no de la acreditación.*

Artículo 5o.- *Satisfechos los requisitos a que se refiere el Código y en términos de este Reglamento, la Secretaría otorgará la acreditación como Prestador de Servicios de Certificación, expedirá el certificado respectivo y lo registrará. Dicho certificado tendrá una vigencia de diez años.*
Para la expedición del certificado la Secretaria comprobará la identidad del Prestador de Servicios de Certificación o su representante, para que éste conforme al procedimiento que determinen las Reglas Generales, genere los Datos de Creación de Firma Electrónica.
La acreditación será publicada en el Diario Oficial de la Federación dentro de los treinta días siguientes a la resolución que determine su procedencia.
Ningún Prestador podrá tener más de una acreditación simultáneamente.

Artículo 6o.- *Para los efectos del artículo 102, inciso A), fracción V del Código, la Secretaría establecerá en las Reglas Generales las condiciones a que se sujetará la fianza que otorgarán los solicitantes previo al otorgamiento de su acreditación como Prestadores de Servicios de Certificación, conforme a lo siguiente:*

I. *Una vez resuelta la procedencia de la solicitud de acreditación, el interesado contará con 30 días para presentar ante la Secretaría una póliza de fianza a favor de la Tesorería de la Federación:*
a) tratándose de un notario o corredor públicos, por un monto equivalente a cinco mil veces el salario mínimo general diario vigente en el Distrito Federal;
b) tratándose de personas morales de carácter privado o instituciones públicas, por el monto resultante de multiplicar cinco mil veces el salario mínimo general diario vigente en el Distrito Federal por cada persona física que directamente, o como integrante de una persona moral distinta, pretenda contemplar 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, y
II. *La Fianza deberá otorgarse y mantenerse vigente y actualizada durante todo el periodo que comprenda la acreditación, inclusive en los casos en que proceda la suspensión temporal del Prestador de Servicios de Certificación.*

Artículo 7o. *Cuando la suspensión sea definitiva, se trate del cese de actividades, o se haya iniciado procedimiento administrativo o judicial en contra del Prestador de Servicios de Certificación, la fianza continuará vigente durante todo el año siguiente a la suspensión o cese, o hasta que concluya el proceso respectivo.*
La Secretaría mantendrá permanentemente actualizado el listado de Prestadores de Servicios de Certificación y de las personas físicas a que se refiere el presente artículo.

CAPÍTULO III
DE LOS CERTIFICADOS

Artículo 8o.- *Para efecto de lo dispuesto por los artículos 107, 108 y 109 del Código, cada Prestador de Servicios de Certificación deberá proporcionar a la Secretaría la dirección electrónica que incluirá en cada certificado que expida, para verificar en forma inmediata su validez, suspensión o revocación. La misma dirección será utilizada por la Secretaría para agregarla a un dominio propio de consulta en línea a través del cual la Parte que Confía podrá cerciorarse del estado que guarda cualquier certificado emitido por un Prestador de Servicios de Certificación.*

Artículo 9o.- *Para efecto de los supuestos previstos en el artículo 113 del Código, una copia de cada certificado generado por un Prestador de Servicios de Certificación deberá ser enviada en línea a la Secretaría mediante el procedimiento que esta establezca en las Reglas Generales, la cual resguardará bajo estrictos mecanismos de seguridad física y lógica.*
El equipo, programa y sistemas que el Prestador de Servicios de Certificación pretenda utilizar en la expedición de certificados no podrán ser de menor seguridad a los que determine la Secretaría en las Reglas Generales.

Artículo 10.- *Para los efectos del artículo 108 fracción III del Código, los datos de acreditación ante la Secretaría incluirán 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.*

Artículo 11. *Para los efectos del artículo 108 fracción VI la fecha y hora de la emisión, suspensión y revocación del certificado se determinará conforme lo establezcan las Reglas Generales, el cual deberá asegurar la utilización de un sello de tiempo.*

Artículo 12. *La emisión, registro y conservación de los certificados por parte de los Prestadores de Servicios de Certificación se efectuará en territorio nacional. La Secretaría, a través de las Reglas Generales se asegurará 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.

CAPÍTULO IV
DE LAS AUDITORÍAS

***Artículo 13**.- Para efecto del artículo 102, inciso A), fracción VI del Código, las auditorias que efectúe la Secretaría a un 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 practicaran de oficio o a petición del Titular del Certificado, Firmante o de la Parte que Confía.*

CAPÍTULO V
DE LAS INFRACCIONES Y SANCIONES

***Artículo 14.** La Secretaría sancionará con suspensión temporal de uno hasta dos meses en el ejercicio de sus funciones al Prestador de Servicios de Certificación que:*

***I.** Omita determinar y hacer del conocimiento de los usuarios si las Firmas Electrónicas Avanzadas o Fiables que les ofrecen cumplen o no los requerimientos dispuestos en las fracciones I a IV del artículo 97 del Código;*
***II.** Deje de cumplir con alguno de los requisitos que establece el Código para el otorgamiento de la acreditación;*
***III**. Actúe en contravención de los procedimientos definidos y específicos para la tramitación de un Certificado;*
***IV.** No permitir que se efectúe la consulta inmediata sobre la validez, suspensión o revocación de los certificados que emita, o*
***V.** No informe, antes de la emisión de un Certificado, a la persona que solicite sus servicios, de su precio, de las condiciones precisas para la utilización del Certificado, de sus limitaciones de uso y, en su caso, de la forma en que garantiza su posible responsabilidad.*
***Artículo 15** La Secretaría sancionará con suspensión temporal de tres meses y hasta cuatro meses en el ejercicio de sus funciones al Prestador de Servicios de Certificación que:*
***I.** Reincida en cualquiera de las conductas u omisiones a que se refiere el artículo anterior;*
***II.** Modifique su objeto social sin dar aviso previo a la Secretaría;*
***III.** No notifique a la Secretaría la iniciación de la prestación de servicios de certificación dentro de los 45 días naturales siguientes al comienzo de dicha actividad;*
***IV.** No cuente con los elementos requeridos para garantizar la seguridad de la información y su confidencialidad;*
***V.** Omita remitir a la Secretaría una copia de cada certificado por él generado;*
***VI.** No ponga a disposición del Firmante los dispositivos de generación de los Datos de Creación y de verificación de la Firma Electrónica, o*
***VII.** No proporcione los medios de acceso que permitan a la Parte que Confía en el certificado determinar los aspectos a que se refiere el artículo 104 fracción IX.*

***Artículo 16** La Secretaría sancionará con suspensión temporal de cinco y hasta seis meses en el ejercicio de sus funciones, al Prestador de Servicios de Certificación que:*
***I.** Reincida en cualquiera de las conductas a que se refiere el artículo anterior;*
***II.** No cuente con fianza vigente por el monto y condiciones que se determinan en forma general en este Reglamento y en las Reglas Generales;*
***III.** Provoque a causa de su negligencia, imprudencia o dolo en la expedición de un certificado la nulidad de un acto jurídico, o*
***IV.** Cambie de domicilio sin la autorización de la Secretaría.*

Artículo 17 *La Secretaría sancionará con suspensión definitiva en el ejercicio de sus funciones al Prestador de Servicios de Certificación que:*
I. *Reincida en cualquiera de las conductas a que se refiere el artículo anterior;*
II. *No compruebe en la identidad de los solicitantes y cualesquiera circunstancias pertinentes para la emisión de un certificado los términos establecidos por el Código y este Reglamento;*
III. *Proporcione documentación o información falsa para obtener la acreditación como Prestador de Servicios de Certificación;*
IV. *Altere, modifique o destruya los certificados que emita sin que medie resolución de la Secretaría o de autoridad judicial que lo justifique;*
V. *Emita, registre o conserve los certificados que expida fuera del territorio nacional;*
V. *Impida a la Secretaría efectuar las auditorias a que se refiere el Código y éste Reglamento;*
VII. *Revele los Datos de Creación de Firma Electrónica que correspondan a su propio certificado, y*
VIII. *No guarde confidencialidad respecto a la información que haya recibido para la prestación del servicio de certificación.*

Artículo 18. *La suspensión definitiva de un Prestador de Servicios de Certificación tendrá aparejada la inhabilitación para desempeñar esa función y la cancelación de la acreditación correspondiente.*

Artículo 19. *Cuando la Secretaría suspenda temporal o definitivamente o inhabilite a un Prestador de Servicios de Certificación en sus funciones, deberá revocar su correspondiente certificado y lo agregará al listado de certificados revocados en el dominio que establezca para tal efecto y publicará un extracto de la resolución en el Diario Oficial de la Federación, a efecto de que cualquier usuario pueda verificar en todo momento si un Prestador de Servicios de Certificación está habilitado o no para ejercer su función.*

Artículo 20. *Para efectos de lo dispuesto por el artículo 113 del Código, cuando se resuelva la suspensión, inhabilitación o cancelación en su ejercicio de un Prestador de Servicios de Certificación, la Secretaría actuará como tal respecto de la administración de los certificados que hubiese expedido aquél, hasta en tanto determina otro Prestador de Servicios de Certificación para este fin.*

T R A N S I T O R I O S

PRIMERO.- *El presente Reglamento entrará en vigor al día siguiente de su publicación en el Diario Oficial de la Federación.*

Anexo D <u>Reglas para la acreditación de los Prestadores de Servicios de Certificación de Firma Electrónica.</u>

Artículo 1.- Objeto
Las presentes reglas tienen por objeto establecer las reglas generales para la expedición de la acreditación como Prestador de Servicios de Certificación en adelante denominados (PSC), con el fin de asegurar la existencia de un sistema de certificación de firma electrónica avanzada y confiable, que confirme su continuidad en el tiempo y que sirva de base para el desarrollo comercial y tecnológico del país.

Artículo 2.- Solicitud de Acreditación y Verificación de Requisitos.
La Secretaría de Economía, en adelante la Secretaría, otorgará la acreditación de PSC a las personas que reúnan los requisitos a que se refiere el artículo 102 inciso A) del Código de Comercio, después de que dichos PSC comprueben el cumplimiento de los mismos, en los siguientes términos y condiciones:

I) Presentación de la solicitud ante la Secretaría, en el formato que se anexa a los presentes como Anexo 1 y en términos de la Ley Federal de Procedimiento Administrativo; acompañada además de la siguiente documentación:

a. Si la solicitud es de las personas a que se refiere la fracción I del artículo 100 del Código de Comercio, se requerirá de copia certificada de la Patente que lo acredite como Notario Público o de la habilitación expedida por la Secretaría en el caso de Corredores Públicos. Para las personas a que se refiere la fracción II del citado artículo, se requerirá de copia certificada del Acta Constitutiva, en su caso el acta de asamblea extraordinaria, u otro instrumento, en donde conste: i) Que se encuentren constituidas como sociedades mercantiles de acuerdo con las leyes mexicanas; ii) que el objeto de la persona moral es el requerido en el artículo 101 del Código de Comercio; iii) que el asiento principal de sus negocios se encuentre en el territorio nacional; iv) los datos de inscripción en el Registro Público de Comercio; y v) la personalidad de su representante con facultades para Actos de Administración o poder especial para este acto, debidamente inscrita en el mencionado Registro Público de Comercio; si se trata de las personas a que se refiere la fracción tercera, se requerirá de copia simple del decreto por el que se crean y, en su caso al mismo, con la fecha de publicación en el Diario Oficial de la Federación, así como el fundamento de la competencia de quien firma la solicitud en representación de la Institución Pública.

b. Comprobante de pago de los derechos por el trámite de acreditación.

c. El PSC para brindar los servicios de certificación deberá contar como mínimo con los siguientes elementos, a efecto de garantizar la seguridad de la información y su confidencialidad:

***Elementos Humanos:** Un Director de Autoridad Certificadora, un Oficial de Seguridad, un Responsable de la entidad acreditadora y un Responsable de la autoridad registradora, los cuales deberán cubrir los perfiles y exámenes a que se refiere el Anexo 2 de las presentes reglas, y presentar el requerimiento de la letra "e" de la presente fracción. Asimismo, deberán contar con un abogado o licenciado en derecho, experto en comercio electrónico que cubra con el perfil que el PSC estipule, mismo que será aprobado por la Secretaría.*

***Elementos Materiales:** Los PSC deberán contar con todos los recursos materiales para ejercer sus funciones, incluyendo de manera enunciativa más no limitativa: con el hardware y software necesarios, los elementos materiales necesarios para*

lograr un plan de continuidad de negocio, la plataforma tecnológica, seguridad física, la operación de las Autoridades Certificadora y Registradora; así como para resguardar la confidencialidad de la información.

Elementos Económicos: *i) Contar con un seguro de responsabilidad civil contra daños y/o pérdidas de terceros, producidas como consecuencia de cualquier error u omisión del PSC, sus equipos o empleados, y del solicitante, por un monto mínimo de quinientos mil pesos, moneda nacional. El seguro deberá mantenerse vigente mientras el PSC permanezca en actividad, e inclusive durante todo el año siguiente a aquél en que haya dejado de ejercer en forma definitiva, siempre y cuando no se haya interpuesto acción de responsabilidad en su contra, en cuyo caso deberá mantenerse vigente hasta que concluya el proceso respectivo. ii) En caso de que el PSC sea de los que refiere la fracción II del artículo 100 del Código de Comercio, deberá contar cuando menos con un capital social y prueba de financiamiento por un millón de pesos moneda nacional, combinados si fuera el caso, entre capital fijo y variable.*

Elementos Tecnológicos: *Una plataforma tecnológica que observe los requerimientos de seguridad física, el Plan de seguridad de sistemas, Plan de administración de llaves, la Política de certificados de firma avanzada, la declaración de prácticas de certificación y los modelos operacionales de las autoridades certificadora y registradora, de acuerdo con el Anexo 2 de las presentes reglas, en el entendido de que los certificados deberán ser generados y almacenados en el territorio nacional.*

Todos estos elementos se mencionan en el anexo 2 de las presentes reglas, mismos que se deben describir en la solicitud, a fin de ser posteriormente auditables para su verificación.

d. Los Procedimientos para la tramitación del Certificado y las medidas que garanticen la seguridad, confiabilidad e integridad, de los Certificados emitidos, la conservación y consulta de los registros, los cuales deberán contener cuando menos las definiciones y especificaciones, mencionadas en el Anexo 2 de las presentes reglas.

e. Relación de las personas que operarán o tendrán acceso a los sistemas de certificación del PSC, y la declaración de las mismas, bajo protesta de decir verdad, de que no se encuentran en alguno de los supuestos del artículo 102 inciso A) fracción IV del Código de Comercio. El formato para dicha declaración se adjunta como Anexo 3 de las presentes reglas.

f. Copia simple del comprobante de domicilio de la empresa y copia de la identificación oficial del representante legal en su caso.

g. Escrito de conformidad por parte del PSC para ser sujeto a Auditoría por parte de la Secretaría, el cual se realizará en el formato que determina el Anexo 4 de las presentes reglas.

h. Mencionar en la solicitud que persona, física o moral, llevará a cabo la comprobación de la identidad de los usuarios del servicio de certificación y cualesquiera otra circunstancia pertinente para la emisión de los certificados, precisando si se llevará a cabo por el PSC o persona diferente y en qué consisten dichas circunstancias.

Asimismo, acreditar que las personas, físicas o morales, que actúen en nombre y por cuenta del PSC, para comprobar la identidad de los usuarios y cualesquiera circunstancias pertinentes para emisión de los Certificados, además de cumplir con

el requisito a que se refiere la fracción IV del inciso a) del artículo 102 del Código de Comercio, se han comprometido por escrito a contratar un seguro por responsabilidad civil contra daños y/o pérdidas de terceros, producidas como consecuencia de cualquier error u omisión de estos, sus equipos o empleados, y del solicitante, por un monto mínimo de cuatrocientos mil pesos, moneda nacional. La póliza del seguro deberá ser remitida a la Secretaría dentro de los veinte días siguientes al inicio de operaciones del PSC.

i. Determinar si la Autoridad Registradora será la misma PSC o alguna otra persona que actué en nombre y por cuenta suyos.

Asimismo, acreditar que las personas, físicas o morales, que actúen en nombre y por cuenta del PSC, como Autoridad Registradora, además de cumplir con el requisito a que se refiere la fracción IV del inciso a) del artículo 102 del Código de Comercio, se han comprometido por escrito a contratar un seguro por responsabilidad civil contra daños y/o pérdidas de terceros, producidas como consecuencia de cualquier error u omisión de estos, sus equipos o empleados, y del solicitante, por un monto mínimo de cuatrocientos mil pesos, moneda nacional. La póliza del seguro deberá ser remitida a la Secretaría dentro de los veinte días siguientes al inicio de operaciones del PSC.

II) Una vez presentada la solicitud con los documentos correspondientes, la Secretaría llevará a cabo una verificación y evaluación de todos los requisitos y documentos, dentro de los 10 días siguientes a la fecha de presentación, dicha visita de verificación en las instalaciones del PSC, tendrá los efectos de primer auditoría, misma que se llevará de acuerdo con la siguiente metodología:

a) Visita de verificación por parte de la Secretaría para comprobar que se cumplan con los requisitos humanos, materiales, económicos y tecnológicos previstos en estas reglas, a efecto de garantizar la seguridad de la información; el procedimiento y metodología de la visita se detalla en el artículo 11 de estas reglas.

b) Visto bueno y evaluación del cumplimiento de los requisitos en la visita de verificación, emitido por la Secretaría, así como cumplir con otra auditoría efectuada por algún consultor externo que le de la certificación de "WEB TRUST" (es una estándar internacional).

***Artículo 3.-** En caso de incumplimiento en cualquiera de los requisitos señalados en el artículo anterior o en el artículo 102 inciso A) del Código de Comercio, la Secretaría deberá prevenir al interesado por escrito y por una sola vez, para que subsanen la omisión dentro del término de 20 días hábiles a partir de su notificación, transcurrido el plazo correspondiente sin desahogar la prevención, se desechará el trámite negando la acreditación al posible PSC.*

***Artículo 4.-** La Secretaría emitirá, en un plazo máximo de 45 días hábiles desde la presentación de la solicitud, una resolución en la que determinará si procede la acreditación o se deniega la misma. De no emitir la resolución en el plazo antes mencionado se tendrá por concedida la acreditación.*

***Artículo 5.-** Una vez determinada la procedencia de la acreditación la Secretaría actuando como autoridad certificadora y registradora en términos del artículo 105 del Código de Comercio, expedirá el certificado digital al PSC y lo registrará. Dicho certificado tendrá una vigencia que no será superior a dos años y el cual podrá ser renovado, si el PSC lo solicita antes de que concluya el período de vigencia.*

***Artículo 6.-** Determinada la procedencia de la acreditación y emitido el certificado, el Secretario de Economía expedirá la acreditación correspondiente. La acreditación deberá contener el nombre, denominación o razón social del PSC, el número de PSC que se le asigne, la plaza en la*

que se encontrará la Autoridad Certificadora, el nombre y fotografía de las personas que operen y tengan acceso a los sistemas de certificación del PSC, los datos del certificado, conforme al artículo 108 del Código de Comercio, sus datos de inscripción ante la Secretaría, y la vigencia de la acreditación la cual será de dos años como máximo, los nombres en su caso de las personas que verifiquen la identidad de los solicitantes y cualesquiera circunstancias pertinentes para la emisión de certificados y que lleven la autoridad registradora. La acreditación será publicada en el Diario Oficial de la Federación dentro de los treinta días hábiles siguientes a la resolución que determine su procedencia.

Artículo 7.- *Los PSC que hayan obtenido la acreditación de la Secretaría están obligados a notificarle el inicio de la prestación de servicios de certificación dentro de los veinticinco días hábiles siguientes al comienzo de dicha actividad, en el formato a que se refiere el Anexo 6. En caso de que no se reciba el mencionado aviso de inicio de prestación de servicios en un plazo de treinta días después de la publicación en el Diario Oficial de la Federación de la acreditación, la Secretaría sancionará al PSC con la suspensión por seis meses de sus funciones.*

Artículo 8.- *La Secretaría sólo autorizará el cambio de plaza de un PSC, cuando:*

a) No exista juicio por responsabilidad civil o denuncia penal en su contra o de algunos de sus empleados, o de las personas que designó como encargados de la verificación de identidad de los usuarios y cualesquiera circunstancias pertinentes para la emisión de los certificados o del encargado de la Autoridad Registradora; y

b) No se hayan interpuesto tres o más amonestaciones o multas al PSC o algunos de sus empleados o personas designadas para llevar a cabo la verificación de la identidad de los solicitantes y cualesquiera circunstancias pertinentes para la emisión de los certificados o del encargado de la Autoridad Registradora.

Si un PSC quiere establecer Autoridades Registradoras en una plaza diferente a la autorizada en la acreditación, necesitará la aprobación de la Secretaría, la cual previa auditoría corroborará que se cumplen con todos los requisitos del Código de Comercio, su Reglamento y estas reglas. Los cambios de domicilio que realice el PSC dentro de una misma plaza observarán los mismos requisitos antes mencionados.

Ningún PSC podrá tener más de una acreditación como Prestador de Servicios de Certificación, ya sea en una misma o en distintas Plazas.

Artículo 9 (antes 11). *Procedimiento y metodología de la visita de verificación.*

La Secretaría procederá a evaluar los requerimientos técnicos, establecidos en el anexo 2 de estas reglas. El solicitante deberá facilitar el acceso de los servidores públicos y expertos que la Secretaría designe para realizar las evaluaciones necesarias, además proporcionará cualquier información adicional solicitada por los mismos.

Realizada la visita de evaluación, la Secretaría resolverá sobre si se cumplen los requisitos y obligaciones exigidas en el Código de Comercio, su Reglamento y estas reglas para las PSC.

En el caso de no cumplir con los requisitos y obligaciones de acreditación definidos por el Código de Comercio, su Reglamento y estas reglas, la Secretaría procederá a dictar una resolución en la que rechaza la solicitud de acreditación, mencionando los requisitos que se consideran no subsanables y el fundamento para la misma.

En el caso que la Secretaría haya admitido la solicitud, pero determine como resultado de la evaluación que existen algunas omisiones o incumplimientos que presenta el PSC solicitante, los cuales son subsanables y no afectan el correcto funcionamiento del sistema, ni los fines previstos en el Código; procederá a prevenir al interesado, indicando los requisitos incumplidos que se deben subsanar, a fin de que en el término de 20 días hábiles a partir de la notificación de los mismos, el

PSC los subsane o haga una propuesta de medidas correctivas, en la que determine el tiempo y forma para subsanar dichas omisiones o incumplimientos.

Una vez recibido el plan de medidas correctivas propuesto por el PSC, la Secretaría contará con un plazo de 20 días hábiles para evaluarlo. En caso de que no lo apruebe, rechazará definitivamente la solicitud de acreditación mencionando los requisitos que se consideran no subsanables.

Artículo 10 (antes 12).- *La Secretaría sólo evaluará el cumplimiento de los requisitos y obligaciones de la acreditación para los PSC, no recomendará medidas correctivas ni propondrá planes para subsanar el incumplimiento de estos requisitos.*

Artículo 11 (antes 13).- *Objetivo de la Evaluación. El objetivo general de la evaluación es verificar el cumplimiento de los requisitos y obligaciones que impone el Código, el Reglamento y las presentes reglas, al Prestador de Servicios de Certificación que solicita la acreditación.*

Artículo 12 (antes 14).- *Escala de Evaluación. Cada requisito será evaluado de conformidad con la siguiente escala:*

Calificación	*Descripción*
A	*El PSC cumple totalmente el requisito exigido.*
A -	*El PSC cumple parcialmente el requisito y se determina que el incumplimiento es subsanable en tanto que no afecta el correcto funcionamiento del sistema ni los fines previstos en el Código en su Título Segundo del Libro Segundo.*
B	*El PSC no cumple el requisito y se determina que no es subsanable o afecta el correcto funcionamiento del sistema o no cumple con los fines previstos en el Código.*

El objetivo de la calificación ***A-*** *es permitir al PSC corregir aquellos requisitos que fueren subsanables en un plazo de 20 días hábiles y así optar a la acreditación durante su primera postulación.*

Artículo 13 (Antes 15).- *Esquema de Evaluación. La verificación del cumplimiento de los requisitos se realizará de conformidad con un procedimiento que tendrá los siguientes elementos:*
1. Revisión de antecedentes y requisitos;
2. Visitas a las instalaciones para verificar antecedentes y requisitos, en los casos que sea necesario;
3. Evaluación de la información obtenida; y
4. Elaboración de informe por la Secretaría.

Artículo 14 (Antes 24) *En el caso que un PSC quiera establecer una o varias Autoridades Registradoras en un lugar diferente al de la plaza en donde se encuentra la Autoridad Certificadora, deberá de contar con la autorización de la Secretaría, la cual previa auditoría corroborará que cuenta con los requisitos necesarios, conforme al Código de Comercio, el Reglamento y las presentes reglas. Dicha autorización se otorgará dentro de los dentro de los 30 días hábiles siguientes a la presentación de la solicitud, y si fuere necesario, contará con 10 días hábiles de prórroga, previa notificación al PSC. Las Autoridades Registradoras que se establezcan en los términos anteriores, sólo podrán recabar la información para la obtención del certificado, el cual siempre será expedido por la Autoridad Certificadora y dentro de la plaza para la que está autorizada ni fuera del territorio nacional.*
El incumplimiento a lo previsto en este lineamiento será sancionado en términos de lo previsto en el Reglamento.

Artículo 15 (Antes 25). *Cambios a las reglas. El contenido de estas reglas puede modificarse, dependiendo de los avances de la tecnología o consideraciones de seguridad nacional, previa consulta con la industria y consumidores.*

Artículo 16 (Antes 26). Costos, Derechos, Gastos y Honorarios. Todos los costos, derechos, gastos y honorarios que se devenguen en el proceso de acreditación serán responsabilidad de la persona o sociedad que solicita la acreditación, incluyendo el Pago de Derechos por Acreditación fijado por la Ley Federal de Derechos.

TRANSITORIOS

PRIMERO.- *Estas reglas entrarán en vigor al día siguiente de su publicación en el Diario Oficial de la Federación.*

Anexo 1. Solicitudes de Acreditación como Prestador de Servicios de Certificación de Firma Electrónica.

1.1 SOLICITUD DE ACREDITACION COMO PRESTADOR DE SERVICIOS DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA. (PERSONAS FÍSICAS)

En México, D.F. a _____ de _____ del 2003.

1. Indicar la condición del solicitante:

1.1 Notario Público		1.2 Corredor Público	

2. _____ _____ _____
   Nombre (s) Apellido Paterno Apellido Materno
3. Fedatario Público. Número._____ Del Estado de_____

4. Fecha de publicación en el Diario Oficial de la Federación, en la Gaceta o Periódico Oficial de la entidad federativa, del acto de autoridad competente para iniciar el ejercicio de sus funciones.

5. Domicilio: _____
_____

6. CURP No_____ RFC _____

7. Fecha de Nacimiento (dd/mm/aaaa): _____./_____./_____.

8. Dirección de correo electrónico _____

Declaro, bajo protesta de decir verdad

1) Que me encuentro en ejercicio de las funciones de (notario o corredor público) y cuento con los elementos humanos, materiales, económicos y tecnológicos, requeridos en los lineamientos para la acreditación de los Prestadores de Servicios de Certificación de Firma Electrónica y a mayor abundamiento los describo en los Documentos que se anexan a la presente.
2) Que me obligo a generar mi firma privada en las instalaciones que la Secretaría de Economía determina, en caso de obtener la acreditación como Prestador de Servicios de Certificación.

FIRMA. _____

Documentos que deberán acompañarse a esta solicitud:

Documentos que deberán acompañarse a esta solicitud:

1. Copia certificada de la patente o FIAT de notario, o habilitación para ser corredor público.
2. Copia simple del Comprobante de domicilio.
3. Copia simple de la Cédula Identificación Fiscal.
4. Copia certificada de la personalidad del representante legal (con actos de Administración o Poder especial para realizar trámites ante cualquier entidad Federativa).

5. Manual de Procedimientos definidos y específicos para la tramitación del Certificado.
6. Manual de Medidas que garanticen la seriedad de los Certificados emitidos, la conservación y consulta de los registros.
7. Descripción de los Elementos Humanos, Materiales, Económicos y Tecnológicos.
8. Relación y declaraciones de las personas que operarán y tendrán acceso a los sistemas de certificación.
9. Fotografía del personal que tendrá acceso a los sistemas de certificación, así como fotografía de todas las instalaciones donde opere el servidor
10. Escrito de conformidad para ser sujeto de Auditoria por parte de Secretaría de Economía.
11. Fianza por el valor de diez mil veces el salario vigente al Distrito Federal.

Todo lo anterior en los términos y condiciones del artículo 2 fracción I de los Lineamientos para la Acreditación de los Prestadores de Servicios de Certificación de Firma Electrónica, publicados en el Diario Oficial el _____.

1.2 SOLICITUD DE ACREDITACION COMO PRESTADOR DE SERVICIOS DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA. (PERSONAS MORALES)

SECRETARIA DE ECONOMIA

En México, D.F. a _____ de _____ del año 2003.

1. Marque la condición del solicitante:

1.1 PERSONAS MORALES DE CARÁCTER PRIVADO	☐
1.2 INSTITUCIONES PÚBLICAS	☐

2. Nombre, Denominación o Razón social _____

_____

3. Domicilio _____

_____

4. R.F.C. _____ 5. C.U.R.P. _____

6. Fecha de Constitución (dd/mm/aaaa): _____./_____./._____.

7. Dirección de correo electrónico: _____

Declaro bajo protesta de decir verdad que cuento con los elementos humanos, materiales, económicos y tecnológicos requeridos establecidos en los lineamientos para la acreditación de los Prestadores de Servicios de Certificación de Firma Electrónica y a mayor abundamiento los describo en el documento que se anexa a la presente.

NOMBRE DEL REPRESENTANTE O REPRESENTANTES LEGALES: _____

_____

FIRMA. _____

Anexo 2 de las Reglas para la acreditación de los Prestadores de Servicios de Certificación de Firma Electrónica.

Lineamientos técnicos en seguridad de los Prestadores de Servicios de Certificación.

1. ESTRUCTURA DE CERTIFICADOS.

1. *El certificado digital emitido por el PSC debe contener los datos que aparecen en el artículo 108 del Código de Comercio, para ser considerado válido.*
2. *La estructura de datos del certificado digital debe cumplir con el estándar ISO/IEC 9594-8; además de contener los datos que se indican en el punto anterior.*
3. *Los algoritmos utilizados para la firma electrónica deben ser los estándares de la industria[1], que provean un nivel adecuado de seguridad tanto para la firma del PSC como del titular.*
4. *El tamaño de las llaves privada y pública deben proveer el nivel de seguridad que prevalezca en la industria tanto para la firma del PSC como del titular.*
5. *Se utilizarán funciones hash estándares de la industria y de preferencia las más recientes que hayan sido aprobadas, que provean el adecuado nivel de seguridad para las firmas tanto del PSC como del titular.*
6. *Contendrán referencia o información suficiente para identificar y/o localizar uno o más sitios de consulta donde se publiquen las notificaciones de revocación o suspensión del certificado.*

2. ESTRUCTURA DE LISTA DE CERTIFICADOS REVOCADOS (CRL)

1. *La estructura e información de la lista de certificados revocados deberá de cumplir con el estándar ISO/IEC 9594-8.*
2. *Debe incluir por lo menos la siguiente información: la lista de los certificados revocados con su número de serie con fecha y hora, la identificación del algoritmo de firma utilizado[1], el nombre del emisor, fecha y hora en que fue emitida la CRL, fecha de la próxima CRL.*

3. REGISTRO DE ACCESO PÚBLICO.

1. *El PSC contará con un sistema de consulta remota al registro de certificados emitidos, indicando el estado del certificado digital: vigente, suspendido o revocado; copia de la CRL actualizada cada 24 hrs. Este registro público de certificados digitales se utilizará para consulta de titulares de manera continua, regular y segura.*
2. *Procedimiento que informe de las características de los procesos de creación y verificación de firma electrónica, y las reglas sobre prácticas de certificación.*
3. *Procedimientos para dejar sin efecto temporal o definitivo los certificados.*
4. *Procedimientos para publicar las resoluciones de la Entidad Acreditadora que le afecten. Además, debe incluir la Política de Certificación de Firma Electrónica y la Declaración de Prácticas de Certificación.*
5. *El sitio debe tener una disponibilidad del 99%, tener mecanismos redundantes o alternativos de conexión y sitios alternos de emergencia que se activen automática o manualmente en caso de desastres.*

---

[1] RFC 3280. Internet X509 Public Key Infraestructure Certificate and Certificate Revocation List (CRL) Profile (Obsoletes 2459), R. Housley, W. Polk, W. Ford, D. Solo, April 2002.

6. *Se protegerá la integridad y disponibilidad de la información utilizando tecnología y medidas de seguridad tanto físicas como lógicas, para mitigar el riesgo y ataques maliciosos en contra del sitio tanto interna como externamente.*
7. *El Registro de Acceso al Público deberá de seguir el estándar ISO/IEC 9594-8*

4. MODELO DE CONFIANZA Y GARANTÍA.

1. *Se establecerá un mecanismo que permita a los receptores de certificados verificar, directamente y mediante consulta electrónica, la validez de todos los certificados que reciban.*
2. *El Modelo de Confianza deberá de seguir el estándar ISO/IEC 9594-8*

5. EVALUACIÓN DE RIESGOS Y AMENAZAS.

1. *Dado que el producto principal de un PSC es la "confianza", el requerimiento fundamental para un PSC es demostrar una clara comprensión de las amenazas de seguridad enfrentadas por el negocio y poder mostrar planes efectivos para reducir el riesgo residual a un nivel aceptable, para ello será necesario un proceso de administración del riesgo que generalmente consta de:*
    a. *Valoración de los riesgos: identificar y valorar riesgos e impactos; así como recomendación de medidas para reducirlos.*
    b. *Disminución de los riesgos: implementación de medidas de seguridad.*
    c. *Manutención: proceso de evaluación continua para adecuar la valoración de riesgos a condiciones cambiantes del entorno.*
2. *Se recomienda seguir un proceso similar al descrito en los documentos que aparecen al pie de nota*[2,3]

6. POLÍTICA DE SEGURIDAD.

1. *Es la declaración de los objetivos de seguridad de la organización del PSC.*
2. *La política de seguridad deberá cumplir con los siguientes requisitos:*
    a. *Los objetivos de seguridad son consecuencia de la evaluación de riesgos y amenazas.*
    b. *Debe estar basada en las recomendaciones del estándar ISO 17799 sección 3.*
    c. *Los objetivos de la política deben ser claros, generales y no técnicos.*
    d. *La política general puede estar soportada por políticas específicas.*
    e. *Los elementos de la política que estén incorporados a la Declaración de Prácticas de Certificación y a la Política de los Certificados de Firma Electrónica Avanzada, deben estar incluidos en este documento.*
    f. *El documento debe identificar los objetivos de seguridad relevantes y las amenazas potenciales relacionadas a los servicios suministrados, y las medidas a tomar para evitar y limitar los efectos de las amenazas.*
    g. *El documento debe describir las reglas, directivas y procedimientos que indiquen como son provistos los servicios y las medidas de seguridad asociadas.*
    h. *La Política de Seguridad debe revisarse y evaluarse periódicamente.*
    i. *La Política de Seguridad debe ser consistente tanto con la Declaración de Prácticas de Certificación como con la Política de Certificados de Firma Electrónica.*

---

[2] Risk Management Guide for Information Technology Systems, Special Publication 800-30. Recommendations of the National Institute of Standards and Technology, October 2001.

[,3] Handbook 3, Risk Management, Version 1., Australian Communications Electronic Security Instruction 33 (ACSI 33).

3. La Política de Seguridad debe incluir los elementos fundamentales, se recomienda seguir un proceso similar al descrito en los documentos que aparecen al pie de nota [4].

7. Plan de Continuidad del Negocio

1. *El PSC tiene la obligación de elaborar un Plan de Continuidad del Negocio y Recuperación ante Desastres, que describa cómo los servicios serán restaurados en caso de desastres, caídas de sistemas o fallas en la seguridad, para disminuir el efecto de interrupciones del servicio.*
2. *El plan debe ser mantenido y probado periódicamente.*
3. *Se deben de describir también los procedimientos de emergencia a seguir en al menos los siguientes casos:*
    a. *Desastre que afecte el funcionamiento de software en el que se basan los servicios del PSC.*
    b. *Incidente de seguridad que afecte la operación del sistema en el que se basan los servicios del PSC.*
    c. *Cuando la llave privada de firma del PSC quede comprometida.*
    d. *Falla de los mecanismos de auditoria.*
    e. *Falla en el hardware donde se ejecuta el producto en el que se basan los servicios del PSC.*
    f. *Se debe considerar el análisis de Impacto en los Negocios, para evaluar el efecto de las interrupciones no planificadas.*
    g. *El plan debe incluir mecanismos para preservar evidencia del mal uso de los sistemas.*
4. *El plan debe seguir los lineamientos descritos en el estándar ISO 17799 sección 11 y estándar ETSI TS 102 042 sección 7.4.8.*
5. *Los planes deben ser coherentes con los niveles de riesgo determinados en una evaluación formal de riesgos. Se recomienda seguir un proceso similar al descrito en los documentos que aparecen al pie de nota [5,6,7]*

8. Plan de Seguridad de Sistemas.

1. *Los PSCs deberán contar con un Plan de Seguridad de Sistemas coherente con la Política de Seguridad.*
2. *El plan debe describir los requerimientos de seguridad de los sistemas y de los controles a implantar y cumplir; así como, delinear responsabilidades y conductas de las personas que acceden a los sistemas.*
3. *El Plan debe considerar los siguientes aspectos: política de seguridad de la información, seguridad organizacional, control y clasificación de activos, administración de operaciones y comunicaciones, control de accesos a sistemas y mantenimiento, desarrollo de sistemas, seguridad del personal, seguridad ambiental y física; y sus controles sean los recomendados por la norma ISO 17799.*
4. *El Plan de Seguridad debe implementar los mecanismos y procedimientos de seguridad, logrando el riesgo residual determinado en la Evaluación de Riesgos.*
5. *El plan de seguridad debe lograr los objetivos de la Política de Seguridad.*
6. *Los procedimientos del Plan deben lograr que la seguridad de los PSCs se mantenga en el tiempo debido a cambios en: amenazas, personal, componentes tecnológicos, etcétera.*

---

[4] Internet Security Policy: A Technical Guide, by the National Institute of Standards and Tehcnologies (NIST)
[5] NIST ITL Bulletin June 2002, Contingency Planning Guide for Information Systems.
[6] NIST Special Publication 800-34, Contingency Planning Guide for Information Systems, June 2002.
[7] NIST Special Publication 800-30 Risk Management Guide.

7. *El Plan debe garantizar el logro de los objetivos de la Política de Certificados de Firma Electrónica y la Declaración de Prácticas de Certificación.*
8. *El Plan debe considerar un Plan de Administración de Llaves Criptográficas para todo el ciclo de vida de las llaves.*
9. *El Plan debe considerar medidas de protección del depósito público de certificados y de información privada obtenida durante el registro.*
10. *El Plan de Seguridad de Sistemas tendrá que considerar por lo menos las secciones 4 a 10 del estándar ISO 17799*

9. ***Implementación del Plan de Seguridad de Sistemas.***

1. *La implementación del Plan de Seguridad de Sistemas debe mostrar que los procedimientos de la administración de la seguridad y la capacidad de administrar las instalaciones están de acuerdo con el Plan de Seguridad.*
2. *Se verificará que operaciones, procedimientos y mecanismos del Plan de Seguridad permitan alcanzar sus objetivos y lograr el riesgo residual determinado en La Evaluación de Riesgos.*
3. *Se evaluarán los controles de los aspectos señalados en el inciso 3 del punto Plan de Seguridad de Sistemas mencionado anteriormente..*
4. *Los procedimientos del Plan deben lograr que la seguridad de los PSCs se mantenga en el tiempo debido a cambios en: amenazas, personal, componentes tecnológicos, etcétera.*
5. *La implementación del Plan debe garantizar el logro de los objetivos de la Política de Certificados de Firma Electrónica y la Declaración de Prácticas de Certificación.*
6. *La implementación del Plan de Seguridad de Sistemas tendrá que considerar por lo menos las secciones 4 a 10 del estándar ISO 17799*

10. Plan de Administración de Llaves.

1. *El Plan de Administración de Llaves se requiere para proteger y administrar las llaves criptográficas.*
2. *La documentación del ciclo de vida completo de las llaves criptográficas debe comprender:*
    a. *Generación de las llaves de la AC .*
    b. *Almacenamiento, respaldo y recuperación de la llave privada de la AC.*
    c. *Distribución de la llave pública de la AC.*
    d. *Uso de la llave privada por parte de la AC.*
    e. *Término del ciclo de vida de la AC.*
3. *Administración del ciclo de vida del hardware criptográfico que utilice la AC.*
4. *Servicios de administración de las llaves de los titulares suministradas por la AC (generación y renovación de llave por vencimiento)*
5. *Preparación de los dispositivos seguros de los usuarios.*
6. *El plan debe ser consistente con la Política de Certificados De Firma Electrónica.*
7. *Se verificará que los procedimientos y mecanismos del Plan de Administración de Llaves permitan lograr el riesgo residual determinado en la Evaluación de Riesgos.*
8. *Los procedimientos implementados de acuerdo al Plan, deben hacer posible que la seguridad de las llaves se mantenga en el tiempo debido a cambios en: amenazas, personal, componentes tecnológicos, etcétera.*
9. *Deben estar considerados los requerimientos de generación de llaves de la AC; almacenamiento, respaldo y recuperación de llaves; distribución de la llave pública de la AC; uso de llave de la AC; fin de ciclo de vida de la llave de la AC; administración de hardware criptográfico de la AC;*
10. *El dispositivo seguro de los usuarios debe cumplir como mínimo con el estándar FIPS-140 nivel 3 o Common Criteria EAL 4, en sus elementos de seguridad e implementación de los algoritmos criptográficos estándares.*

11. *El Plan de Administración de Llaves tendrá que considerar por lo menos el estándar ETSI TS 102 042 sección 7.2 (Generación de la Llave de la AC, Almacenamiento, Respaldo y Recuperación de la Llave de la AC, Distribución de la Llave Pública de la AC, Uso de Llave de la AC, Fin del Ciclo de Vida de la AC y Administración del Ciclo de Vida del Hardware Criptográfico).*

11. Evaluación de la Plataforma Tecnológica.

1. *Se evaluará la seguridad de los elementos que constituyen la plataforma tecnológica del PSC, incluyendo los componentes de software y hardware de la PKI del PSC, y de los elementos de apoyo a su operación e interrelación, como:*
    a. *Módulo criptográfico.*
    b. *Módulo de la Autoridad Certificadora (AC).*
    c. *Módulo de la Autoridad Registradora (AR).*
    d. *Módulo de almacenamiento y publicación de los certificados.*
    e. *Protocolos de comunicación entre AC y AR*
    f. *Elementos de administración de log y auditoria.*
2. *Se evaluará el módulo criptográfico en cuanto a las siguientes capacidades:*
    a. *Generación de pares de llaves privada y pública con longitud de llaves de al menos 1024 bit, con capacidad para cifrado y firma.*
    b. *Sistemas de control de acceso para acceder a la llave privada y a la funcionalidad de firma y cifrado.*
    c. *Respaldo de la llave privada en forma segura.*
    d. *Recuperación de la llave privada de back-up.*
    e. *Generación de log auditable para administración de contingencia y accesos maliciosos.*
    f. *Manuales de operación, configuración y puesta en marcha.*
    g. *Procedimiento de recuperación ante contingencia.*
3. *Se evaluará el módulo de Autoridad Certificadora en cuanto a las siguientes capacidades:*
    a. *Generación de certificados con llaves de al menos 1024 bit.*
    b. *Suspensión y revocación de certificados.*
    c. *Generación de CRLs.*
    d. *Fecha de publicación y de renovación de la CRL.*
    e. *Generación de certificados de firma electrónica avanzada.*
    f. *Entrega de certificados y CRLs a directorios públicos X500.*
    g. *Existencia de sistemas de control de acceso para acceder a la generación de certificados y a los sistemas de administración y auditoria.*
    h. *Revocación de certificado raíz y generación de uno nuevo.*
    i. *Generación de logs auditables para administración de contingencia, actividades diarias del personal autorizado y accesos maliciosos.*
    j. *Manuales de operación, configuración y puesta en marcha.*
    k. *Procedimiento de recuperación ante contingencia.*
4. *Se evaluará el módulo de Autoridad Registradora en cuanto a las siguientes capacidades:*
    a. *Recepción de requerimientos de certificados.*
    b. *Solicitud de certificado a la AC.*
    c. *Sistema de control de acceso para acceder a la generación de certificados y sistemas de administración y auditoria.*
    d. *Suspensión y revocación de certificados.*
    e. *Revocación de certificado raíz y generación de uno nuevo.*
    f. *Generación de logs auditables para administración de contingencia, actividades diarias del personal autorizado y accesos maliciosos.*
    g. *Manuales de operación, configuración y puesta en marcha.*
    h. *Procedimiento de recuperación ante contingencia.*

5. *Se evaluará el módulo de almacenamiento y publicación de certificados en cuanto a las siguientes capacidades:*
    a. *Almacenamiento de certificados en base de datos X500 y publicación a través de protocolos LDAP V2.0 y/o OCSP VX.X*
6. *Se evaluarán protocolos de comunicación entre AC y AR en cuanto a las siguientes capacidades:*
    a. *Generación de certificados de comunicación segura entre AC y AR.*
7. *Se evaluarán elementos de administración de log y auditoria en cuanto a las siguientes capacidades:*
    a. *Módulos de log y auditoria que permitan verificar los intentos de acceso, los accesos y operaciones dañinas intencionales o no.*

8. La Plataforma Tecnológica tendrá que considerar por lo menos el estándar FIPS 140-1, ISO/IEC 15408 o equivalente.

12. Seguridad Física.

1. *Se verificará que el control de acceso a los servicios que manejan información sensible estén controlados; así como los riesgos físicos para los activos reducidos a su valor residual.*
2. *Los accesos físicos a las áreas de generación de certificados, gestión de revocación y suspensión de certificados y área residencia de servidores de la PSC, deben estar limitados sólo a personal autorizado y mediante controles de autenticación de por lo menos dos factores, asegurando que no habrá accesos no autorizados. Estas áreas deberán estar bien protegidas con puertas y muros firmes, chapas seguras, controles de acceso, alarmas de seguridad e incendio.*
3. *Las implementaciones de los controles deben evitar pérdida daño o compromiso de los activos de la PSC, y el compromiso y robo de información.*
4. *Se deben crear perímetros de seguridad físicos claramente definidos y eficientes alrededor de las áreas de generación de certificados, gestión de revocación y suspensión de certificados, y área residencia de servidores de la PSC. Las barreras de entrada a los perímetros deben ser suficientemente fuertes y en conformidad al análisis de riesgos realizado por el PSC. Los servicios compartidos por otra organización deben estar fuera del perímetro de seguridad.*
5. *La política de seguridad física del PSC debe contemplar por lo menos los siguientes aspectos: control físico de acceso; protección y recuperación ante desastres; protección contra robo, forzamiento y entrada; medidas de protección en caso de incendio; medidas contra fallas de servicios (electricidad, telecomunicaciones, etcétera).*
6. *El acceso de visitas a las áreas críticas debe estar autorizado por el oficial de seguridad. El visitante debe portar una credencial en todo momento para identificarse. Se debe registrar toda actividad que realice con la fecha y hora de ingreso y salida.*
7. *Se debe crear un procedimiento de actualización de la autorización de acceso al personal a las áreas restringidas.*
8. *Las áreas seguras deben ser oficinas cerradas dentro del perímetro de seguridad físico. Deben contener mobiliario con gabinetes con chapas seguras.*
9. *Para la selección y el diseño de áreas seguras se debe tomar en cuenta la posibilidad de daños por fuego, sismo, inundación, explosiones, desordenes civiles, y otras formas de desastres naturales y causadas por el hombre.*
10. *Todos los servicios claves deben situarse alejados del acceso o atención al público.*
11. *Dispositivos como fax y fotocopiadoras deben ubicarse dentro de las áreas seguras que así lo requieran, pero siempre bajo control para no comprometer la seguridad de la información.*
12. *Todo material de desecho debe ser destruido sin posibilidad de recuperación antes de desecharlo.*

13. *Las puertas y ventanas deben estar siempre cerradas y aseguradas, instalando protecciones externas en las ventanas.*
14. *Debe instalarse sistemas de detección de intrusión física en puertas y ventanas del perímetro de seguridad. Aquellas salas desocupadas que estén dentro del perímetro de seguridad deben tener activado el sistema de detección de intrusos todo el tiempo.*
15. *La gestión de los servicios de procesamiento de información debe estar físicamente separada del resto de los servicios.*
16. *Debe haber procedimientos y prácticas de seguridad del personal dentro del perímetro de seguridad, contemplando por lo menos lo siguiente:*
    a. *El personal debe conocer y entender los procedimientos y prácticas de seguridad dentro del perímetro de seguridad.*
    b. *Las áreas vacías deben cerrarse y revisarse periódicamente.*
    c. *El personal de soporte que no es parte del personal del PSC, debe acceder a las áreas restringidas sólo en caso necesario y si es autorizado, además deberá ser escoltado.*
    d. *No se debe permitir dentro del perímetro de seguridad equipo de grabación ni de audio ni de video.*
    e. *Las actividades sin supervisión dentro de las áreas seguras debe definirse para evitar problemas de seguridad y prevenir actividades maliciosas.*
    f. *La recepción de insumos y salida de basura deben estar controladas y separadas del área de procesamiento de la información para evitar accesos no autorizados.*
    g. *Los requerimientos de seguridad para las áreas de atención a clientes se determinarán a partir de la evaluación de riesgos.*
    h. *El personal que acceda a las áreas externas de recepción de insumos y de desechos debe estar debidamente controlado.*
    i. *Se debe verificar que el personal no autorizado no pueda acceder a través de estas áreas al perímetro de seguridad.*
    j. *Debe haber procedimientos y prácticas para inspeccionar el material que entre, en busca de potenciales peligros antes de ser trasladados desde las áreas externas a las áreas de uso.*
    k. *Se debe verificar que el equipo sea instalado y protegido para reducir los riesgos de amenazas, peligros ambientales y accesos no autorizados.*
    l. *Es necesario contar con respaldo de sistemas no interrumpible de energía eléctrica, y con una planta de energía eléctrica de emergencia para asegurar la continuidad de los equipos instalados y de los servicios sensibles y para la operación del PSC.*
    m. *Tanto el cableado de datos como el eléctrico debe estar protegido contra intercepciones y daños.*
    n. *El cableado de eléctrico y de datos de los servicios de información sensible debe estar bajo piso o bien protegidos.*
    o. *El cableado eléctrico debe estar protegido contra intercepción y daño no autorizado.*
    p. *Las líneas eléctricas y las de datos deben estar suficientemente separadas para evitar interferencias.*
    q. *Al equipo sensible se le debe dar el mantenimiento requerido para garantizar su continua disponibilidad e integridad.*
    r. *El mantenimiento a los equipos se debe dar de acuerdo a las especificaciones y períodos recomendado por los fabricantes.*
    s. *Los equipos deben repararse fuera de las instalaciones del PSC sólo por personal calificado y autorizado.*
    t. *Cuando se reparen equipos se debe tener cuidado de no permitir la salida del PSC de medios de grabación (discos duros, cintas, etcétera) que contengan información.*

u. *Se debe guardar registro de mal funcionamiento, fallas, mantenimientos preventivos y correctivos de los equipos sensibles para la operación del PSC.*
v. *Se debe de contar con procedimientos y prácticas que evite que equipo portátil contenga información sensible. Si hay alguna razón que justifique equipos portátiles que contengan información sensible o procesos críticos de la operación del PSC o información de los titulares de los certificados, éstos nunca deben salir del perímetro de seguridad designado*
w. *Debe haber procedimientos y prácticas que eviten que equipos sean reutilizados o queden en desuso conteniendo información sensible.*
x. *Los discos duros, disquetes y demás medios de grabación magnético u óptico que ya no se utilicen deben ser destruidos antes de salir del perímetro de seguridad.*
y. *Se debe adoptar la política de "escritorio limpio" y "pantalla limpia" para evitar riesgos de acceso no autorizado, pérdidas o daños a la información durante o fuera del horario de trabajo.*
z. *Debe haber procedimientos y prácticas que evite que equipos, información y software salgan de los perímetros de seguridad sin autorización.*

17. La Seguridad Física tendrá que considerar por lo menos el estándar ETSI 102 042 (sección 7.4.4 Physical and Environment security) e ISO/IEC 17799 (secciones 7.1.1 a 7.1.5; 7.2.1 a 7.2.6; y 7.3.1 a 7.3.2)

13. Política de Certificados de Firma Avanzada

1. *La Política de Certificados de Firma Electrónica Avanzada, debe ofrecer la confianza para que los documentos firmados en forma electrónica por el titular de un certificado, sean equivalentes a una firma autógrafa en las circunstancias que indica la Ley.*
2. *Una firma electrónica califica como Avanzada o Fiable si cumple con los requisitos indicados en el artículo 97 fracc. I a IV del Código de Comercio.*
3. *La Política de Certificados de Firma Avanzada deberá permitir la interoperabilidad con los demás PSC.*
4. *Las Prácticas de Certificación deberán establecer como el PSC entrega la confianza establecida en la Política de Certificados de Firma Avanzada.*
5. *La Política de Certificación debe indicar a quién se le puede otorgar un certificado digital.*
6. *En el proceso de registro se verificará: la identidad en forma fehaciente y forma de política para verificar el nombre del titular. Para que el certificado pueda ser utilizado para firma avanzada.*
7. *La Política de Certificación deberá indicar los propósitos para el cual fue emitido el certificado y sus limitaciones.*
8. *Se debe describir las obligaciones que contraen las entidades (AC, AR, titulares y receptores de certificados) en la emisión y utilización de un certificado.*
9. *El PSC debe cuidar que haya concordancia de las Prácticas de Certificación y la Política de Certificados con los procedimientos operacionales.*
10. *Las políticas de privacidad y de protección de datos deben ser apropiadas para la firma electrónica y publicadas y del conocimiento del subscriptor.*
11. *Decidir bajo que circunstancias se puede suspender y revocar un certificado y quiénes pueden solicitarlo.*
12. *La Política de Certificados tendrá que considerar por lo menos el estándar ETSI TS 102 042*

14. Declaración de Practicas de Certificación.

1. *Este documento deberá señalar los procedimientos de operación tanto para otorgar certificados digitales como el marco de aplicación de los mismos.*
2. *Se deben delimitar las responsabilidades y obligaciones del PSC y de la persona a identificar digitalmente.*
3. *Debe quedar explícito el ciclo de vida de los certificados y del PSC.*
4. *Debe de contener una declaración de las obligaciones y deberes del PSC.*
5. *Debe de contener un método de verificación de identidad utilizado para la emisión de los certificados.*
6. *Debe de contener procedimientos de protección de confidencialidad de la información de los solicitantes.*
7. *Debe de contener definiciones de los deberes y obligaciones de los solicitantes.*
8. *Debe de contener procedimientos que definan el ciclo de vida de los certificados.*
9. *Debe de contener deberes y procedimientos del PSC para emitir, revocar, suspender, renovar certificados y definiciones sobre la expiración de los mismos.*
10. *Debe de contener un procedimiento para registrar la fecha y hora de todas las operaciones relacionadas con la emisión de un certificado y conservarlas de manera confiable.*
11. *Debe de contener procedimientos de finalización de giro del PSC, que incluya procedimientos de término y traspaso a otro PSC u organismo que acepte la responsabilidad de la continuidad de los servicios, si hay certificados vigentes.*
12. *Debe haber medidas de seguridad adoptadas por el PSC para proteger sus datos de creación de firma electrónica avanzada.*
13. *Debe haber controles utilizados por el PSC para asegurar la generación de datos de creación de firma electrónica, autenticación de titulares, emisión de certificados, suspensión y revocación de certificados, auditoria y almacenamiento de información relevante.*
14. *La Declaración de Prácticas de Certificación tendrá que considerar por lo menos el estándar ETSI 102 042 y el RFC 2527*

15. Modelo Operacional de la Autoridad Certificadora.

1. *El modelo operacional debe cumplir con los requerimientos y obligaciones que dispone el Código, en relación con la confiabilidad e interoperabilidad en la forma de operar y prestar los servicios de la Autoridad Certificadora (AC) en un PSC.*
2. *Este modelo deberá responder por lo menos a las siguientes preguntas:*
    a. *¿Cuáles son los servicios prestados por la AC del PSC?*
    b. *¿Cómo se interrelacionan los diferentes servicios?*
    c. *¿En que lugares se operará?*
    d. *¿Qué tipos de certificados se entregarán?*
    e. *¿Hay certificados con diferentes niveles de seguridad?*
    f. *¿Cuáles son las políticas y procedimientos de cada tipo de certificado?*
    g. *¿Cómo se pretende hacer esto, incluyendo servicios externalizados?*
    h. *¿Cómo se protegerán los activos?*
3. *Debe contener un resumen que incluya:*
    a. *Un resumen del contenido del documento*
    b. *La historia de la empresa.*
    c. *Relaciones comerciales con proveedores de insumos o servicios para sus operaciones.*
4. *El modelo debe comprender los siguientes aspectos:*
    a. *Interfaces con AR.*
    b. *Implementación de elementos de seguridad.*
    c. *Procesos de administración.*
    d. *Sistema de directorios para los certificados.*
    e. *Procesos de auditoria y respaldo.*

   f. *Bases de Datos.*
   g. *Privacidad.*
   h. *Entrenamiento del personal.*
5. *El modelo debe considerar la generación de llaves para el titular de acuerdo a las políticas de certificación.*
6. *El modelo debe considerar la auditoria de lo siguiente:*
   a. *Seguridad y dispositivos de seguridad.*
   b. *Restricciones del personal.*
   c. *Interfaces de administración.*
   d. *Procedimientos de recuperación de desastres.*
   e. *Procedimientos de respaldo.*
7. *El modelo debe incluir los requerimientos de:*
   a. *La seguridad física de las instalaciones.*
   b. *Seguridad del personal.*
   c. *Nivel de seguridad del módulo criptográfico.*

16. ***Modelo Operacional de la Autoridad Registradora.***

1. *El modelo debe estar en conformidad con los requisitos de confiabilidad e interoperabilidad en la forma de operar y prestar sus servicios.*
2. *El modelo operacional deberá responder a:*
   a. *¿Cuáles son los servicios de registro prestados por el PSC?*
   b. *¿En qué lugares se ofrecerán dichos servicios?*
   c. *¿Qué tipos de certificados se entregarán?*
   d. *¿Cómo se pretende hacer esto, incluyendo los servicios externalizados?*
3. *El PSC tiene la obligación de generar y entregar en forma segura la llave privada del titular de un certificado de firma electrónica avanzada emitido por él, asegurándose además de la fiabilidad del dispositivo seguro y los mecanismos que el titular utiliza para firmar.*
4. *El modelo debe comprender los siguientes aspectos:*
   a. *Interfaces con CA.*
   b. *Implementación de dispositivos de seguridad.*
   c. *Procesos de administración.*
   d. *Procesos de auditoria y respaldo.*
   e. *Bases de Datos.*
   f. *Privacidad.*
   g. *Entrenamiento del personal.*
5. *El modelo de registro del titular debe proveer de una identificación unívoca del titular y el modelo de uso de la llave privada proveer la confianza requerida en el sistema.*
6. *El modelo de la AR debe incluir la auditoria de lo siguiente:*
   a. *Dispositivos de seguridad.*
   b. *Seguridad.*
   c. *Restricciones del personal.*
   d. *Interfaces de administración.*
   e. *Procedimientos de recuperación de desastres.*
   f. *Procedimientos de respaldo.*
7. *El modelo de la AR debe incluir lo siguiente:*
   a. *Descripción de la seguridad física de las instalaciones.*
   b. *Seguridad del personal.*
8. *El método de verificación de identidad utilizado para el registro de los solicitantes de certificado de firma electrónica.*

17. Manual de Operaciones de Autoridad Certificadora.

1. *Se comprobarán los aspectos operacionales mínimos con relación a los requisitos de confiabilidad e interoperabilidad en la forma de operar y prestar los servicios de la Autoridad Certificadora (AC) de un PSC.*
2. *Se describirá la administración diaria y las prácticas operacionales de la AC; además, podrá garantizar que las directrices primarias de la Política de Certificación están implementadas operacionalmente.*
3. *El manual de operaciones de la AC deberá tener a lo menos las siguientes características:*
    a. *Deberá ser consistente con la Política de Certificación.*
    b. *Deberá incluir la interacción entra la AC y la AR.*
    c. *Deberá describir los controles de seguridad física, de red, del personal y de procedimientos.*
    d. *Deberá incluir los procedimientos adoptados para el manejo de llaves públicas y privadas.*
4. *Mostrar la nómina de los cargos de personal, con la descripción de las responsabilidades y los procedimientos en que los empleados realizan sus funciones.*
5. *Hacer referencia del personal en los planes de continuidad del negocio y los planes de recuperación de desastres y emergencia.*
6. *Describir los planes de contingencia.*
7. *Describir detalladamente los siguientes procedimientos de operación:*
    a. *Generación de pares de llaves.*
    b. *Publicación de la CRL.*
    c. *Publicación de la información del certificado.*
    d. *Distribución de llaves y certificados.*
    e. *Renovación de certificados.*
    f. *Renovación de certificados luego de una revocación.*
    g. *Medidas de control de acceso.*
    h. *Procedimientos de respaldo y recuperación.*

8. El Manual de Operaciones de Autoridad Certificadora tendrá que considerar por lo menos el estándar ETSI 102 042 y el RFC 2527

18. Manual de Operaciones de la Autoridad Registradora.

1. *Se comprobarán los aspectos operacionales mínimos con relación a los requisitos de confiabilidad e interoperabilidad en la forma de operar de la Autoridad Registradora (AR) de un PSC.*
2. *Se describirá la administración diaria y las prácticas operacionales de la AR; como mínimo debe contemplar las siguientes características:*
    a. *Ser consistente con las políticas de certificación.*
    b. *Describir el plan de entrenamiento de los empleados.*
    c. *Incluir la forma en que se verifica la identidad de las personas.*
    d. *Incluir procedimientos de entrega y uso de la llave privada por los titulares de los certificados. Según la norma ETSI TS 102 042 se entiende que el PSC tiene la obligación de generar y entregar en forma segura la llave privada del titular de un certificado de firma electrónica avanzada emitido por él, asegurándose además de la fiabilidad del dispositivo seguro y los mecanismos que el titular utiliza para firmar.*
    e. *Incluir la metodología adoptada para manejar los temas de:*
        - *Análisis de riesgos*
        - *Plan de recuperación de desastres*
        - *Plan de seguridad*
        - *Incluir la interacción entre las unidades internas que cumplen la función de AC y AR.*

f. Mostrar la nómina de los cargos de personal, con la descripción de las responsabilidades y los procedimientos en que los empleados realizan sus funciones.
g. Se autenticará la identidad del titular y forma de política para verificar el nombre del titular.
h. El PSC debe tener implementados procedimientos y prácticas que permitan entregar en forma personal y segura los datos de creación de firma al titular del certificado.
i. El PSC debe tener implementados procedimientos y prácticas que aseguren que una vez entregados los datos de creación de firma sólo el titular tenga control de ellos. El dispositivo seguro entregado al titular debe firmar internamente el documento sin ser jamás accesible la llave privada del titular. El mecanismo de control de acceso a la llave privada sólo debe ser conocido por el titular al momento de la entrega del dispositivo y en lo posible modificable por el mismo titular, antes de ser utilizado por primera vez. El dispositivo seguro debe contar con mecanismos que inhabiliten el dispositivo en caso de reiterados intentos fallidos de acceso. El PSC debe entregar al titular herramientas, aplicaciones e instrucciones para que el titular pueda firmar en forma segura.
j. El PSC debe tener implementados procedimientos de capacitación que permitan al titular manejar en forma segura e informada el dispositivo de firma, y además mantener un servicio de atención para responder y solucionar dudas de los usuarios.
a. Hacer referencia del personal en los planes de continuidad del negocio y los planes de recuperación de desastres y contingencia.
k. Describir los planes de emergencia.
l. Descripción detallada de las siguientes operaciones:
  - *Procedimiento seguro de suspensión y revocación de certificados.*
  - *Medidas de control de acceso.*
  - *Procedimientos de respaldo y recuperación.*

m. El documento debe cubrir los procedimientos que involucren la interacción entre la AC y AR

3. El Manual de Operaciones de Autoridad Registradora tendrá que considerar por lo menos el RFC 2527.

19. Examen del personal. 4.

1. Verificar que el PSC emplea personal calificado para la prestación de los servicios ofrecidos, en el ámbito de la firma electrónica y los procedimientos de seguridad y de gestión, con el fin de minimizar los riesgos de errores humanos, robos o mal uso de los atributos del cargo, verificando la concordancia de los perfiles en cada cargo y función, con el análisis de riesgos.
2. Se evaluará en conformidad al análisis de riesgos del PSC que el personal que maneja o tiene acceso a sistemas e información sensible cumpla al menos con las siguientes condiciones:

a. Que califique como técnico o profesional para el cargo o función que desempeña.
b. Que tenga la experiencia mínima requerida para el cargo y función que desempeña.
c. Que no posea antecedentes penales o comerciales que lo inhabiliten.
d. Que conozca los procedimientos mínimos de seguridad que debe guardar en su función.

Se evaluará el procedimiento que utilice el PSC para reclutar, seleccionar, evaluar y contratar personal crítico.

Se evaluará el procedimiento que utilice el PSC para comprobar los antecedentes del personal crítico antes de contratarlo y el procedimiento para verificar antecedentes del personal contratado.

El personal de operaciones y sistemas no debería tener acceso a funciones de confianza, hasta que todos sus antecedentes hayan sido razonablemente verificados.
El personal que maneje información sensible, deberá ser personal de planta, existiendo contratos de confidencialidad que se extiendan mas allá de la vigencia del contrato del empleado y/o empresa externa.
Se evaluará que el personal tenga entrenamiento, capacitación y un pleno conocimiento de las políticas y procedimientos.

3. *Verificar la capacidad técnica y los antecedentes del Oficial de Seguridad empleado por el PSC.*
4. *El Oficial de Seguridad debe velar por el diseño, implantación y cumplimiento de los procedimientos y prácticas de seguridad en las instalaciones del PSC. Esta función demanda que el perfil del Oficial y los procedimientos de reclutamiento, evaluación, selección, y verificación de antecedentes penales y comerciales de este personal deben cumplir un alto estándar de exigencia. En particular se debe comprobar que el Oficial cumpla al menos los siguiente requisitos:*

    a. *Que tenga la calificación profesional en el ámbito de la seguridad tanto lógica como física. El perfil recomendado como mínimo es Ingeniero en Computación o equivalente con certificación y/o experiencia de al menos 5 años en el ámbito de la seguridad informática.*
    b. *Que no posea antecedentes penales o comerciales que lo <u>inhabiliten</u> **<u>en México o en el extranjero.</u>***

Se evaluará el procedimiento que utiliza el PSC para reclutar, evaluar y seleccionar al Oficial de Seguridad.

Se evaluará el procedimiento definido por el PSC para comprobar los antecedentes del OS una vez seleccionado.

Se evaluará el procedimiento y las fuentes que utiliza el PSC para comprobar los antecedentes del Oficial de Seguridad.

Adicionalmente, se evaluarán las cláusulas contractuales, de modo que aseguren que la vigencia de compromisos de no divulgación de información más allá de la vigencia de los contratos, en caso de cesación del profesional en el cargo.

5. *El Examen del Personal (calificado) tendrá que considerar por lo menos el estándar ISO 17799 y ETSI TS 102 042.*
6. *El Examen del Personal (Oficial de Seguridad) tendrá que considerar por lo menos el ISO 17799*

20. Se debe utilizar los siguientes estándares abiertos de la industria de Infraestructura de Llave Pública:

1. *Certificados digitales: X.509 V3 de ITU-T.*
2. *Atributos de certificados digitales: X.520 de ITU-T.*
3. *Lista de Certificados Revocados: X.509 V2 de ITU-T y OCSP V (RFC 2560).*
4. *Infraestructura de Llave Pública: PKIX.*
5. *Directorio de certificados: X.509 V3 y LDAP V2 (RFC 2587).*

6. *Algoritmos de llave pública: RSA (RFC 2313) y DSA.*
7. *Algoritmos de llave secreta/sesión: AES, DES, 3DES, RC2 y RC4.*
8. *Estándar de firmas digitales: FIPS PUB 186-2.*
9. *Funciones hash: MD5 (RFC 1321) y SHA-1 (RFC 3174).*
10. *Email: S/MIME y PEM.*
11. *Tecnología de llaves públicas: PKCS.*
12. *Auditorias de la Autoridad Certificadora: SAS 70 tipo II, CA Web Trust e ISO 17799.*
13. *Conservación de mensajes de datos: NOM 151.*
14. *Reglas de seguridad para EDIFACT: ISO 9735.*
15. *Requerimiento enviado a una Autoridad de Estampas de Tiempo: RFC 3161.*
16. *Certificado de la Infraestructura de la Llave Pública y Lista de Revocación de Certificados: RFC 3280, Internet X.509*
17. *Plan de Administración de Llaves: FIPS-140 Nivel 3 o Common Criteria EAL 4*
18. *Declaración de Prácticas de Certificación: RFC 2527 y ETSI 102 042*

Anexo 3 de las Reglas para la acreditación de los Prestadores de Servicios de Certificación de Firma Electrónica.

Carta de no encontrarse dentro de ninguno de los supuestos comprendidos en el artículo 102 inciso A) fracción IV del Código de Comercio.

MEMBRETE DEL SOLICITANTE A PSC

_____
DIRECTOR DE PRESTADORES DE SERVICIOS
DE CERTIFICACIÓN DIGITAL.
SECRETARÍA DE ECONOMÍA
P R E S E N T E.

En México, D.F. a _____ de _____ del 2003.

Yo ....., declaro bajo protesta de decir verdad que no me encuentro dentro de ninguno de los supuestos comprendidos en el artículo 102 inciso A) fracción IV del Código de Comercio, lo anterior para efectos de que se otorgue a _____ su acreditación como Prestador de Servicios de Certificación y dado mi carácter de _____ opero y/o tengo acceso a los sistemas de certificación de _____.

Sin más por el momento le reitero las seguridades de mi consideración más distinguida.

_____
NOMBRE COMPLETO, CARGO Y FIRMA

Anexo 3.4 de las Reglas para la acreditación de los Prestadores de Servicios de Certificación de Firma Electrónica.

Carta de autorización para ser sujeto a auditoria por parte de la Secretaría.

MEMBRETE DEL SOLICITANTE A PSC

_____.
DIRECTOR DE PRESTADORES DE SERVICIOS
DE CERTIFICACIÓN DIGITAL.
SECRETARÍA DE ECONOMÍA
P R E S E N T E.

En México, D.F. a _____ de _____ del 2003.

.....con la personalidad que ostento a nombre.....
me permito manifestar lo siguiente:

Autorizo a la Secretaría de Economía o a la persona física o moral que esta designe, a llevar a cabo la más amplia auditoria que legalmente proceda, lo anterior de conformidad con el artículo 102, inciso A) fracción VI del Código de Comercio, a fin de que verifiquen que cumplo con todos los requisitos para obtener o mantener mi acreditación como Prestador de Servicios de Certificación.

En el entendido de que debo reunir todos los elementos Humanos, Materiales, Económicos y Tecnológicos para realizar mis funciones.

Sin más por el momento le reitero la seguridad de mi consideración más distinguida.

_____
NOMBRE COMPLETO, CARGO Y FIRMA

1. En caso de ser representante legal, acompañar la documentación que acredite su personalidad en los términos de ley.

Anexo 5 de las Reglas para la acreditación de los Prestadores de Servicios de Certificación de Firma Electrónica.

Póliza de fianza.

<table>
<tr><td colspan="2">AFIANZADORA
_____</td><td colspan="2">FOLIO
_____</td><td colspan="2">PÓLIZA DE FIANZA

BENEFICIARIO</td></tr>
<tr><td colspan="3">Fecha de Expedición
Día | Mes | Año</td><td>Fianza Número</td><td>Monto de la Fianza</td><td>Endoso</td></tr>
</table>

AFIANZADORA _____ en ejercicio de la autorización que le otorgó el Gobierno Federal a través de la Secretaría de Hacienda y Crédito Público en los términos de los artículos 5° y 6° de la Ley Federal de Instituciones de Fianzas se constituye fiadora hasta por el monto de:

(Aquí va el monto de la fianza con letra)

POR: (NOMBRE DEL PSC)

ANTE: TESORERÍA DE LA FEDERACIÓN

PARA GARANTIZAR EN LOS TERMINOS DE LOS ARTÍCULOS 102 INCISO A), FRACCIÓN QUINTA DEL CÓDIGO DE COMERCIO; __ Y __ DEL REGLAMENTO DEL PROPIO CÓDIGO Y __ DE LOS LINEAMIENTOS PARA LA ACREDITACIÓN DE PRESTADORES DE SERVICIOS DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA, LA ACTUACIÓN DE LA (NOMBRE DEL PSC), COMO PRESTADOR DE SERVICIOS DE CERTIFICACIÓN NÚMERO DIEZ EN LA PLAZA DEL ESTADO DE _____, EL PAGO DE LA RESPONSABILIDAD CIVIL CONTRAÍDA POR DICHO PRESTADOR DE SERVICIOS DE CERTIFICACIÓN, EL PAGO DE LAS MULTAS QUE SE LE IMPUSIEREN A LA MISMA, ASÍ COMO TODAS Y CADA UNA DE LAS OBLIGACIONES A SU CARGO. ESTA FIANZA SURTE SUS EFECTOS A PARTIR DEL DÍA ____ DE JULIO DEL AÑO DOS MIL TRES Y ESTARÁ VIGENTE HASTA EL DÍA _____ DE JULIO DEL AÑO DOS MIL CUATRO, Y NO PODRÁ SER CANCELADA SINO POR ACUERDO EXPRESO DE LA TESORERÍA DE LA FEDERACIÓN. LA INSTITUCIÓN AFIANZADORA SE SOMETE EXPRESAMENTE AL PROCEDIMIENTO DE EJECUCIÓN ESTABLECIDO EN LOS TERMINOS DE LOS ARTÍCULOS 95, 95 BIS Y 118 DE LA LEY FEDERAL DE INSTITUCIONES DE FIANZAS VIGENTE. LA PRESENTE FIANZA PERMANECERÁ VIGENTE Y ACTUALIZADA MIENTRAS EL PRESTDOR DE SERVICIOS DE CERTIFICACIÓN SE ENCUENTRE EN FUNCIONES, E INCLUSIVE DURANTE TODO EL AÑO SIGUIENTE A AQUÉL EN QUE HAYA DEJADO DE EJERCER EN FORMA DEFINITIVA, SIEMPRE Y CUANDO NO SE HAYA INTERPUESTO ACCIÓN DE RESPONSABILIDAD EN SU CONTRA, EN CUYO CASO LA GARANTÍA PERMANECERÁ VIGENTE Y ACTUALIZADA HASTA QUE SE CONCLUYA EL PROCESO RESPECTIVO. =FIN DE TEXTO=

DE ACUERDO A LAS DISPOSICIONES DE LA COMISIÓN NACIONAL DE SEGUROS Y FIANZAS CONTENIDAS EN LA CIRCULAR F-10.1.4 DE FECHA 4 DE NOVIEMBRE DE 1999, SE INSERTA LA SIGUIENTE DISPOSICIÓN: " ESAS INSTITUCIONES DE FIANZAS DEBERÁN VERIFICAR QUE LOS ESCRITOS DE LAS RECLAMACIONES RECIBIDAS QUE SE PRESENTEN EN EL DOMICILIO DE SUS OFICINAS O SUCURSALES SEAN ORIGINALES, FIRMADOS POR EL (LOS) BENEFICIARIO (S) DE LA FIANZA (S) Y DEBERÁN CONTENER COMO MÍNIMO LOS SIGUIENTES DATOS, CON EL OBJETO DE QUE ESAS INSTITUCIONES CUENTEN CON ELEMENTOS PARA LA DETERMINACIÓN DE SU PROCEDENCIA (TOTAL O PARCIAL) O IMPROCEDENCIA: A) FECHA DE RECLAMACIÓN, B) NÚMERO DE PÓLIZA DE FIANZA RELACIONADO CON LA RECLAMACIÓN RECIBIDA, C) FECHA DE EXPEDICIÓN DE LA FIANZA, D) MONTO DE LA FIANZA, E) NOMBRE O DENOMINACIÓN DEL FIADO, F) NOMBRE O DENOMINACIÓN DEL BENEFICIARIO, G) DOMICILIO DEL BENEFICIARIO PARA OÍR Y RECIBIR NOTIFICACIONES, H) DESCRIPCIÓN DE LA OBLIGACIÓN GARANTIZADA, I) REFERENCIA DEL CONTRATO FUENTE (FECHAS, NÚMERO DE CONTRATO, ETC.); J) DESCRIPCIÓN DEL INCUMPLIMIENTO DE LA OBLIGACIÓN GARANTIZADA QUE MOTIVA LA PRESENTE DE LA RECLAMACIÓN, ACOMPAÑANDO LA DOCUMENTACIÓN QUE SIRVA COMO SOPORTE PARA COMPROBAR LO DECLARADO, Y K) IMPORTE DE LO RECLAMADO, QUE NUNCA PODRÁ SER SUPERIOR AL MONTO DE LA FIANZA". =FIN DE TEXTO=

Anexo 6 de las Reglas para la acreditación de los Prestadores de Servicios de Certificación de Firma Electrónica.

Carta de inicio de las funciones de prestación de servicios de certificación de firma electrónica.

_____.
DIRECTOR DE PRESTADORES DE SERVICIOS
DE CERTIFICACIÓN DIGITAL.
SECRETARÍA DE ECONOMÍA
P R E S E N T E.

En México, D.F. a _____ de _____ del 2003.

_____, en mi carácter de Prestador de Servicios de Certificación, número _____ de la Plaza _____, el que consta en la acreditación publicada en el Diario Oficial de la Federación, con fecha._____, me permito manifestar lo siguiente:

Que con fecha _____, he iniciado mis funciones de prestación de servicios de certificación de firma electrónica, lo anterior, para efectos de lo establecido en el artículo séptimo de los Lineamientos para la Acreditación de los Prestadores de Certificación de Firma Electrónica publicados en el Diario Oficial de la Federación el día _____.

Sin más por el momento, le reitero las seguridades de mi consideración más distinguida,

_____
NOMBRE COMPLETO, CARGO Y FIRMA

1. En caso de ser representante legal, acompañar la documentación acreditativa en los términos de ley.