UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

LA AFIRMATIVA FICTA EN LA ACREDITACIÓN DE ENTIDADES DE CERTIFICACIÓN.

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADA EN DERECHO

P R E S E N T A:

VIRIDIANA TRUCHÉ MOYSÉN

ASESOR:
MTRA. CLAUDIA ZULIAM MENES SALINAS

Nezahualcóyotl, Estado de México, Noviembre de 2014

DEDICATORIAS.

A mi familia por apoyarme en todo momento y no perder la fe en mí, porque nunca podre pagarles todo lo que han hecho por mí, mil gracias.

A la Universidad Nacional Autónoma de México, en especial a la Facultad de Estudios Superiores Aragón, por haberme permitido formarme profesionalmente en sus aulas y con sus maestros y por permitirme lograr mí sueño.

A mi asesora la Mtra. Claudia Zuliam Menes Salinas gracias por su tiempo, paciencia y apoyo a lo largo de la realización del presente trabajo.

A mis amigos gracias por brindarme desinteresadamente su amistad, por los buenos momentos que pasamos y por apoyarme siempre.

A todas las personas que no creyeron que llegaría tan lejos en la vida, gracias porque por sus criticas me hice mas fuerte cada día.

“Tienes que conocer las reglas del juego. Y entonces tienes que jugar mejor que nadie más.” ***Albert Einstein***

ÍNDICE

INTRODUCCIÓN.

En la actualidad vivimos en una era digital, en la que los avances tecnológicos han cambiado aspectos sociales y económicos en todo el planeta, estas transformaciones se han dado principalmente gracias a las nuevas Tecnologías de la Información y la Comunicación que se ha convertido en parte importante de nuestra vida cotidiana.

En el ámbito comercial los avances tecnológicos han propiciado que se lleven a cabo operaciones comerciales de manera internacional de forma más rápida, el denominado comercio electrónico, por lo menos en los países de habla hispana, ha abierto un mundo de posibilidades a miles de comerciantes y no comerciantes en todo el mundo, pero también ha traído consigo muchos problemas en materia de seguridad informática. Es por ello que existen legislaciones internacionales y legislaciones locales para resolver todos los inconvenientes que se susciten en este tipo de comercio.

Es así que aparecen las figuras jurídicas llamadas firma electrónica y prestador de servicios de certificación, instauradas para brindar confiabilidad y certeza al comercio electrónico. Su propósito es que a través de ellas los usuarios tengan plena confianza en las transacciones comerciales que se realicen por medios electrónicos, ya que este es el único medio que tienen los comerciantes y no comerciantes para corroborar la identidad del remitente de un mensaje de datos.

Así pues, el papel que tienen los prestadores de servicios de certificación o entidades de certificación en el comercio electrónico es muy significativo, ya que estas entidades, además de las firmas electrónicas, le brindaron certidumbre al comercio electrónico. Aparte de esto, al realizar su trabajo estas entidades manejan datos personales de sus usuarios, lo cual involucra una gran responsabilidad para la entidad de certificación.

La presente investigación se centra en la propuesta de derogación del apartado B del artículo 102 del Código de Comercio Vigente, el cual permite que las entidades de certificación reciban su acreditación a través de una afirmativa ficta, ya que esta aceptación por parte de la ley comercial de nuestro país pone en peligro la seguridad jurídica de los comerciantes y no comerciantes que realizan actos de comercio a través de medios electrónicos, porque si el prestador de servicios de certificación realiza de forma negligente sus funciones o no cumple con sus obligación provocarían la nulidad del acto jurídico o que se haga un mal tratamiento de los datos personales recabados para emitir los certificados digitales lo cual provocaría la difusión de los mismos o que sean vulnerables a un ataque cibernético.

Por medio de una investigación documental, con la utilización de doctrina nacional y extranjera se demostrará que debido a la importancia que tienen los prestadores de servicios de certificación en el comercio electrónico es incongruente que la ley permita que estas entidades sean acreditadas como tales por el simple transcurso del plazo de 45 días que se marca en el artículo mencionado con anterioridad, sin que los peticionarios pasen por un riguroso proceso para cerciorarse de que cuenta con los elementos requeridos y suficientes para brindar el servicio de expedición de certificados digitales y que sus servicios se realizarán de forma responsable.

Dividida en cuatro capítulos, la presente tesis abarca:

Primer Capítulo: se explican los antecedentes del comercio electrónico y de los prestadores de servicios de certificación, así como las definiciones de ambas figuras y de otras figuras que les son afines.

Segundo Capítulo: las legislaciones que les son aplicadas a las entidades de certificación en materia internacional y nacional.

Tercer Capítulo: se analizan los aspectos concernientes a dichas entidades, como sus funciones, obligaciones, sanciones y sus requisitos de acreditación.

Cuarto Capítulo: se expone la propuesta integral de derogación del apartado B del artículo 102 del Código de Comercio Vigente, por poner en peligro los derechos de los comerciantes y no comerciantes.

Para que los comerciantes y no comerciantes tengan mayor confianza al realizar operaciones comerciales a través de cualquier medio electrónico es indispensable que la Secretaría de Economía, como autoridad responsable de vigilar y acreditar a las entidades de certificación, garantice que la seguridad de estos no se verá violada. Así, es necesario derogar el apartado B del artículo 102 del Código de Comercio Vigente para no permitir que las entidades de certificación sean acreditadas a través de una afirmativa ficta, sino que pasen por un procedimiento más complejo para asegurarse de que realizarán su trabajo de manera eficaz y segura.

Ya que la tecnología avanza diariamente las legislaciones comerciales que regulan al comercio electrónico deben ir mejorando a la par de ellas, ya que este tipo de comercio no solo comprende la compra, venta e intercambio de bienes y servicios sino que también se refiere al intercambio electrónico de datos, además que en la actualidad esto se puede realizar en cualquier lugar y desde diversos dispositivos electrónicos, como por ejemplo computadoras, celulares inteligentes, tabletas electrónicas, etc.

A pesar de que las reformas en las legislaciones mexicanas se hicieron hace más de 10 años, las deficiencias que se tienen en materia de comercio electrónico y todo lo concerniente a este aun son muchas, y debido a que éste tipo de comercio cada vez tiene mayor auge e importancia en las sociedades de todo el mundo y ya que la mayoría de la población mundial tiene acceso a Internet, es necesario resolver esas carencias en las legislaciones, antes de que ocasionen controversias a nivel internacional y grandes pérdidas económicas.

CAPÍTULO PRIMERO.

COMERCIO ELECTRÓNICO Y ENTIDADES DE CERTIFICACIÓN.

La evolución del comercio a lo largo de la historia aunado a los avances tecnológicos, sobre todo lo relacionado a las nuevas tecnologías de comunicación, han tenido como consecuencia que sea posible que comerciantes alrededor del mundo lleven a cabo transacciones comerciales sin que sea necesario trasladarse al lugar de residencia de alguno de ellos. Y con la creación del Internet ha sido más fácil celebrar este tipo de actividades entre ausentes, pero también existen muchos problemas en cuestión de seguridad y confiabilidad en este tipo de comercio.

Es por ello que en los últimos años se han creado legislaciones que regulan este nuevo tipo de comercio, al cual se denomina comercio electrónico; para poder identificar a los sujetos que actúan en él se crearon las firmas electrónicas y para darle fiabilidad a estas últimas se establecieron las entidades de certificación. Así que, en este capítulo analizamos los conceptos de estas figuras así como otros términos que son afines al comercio electrónico; de igual forma se hace referencia a los antecedentes tanto del comercio electrónico, como de las entidades de certificación.

1.1 Comercio Electrónico.

Para entender el concepto de comercio electrónico primero debemos analizar la definición de comercio en términos generales, para posterioridad señalar las distintas definiciones de este tipo de comercio y sus antecedentes.

1.1.1 Concepto de comercio.

El Doctor Raúl Cervantes Ahumada[1] menciona que etimológicamente la palabra comercio proviene del latín *commercium*, que se compone de las voces *cum* y *merx* lo cual significa con-mercancía; encontrando en esta expresión las ideas de cambio y del tráfico.

Es por ello, que los inicios del comercio están en el trueque, una forma de cambiar una mercancía por otra y de esta manera satisfacer las necesidades de las personas; y a partir de este punto ha ido evolucionando, adaptándose a la transformación de las sociedades, hasta llegar al actual comercio electrónico, pero sin perder la esencia de lo que era en sus orígenes.

Con base en el vocablo latina, el diccionario Larousse[2] lo define como la acción de comerciar, entendiendo ésta como la compra, venta o permuta de géneros, con fin lucrativo. Pero, este concepto solo abarca una parte del comercio, ya que como lo marca el artículo 75 del Código de Comercio existe una gran variedad de actos de comercio en los que se ve reflejado el mismo.

En términos económicos, el jurista Rafael de Pina Vara lo concibe como: "una actividad de mediación o interposición entre productores y consumidores, con propósito de lucro."[3]

En el mismo sentido, el Diccionario de Derecho Mercantil refiere que es: "una actividad lucrativa que consiste en la intermediación directa o indirecta

---

[1] *Vid.* CERVANTES AHUMADA, Raúl, Derecho Mercantil, 3ª edición, Editorial Porrúa, México, 2004, p. 2.
[2] *Vid.* LUCENA CAYUELA, Núria (coord.), Pequeño Larousse, 9ª edición, Editorial Larousse, México, 2003, p. 267.
[3] PINA VARA, Rafael de, Elementos de Derecho Mercantil Mexicano, 29ª edición, Editorial Porrúa, México, 2003, p. 3.

entre productores y consumidores de bienes y servicios a fin de facilitar y promover la circulación de la riqueza."[4]

En conclusión, la palabra comercio es un término inherentemente económico, el cual se entiende como la actividad de mediación entre productores y consumidores de bienes y servicios, de forma directa o indirecta, que tiene como finalidad un lucro para el productor y la satisfacción de una necesidad del consumidor.

1.1.2 Concepto de comerciante. (Persona física y persona moral).

El concepto originario de comerciante es descrito por el teórico Rafael de Pina Vara, como: "las personas que negocian comprando y vendiendo o permutando géneros o mercancías."[5]

En cambio en una perspectiva más amplia, el Maestro Ignacio Quevedo Coronado señala que el comerciante es: "la persona que, buscando el lucro, realizan actos de comercio haciendo de ello su profesión habitual, su *modus vivendi*."[6]

En un enfoque diferente, el Diccionario de Derecho Mercantil[7] enlista tres criterios diferentes para definir al comerciante, los cuales son:

1. Subjetivo: son comerciantes, conforme al artículo 4 del Código de Comercio, las personas que no teniendo la calidad de tal, con establecimiento fijo o no, realizan de manera accidental una actividad comercial.

---

[4] QUINTANA ADRIANO, Elvia Arcelia (coord.), Diccionario de Derecho Mercantil, Editorial Porrúa, México, 2001, p. 106.
[5] PINA VARA, Rafael de, *Op. Cit.* pág. 47.
[6] QUEVEDO CORONADO, Ignacio F., Derecho Mercantil, 2ª edición, Editorial Pearson, México, 2004, p. 15.
[7] *Vid.* QUINTANA ADRIANO, Elvia Arcelia (coord.), *Op. Cit.* p. 104.

2. Objetivo: las personas que cuentan con capacidad legal para ejercer actos de comercio y que hagan de ello su ocupación ordinaria.

3. Formal: las personas morales establecidas conforme con la legislación mercantil.

Por su parte, el artículo 3 del Código de Comercio menciona que son comerciantes:

1. Las personas físicas: el individuo que cuente con la capacidad legal para ejercer el comercio y que haga de él su ocupación ordinaria.

2. Las personas morales: entendiendo éstas como las sociedades mercantiles que se constituyan con arreglo a las leyes mercantiles de nuestro país que les son aplicables.

3. Las sociedades extranjeras: es decir, sociedades mercantiles que encontrándose establecidas en el extranjero realizan actos de comercio en nuestro país, por sí mismas o a través de sus agencias o sucursales.

Así, el comerciante es la persona física o moral, nacional o extranjera, que participan en el comercio, y que por ende tiene capacidad legal para ejercer el mismo y lo hace de manera reiterada. Aunque, también será considerado como tal aquellas personas, que de manera accidental, realizan actividades comerciales.

En el caso del comercio electrónico, los comerciantes son llamados iniciador y destinatario, pero ya que en este tipo de comercio las partes no se ven físicamente, existe un tercer sujeto denominado entidad de certificación que se encarga de autentificar las firmas electrónicas y de brindar protección a los partes que participan en estas actividades comerciales, sobre todo a los destinatarios y en especial si no son comerciantes como tal, pero realizan accidentalmente actos de comercio, ya que ellos son la parte que confía en los certificados digitales.

1.1.3 Concepto de comercio electrónico.

De acuerdo con la Asociación Mexicana de Internet (AMIPCI) el comercio electrónico es: “el intercambio de bienes y servicios realizado a través de las Tecnologías de la Información y las Comunicaciones, habitualmente con el soporte de plataformas y protocolos estandarizados.”[8]

Por su parte, el doctrinario Salomón Vargas García menciona que: “el comercio electrónico se entiende como el conjunto de actividades mercantiles que se desarrollan mediante el uso de sistemas de procesamiento de datos y de comunicaciones sin que exista un contacto físico entre quien oferta un bien o un servicio y quien lo demanda”[9]

La Organización para la Cooperación y el Desarrollo Económico (OCDE) señala que:”el comercio electrónico es el proceso de compra, venta o intercambio de bienes, servicios e información a través de las redes de comunicación.” [10]

Igualmente el Doctor Julio Téllez Valdés lo define como: “cualquier forma de transacción o intercambio de información comercial basada en la transmisión de datos sobre redes de comunicación como Internet.”[11]

Entonces, el comercio electrónico no solo abarca la compra, venta o el intercambio de bienes o servicios, sino que también el uso de las redes de

---

[8] Asociación Mexicana de Internet, Glosario de Términos, [En línea]. Disponible: http://www.amipci.org.mx/?P=glosario 12 de Agosto de 2013. 15:20 PM.

[9] VARGAS GARCÍA, Salomón, Algunos Comentarios sobre el Comercio Electrónico y la Correduría Pública en México, Editorial Porrúa, México, 2004, p. 9.

[10] Procuraduría Federal del Consumidor, Comercio Electrónico, última modificación 15 de febrero de 2013. [En línea]. Disponible: http://www.profeco.gob.mx/internacionales/com_elec.asp 27 de Agosto de 2013. 12:30 PM.

[11] TÉLLEZ VALDÉS, Julio, Derecho Informático, 2ª. Edición, Ed. McGraw Hill, México, 1996, p. 188.

comunicación para las actividades anteriores o posteriores a la transacción comercial, es decir para compartir información.

Este tipo de comercio, de acuerdo con el Diccionario de Microsoft[12], puede llevarse a cabo entre un usuario y un fabricante por medio de Internet o de un servicio de información en línea o de un tablón de anuncios electrónicos, o bien por medio de las computadoras del fabricante y el cliente por medio del intercambio electrónico de datos.

Por otra parte, la Licenciada Eva Fernández Gómez[13] menciona que existen diversos tipos de comercio electrónico, los cuales son:

- *Business to Business (B2B)*: es el comercio entre empresas.
- *Business to Consumer (B2C)*: empresas que ofertan bienes o servicios a los consumidores.
- *Consumer to Consumer (C2C):* consumidores realizando ofertas a otros consumidores.
- *Business to Enploy (B2Y):* cuando una empresa ofrece servicios a sus propios trabajadores.

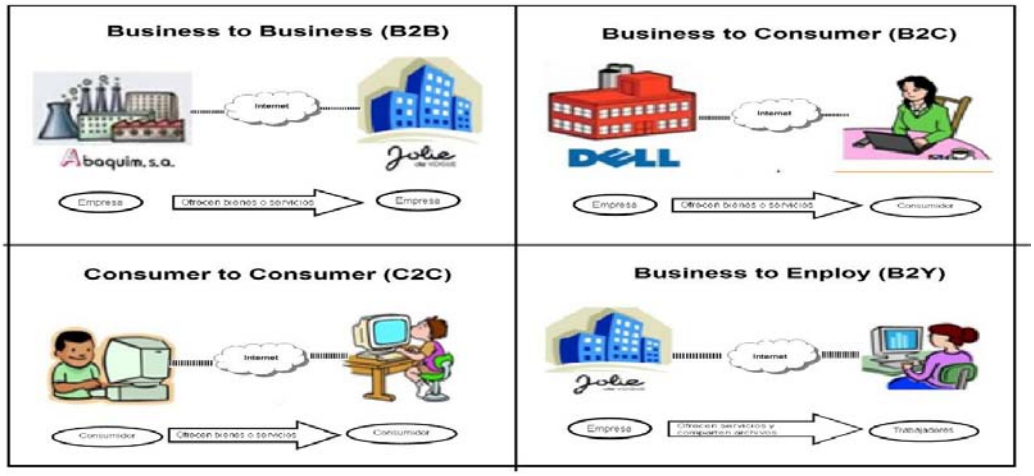

Ilustración 1. Tipos de Comercio Electrónico.

[12] *Vid.* MICROSOFT CORPORATION, Diccionario de Informática e Internet de Microsoft, 2ª edición, Editorial McGraw-Hill, Madrid, 2005, p. 169.
[13] *Vid.* FERNÁNDEZ GÓMEZ, Eva, Comercio Electrónico, Editorial McGraw-Hill, Madrid, 2002, p. 96.

Así pues, entendemos que el comercio electrónico es el intercambio de bienes, servicios e información mediante redes de comunicación, en el cual no existe una reunión física entre quien ofrece el bien o servicio y quien los demanda, donde al igual que cualquier otro tipo de comercio se tiene como finalidad obtener un lucro para el iniciador y la satisfacción de una necesidad para el destinatario.

1.1.4 Antecedentes del comercio electrónico.

El origen del comercio electrónico o *electronic comerse, e-commerce o comerse*, estos últimos términos acuñados por el derecho anglosajón, como alude el jurista Óscar Vásquez del Mercado[14] se remonta a la década de los 60´s en los Estados Unidos de América cuando varias empresas acordaron conectar sus computadoras para el intercambio de información denominado Intercambio Electrónico de Información conocido como EDI, esto con la finalidad de fortalecer la calidad de los datos que estas empresas intercambiaban con otros miembros de la cadena de proveedores así como satisfacer sus necesidades de aceleración y control de procesos, reducción de los costos administrativos de organizaciones empresariales y gubernamentales.

Posteriormente en la década de los 70´s se dio la Transferencia Electrónica de Fondos (TEF), esto se llevó a cabo a través de redes de seguridad privadas dentro de las instituciones financieras, lo cual trajo como consecuencia la expansión del uso de tecnologías de telecomunicación para propósitos comerciales, lo cual permitió el desarrollo del intercambio computador a computador de la información operacional comercial en el área financiera.

---

[14] *Vid.* REYES DÍAZ, Carlos Humberto (coord.), Temas Selectos de Comercio Internacional, Editorial Porrúa, México, 2008, p. 488.

Pero el comercio electrónico como lo conocemos ahora inició años después del surgimiento del Internet, ya que en un principio, en el año de 1969, el Internet surgió como un proyecto de estrategia militar de Estados Unidos durante la Guerra Fría, conocido entonces como red ARPANet (*Advanced Research Projets Administration Network*). Después de la guerra, el Internet fue utilizado para fines educativos y de investigación, fue hasta muchos años después, y con la invención del *World Wide Web,* que inició la compra y venta de bienes y servicios a través de la red de Internet, conocido entonces como comercio en la red.

No obstante lo anterior, el escritor Eloy Seoane Balado[15] explica que la historia del comercio electrónico, como se le conoce actualmente, puede ser dividida en cuatro etapas, las cuales son:

- Primera generación: en el año de 1993 las grandes empresas crean páginas web que hablaban solo de su organización; con posterioridad aparecen los primeros catálogos en la red, aunque en esta primera etapa no se puede comprar a través de la red.
- Segunda generación: en esta fase se comienza a comprar a través de la red; de igual manera aparecen los centros comerciales virtuales, en cuanto a los medios de pago se suelen emplear el pago contra reembolso, cheques, transferencias y pagos mediante tarjeta electrónica.
- Tercera generación: en ésta, para automatizar el proceso de selección y envío de los datos acerca de los productos comprados se implementan bases de datos junto con aplicaciones web. Aparecen los primeros contenidos dinámicos y el pago se realiza por medio de tarjetas.
- Cuarta generación: se mejora la seguridad de los sitios en la red y se implementan diversos mecanismos de pago, así como los servicios de seguimiento del pedido desde que se acepta hasta que se entrega al usuario.

[15] *Vid.* SEOANE BALADO, Eloy, La Nueva Era del Comercio: El Comercio Electrónico, Ideaspropias Editorial, España, 2005, p. 10 [En línea]. Disponible: http://books.google.com.mx/books?id=evLz521ZVmAC&printsec=frontcover&hl=es#v=onepage&q&f=false 7 de Septiembre de 2013. 17:45 PM.

En este período aparecen las primeras legislaciones sobre comercio electrónico.

Esta última es la más importante, ya que es la que abarca los últimos años cuando fueron adoptadas las Leyes Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional sobre comercio electrónico y sobre firmas electrónicas.

Posteriormente, éstas fueron adaptadas a las legislaciones mexicanas en el año 2000 y 2003 respectivamente; y que se ven reflejadas en las reformas realizadas en estos años en el Código de Comercio, así como en el Código Civil Federal, Código Federal de Procedimientos Civiles y en la Ley Federal de Protección al Consumidor.

1.2 Entidades de Certificación.

A pesar de que se habla en el punto 1.3.9 de este capítulo y en los siguientes apartados más detalladamente sobre las entidades de certificación, a continuación observamos cuales son los antecedentes que dieron nacimiento al compendio normativo que actualmente regula a estas entidades.

1.2.1 Antecedentes de las Entidades de Certificación.

Las entidades de certificación, prestadores de servicios de certificación o autoridades certificadoras son personas físicas o morales e incluso instituciones públicas cuya principal función es expedir certificados de firma electrónica, así como prestar otros servicios inherentes a estas últimas.

En cuanto a sus antecedentes, estos se encuentran entrañablemente relacionados con los del comercio electrónico, esto debido a que para que

pudieran existir las entidades de certificación tuvo que nacer primero el comercio electrónico.

El primer antecedente es la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional sobre Firmas Electrónicas, ésta fue creada el 12 de diciembre de 2001, con la finalidad de complementar algunos aspectos relacionados con las firmas electrónicas en la Ley Modelo sobre Comercio Electrónico, de la cual se habla más a detalle en el capítulo segundo, basta destacar que ésta fue la primera normatividad en hablar de entidades de certificación y la base de las modificaciones en la legislación mexicana sobre el tema.

Dichas modificaciones se plasmaron en el Código de Comercio, con las reformas en materia de firma electrónica publicadas en el Diario Oficial de la Federación el 29 de agosto del 2003, las cuales entraron en vigor el 27 de noviembre del mismo año. Con posterioridad el 19 de julio 2004 se publicó en el mismo Diario el Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación.

El mismo año que se publicó el reglamento antes mencionado, y siguiendo lo dispuesto en los artículos 102 inciso A) fracción V, 114 fracción IV y 113 del Código de Comercio en los cuales se señalaba que la Secretaría de Economía establecería las Reglas Generales, se publicaron dichas reglas el 10 de agosto en el Diario Oficial de la Federación.

El último antecedente es la divulgación de la Ley Federal de Derechos, en cuyo artículo 78, se prevé el cobro de derechos por la acreditación de los prestadores de servicios de certificación de firma electrónica.

Como se puede observar de los antecedentes antes mencionados, a pesar de que la ley modelo fue publicada en el 2001 las reformas en la

legislación mexicana se comenzaron a realizar hasta el año 2003, todos estos antecedentes se estudian más a fondo en el siguiente capítulo.

1.3 Conceptos básicos.

Debido a la complejidad técnica que tiene el comercio electrónico es necesario conocer los términos utilizados en este tipo de comercio para entender mejor tanto su funcionamiento como el de las entidades de certificación; a continuación se definen algunos de ellos.

1.3.1 Computadora o computador.

La computadora, computador u ordenador es definido, por el Doctor Julio Téllez Valdés como: "una máquina electrónica capaz de procesar información siguiendo instrucciones almacenadas en programas."[16]

Otra definición es la que nos proporciona la Asociación Mexicana de Internet (AMIPCI) la cual señala que es: "una máquina electrónica capaz de procesar información en modo digital."[17]

En el mismo tenor, el Diccionario de Informática e Internet de Microsoft[18] la concibe como el dispositivo que es apto para procesar información y con ello producir el resultado deseado por el usuario, estos aparatos se clasifican según su tamaño, generación o modo de procesamiento; pero sin importar esto procesan la información en 3 pasos, los cuales son: aceptación de la entrada; procesamiento de la entrada según las reglas; y producción de la salida.

---

[16] TÉLLEZ VALDÉS, Julio, *Op. Cit.* p. 454.
[17] Asociación Mexicana de Internet, Glosario de Términos, [En línea]. Disponible: http://www.amipci.org.mx/?P=glosario 13 de Agosto de 2013. 17:00 PM.
[18] *Vid.* MICROSOFT CORPORATION, *Op. Cit.* p. 178.

Por su parte, el Diccionario de la Real Academia de la Lengua Española, manifiesta que es: "la máquina electrónica, analógica o digital, dotada de una memoria de gran capacidad y de métodos de tratamiento de la información, capaz de resolver problemas matemáticos y lógicos mediante la utilización automática de programas informáticos."[19]

En términos informáticos, el Diccionario Larousse[20] la concibe como la máquina cuya función es el tratamiento de la información a través de programas constituidos por una amplia sucesión de operaciones aritméticas y lógicas.

Es decir, el computador es una máquina eléctrica que procesa información de acuerdo a las instrucciones que se encuentran almacenadas en programas informáticos, con la finalidad de producir un resultado deseado por el usuario.

1.3.2 Software.

En el glosario citado por el jurista Julio Téllez Valdés se refiere al *software* como: "los programas o elementos lógicos que hacen funcionar una computadora o una red, o que se ejecutan en ellos, en contraposición con los componentes físicos del computadora o red" [21]

De forma más simple, el Diccionario de Términos de Informática e Internet[22] señala que es la palabra inglesa que se utiliza para referirse a los programas que se encuentran instalados y almacenados en una computadora u ordenador.

---

[19] Real Academia Española, Diccionario de la Lengua Española, [En línea]. Disponible: http://lema.rae.es/drae/?val=computadora 12 de Noviembre de 2013. 14:30 PM.
[20] *Vid.* LUCENA CAYUELA, Núria (coord.), *Op. Cit.* p. 271.
[21] TÉLLEZ VALDÉS, Julio, *Op. Cit.* p. 496.
[22] ALARCÓN ÁLVAREZ, Enrique de, Diccionario de Términos Informáticos e Internet, 3ª edición, Editorial Anaya Multimedia, Madrid, 2004, p. 343.

Por su parte la Asociación Mexicana de Internet (AMIPCI) lo define como: "los programas o elementos lógicos que hacen funcionar un ordenador o una red, o que se ejecutan en ellos, en contraposición con los componentes físicos del ordenador o la red, agrupados bajo el nombre de *hardware*." [23]

Coincidiendo con esta definición, el teorizante Oscar Rodrigo González López, lo concibe como: "programas o elementos lógicos que hacen funcionar un ordenador o una red, o que se ejecutan en ellos, en contraposición con los componentes físicos del ordenador o la red."[24]

En el mismo enfoque, la escritora Eva Fernández Gómez, expresa que: "a diferencia del *hardware*, es lo que no se ve, es decir los programas y aplicaciones que están guardadas en un disco duro, CD-ROM o disquetes."[25]

Como se ve el *software* son los programas que se encuentran instalados en la computadora y por medio de los cuales ejecuta sus funciones, estos programas no son tangibles a diferencia del *hardware* que vemos a continuación.

1.3.3 Hardware.

El Doctor Julio Téllez Valdés define al *hardware* como: "los componentes físicos de un computadora o de una red, en contraposición con los programas o elementos lógicos que los hacen funcionar"[26]

De igual forma, el Diccionario de Términos Informáticos e Internet indica que es: "un conjunto de piezas físicas que forman un sistema informático o

---

[23] Asociación Mexicana de Internet, *Op. Cit.* 25 de Agosto de 2013.13:20 PM.
[24] GONZÁLEZ LÓPEZ, Óscar Rodrigo, Comercio Electrónico, Ediciones Anaya Multimedia, España, 2002, p. 358-359.
[25] FERNÁNDEZ GÓMEZ, Eva, *Op. Cit.* p. 168.
[26] TÉLLEZ VALDÉS, Julio, *Op. Cit.* p. 470.

dicho de otra forma cada una de las partes físicas que componen un ordenador, incluidos sus periféricos."[27]

La investigadora Eva Fernández Gómez se refiere al *hardware* como: "todos aquellos componentes físicos de un computador, todo lo visible y tangible. Por extensión, se aplica también a otros componentes electrónicos que no necesariamente forman parte de un computador."[28]

De manera sencilla, el Diccionario de la Real Academia de la Lengua Española, señala que son: "conjunto de los componentes que integran la parte material de la computadora"[29]

Por tanto, el *hardware* son los dispositivos físicos de la computadora, por ejemplo el teclado, el mouse o el monitor. A diferencia del *software*, el hardware es tangible, es la parte de la computadora que podemos tocar y manipular.

1.3.4 Internet.

De acuerdo con el Diccionario de Términos de Informática e Internet[30], la palabra *Internet* proviene de la unión de las palabra inglesas *INTERnational* y *NETwork*, que unidas significan red internacional. Y se refiere a la gigantesca red internacional creada a partir de la conexión de millones de redes informáticas que permiten la comunicación entre los usuarios alrededor del mundo.

---

[27] ALARCÓN ÁLVAREZ, Enrique de, *Op. Cit.* p. 175.
[28] FERNÁNDEZ GÓMEZ, Eva, *Op. Cit.* p. 165.
[29] Real Academia Española, Diccionario de la Lengua Española, [En línea]. Disponible: http://lema.rae.es/drae/?val 12 de Noviembre de 2013. 14:30 PM.
[30] *Vid.* ALARCÓN ÁLVAREZ, Enrique de, *Op. Cit.* p. 198.

De forma simple, la estudiosa Eva Fernández Gómez lo define como: "una red global de redes que conectan toda clase de ordenadores usando el protocolo *Internet* para compartir servicios y comunicarse."[31]

Haciendo más referencia a su historia que a su concepto, el doctrinario Julio Téllez Valdés menciona que: "una *internet* (con i minúscula) es un conjunto de redes. Red de telecomunicaciones nacida en 1969 en los Estados Unidos, a la cual están conectados centenares de millones de personas, organismos y empresas de todo el mundo, cuyo rápido desarrollo tiene importantes efectos sociales, económicos y culturales, convirtiéndose de esta manera en uno de los medios más influyentes de la sociedad de la información y en la autopista de la información por excelencia. Fue conocida como ARPANET hasta 1974."[32]

Por su parte la Asociación Mexicana de Internet (AMIPCI) manifiesta que: "una internet (con i minúscula) es un conjunto de redes conectadas entre sí. Internet es la mayor red de interconexiones de redes del mundo. Tiene una jerarquía de tres niveles formados por redes de eje central (*backbones* como por ejemplo *NSFBET* y *MILNET*), redes de nivel intermedio, y redes aisladas (*stub networks*). Internet es una red multiprotocolo, que permite a todos sus usuarios la utilización de sus servicios (*World Wide Web*, correo electrónico, grupos de noticias, etc.) por medio de la simple conexión a uno de los millones de servidores que proporcionan acceso a la red."[33]

En conclusión Internet, es un conjunto de redes conectadas entre sí que permite la comunicación entre sus usuarios en todo el planeta. En el entendido de que, como lo expresa la Asociación Mexicana de Internet[34,] una red es un sistema de comunicación de datos, compuestos por diversos elementos de

[31] FERNÁNDEZ GÓMEZ, Eva, *Op. Cit.* p. 165.
[32] TÉLLEZ VALDÉS, Julio, *Op. Cit.* p. 475.
[33] Asociación Mexicana de Internet, *Op. Cit.* 19 de Septiembre de 2013. 16:45 PM.
[34] *Vid. Ídem.*

hardware y *software*, que conecta entre sí sistemas de información situados en diferentes lugares.

Así, una red es un conjunto de dispositivos electrónicos conectados entre sí en todo el planeta, que a través del protocolo de Internet permite la comunicación entre sus usuarios y que los mismos accedan a todos los servicios que esta plataforma proporciona.

1.3.5 Web.

En cuanto a la definición de *web*, el investigador Julio Téllez Valdés explica que es: "un servidor de información www. Se utiliza también para definir el universo www en su conjunto." [35]

En el mismo tenor, la Asociación Mexicana de Internet (AMIPCI) señala que: "el término se utiliza para definir el universo del *world wide web*, los sitios, la información y los servicios de la telaraña. Han existido diversos intentos de imponer una traducción adecuada al español, pero continua utilizándose, sin más, *web*."[36]

Al contrario, el escritor Oscar Rodrigo González López se refiere a él como página web, expresando que: "es un documento escrito en un lenguaje, siendo el más común el HTML, y en la cual se recoge la información que quiere suministrar el propietario de dicha página."[37]

El Diccionario Larousse, expresa que la web es: "sistema lógico de acceso y búsqueda de la información disponible en Internet, cuyas unidades informáticas son las páginas web."[38]

---

[35] TÉLLEZ VALDÉS, Julio, *Op. Cit.* p. 504
[36] Asociación Mexicana de Internet, *Op. Cit.* 19 de Septiembre de 2013. 18:35 PM.
[37] GONZÁLEZ LÓPEZ, Oscar Rodrigo, *Op. Cit.* p. 38.
[38] LUCENA CAYUELA, Núria (coord.), *Op. Cit.* p. 1048.

Por lo tanto, la web son los sitios, la información y los servicios del Internet, es decir es el sistema que nos permite acceder a la información almacenada en el infinito universo de la www.

1.3.6 World Wide Web (WWW).

La Asociación Mexicana de Internet (AMIPCI) pondera que la *World Wide Web* (www) es: "un sistema de información distribuido, basado en hipertexto, creado a principios de los años noventa por Tim Berners-Lee, investigador en el CERN, Siuza. La información puede ser de cualquier formato (texto, gráfico, audio, imagen fija o en movimiento) y es fácilmente accesible a los usuarios mediante los programas navegadores. La popularización del WWW facilitó en gran medida el acceso masivo del público a Internet."[39]

Por el contrario, la intelectual Eva Fernández Gómez la llama telaraña de cobertura mundial, la cual define como: "un sistema de distribución de información en hipertexto que permite a los usuarios crear, navegar o editar documentos en hipertexto."[40]

Por su parte, el Diccionario de Informática e Internet de Microsoft explica que la triple W es: "el conjunto completo de documentos de hipertexto intervinculados contenidos en los servidores HTTP repartidos por todo el mundo."[41]

Así pues, la triple w es un sistema de información creado en los años 90´s la cual facilitó el acceso masivo del público a Internet, ya que por medio de hipertextos permite a los usuarios acceder a la información sin importar el formato en el que se encuentre, así como crear o modificar dichos hipertextos.

---

[39] Asociación Mexicana de Internet, *Op. Cit.* 22 de Septiembre de 2013. 14:45 PM.
[40] FERNÁNDEZ GÓMEZ, Eva, *Op. Cit.* p. 169.
[41] MICROSOFT CORPORATION, *Op. Cit.* p. 817.

1.3.7 Iniciador.

El jurista Arturo Díaz Bravo al hacer referencia a iniciador o emisor, refiere que es: “la persona física o jurídica que, conforme al mensaje de datos, actúe a nombre propio o en cuyo nombre se envíe o genere el mensaje, siempre que no actúe a título de intermediario.”[42]

En el mismo enfoque, el estudioso Víctor Manuel Rojas Amandi señala que es: “quien genera un mensaje de datos directamente o a cuyo nombre se ha programado una terminal informática que es capaz de generar automáticamente mensajes de datos sin intervención humana directa.”[43]

De acuerdo con la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional sobre Firmas Electrónicas, se debe entender por iniciador a toda persona que, a tenor del mensaje, haya actuado por su cuenta o en cuyo nombre se haya actuado para enviar o generar ese mensaje antes de ser archivado, si éste es el caso, pero que no haya actuado a título de intermediario con respecto a él.

En el mismo tenor el artículo 89 del Código de Comercio, lo denomina emisor y puntualiza que es toda persona que, al tenor del mensaje de datos, haya actuado a nombre propio o en cuyo nombre se haya enviado o generado ese mensaje antes de ser archivado, si éste es el caso, pero que no haya actuado a título de Intermediario.

---

[42] DÍAZ BRAVO, Arturo, Contratos Mercantiles, 9ª Edición, IURE Editores, México, 2008, p. 76.

[43] ROJAS AMANDI, Víctor Manuel, Regulación del Comercio Electrónico en México, Anuario de Derecho de la Universidad Iberoamericana, anual, número 30, México, 2000, p. 391 [En línea]. Disponible: http://www.juridicas.unam.mx/publica/librev/rev/jurid/cont/30/cnt/cnt16.pdf 13 de Noviembre de 2013. 18:35 PM.

Entonces, el iniciador o emisor de un mensaje de datos es aquella persona que expida por cuenta propia o que en su nombre se envíe o haya generado un mensaje de datos, pero un intermediario no podrá ser iniciador en este tipo de comercio.

1.3.8 Destinatario.

El destinatario, que puede ser la parte que confía, es definido por el doctrinario Arturo Díaz Bravo como: "la persona a la que se dirige el mensaje de datos."[44]

Por su parte, el teórico Víctor Manuel Rojas Amandi lo describe como: "la persona con quien el iniciador tiene la intención de comunicarse mediante la transmisión del mensaje."[45]

Ambos definiciones coinciden con lo dispuesto en la Ley Modelo sobre Firmas Electrónicas, ya que dicho ordenamiento concibe al destinatario como la persona designada por el iniciador para recibir el mensaje, pero que no esté actuando a título de intermediario con respecto a él.

Coincidiendo con ello, el artículo 89 del Código de Comercio define al destinatario como la persona designada por el emisor para recibir el mensaje de datos, pero que no esté actuando a título de Intermediario con respecto al mismo.

Entonces, el destinatario de un mensaje de datos es aquella persona a la que el iniciador o emisor le envía y además lo ha designado para recibir el mensaje de datos, al igual que en el caso del iniciador, el emisor no puede ser un intermediario.

---

[44] DÍAZ BRAVO, Arturo, *Op. Cit.* p. 76.
[45] ROJAS AMANDI, Víctor Manuel, *Op. Cit.* p. 391.

1.3.9 Prestador de servicios de certificación.

Como quedó señalado en el apartado 1.2.1 de este capítulo, los prestadores de servicios de certificación son entidades públicas o privadas que realizan servicios relacionados con la firma electrónica.

La Maestra Soyla León Tovar manifiesta que es: "una persona física o moral (persona física, solamente en el caso de notarios públicos o corredores públicos) o una institución pública debidamente acreditada para prestar servicios de verificación de identidad de firmantes y su vinculación con los medios de identificación electrónica."[46]

El Doctor Alfredo Alejandro Reyes Krafft, citando a la Comisión Europea, explica que el cometido de las autoridades de certificación es: "autentificar la propiedad y las características de una clave pública, de manera que resulte digna de confianza, y expedir certificados."[47]

Siguiendo con las definiciones doctrinales, la Licenciada Eva Fernández refiere que una autoridad de certificación es: "la entidad encargada de establecer y garantizar la identidad de un remitente, así como de emitir y gestionar firmas digitales."[48]

Dentro del enfoque legislativo, la Ley Modelo sobre Firmas Electrónicas menciona que se entiende como prestador de servicios de certificación a la persona que expide certificados y puede prestar otros servicios relacionados con las firmas electrónicas.

---

[46] LEÓN TOVAR, Soyla H., La Firma Electrónica Avanzada, 1ª Reimpresión, Oxford University Press, México, 2006, p. 111
[47] REYES KRAFFT, Alfredo Alejandro, La Firma Electrónica y las Entidades de Certificación, Editorial Porrúa, México, 2003, p. 172
[48] FERNÁNDEZ GÓMEZ, Eva, *Op Cit.* p. 161.

En términos semejantes, la Ley de Comercio Electrónico colombiana, citada por el jurista Julio Téllez Valdés, dispone que es: "la persona que, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrece o facilita los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales."[49]

Otra definición legislativa es la referida en la Ley de Firmas y Certificados Digitales de Perú, igualmente citada por el doctrinario antes mencionado, la cual explica que: "una entidad de registro o verificación cumple con la función de levantamiento de datos y comprobación de la información de un solicitante de certificado digital; identificación y autentificación del suscriptor de firma digital; aceptación y autorización de solicitudes de emisión y cancelación de certificados digitales."[50]

Por su parte la legislación mercantil de nuestro país instaura, en el artículo 89 del Código de Comercio, que el prestador de servicios de certificación es la persona o institución pública que preste servicios relacionados con firmas electrónicas y que expide los certificados digitales, en su caso.

En conclusión, un prestador de servicios de certificación es la persona física o moral que emite certificados digitales y que además se encarga de confirmar la identidad del firmante, con respecto a su firma electrónica, en un mensaje de datos. Esta entidad se analiza más detalladamente en el capítulo tercero del presente trabajo de investigación.

[49] TÉLLEZ VALDÉS, Julio, *Op. Cit.* p. 206
[50] *Ídem.*

1.3.10 Mensaje de datos.

En términos de comercio electrónico, la jurista Soyla León Tovar[51] señala que el mensaje de datos es el medio por el cual se expresa la voluntad de las partes, con el efecto de crear, modificar o extinguir derechos y obligaciones, es decir, es el equivalente al documento escrito.

En el mismo tenor, pero de forma técnica, el Doctor Alfredo Reyes Krafft postula que es: "la información generada, enviada, recibida o archivada o comunicada por medio electrónicos, ópticos o similares como son el intercambio electrónico de datos, el correo electrónico, telegrama, télex o telefax."[52]

El escritor Víctor Manuel Rojas Amandi[53] explica que el mensaje de datos utilizado en el comercio electrónico, independientemente de la tecnología utilizada para crearlo, archivarlo o transmitirlo, es el soporte informático que consigna la manifestación de la voluntad de las partes.

Por su parte, el artículo 89 del Código de Comercio describe como mensaje de datos a la información generada, enviada, recibida o archivada por medios electrónicos, ópticos o cualquier otra tecnología.

En cuanto a las personas que intervienen en el mensaje de datos, estas son:

a) Emisor o iniciador: es la persona que a nombre propio o a cuyo nombre se haya creado y enviado un mensaje de datos.

b) Destinatario: es la persona designada por el emisor para recibir el mensaje de datos.

---

[51] *Vid.* LEÓN TOVAR, Soyla H., *Op. Cit.* p. 67

[52] REYES KRAFFT, Alfredo Alejandro, *Op. Cit.* p. 164

[53] *Vid.* ROJAS AMANDI, Víctor Manuel, *Op. Cit.* p. 391, 13 de Noviembre de 2013. 18:35 PM.

c) Intermediario: es la persona que envía, recibe o archiva un mensaje de datos determinado, siempre que actué por cuenta de otra persona.

d) Prestador de servicios de certificación: es la entidad que presta servicios relacionados con la firma electrónica y expide certificados de la misma.

e) Parte que confía: es la persona que siendo o no el destinatario, actúa basándose en un certificado o una firma electrónica.

Todas las personas señaladas pueden o no intervenir en un mensaje de datos; pero deberán existir en el mensaje el emisor y el destinatario, además de algún elemento para que el mensaje pueda ser vinculado a ambas partes, generalmente una firma electrónica, porque de lo contario el mensaje de datos no tendrá efectos jurídicos plenos.

Entonces, el mensaje de datos es toda información que sea creada y transmitida entre el iniciador y el destinatario, sin importar la tecnología que utilicen, y que con posterioridad serán archivados.

1.3.11 Certificado digital.

El certificado digital es definido, por el Grupo de Estudios en Internet, Comercio Electrónico y Telecomunicaciones e Informática de la Universidad de los Andes como la: “acreditación emitida por una entidad o un particular debidamente autorizado garantizando que determinado dato (por ejemplo, una firma electrónica o una clave pública) pertenece realmente a quien se supone.”[54]

Por su parte, el jurista Alfredo Reyes Krafft menciona que los certificados digitales: “atestigua la validez de la identidad de un individuo o entidad.

[54] CASTRO F., Juan Alberto (ed.), Comercio Electrónico, Editorial Legis, Colombia, 2005, p. 75

Generalmente es emitido por una Autoridad Certificadora quien al firmar digitalmente une una llave con el nombre de un individuo o entidad"[55]

La Maestra Soyla León Tovar señala que un certificado digital: "es el conjunto de información única, almacenada y procesada electrónicamente que identifica, verifica y autentifica a un usuario como parte del proceso de generación de su firma electrónica"[56]

Pero en un enfoque legislativo, tanto la Ley Modelo sobre Firmas Electrónicas como el Código de Comercio disponen que se entiende por certificado todo mensaje de datos u otro registro que confirme el vínculo entre un firmante y los datos de creación de la firma.

En relación con el mensaje de datos y el certificado digital, la Licenciada Eva Fernández Gómez[57], refiere que funcionan de la siguiente manera: una vez que se ha obtenido el certificado, éste que contiene la clave pública será enviado junto con el mensaje cifrado con la clave privada al destinatario del mensaje el cual podrá descifrarlo utilizando la clave pública; de esta forma el destinatario tiene la seguridad de que el mensaje fue enviado por el emisor. Tal y como se aprecia en el siguiente esquema:

Ilustración 2. Funcionamiento del mensaje de datos y certificado digital.

[55] REYES KRAFFT, Alfredo Alejandro, *Op. Cit.* p. 190
[56] LEÓN TOVAR, Soyla H., *Op. Cit.* p. 120
[57] *Vid.* FERNÁNDEZ GÓMEZ, Eva, *Op. Cit.* p. 118

Como se observa, un certificado digital es un documento emitido por una autoridad de certificación, en el cual confirma la vinculación del firmante con los datos de creación de la firma. Es decir, un certificado atestigua que la firma pertenece al individuo o entidad que dice ser.

1.3.12 Firma.

La palabra firma tiene su origen en la palabra latina *firmare* que significa afirmar o dar fuerza. Con base en dicha palabra el diccionario de la Real Academia de la Lengua Española la define como: "el nombre y apellido, o título, que una persona escribe de su propia mano en un documento para darle autenticidad o para expresar que aprueba su contenido."[58]

En cambio, el Licenciado Alfredo Baltierra Guerrero asevera que la firma autógrafa es: "el signo distintivo de la persona jurídica que lo estampa (ya sea por sí tratándose de personas físicas, o por medio de sus representantes legales, tratándose de personas morales), con el ánimo de obligarse, esto es, de adherirse al postulado del escrito, de indicar su consentimiento expreso con el contexto de que se trate."[59]

Por otra parte, la jurista Lizbeth Barreto Zúñiga puntualiza que la firma manuscrita desde el punto de vista jurídico es: "el signo distintivo de la persona que lo estampa, con el ánimo de adherirse al postulado del escrito e indicar su consentimiento expreso con el contexto de que se trate."[60]

---

[58] Real Academia Española, *Op. Cit.* 12 de Enero de 2014. 13:40 PM.
[59] BALTIERRA GUERRERO, Alfredo, La Firma Autógrafa en el Derecho Bancario, Revista de la Facultad de Derecho de México, número 121-122-123, Enero-Junio 1982, p. 17-18 [En línea] Disponible: http://www.juridicas.unam.mx/publica/librev/rev/facdermx/cont/121/pr/pr3.pdf 12 de Enero de 2014. 16:25 PM.
[60] BARRETO ZÚÑIGA, Lizbeth Angélica, Evolución de la Firma Autógrafa a la Firma Electrónica Avanzada, Revista Digital Universitaria, mensual, volumen 12, número 3, marzo 2011, p. 4-xx [En línea] Disponible: http://www.revista.unam.mx/vol.12/num3/art34/art34.pdf 12 de Noviembre de 2013. 17:45 PM.

En el mismo sentido, el doctrinario Alfredo Reyes Krafft refiere que la firma es: “el conjunto de letras y signos entrelazados, que identifican a la persona que la estampa, con un documento o texto.”[61] Además, señala que la firma es “una inscripción que indica el nombre de una persona que entiende hacer suyas las declaraciones del acto.”[62]

Al hacer referencia a la firma autógrafa el jurista Miguel Acosta Romero, citado por el Doctor Alfredo Reyes Krafft, señala que es: “la que suscribe la persona física con su propia mano y consiste en un conjunto de letras o bien algún componente de su nombre y a veces el nombre y apellido, aunado a una serie de trazos que pueden abarcar toda gama de evoluciones del instrumento de escritura, que señalan e identifican al sujeto y lo separan de otros, en los documentos que suscribe y es un elemento que refleja permanentemente su voluntad de expresar lo que firma, o de obligarse al tenor del texto que suscribe.”[63]

Así, la firma manuscrita es el nombre y apellido, título o un conjunto de letras que junto a una serie de trazos, plasma una persona física con su propia mano al final de un documento, en el caso de la persona moral, a través de su representante legal. Esta firma es la forma por medio de la cual una persona expresa su voluntad o se obliga a lo contenido en el documento en el cual es escrita.

1.3.13 Firma electrónica.

La firma electrónica es definida por el doctrinario Alfredo Reyes Krafft como: “los datos en forma electrónica consignados en un mensaje de datos o adjuntados o lógicamente asociados al mismo, que pueden ser utilizados para

---

[61] REYES KRAFFT, Alfredo Alejandro, *Op. Cit.* p. 87.
[62] *Ibídem.,* p. 88.
[63] *Ibídem.*, p. 87.

identificar y/o vincular al firmante en relación con el mensaje de datos, en forma equivalente a la firma manuscrita."[64]

Otra definición es la que refiere la Licenciada Lizbeth Barreto Zúñiga, la cual señala que es: "el conjunto de datos electrónicos, unido a un documento electrónico y utilizado cuando un emisor envía un mensaje al receptor, y dicho mensaje va cifrado, de manera que nadie pueda modificarlo ni alterarlo. Su finalidad es, además, identificar al sujeto que la utiliza."[65]

Por otra parte, el jurista Arturo Díaz Bravo la concibe como: "los datos electrónicamente consignados en un mensaje de datos o acompañados al mismo mediante empleo de cualquier tecnología, que se utilicen para identificar al firmante y dejar indicado que aprueba la información respectiva, de tal manera que tal conjunto de datos deberá producir los mismos efectos jurídicos que la firma autógrafa y, por tanto, serán admisibles como prueba en juicio."[66]

Asimismo, la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional sobre Firma Electrónica, señala que por firma electrónica se entenderán los datos en forma electrónica consignados en un mensaje, adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mismo.

Dicha percepción fue adoptada por la legislación mexicana, quedando plasmada en el artículo 89 del Código de Comercio, añadiendo a la misma que la firma electrónica produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio.

---

[64] *Ibídem.* p. 164.
[65] BARRETO ZÚÑIGA, Lizbeth Angélica, *Op. Cit.* p. 5-xx
[66] DÍAZ BRAVO, Arturo, *Op. Cit.* p. 77.

De acuerdo con la Maestra Soyla León Tovar[67], existen dos tipos de firmas electrónicas reconocidas por la legislación mexicana, las cuales son:

a) La firma electrónica simple: es de la que se ha estado hablando en este apartado y cuya definición ya se mencionó.

b) La firma electrónica avanzada: esta firma es parecida a la firma electrónica simple con la diferencia de que esta es creada bajo un método más seguro de autenticación e identificación del firmante.

La firma electrónica es creada utilizando técnicas criptográficas basadas en logaritmos matemáticos de menor y mayor complejidad en relación con el cifrado, que en este caso es simétrico, el cual convierte un mensaje legible en ilegible, así los terceros que desconozcan la clave para descifrarlo no podrán conocer el contenido del mismo.

De esta forma, en el método simétrico se puede encriptar y desencriptar comunicaciones con la misma llave, que deberá ser conocida por el emisor y el receptor, por ello se requiere que exista confianza entre las partes y del medio por el cual intercambiaran datos.

Ilustración 3. Clave simétrica.

Tomando como referencia estas definiciones, la firma electrónica simple son los datos que ya sea que se encuentren en el mensaje de datos, adjuntos o asociados a él, se utilizan para identificar al firmante con relación al mismo, y con lo cual el firmante expresa su voluntad.

[67] LEÓN TOVAR, Soyla H., *Op. Cit.* p. 99

1.3.14 Firma electrónica avanzada.

En lo referente a la firma electrónica avanzada, fiable o reconocida, la Maestra Soyla León describe a la misma como un: "conjunto o bloque de caracteres, códigos o claves criptográficas privadas, en forma electrónica, que viajan junto, asociado o anexado a un documento digital, y mediante el cual se acredita quien es el autor o emisor del mismo."[68]

En un enfoque diferente, el teórico Alfredo Reyes Krafft señala que es: "la firma electrónica que permite la identificación del firmante y ha sido generada bajo su exclusivo control, conocido también como firma digital, que vincula exclusivamente al mismo con el mensaje de datos al que se adjunta o se asocia, lo que permite que sea detectable cualquier modificación ulterior de éste."[69]

El Servicio de Administración Tributaria (por sus siglas SAT) menciona que la firma electrónica avanzada (FIEL) es: "un conjunto de datos que se adjuntan a un mensaje electrónico, cuyo propósito es identificar al emisor del mensaje como autor legítimo de éste, tal y como si se tratara de una firma autógrafa."[70]

Es decir, la firma electrónica avanzada, es parecida a una firma electrónica simple, la diferencia radica en que la primera permite identificar al firmante del mensaje de datos con mayor certeza y confiabilidad.

---

[68] *Ibídem*. p. 99.
[69] REYES KRAFFT, Alfredo Alejandro, *Op. Cit.* p. 164.
[70] Servicio de Administración Tributaria, Qué es y para qué sirve la firma electrónica avanzada, [En línea] Disponible: http://www.sat.gob.mx/sitio_internet/e_sat/tu_firma/60_11498.html 26 de Octubre de 2013. 16:25 PM.

El Código de Comercio establece que para que una firma sea considerada como firma electrónica avanzada, ésta debe cubrir los requisitos señalados en su artículo 97, los cuales son:

1. Los Datos de Creación de la Firma, en el contexto en que son utilizados, corresponden exclusivamente al Firmante.
2. Los Datos de Creación de la Firma estaban, en el momento de la firma, bajo el control exclusivo del Firmante.
3. Es posible detectar cualquier alteración de la Firma Electrónica hecha después de que esta sea plasmada en el mensaje de datos.
4. Respecto a la integridad de la información de un Mensaje de Datos, es posible detectar cualquier alteración de ésta hecha con posterioridad a la colocación de la firma.

Luego, la firma electrónica avanzada o fiable en términos del artículo 89 es una firma electrónica cuyos datos de creación son exclusivos del firmante y están bajo el control de él al momento de firmar; además de que es posible detectar si la firma electrónica es alterada o si el mensaje de datos sufrió alguna modificación después de firmado.

Lo que hace más confiable a esta firma a diferencia de la firma electrónica simple, es su diseño ya que está creada bajo una tecnología de infraestructura de clave pública (en inglés *Public Key Infrastructure* o PIK); en este tipo de infraestructura se crean dos claves por medio de criptografía asimétrica, este sistema convierte el mensaje a una forma aparentemente incomprensible y posteriormente lo regresa a su forma original.

El Servicio de Administración Tributaria[71] describe que estas claves son:

1. Clave privada: solo el firmante la conoce y sirve para cifrar los datos.

2. Clave pública: es la que conocen todas las personas que la requieran para descifrar los datos de la firma.

[71] *Vid. Ídem.*

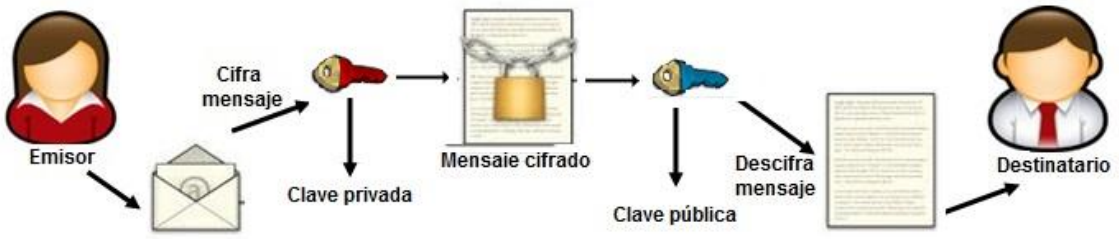

Ilustración 4. Clave asimétrica.

Es por este sistema de claves que la firma digital, como lo postula la jurista Lizbeth Angélica Barreto Zúñiga[72], tiene las siguientes características:

a) Autenticación: se refiere a que con la firma electrónica avanzada es posible validar e identificar al firmante del mensaje de datos, por medio de la verificación de ambas claves.

b) Confidencialidad: la firma digital garantiza que solo las personas involucradas conocerán el contenido del mensaje de datos.

c) Integridad: los datos del mensaje se mantienen protegido de terceros, para que no puedan ser alterados o suprimidos.

d) No repudio: se refiere a que el iniciador del mensaje no podrá negar la emisión de dicho mensaje de datos, siempre y cuando este contenga su firma electrónica avanzada; esto sirve como una garantía para el destinatario de que dicho mensaje fue enviado por el firmante del mismo.

Por consiguiente, lo que hace diferentes a la firma electrónica avanzada de la firma electrónica simple es que:

- la firma electrónica avanzada exige una serie de elementos indispensables para ser considerada como tal, de lo contrario es una firma electrónica simple.
- la firma digital es más confiable y certera que la electrónica simple, esto debido a su diseño de dos claves, como se describió ya.

[72] *Vid.* BARRETO ZÚÑIGA, Lizbeth Angélica, *Op. Cit.* p. 7-xx, 12 de Noviembre de 2013. 17:45 PM.

1.3.15 Secretaría de Economía.

Las Secretarías de Estado, de acuerdo con el Diccionario Jurídico del Instituto de Investigaciones Jurídicas de la UNAM, son: "órganos que pertenecen a la administración pública centralizada, que auxilia directamente al titular del Poder Ejecutivo Federal."[73]

Es por ello, que la Secretaría de Economía es una dependencia del Poder Ejecutivo Federal, que se encuentra contemplada en el artículo 34 de la Ley Orgánica de la Administración Pública Federal, en el cual se dispone que las funciones de dicha Secretaría son, entre otras: formular y conducir las políticas generales de industria, comercio exterior, interior, abasto y precios del país; regular, promover y vigilar la comercialización, distribución y consumo de bienes y servicios; estudiar, proyectar y determinar los aranceles; regular, orientar y estimular las medidas de protección al consumidor; regular y vigilar la prestación del servicio registral mercantil.

Es por ello, que como la misma Secretaría de Economía[74] afirma su visión es ser una dependencia del gobierno federal que por medio de políticas públicas impulse la creación de empleos de calidad y el crecimiento económico de nuestro país.

Así que, la Secretaría de Economía es la dependencia del gobierno federal que se encarga de promover políticas públicas destinadas a generar empleos de calidad, a promover la competitividad de las empresas, para contribuir al desarrollo económico del país.

---

[73] Instituto de Investigaciones Jurídicas UNAM, Diccionario Jurídico Mexicano, Tomo 4. P-Z, Editorial Porrúa, México, 2005, p. 3419

[74] Secretaría de Economía, Misión y visión, [En línea] Disponible: http://www.economia.gob.mx/conoce-la-se/mision-y-vision-se 20 de Diciembre 2013. 14:35 PM.

En el caso del comercio electrónico y de las entidades de certificación, la Secretaría de Economía es la autoridad encargada, a través de su Dirección General de Normatividad Mercantil, de acreditar a los prestadores de servicios de certificación; realizar auditorías para vigilar que las entidades cumplan con sus obligaciones y sancionarlas en caso de ser necesario; emitir las reglas generales a las que están sujetas dichas entidades; además de actuar como autoridad certificadora de los prestadores de servicios de certificación.

1.3.16 Norma Oficial Mexicana.

Las Normas Oficiales Mexicanas (NOMS), como lo postula la jurista Carla Huerta Ochoa, desde el punto de vista de su naturaleza jurídica: "se configuran como normas jurídicas de carácter técnico, a pesar de ser expedidas por órganos de la administración pública."[75] Asimismo, señala que de acuerdo con su regulación son: "normas técnicas cuyo objetivo es uniformar determinados procesos, productos o servicios con el fin de proteger la vida, la seguridad y el medio ambiente."[76]

Por su parte, la fracción XI del artículo 3º de la Ley Federal sobre Metrología y Normalización, las define como la regulación técnica de observancia obligatoria que es expedida por una dependencia que sea competente en el ámbito en el que será expedida, que establece reglas, especificaciones, atributos, directrices, características o prescripciones aplicables a un producto, proceso, instalación, sistema, actividad, servicio, o método de producción u operación, así como las relacionadas con terminología, simbología, embalaje, marcado o etiquetado y las que se refieren a su cumplimiento o aplicación.

---

[75] HUERTA OCHOA, Carla, Las Normas Oficiales Mexicanas en el Ordenamiento Jurídico Mexicano, Boletín Mexicano de Derecho Comparado, número 92, año XXXI, México, mayo-agosto 1998, p. 381

[76] *Ídem.*

Estas normas son emitidas por el gobierno, a través de las dependencias de la administración pública federal, pero son discutidas previo a su publicación por comités técnicos integrados por todos los sectores interesados en el tema, como investigadores, académicos y cámaras industriales o colegios de profesionistas.

Por lo tanto, las Normas Oficiales Mexicanas son regulaciones que emite un organismo del gobierno con el propósito de establecer ciertos parámetros para regular una situación en específico, con la finalidad de proteger la vida, la seguridad y el medio ambiente.

En lo referente a los prestadores de servicios de certificación, las Normas Oficiales Mexicanas son importantes debido a que fue la Norma Oficial Mexicana NOM-151-SCFI-2002 sobre prácticas comerciales, la que fijó los primeros parámetros a seguir en cuestión a la conservación de los mensajes de datos y lo que tuvo como consecuencia las reformas realizadas en materia de comercio electrónico, y por ende las relacionadas a las entidades de certificación, misma norma que se estudia con mayor detalle en el capítulo siguiente.

En conclusión, el comercio electrónico es una forma de realizar transacciones comerciales en todo el mundo mediante redes de comunicación, este tipo de comercio inició como un simple intercambio electrónico de datos, pero gracias a las nuevas Tecnologías de la Información y las Comunicaciones se puede llevar a cabo a través de Internet, en páginas web o de un tablón de anuncios electrónicos o por medio del correo electrónico.

Con la incorporación del comercio electrónico en los diversos ordenamientos, nacieron nuevas figuras jurídicas como son: los prestadores de servicios de certificación, entidades públicas o privadas encargadas de brindar servicios relacionados con la firma electrónica simple y la firma electrónica

avanzada; así como el certificado digital; iniciador; destinatario; mensaje de datos, elementos necesarios no solo para efectuar actividades comerciales por medios electrónicos, sino también instauradas con el propósito de brindar seguridad, confianza y certeza a los sujetos que intervendrán en el mismo, fines de los que nos ocuparemos de analizar posteriormente.

CAPÍTULO SEGUNDO.

LEGISLACIÓN APLICABLE A LAS ENTIDADES DE CERTIFICACIÓN.

El jurista Óscar Vásquez del Mercado[77] refiere que el fenómeno de la globalización, tuvo como consecuencia, que se abrieran las fronteras de la mayoría de los países alrededor del mundo a la comercialización de una gran diversidad de bienes y servicios; aunado a esto la creación de las nuevas Tecnologías de la Información y la Comunicación contribuyeron a que estas transacciones se llevarán a cabo por medios electrónicos, lo cual reporta múltiples benéficos a los comerciantes y no comerciantes alrededor del planeta, pero al mismo tiempo genera serios problemas con relación a la seguridad, confiabilidad y certeza que se tiene en el comercio electrónico; por ello se crearon nuevas figuras jurídicas denominadas firma electrónica avanzada y prestador de servicios de certificación, las cuales resuelven estas contrariedades.

Asimismo, se crearon legislaciones que regulan estas nuevas figuras y fijan los parámetros que se deben seguir para realizar actividades comerciales por medios electrónicos y así brindar protección a los usuarios de este tipo de comercio. A continuación analizamos dichas legislaciones, en específico las que regulan a las entidades de certificación.

2.1. Constitución Política de los Estados Unidos Mexicanos.

La base legal del comercio electrónico en nuestro país, del cual se desprende el fundamento legal de las entidades de certificación, es en primer lugar el artículo 5 constitucional toda vez que dicho precepto señala en su

[77] *Vid.* REYES DÍAZ, Carlos Humberto (coord.), *Op. Cit.* p. 483

primer párrafo que: a ninguna persona podrá impedirse que se dedique a la profesión, industria, comercio o trabajo que le acomode, siendo lícitos. El ejercicio de esta libertad sólo podrá vedarse por determinación judicial, cuando se ataquen los derechos de tercero, o por resolución gubernativa, dictada en los términos que marque la ley, cuando se ofendan los derechos de la sociedad.

Además del artículo anterior, en el artículo 73 fracción X de nuestra Constitución, establece la facultad del Congreso de la Unión para: legislar en toda la República sobre hidrocarburos, minería, sustancias químicas, explosivos, pirotecnia, industria cinematográfica, comercio, juegos con apuestas y sorteos, intermediación y servicios financieros, energía eléctrica y nuclear y para expedir las leyes del trabajo reglamentarias del artículo 123.

Ahora bien, aunque los artículos constitucionales no hablan como tal de comercio electrónico, se entiende que son aplicables a todos los tipos de comercio.

Por lo tanto en nuestro país está permitida la práctica del comercio electrónico siempre y cuando se haga de manera lícita, a excepción de las personas que de acuerdo a las leyes se encuentre impedidas para realizar estas actividades.

Igualmente, es el Congreso de la Unión el único facultado para legislar en materia de comercio, por ende es el encargado de expedir las leyes que regulan al comercio electrónico, y en consecuencia la normatividad aplicable a las autoridades de certificación.

2.2. Ley Modelo de la CNUDMI sobre Comercio Electrónico.

Aprobada el 12 de junio de 1996 por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional o CNUDMI (por sus siglas en inglés

UNCITRAL) junto a su guía para la incorporación al derecho interno. Sin embargo, en el año de 1998 se adiciona el artículo 5 Bis, posteriormente en el año 2000 fue adoptada la Ley Modelo por nuestro país.

Conformada por 17 artículos, la Ley Modelo tiene como objetivo, de acuerdo con la propia Comisión: "posibilitar y facilitar el comercio por medios electrónicos ofreciendo a los legisladores un conjunto de reglas internacionalmente aceptables encaminadas a suprimir los obstáculos jurídicos y a dar una mayor previsibilidad al comercio electrónico." [78]

Así, el objetivo de esta ley es proporcionar a los legisladores de los Estados que la adoptaron una serie de reglas aceptadas internacionalmente para llevar a cabo este tipo de comercio, para que de esta forma al ser similares las legislaciones, en caso de que se suscite algún conflicto sea más fácil resolverlo.

Cada uno de sus artículos fue creado bajo los principios de:

- No discriminación: no se negará validez, efectos jurídicos o ejecución a un documento solo por estar de forma electrónica.
- Neutralidad tecnológica: no se discriminará ningún tipo de tecnología, debido al gran avance tecnológico que ocurre todos los días.
- Equivalencia funcional: todos los documentos electrónicos empleados en el comercio electrónico serán iguales a los documentos en papel.

Esta ley expone aspectos generales relacionados con el comercio electrónico, como el ámbito de aplicación, el cual se limita a los mensajes de

[78] Ley Modelo de la CNUDMI sobre comercio electrónico (1996), Comisión de las Naciones Unidas para el Derecho Mercantil Internacional [En línea] Disponible: http://www.uncitral.org/uncitral/es/uncitral_texts/electronic_commerce/1996Model.html 25 de Noviembre de 2013. 12:20 PM.

datos realizados con motivo de una actividad comercial; la firma electrónica; originales y copias; el problema de la prueba y la conservación de los mensajes de datos.

En el caso de la presente investigación, el apartado relacionado con las entidades de certificación es el artículo 7 el cual hace mención a la firma, el cual dispone que:

1) Cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos:

a) Si se utiliza un método para identificar a esa persona y para indicar que esa persona aprueba la información que figura en el mensaje de datos; y

b) Si ese método es tan fiable como sea apropiado para los fines para los que se generó o comunicó el mensaje de datos, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo pertinente.

2) El párrafo 1) será aplicable tanto si el requisito en él previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que no exista una firma.

3) Lo dispuesto en el presente artículo no será aplicable a: [...]

Este precepto señala dos funciones de la firma: la primera de ellas es identificar al iniciador del mensaje de datos y en segundo lugar verificar que el autor del mensaje acepta el contenido del mismo; en este caso ambas funciones se verán satisfechas por medio de cualquier método que las partes utilicen.

Ahora bien, la Guía para la incorporación de esta ley al derecho interno menciona que para determinar si el método que eligieron las partes, para cubrir el requisito de la firma es el apropiado se debe tener en cuenta los siguientes factores jurídicos, técnicos y comerciales:

1) La perfección técnica del equipo utilizado por cada una de las partes.

2) La naturaleza de su actividad comercial.

3) La frecuencia de sus relaciones comerciales.

4) El tipo y la magnitud de la operación.

5) La función de los requisitos de firma con arreglo a la norma legal o reglamentaria aplicable.

6) La capacidad de los sistemas de comunicación.

7) La observación de los procedimientos de autenticación establecidos por intermediarios.

8) La gama de procedimientos de autenticación que ofrecen los intermediarios.

9) La observancia de los usos y prácticas comerciales.

10) La existencia de mecanismos de aseguramiento contra el riesgo de mensajes no autorizados.

11) La importancia y el valor de la información contenida en el mensaje de datos.

12) La disponibilidad de otros métodos de identificación y el costo de su aplicación.

13) El grado de aceptación o no aceptación del método de identificación en la industria o esfera pertinente, tanto en el momento cuando se acordó el método como cuando se comunicó el mensaje de datos.

Por consiguiente, es necesario analizar todos estos aspectos para determinar el método indicado para identificar al sujeto y que será equivalente a la firma manuscrita; a pesar de que en esta ley no se encuentra como tal la figura de los prestadores de servicios de certificación si se habla, por ejemplo, en el caso del octavo punto de los procedimientos de autenticación que ofrecen los intermediarios.

En lo referente a la conservación de documentos, registros o informaciones, el artículo 10 en su inciso 3) explica que se podrán solicitar los servicios de un tercero para cumplir con este requisito mediante la conservación

de mensajes de datos, siempre que este tercero cumpla con las siguientes condiciones:

a) Que la información esté disponible para consultas posteriores.
b) Que el mensaje de datos sea conservado en su formato original o en un formato que reproduzca con exactitud la información.
c) Que se conserven los datos que permitan determinar el origen y destino del mensaje y la fecha y hora en que fue enviado y recibido.

Así que, esta Ley Modelo fue el primer ordenamiento en instaurar los parámetros generales para regular el comercio electrónico y si bien no describe como tal a las entidades de certificación si se refiere a ellas como un tercero que auxilia a los usuarios del comercio electrónico en la conservación de mensajes de datos y como un intermediario que autentifica las firmas electrónicas.

2.3. Ley Modelo de la CNUDMI sobre Firmas Electrónicas.

Como lo explica la maestra Soyla León Tovar,[79] la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) cumpliendo con su objetivo de fomentar la armonización y unificación del derecho mercantil internacional, y debido al crecimiento continuo del comercio electrónico y la utilización de mensajes de datos en este tipo de comercio, elaboró y posteriormente adoptó el 5 de julio de 2001 un proyecto sobre firmas electrónicas denominado Ley Modelo de la CNUDMI sobre Firmas Electrónicas, junto a su guía para la incorporación de la misma al derecho interno de cada país.

[79] *Vid.* LEÓN TOVAR, Soyla H., Contratos Mercantiles, Editorial Oxford University Press, México, 2004, p. 93.

Conformada por 12 artículos esta ley tiene como finalidad, conforme a lo establecido por la propia Comisión: “ayudar a los Estados a establecer un marco legislativo moderno, armonizado y equitativo que permite regular con eficacia el trato jurídico de las firmas electrónicas de modo que su utilización no dé lugar a dudas sobre su seguridad.”[80]

El artículo 3 de esta ley dispone que para cumplir con el requisito de la firma se reconocen tanto las firmas electrónicas simples como la firma electrónica avanzada o digital. Y en cuanto a su fiabilidad, el artículo 6 señala que la firma electrónica o digital será fiable sí:

a) Los datos de creación de la firma corresponden exclusivamente al firmante.

b) Los datos de creación de la firma electrónica estaban, en el momento de la firma, bajo el control exclusivo del firmante.

c) Es posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma.

d) Es posible detectar cualquier alteración de la información hecha después del momento de la firma.

Esto se entenderá sin perjuicio de que cualquier persona: demuestre de cualquier otra manera, la fiabilidad de la firma; o aporte pruebas de que una firma electrónica no es fiable.

Asimismo, el artículo 7 menciona que el Estado otorgará competencia a una persona, órgano u entidad para determinar que las firmas electrónicas cumplen los requisitos indicados en el precepto anteriormente mencionado.

---

[80] Ley Modelo de la CNUDMI sobre las firmas electrónicas (2001), Comisión de las Naciones Unidas para el Derecho Mercantil Internacional [En línea] Disponible: http://www.uncitral.org/uncitral/es/uncitral_texts/electronic_commerce/2001Model_signatures.html 25 de Noviembre de 2013. 12:20 PM.

En cuanto al proceder del firmante, el artículo 8 refiere que cada firmante, en cuanto a los datos de creación de la firma, deberá cumplir una serie de requisitos que de no ser cumplidos, el firmante será responsable de las consecuencias jurídicas que entrañe el incumplimiento. Los requisitos que deberá cumplir son:

a) Actuar con diligencia para evitar la utilización no autorizada de los datos de creación de la firma.

b) Utilizar los medios que le proporcione el prestador de servicios de certificación o cualquier otro medio, para dar aviso a cualquier persona que, de acuerdo con el firmante, pueda considerar fiable la firma electrónica o prestar servicios que la apoyen si: el firmante o las circunstancias de que tiene conocimiento dan lugar al riesgo de que los datos de creación de la firma han quedado en entredicho.

c) Cuando emplee un certificado para acreditar su firma electrónica, debe actuar con diligencia para cerciorarse de que todas las declaraciones relacionadas a la caducidad del certificado o que hayan de consignarse en el mismo son exactas y cabales

Por otra parte, los prestadores de servicios de certificación se encuentran en el artículo 9, el cual expone que en caso de que estos presten servicios de apoyo a una firma electrónica deberán:

a. Actuar de conformidad con las declaraciones que haga respecto de sus normas y prácticas.

b. Actuar con diligencia para cerciorarse de que todas las declaraciones importantes que haya hecho sobre la caducidad del certificado o que estén consignadas en él son exactas y cabales.

c. Proporcionar a la parte que confía en el certificado medios razonablemente accesibles que permitan a ésta determinar mediante el certificado: la identidad del prestador de servicios de certificación; que el firmante tiene bajo su control los datos de creación de la firma en el momento

de expedición del certificado; que los datos de creación eran válidos en la fecha de expedición del certificado o antes de ella.

d. De igual forma proporcionar medios a la parte que confía que le permitan determinar, por medio del certificado o de otra manera: el método utilizado para comprobar la identidad del firmante; la limitación de los fines o del valor respecto de los cuales puedan utilizarse los datos de creación de la firma o el certificado; si los datos de creación de la firma son válidos y no están en entredicho; limitaciones del alcance o del grado de responsabilidad del prestador de servicios de certificación; si existe un medio para que el firmante de aviso de que los datos de creación de la firma están en entredicho; si ofrece un servicio para revocar oportunamente un certificado.

e. Al prestar sus servicios utilizar sistemas, procedimientos y recursos humanos fiables. El prestador de servicios de certificación será responsable de las consecuencias jurídicas que impliquen el hecho de no haber cumplido con los requisitos antes señalados.

Además, con relación a este último inciso, el artículo 10 explica que para determinar que los sistemas, procedimientos o recursos humanos utilizados por el prestador de servicios de certificación son fiables, se deberá tener en cuenta: los recursos humanos y financieros, incluida la existencia de activos; la calidad de los equipos y programas informáticos; los procedimientos para la tramitación de certificados, la solicitud de los mismos y la conservación de registros; la disponibilidad de la información para los firmantes y la parte que confía; la periodicidad y el alcance de la auditoría realizada por un órgano independiente; la declaración del Estado, órgano de acreditación o del prestador de servicios de certificación respecto al cumplimiento de los factores antes mencionados; y cualquier otro factor pertinente.

En cuanto al proceder de la parte que confía en el certificado, el artículo 11 refiere que son su responsabilidad las consecuencias jurídicas por el hecho de no tomar medidas para: verificar la fiabilidad de la firma electrónica, o

cuando la firma este avalada por un certificado: verificar la validez, suspensión o revocación del mismo y tener en cuenta las limitaciones relacionadas al certificado.

Finalmente, el artículo 12 proporciona una serie de medidas para el reconocimiento de certificados y firmas electrónicas extranjeras, para determinar si producen efectos jurídicos y en qué medida. Advirtiendo que no se debe considerar: el lugar en el que fue expedido el certificado o creado o utilizado la firma electrónica; ni el lugar donde se encuentre el establecimiento del expedidor o del firmante. Asimismo, señala que los certificados y las firmas electrónicas expedidos, creadas o utilizadas fuera del país promulgante producirán los mismos efectos jurídicos que si se hubiera sido expedida, creada o utilizada en el país promulgante, siempre y cuando presenten un grado de fiabilidad sustancialmente equivalente, para determinar dicha fiabilidad se tomarán en cuenta las normas internacionales reconocidas por los países y cualquier otro factor pertinente.

Así, esta Ley Modelo determinó las bases para que los países que la acepten incorporen en sus legislaciones la regulación de las firmas electrónicas y todo lo relacionado con ellas, por ende a los prestadores de servicios de certificación.

A pesar de que esta ley modelo fue aprobada por la CNUDMI en el año 2001, fue hasta el año 2003 que México la adoptó, por lo que esta ley se convirtió en el antecedente de los cambios que se realizarían con posterioridad en la legislación comercial de nuestro país en materia de firmas electrónicas y de prestadores de servicios de certificación.

2.4. Código de Comercio.

Como lo describe el doctrinario Salomón Vargas García[81], las primeras reformas al Código de Comercio fueron en materia de comercio electrónico, publicadas en el Diario Oficial de la Federación el 29 de mayo de 2000, adicionando el Título Segundo denominado "Del Comercio Electrónico", dicho título comprende los artículos 89 al 94, e igualmente se alteró el texto de los artículos 1205 y 1298-A.

Aunque, como explica el jurista Edgar Elías Azar[82], unos años después se modificó nuevamente el Código de Comercio para incorporar la regulación de la firma electrónica y lo relacionado con ella siguiendo lo establecido en la Ley Modelo de la CNUDMI sobre firmas electrónicas, estos cambios fueron publicados el 29 de agosto de 2003. Estos últimos abarcaron los artículos 89 al 114 y se agregaron los artículos 89 bis, 90 bis, 91 bis y 93 bis.

En lo concerniente a los prestadores de servicios de certificación, estos se encuentran contemplados en los artículos 89, 98 y del 100 al 114. El primero de ellos hace referencia a lo que se entenderá como entidad de certificación, misma que se señaló en el capítulo anterior, y que manifiesta que es la persona o institución pública que presta servicios relacionados con la firma electrónica y que expide certificados.

Por otra parte, el artículo 98 menciona que son las entidades de certificación las que determinarán y harán del conocimiento de los usuarios si la firma electrónica avanzada cumple con los requisitos enumerados en el artículo 97, que ya se explicaron, los cuales son:

1. Los datos de creación de la firma corresponden exclusivamente al firmante.

---

[81] *Vid.* VARGAS GARCÍA, Salomón, *Op. Cit.* p. 37- 38.
[82] *Vid.* ELÍAS AZAR, Edgar, La contratación por medios electrónicos, Editorial Porrúa, México, 2005, p. 71.

2. Los datos de creación de la firma estaban, en el momento de firmar, bajo el control exclusivo del firmante.

3. Es posible detectar cualquier alteración de la firma electrónica posterior al momento de firmar.

4. Es posible detectar cualquier alteración a la información de un mensaje de datos después de firmado el mensaje.

Además, dicha determinación debe hacerse con arreglo a normas y criterios internacionalmente reconocidos, y sin perjuicio de la aplicación de las normas del derecho internacional privado.

Pero, antes de poder realizar estas determinaciones los prestadores de servicios de certificación deben contar con una acreditación expedida por la Secretaría de Economía, y como lo indica el artículo 100 solo podrán ser entidades de certificación: los notarios y corredores públicos, las personas morales de carácter privado y las instituciones públicas.

En el caso de los notarios y corredores públicos, el mismo artículo hace la aclaración de que expedir certificados no conlleva por sí misma la fe pública, por lo que se podrán llevar acabo certificaciones con o sin fe pública en documentos en papel, archivos electrónicos, o cualquier otro medio o sustancia que incluya información.

Igualmente, las personas morales de carácter privado, de acuerdo con el artículo 101, contendrán en su objeto social las actividades de:

a) Verificar la identidad de los usuarios y su vinculación con los medios de identificación electrónica.

b) Comprobar la integridad y suficiencia del mensaje de datos del solicitante y verificar su firma electrónica.

c) Llevar a cabo un registro de los elementos de identificación de los firmantes y de la información con la que se verificó la fiabilidad de las firmas y emitir el certificado.

d) Cualquier otra actividad, siempre que no sea incompatible con las anteriores.

No obstante lo anterior, la Secretaría de Economía también es autoridad de certificación y registradora, sólo respecto de los demás prestadores de estos servicios, como lo refiere el artículo 105. Asimismo, el artículo 106 explica que para la prestación de servicios de certificación, las instituciones financieras y las empresas que les proporcionen servicios auxiliares o complementarios con relación a la transferencia de fondos y valores, quedarán sujetas a las leyes que las regulan y de las disposiciones y autorizaciones que emitan las autoridades financieras.

Como se mencionó anteriormente, las entidades de certificación deberán contar con una acreditación para iniciar sus operaciones, es por ello que el artículo 102 inciso A) describe los requisitos que debe cubrir el solicitante, los cuales explicaremos más adelante. Igualmente dispone que si se cubren dichos requisitos la Secretaría de Economía no podrá negar la petición al solicitante y una vez que la obtenga, deberá notificar a la Secretaría el inicio de sus funciones dentro de los 45 días naturales siguientes al comienzo de sus servicios. También alude en su inciso B) que si la Secretaría no resuelve su solicitud dentro de los 45 días siguientes a la presentación de la misma, **se tendrá por concedida la acreditación.**

En lo referente a las responsabilidades de las autoridades de certificación, el artículo 103 menciona que estas deberán estipularse en el contrato con los firmantes.

En cuanto a sus funciones, estas se encuentran en el artículo 104, algunas de estas son: comprobar la identidad del solicitante y emitir el certificado digital correspondiente; mantener un registro de certificados y de las circunstancias que afectan su vigencia; guardar confidencialidad respecto de la

información que reciba para la expedición del certificado, etc. Dichas obligaciones se describen con mayor detalle en el siguiente capítulo.

En lo que concierne a el destinatario y la parte que confía, el artículo 107 señala que serán responsables de las consecuencias jurídicas por el hecho de no tomar medias para verificar la fiabilidad de la firma electrónica o, cuando ésta se encuentre sustentada por un certificado, verificar la validez, suspensión o revocación del mismo o tener en cuenta las limitaciones de uso.

Por otra parte, el artículo 108 indica que el certificado será considerado válido, si contiene:

1. La indicación de que se expiden como tales.
2. El código de identificación del certificado.
3. La identificación, razón social, domicilio, dirección de correo electrónico y los datos de acreditación del prestador de servicios de certificación que expidió el certificado.
4. El nombre del titular del certificado.
5. La vigencia del mismo.
6. La fecha y hora de su expedición, suspensión y revocación del mismo.
7. El alcance de las responsabilidades de la entidad certificadora.
8. Mención de la tecnología utilizada para crear la firma electrónica.

Al contrario, el artículo 109 refiere que el certificado dejará de surtir efectos cuando:

a. Expire el periodo de vigencia del certificado, el cual no puede ser superior a dos años, en el entendido de que el firmante puede renovarlo antes de que concluya la vigencia.

b. Se revoque por la entidad el certificado a petición del firmante o quien actué en su nombre.

c. Por pérdida, u inutilización o por daño en el dispositivo que lo contiene.

d. Se demuestre que en el momento de la expedición no cumplía con los requisitos señalados en el artículo 108, lo cual no afecta derechos de terceros de buena fe.

e. Por resolución judicial o de la autoridad competente.

Ahora bien, el artículo 110 explica que si la entidad certificadora incumple con sus obligaciones, previa garantía de audiencia y mediante resolución fundada y motivada, y en razón de la gravedad de los actos y la reincidencia, será sancionada por la Secretaría de Economía con suspensión temporal o permanente de sus funciones, en este caso el procedimiento se regirá por la Ley Federal de Procedimiento Administrativo. Pese a ello, el artículo 111 manifiesta que estas sanciones se aplicarán sin perjuicio de la responsabilidad civil o penal o de las penas que correspondan por los delitos cometidos por la entidad de certificación.

Incluso, el artículo 112 determina que las autoridades competentes podrán auxiliarse de la fuerza pública para ejecutar la sentencia o medidas de seguridad que procedan, además en el proceso se podrán solicitar las medidas cautelares necesarias para garantizar la eficacia de la resolución definitiva. Y en el caso de que la sanción sea la suspensión, inhabilitación o cancelación en el ejercicio de las funciones de la entidad de certificación, como lo menciona el artículo 113, el registro y los certificados emitidos por ella pasarán para su administración a otra entidad designada por la Secretaría de Economía.

Finalmente, el artículo 114 dispone que los certificados y las firmas extranjeras producen efectos jurídicos sin importar el lugar en donde se expidieron o se crearon o se utilizaron respectivamente ni el lugar donde está el establecimiento de la entidad certificadora o del firmante, siempre que tengan un grado de fiabilidad equivalente al descrito en la legislación comercial correspondiente, en la inteligencia de que para medir el grado de fiabilidad se

tomarán en cuenta las normas internacionales reconocidas por nuestro país y otro medio de convicción pertinente.

Asimismo, el artículo anterior menciona que cuando las partes hayan convenido sobre la utilización de determinada firma electrónica y certificado, dicho acuerdo es suficiente para efectos del reconocimiento transfronterizo, salvo que el acuerdo no sea eficaz o válido de acuerdo con la norma aplicable.

De esta forma están instauradas las bases regulatorias de las entidades de certificación en la legislación comercial de nuestro país, reflejo de las leyes modelo, así quedan dispuestas las normas relacionadas con la acreditación de los prestadores de servicios de certificación, las obligaciones que éstas tienen y las sanciones a las que serán acreedoras en caso de incumplimiento de las mismas; y lo concerniente a la emisión certificados digitales, principal función de las entidades de certificación. Aunque estos aspectos solo se señalan de manera general, el Reglamento correspondiente y las Reglas Generales los disponen de forma más específica.

2.5. Código Civil Federal.

Al igual que el Código de Comercio, el Código Civil Federal sufrió algunas reformas para integrar al comercio electrónico a la legislación de nuestro país, ya que este último código se aplica de forma supletoria en materia comercial, es por ello que los cambios se realizaron en los artículos 1803, 1805, 1811 y la adición del artículo 1834 bis, estas reformas fueron publicadas el 29 de mayo del año 2000 en el Diario Oficial de la Federación.

Primeramente, el artículo 1803 habla del consentimiento, y estipula que el consentimiento será expreso cuando la voluntad se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o cualquier otra tecnología, o por signos inequívocos; y el tácito resultará de hechos o actos inequívocos que lo

presupongan o autoricen presumirlo, salvo que la ley o las partes exijan manifestar el consentimiento expresamente.

De esta forma se permite por la ley que el consentimiento se manifieste a través del uso de tecnologías, y con ello surta efectos jurídicos plenos.

Por otra parte, respecto a la aceptación se encuentra regulado en los artículos 1805, 1811 y 1834 Bis, el primero de ellos impera que cuando la oferta se haga a una persona presente, y no se fije tiempo para aceptarla, la aceptación se debe hacer inmediatamente, de lo contrario el autor de la oferta se desligará de la misma; esto será aplicable a las ofertas hechas por teléfono o por medios electrónicos, ópticos u otras tecnologías, siempre y cuando permitan la expresión de la oferta y la aceptación de la misma de forma inmediata. Esto es debido a que se entiende que la transacción se está llevando a cabo en tiempo real y que las partes están frente a frente lo que permite la aceptación o rechazo de la oferta en el momento.

Igualmente, el artículo 1811 hace alusión a que en el caso de ofertas y aceptaciones por medios electrónicos, ópticos o por otras tecnologías no se requiere de un acuerdo previo entre las partes para que produzca efectos su acuerdo.

En cuanto a la forma y a las firmas, el artículo 1834 Bis indica que cuando se exija la forma escrita para el contrato, todos los documentos relativos deben ser firmados por las personas obligadas, esto se tendrá por cumplido mediante la utilización de medios electrónicos, ópticos o de cualquier otra tecnología siempre que la información generada o comunicada y las firmas puedan atribuirse a las partes, además de que la información se conserve de manera íntegra y sea accesible para consultas posteriores. Y en el caso de que se tenga que ser otorgado el acto jurídico por instrumento ante fedatario, las partes podrán generar, archivar, enviar, recibir o comunicar la información en

los términos exactos en los que quedan obligados, por medios electrónicos, ópticos u otra tecnología, y el fedatario público deberá colocar esto en el instrumento respectivo y conservarlo para consultas posteriores.

Aunque estos artículos no se refieren a los prestadores de servicios de certificación, si mencionan a la firma electrónica y a la conservación de los mensajes de datos, y puesto que son los certificados digitales expedidos por una entidad de certificación el instrumento que le da fiabilidad a las firmas e incluso son estas mismas entidades las que en la mayoría de los casos se encargan de la preservación de la información intercambiada entre las partes, las normas antes descritas se aplican a la autoridad de certificación de manera indirecta.

2.6. Código Federal de Procedimientos Civiles.

La adición al Código Federal de Procedimientos Civiles se publicó en la misma fecha que las del Código Civil Federal, pero en este caso la modificación fue mínima, ya que solo fue en materia de pruebas, la cual permite la utilización como prueba la información generada por algún tipo de tecnología en una controversia.

Es decir, se adicionó el artículo 210 – A, estipulando lo mismo que los artículos 1205 y 1298 – A del Código de Comercio, para regular las pruebas provenientes del uso de las nuevas tecnologías, este precepto expresa que se reconocen como pruebas la información generada o comunicada que conste en medios electrónicos, ópticos o en otra tecnología; el valor probatorio de éstas se estimará la fiabilidad del método con el que se generó, archivó, comunicó o recibió la información, y de igual forma que la información sea atribuible a las partes y que esté accesible para ser consultada posteriores.

Asimismo, el último párrafo del precepto anterior dispone que en caso de que se requiera conservar o presentar en su forma original algún documento, se satisface si se acredita que la información generada, comunicada, archivada o recibida por medios electrónicos, ópticos u otra tecnología, se ha mantenido integra e inalterada desde el momento en que se generó y está disponible para ser consultada.

Al igual que en el Código Civil Federal, la modificación en el Código Federal de Procedimientos Civiles en materia de pruebas no trata a las entidades de certificación de forma directa, pero sí hace referencia a la conservación de mensajes de datos, servicio brindado por algunos prestadores de servicios de certificación y estos deben garantizar que la información contenida en dichas comunicaciones no será alterada.

2.7. Ley Federal de Protección al Consumidor.

El doctrinario Salomón Vargas García[83] menciona que las actividades que se llevan a cabo en el comercio electrónico han tenido tal relevancia los últimos años que como consecuencia se modificó la Ley Federal de Protección al Consumidor, para de esta forma poder brindar protección a los usuarios de este nuevo tipo de comercio, sobre todo a los consumidores.

Las reformas se ven reflejadas en el párrafo primero del artículo 128, la adición de la fracción VIII al artículo 1, la fracción IX bis al artículo 24 y el capítulo VIII bis que contiene al artículo 76 bis, mismas que se hicieron con base en los principios de la Ley Modelo de la CNUDMI sobre comercio electrónico.

El objetivo de estas reformas se encuentra expresado en la fracción VIII del artículo 1 la cual señala que es un principio en las relaciones de consumo: la

[83] *Vid.* VARGAS GARCÍA, Salomón, *Op. Cit.*, p. 41

efectiva protección al consumidor en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología y la adecuada utilización de los datos aportados.

Y para cumplir dicho principio se le otorga una nueva atribución a la Procuraduría Federal del Consumidor para promover, en coordinación con la Secretaría de Economía la formulación, difusión y uso de códigos de ética, por parte de los proveedores para incorporar el principio descrito en la fracción anterior para el caso de las transacciones llevadas a cabo por medios electrónicos, ópticos u otras tecnologías.

Por ende, el Capítulo VIII bis denominado “De los derechos de los consumidores en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología”, el cual está compuesto únicamente por el artículo 76 bis estipula que en las relaciones de proveedores y consumidores, en este tipo de transacciones deberán cumplirse los siguientes puntos:

1. El proveedor deberá mantener la información proporcionada por el consumidor de manera confidencial, sólo podrá difundirla o transmitirla con la autorización del consumidor o por requerimiento de la autoridad competente.
2. El proveedor utilizará elementos técnicos disponibles para brindar seguridad y confidencialidad a la información del consumidor, y deberá informar a este último de las características de dichos elementos antes de celebrar la transacción.
3. El proveedor deberá proporcionarle al consumidor, antes de realizar la transacción, su domicilio, número de teléfono y demás datos que el consumidor pueda utilizar para presentar sus reclamaciones o aclaraciones.
4. El proveedor deberá evitar las prácticas comerciales engañosas en relación a las características de sus productos, por lo que deberá de cumplir con las disposiciones relativas a este tema.

5. El consumidor tiene derecho a conocer los términos, costos, condiciones, cargos adicionales y formas de pago de los bienes y servicios que ofrece el proveedor.

6. El proveedor deberá respetar las decisiones del consumidor en cuanto a la cantidad y calidad de los productos, y de no recibir avisos comerciales.

7. El proveedor no deberá utilizar estrategias de ventas o publicidad que no proporcione información clara y suficiente al consumidor sobre los servicios ofrecidos, igualmente cuidará que las prácticas de mercadotecnia advierta que no es apta para niños, ancianos y enfermos.

Por último, el artículo 128 expone que en caso de infracción a lo dispuesto en el artículo anterior, serán sancionados con una multa equivalente a una y hasta dos mil quinientas veces el salario mínimo vigente en el Distrito Federal.

Así, aun cuando esta ley no hace mención de los prestadores de servicios de certificación, al igual que los dos códigos anteriores, se entiende que para que las empresas que realizan actividades comerciales con el consumidor final de sus productos por medios electrónicos deben contar con un certificado digital emitido por una entidad de certificación, con el cual se avalan los datos del comerciante lo cual le asegura que es una persona confiable. Además, el certificado o sello de confianza contiene una leyenda que asegura la protección de los datos personales que proporcione el comprador al momento de realizar la transacción. Con esto se cumple con algunos de los puntos del artículo 76 bis de esta ley, y con ello se mantiene en resguardo los derechos de los usuarios cuando realicen negocios por medio del comercio electrónico.

2.8. Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Esta ley es relativamente nueva, así que no forma parte de los códigos y leyes que fueron reformados para integrar en ellos al comercio electrónico, pero si es importante hacer hincapié en ella ya que los prestadores de servicios de certificación son particulares que reciben y almacenan datos personales de sus usuarios para llevar a cabo sus servicios.

Publicada en el Diario Oficial de la Federación el 5 de julio de 2010, se encuentra integrada por 69 artículos.

Primeramente, como lo marca el artículo 2 se sujetarán a esta ley las personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales, salvo las sociedades de información crediticia y las personas que recolecten y almacén datos personales para uso exclusivamente personal, sin fines de divulgación o utilización comercial

Ahora bien, el artículo 3 explica que se entenderán como datos personales cualquier información concerniente a una persona física identificada o identificable, esta última considerada como titular de los mismos; de igual forma se entenderá por tratamiento la obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio; y como responsable la persona física o moral de carácter privado que decide sobre el tratamiento de datos personales; y por aviso de privacidad el documento que el responsable pondrá a disposición del titular de forma física, electrónica o por cualquier otro formato, antes del tratamiento de los datos.

Los responsables en el tratamiento de datos personales deberán, de acuerdo con el artículo 6, observar los siguientes principios:

a. Licitud: los datos personales deberán recabarse y tratarse de manera lícita, conforme a las disposiciones y normativas aplicables.

b. Consentimiento: ya que el tratamiento de los datos está sujeto al consentimiento del titular, salvo excepción de la ley.

c. Información: expuesto en el artículo 15, el responsable tiene la obligación de informar a los titulares la información que se recaba de ellos y con qué fines, mediante el aviso de privacidad.

d. Calidad: como lo menciona el artículo 11, los datos que se encuentren en las bases de datos deberán ser pertinentes, correctos y actualizados para los fines por los que fueron recabados. Cuando los datos dejen de ser necesarios para el cumplimiento de las finalidades previstas deberán ser cancelados, de igual forma el responsable deberá eliminar la información relacionada con el incumplimiento de las obligaciones contractuales, en un plazo de 72 meses contado a partir del incumplimiento.

e. Finalidad: el tratamiento de los datos se limitará, de acuerdo con el artículo 12, a los fines pactados en el aviso de privacidad, si el responsable pretende tratarlos con otro fin requerirá nuevamente del consentimiento del titular.

f. Lealtad: en el entendido, de que en el tratamiento de datos se presume que existe la expectativa de privacidad, entendida como la confianza que deposita una persona en otra, en relación a los datos personales el artículo 7 indica, que serán tratados de acuerdo a lo acordado entre las partes, por lo que la obtención de la información no puede hacerse por medios engañosos o fraudulentos.

g. Proporcionalidad: el tratamiento de los datos, el artículo 13 refiere que, solo será el necesario, adecuado y relevante con relación a las finalidades estipuladas en el aviso de privacidad; en el caso de datos personales sensibles el responsable deberá realizar esfuerzos razonables para que el periodo de tratamiento de los datos sea mínimo.

h. Responsabilidad: el responsable, como lo alude el artículo 14, deberá velar por el cumplimiento de los principios anteriormente señalados, para lo cual

deberá adoptar las medidas pertinentes, esto se aplica de igual manera aun cuando sea un tercero el que tratará los datos a solicitud del responsable. De igual manera, el responsable deberá tomar las medidas necesarias para garantizar que el aviso de privacidad se respete en todo momento por él, y si es el caso, por un tercero.

No obstante lo anterior, el artículo 8 describe que el consentimiento puede ser expreso, cuando se manifiesta la voluntad verbalmente, por escrito, por medios electrónicos, ópticos u otra tecnologías, o por signos inequívocos, la ley hace la aclaración de que se tendrá que consentir de esta manera en caso de datos financieros o patrimoniales, salvo excepción; por el contrario será tácito cuando habiéndose puesto a disposición del titular el aviso de privacidad no manifieste su oposición. El consentimiento podrá ser revocado sin que se atribuyan efectos retroactivos.

En el caso de que se traten datos personales sensibles, entendiendo estos como aquellos que afecten la esfera más íntima de su titular, o que su utilización indebida de origen a discriminación o un riesgo grave para este último, el artículo 9 refiere que se requerirá el consentimiento expreso y por escrito del titular para el tratamiento de los datos, a través de su firma autógrafa, electrónica u otro mecanismo de autenticación. Para la creación de bases de datos sensibles se deberá justificar por parte del responsable la finalidad legítima, concreta y acorde a sus actividades.

Por el contrario no se requerirá consentimiento, como lo menciona el artículo 10, cuando: esté previsto por la ley; los datos estén en fuentes de acceso público; los datos se sometan a un procedimiento de disociación; se cumplan obligaciones derivadas de la relación entre titular y responsable; por emergencia que pueda dañar a un individuo en su persona o bienes; cuando el titular no esté en condiciones de darlo y requiera atención medica, preventiva, diagnostico, asistencia sanitaria, y el tratamiento de datos se haga por persona

sujeta al secreto profesional u obligación equivalente; por resolución de autoridad competente.

Por otra parte, el aviso de privacidad al que se alude en el principio de información, el artículo 16 expone que deberá contener: identidad y domicilio del responsable; finalidades del tratamiento de datos; opciones y medios que ofrece el responsable para limitar el uso o divulgación de datos; medios para ejercer los derechos de acceso, rectificación, cancelación u oposición; la transferencia de datos efectuada, si es el caso; y procedimiento y medios por el cual se le informará al titular el cambio de aviso de privacidad.

Dicho aviso, como lo marca el artículo 17, deberá ser puesto a disposición de los titulares en formato impreso, digital, visual, sonoro u otra tecnología, de la manera siguiente:

a) Si la información fue obtenida personalmente del titular, se le debe facilitar de manera inmediata el aviso de forma clara y fehaciente, a no ser que se haya hecho con anterioridad.

b) Cuando hayan sido obtenidos por el titular a través de medios electrónicos, ópticos, sonoros, visuales o a través de otra tecnología, se le deberá proporcionar los dos primeros datos antes referidos y proveer un mecanismo con el que el titular pueda conocer el texto completo del aviso. En cambio, el artículo 18 explica que si la información no se obtiene directamente del titular, el responsable deberá dar a conocer el cambio del aviso, salvo que el tratamiento de datos sea con fines históricos, estadísticos o científicos.

Pero cuando sea imposible dar a conocer el aviso al titular o exija esfuerzos desproporcionados dárselo a conocer, se podrán instrumentar las medidas compensatorias aplicables. Entendiendo estas medidas, de acuerdo con el Instituto Federal de Acceso a la Información y Protección de Datos, como “mecanismos alternos para dar a conocer a los titulares el aviso de privacidad, a través de su difusión por medios masivos de comunicación u otros mecanismos

de amplio alcance."[84] Estos mecanismos pueden ser: diarios de circulación nacional; diarios locales o revistas especializadas; página de Internet del responsable; carteles informativos, etc.

Además, el artículo 19 señala que los responsables que lleven a cabo tratamiento de datos personales deberán establecer y mantener medidas de seguridad administrativa, técnicas y físicas para proteger los datos contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. Es por ello que el responsable, como lo dispone el artículo 20, debe informar de forma inmediata al titular cualquier vulneración de la seguridad durante el tratamiento que afecte de forma significativa sus derechos patrimoniales o morales, para que el titular pueda tomar las medidas correspondientes para defender sus derechos.

Asimismo, los responsables o terceros que intervengan en el tratamiento de la información deberán guardar confidencialidad respecto de ésta, dicha obligación prevalecerá aun después de finalizada su relación con el titular, lo anterior se encuentra indicado en el artículo 21.

En cuanto a los derechos que tienen los titulares de datos personales, con apego al artículo 22, son:

1. Acceso: establecido en el artículo 23, el titular tiene derecho a acceder a su información que se encuentren en poder del responsable, así como al aviso de privacidad

2. Rectificación: referido en el artículo 24, será en el caso de que los datos sean inexactos o incompletos.

3. Cancelación: en este caso, el artículo 25 marca que la cancelación dará origen a un bloqueo que durará lo equivalente al plazo de prescripción de

[84] Instituto Federal de Acceso a la Información y Protección de Datos, "Guía para instrumentar medidas compensatorias", [En línea] Disponible: http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_para_instrumentar_medidas_compensatorias.pdf 3 de septiembre 2014, 11:13 P.M.

las acciones que se derivan de la relación jurídica que dio motivo al tratamiento de datos, una vez concluido el plazo se suprimirán los datos, hecha la cancelación se le dará aviso al titular. El responsable podrá conservar la información solo para el caso de la responsabilidad derivada del tratamiento. De igual forma, el responsable deberá informar, si es el caso, al tercero para que proceda a realizarla.

4. Oposición: como menciona el artículo 27, siempre que sea por causa legítima, y en caso de ser procedente el responsable no podrá tratar los datos del titular.

Contrariamente a lo dicho en el caso de la cancelación, el artículo 26 aclara que el responsable no está obligado a cancelar la información cuando:

a) Se refieran a partes de un contrato privado, social o administrativo, y sean necesarios para su cumplimiento.

b) Son tratados por disposición legal.

c) Obstaculice actuaciones judiciales o administrativas de carácter fiscal, la investigación o persecución de delitos o la actualización de sanciones administrativas.

d) Sean necesarias para proteger los intereses jurídicamente tutelados del titular, o para realizar una acción en función del interés público, o para hacer cumplir una obligación legalmente adquirida por el titular.

e) El tratamiento de la información sea para la prevención o para diagnóstico médico o gestión de servicios de salud, siempre que éste se proporcione por profesionales de la salud sujetos a secreto profesional.

Por tanto, el artículo 22 indica que, estos derechos podrán ejercitarse por el titular o por su representante legal en el momento que lo estime pertinente, sin que la solicitud de uno impida el ejercicio de otro, por lo que los datos personales deben ser resguardados de tal manera que permitan el inmediato ejercicio de los derechos antes descritos.

Estas solicitudes, como lo expone el artículo 30, se tramitarán con la persona o departamento que designe el responsable para desempeñar tal función, asimismo deberá fomentar dentro de su organización la protección de los datos personales. El plazo para dar una resolución a la solicitud, dispone el artículo 32, es de máximo 20 días contados desde el día que se recibió la solicitud, en el caso de que la solicitud sea aceptada deberá cumplirse dentro de los 15 días siguientes a que se comunique la respuesta, ambos términos podrán ser ampliados solo una vez por un periodo igual.

En caso de que la solicitud sea de acceso, el artículo 33 refiere que, se tendrá por cumplida cuando se ponga a disposición del titular los datos o copias simples, documentos electrónicos o por otro medios. En cuanto a la entrega, el artículo 35 alude que se hará de forma gratuita, pero el titular debe pagar los gastos de envió o el costo de reproducción en copias u otros formatos.

Empero, el artículo 34 señala que el responsable podrá negar la solicitud de cualquiera de los derechos, cuando: no sea el titular quien lo solicite, o si el representante no está debidamente acreditado; si no se encuentren los datos personales del solicitante; haya un impedimento legal o la resolución de una autoridad competente que lo prohíba; y si la rectificación, cancelación u oposición ya hayan sido realizadas.

Igualmente, existe otro procedimiento denominado protección de datos este podrá solicitarse por el titular, como lo determina el artículo 35, cuando no esté de acuerdo con la respuesta del responsable o la falta de ella, o de acuerdo con el artículo 45, si el responsable no entrega al titular los datos personales solicitados. La solicitud deberá ser presentada ante el Instituto Federal de Acceso a la Información y Protección de Datos (IFAI), dentro de los 15 días siguientes a la recepción de la respuesta del responsable o de que haya vencido el plazo para recibir respuesta, dicha solicitud podrá presentarse por

escrito o a través de formato del sistema electrónico que proporciona el Instituto.

Dicha petición, como lo indica el artículo 46, deberá acompañarse de la solicitud del derecho y la respuesta que emitió el responsable, en caso de que la petición sea por falta de respuesta solo se requerirá la solicitud del derecho respectivo.

El artículo 47 menciona que el Instituto tendrá un plazo máximo de 50 días para resolver sobre la solicitud, contados a partir de la presentación de la misma. La resolución será en sentido de revocar, confirmar, o modificar la respuesta del responsable o sobreseer o desechar la solicitud de protección de derechos, como lo señala el artículo 51. En caso de que la resolución favorezca al titular, el artículo 48 alude que el responsable tendrá un plazo de 10 días siguientes a la notificación para cumplirla y avisar de ello al Instituto. Contra la resolución, el artículo 56 marca que, se podrá promover juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa.

Ahora bien, el artículo 36 determina que en el caso de que el responsable pretenda transferir la información a terceros, sean nacionales o extranjeros, deberá de estar indicado en el aviso de privacidad y las finalidades del tratamiento de los datos, en dicho aviso deberá existir una cláusula que indique si el titular acepta o no esto.

A pesar de lo anterior, el artículo 37 dispone que la transferencia de datos a terceros pueda llevarse a cabo sin consentimiento del titular cuando:

- Esté previsto en una ley o tratado del que México sea parte.
- Sea necesaria para la prevención o diagnóstico médico, asistencia sanitaria, tratamiento médico o gestión de servicios sanitarios.
- Sea efectuada a sociedades controladoras, subsidiarias, filiales, sociedad matriz o cualquier otra sociedad del mismo grupo que el responsable.

- Sea necesario por virtud de un contrato celebrado o por celebrarse entre el responsable y un tercero, en interés del titular.
- Es necesario o legalmente exigido para salvaguardar un interés público o la procuración y administración de la justicia.
- Se requiera para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
- Sea preciso para el mantenimiento o cumplimiento de una relación jurídica entre responsable y titular.

En lo referente a la vigilancia, el artículo 59 establece que el el Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) verificará que los particulares que están sujetos a esta ley cumplan los principios y respeten los derechos enumerados con anterioridad. Por lo que podrá iniciarse un procedimiento de verificación, ya sea a petición de parte o por oficio. Iniciado este procedimiento, como lo marca el artículo 60, el Instituto tendrá acceso a la información y documentación necesaria, de acuerdo a la razón que motive el procedimiento, además de que el Instituto está obligado a guardar confidencialidad sobre esta información.

Si con motivo del procedimiento anterior o del procedimiento de protección de derechos el Instituto tuviera conocimiento del incumplimiento de alguno de los principios de protección de datos personales o de la normativa aplicable, el artículo 61 indica que se iniciará un procedimiento denominado procedimiento de imposición de sanciones con la finalidad de aplicar la sanción que corresponda de acuerdo con la infracción cometida.

Por último, en lo referente a la comisión de delitos en materia de tratamiento indebido de datos personales, el artículo 67 manifiesta que se imponen penas de 3 meses a 3 años de prisión al responsable o tercero autorizado para tratar la información, que con ánimo de lucro, provoque la vulneración de la seguridad de las bases de datos que se encuentran bajo su

custodia; igualmente, el artículo 68 señala que se impondrá la pena de 6 meses a 5 años de prisión al que, con la finalidad de obtener un lucro indebido, trate datos personales mediante engaño o se aproveche del error en que se encuentre el titular. El artículo 69 hace la aclaración de que en caso de que los datos sean sensibles, las penas se impondrán al doble.

Entonces, esta ley no sólo regula la protección de datos personales sino también su utilización, es por ello que debe ser observada por las entidades de certificación ya que son en algunos casos particulares que manejan datos personales al realizar sus actividades relacionadas con la firma electrónica, por lo cual deben cumplir con lo dispuesto con los artículos anteriores, con la finalidad de que el tratamiento de los datos personales de los solicitantes de sus servicios se lleve a cabo con total seguridad y confidencialidad, sin que esto exente a las entidades de satisfacer las obligaciones que le impone la legislación comercial.

Así, al permitir que existan entidades de certificación que obtengan su acreditación por medio de una afirmativa ficta, sin verificar que cumplen con los elementos necesarios para operar, pone en peligro el derecho de protección y conservación de datos personales, descrito en esta ley, de los solicitantes de sus servicios.

2.9. Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación.

Publicado en el Diario Oficial de la Federación el 19 de julio de 2004, este Reglamento del Código de Comercio, de acuerdo con su artículo 1º tiene como objetivo establecer las normas reglamentarias que deberán cumplir los prestadores de servicios de certificación en cuestiones relativas a la firma electrónica y la expedición de certificados para actos comerciales.

El artículo 3 alude que la Secretaría de Economía deberá mantener una relación, actualizada y disponible, de todos los prestadores de servicios de certificación, acreditados o suspendidos, de las personas físicas o morales que actúan a su nombre y de las personas físicas que formen parte de su personal. De igual forma, el artículo 4 explica que la Secretaría deberá integrar un padrón de profesionistas en las materias jurídicas e informática, los cuales se capacitarán con el propósito de que puedan ser peritos o árbitros en materia de prestadores de servicios de certificación y de firma electrónica.

En cuanto a los requisitos que debe cumplir para ser acreditado como entidad certificadora, en relación a lo establecido por el artículo 102 inciso A) del Código de Comercio, el artículo 5 fracción II de este Reglamento indica que se deberá adjuntar a la solicitud el documento que lo acredite para estar en ejercicio de la fe pública en el caso de los fedatarios públicos, o su acta constitutiva para las instituciones públicas y las personas morales de carácter privado. Asimismo, la fracción III de dicho artículo en concordancia con la fracción II del artículo 102 apartado A) del Código de Comercio, instaura que la entidad de certificación deberá comprobar que cuenta con los elementos humanos, materiales, económicos y tecnológicos necesarios para operar.

En el caso de los notarios y de corredores públicos podrán solicitar su acreditación por medio de personas morales, pero el artículo 6 aclara que esto no los eximirá de su responsabilidad individual, ni aun cuando compartan la infraestructura que les permita realizar los servicios para obtener la acreditación.

Previo al inicio de sus operaciones, el artículo 8 menciona que la entidad certificadora tendrá un plazo de 10 días siguientes a que se haya autorizado la procedencia de su acreditación, para obtener de una compañía debidamente autorizada la fianza que presentará a la Secretaría.

La fianza deberá mantenerse vigente y actualizada, como indica el artículo 12, en los siguientes casos: durante su acreditación y el año siguiente a su término, cese o revocación; cuando sea suspendido temporalmente; y cuando se haya iniciado un procedimiento administrativo o judicial en contra de la entidad certificadora y hasta que concluya.

El artículo 13 establece que la fianza podrá hacerse efectiva, cuando el prestador de servicios de certificación cause daños o perjuicios a sus usuarios por incumplimiento de sus obligaciones o por el indebido desempeño de sus funciones, la fianza también cubrirá los gastos que haga la Secretaría por sustituirlo cuando sea suspendido, inhabilitado o cancelado su ejercicio.

El artículo 9 dispone que una vez que se presente la fianza, la Secretaría de Economía verificará que cumpla con los requisitos necesarios, para posteriormente expedir el certificado respectivo a la entidad de certificación y lo registrará para que pueda iniciar sus operaciones, dicho certificado tendrá una vigencia de 10 años.

Además, el artículo 10 señala que la Secretaría como autoridad certificadora y registradora, comprobará la identidad del Prestador de Servicios de Certificación o su representante, con el propósito de generar con sus datos de creación su firma electrónica.

Una vez que se cumpla lo anterior, como lo indica el artículo 14, el prestador de servicios de certificación deberá notificarle a la Secretaría por escrito del inicio de sus funciones, dentro de los 45 días después de iniciada su actividad.

Por otra parte, el artículo 15 expone que las entidades de certificación deberán proporcionarle a la Secretaría de Economía su dirección electrónica, la cual deberá incluirse en todos los certificados que expida, para poder verificar

de manera inmediata su validez, suspensión o revocación; la Secretaría la agregará a un dominio propio de consulta en línea a través del cual la parte que confía podrá cerciorarse del estado del certificado.

De igual forma, el artículo 16 estipula que las entidades certificadoras deberán enviar por línea una copia de los certificados que expidan, éstos serán resguardados por la Secretaría bajo el más estricto mecanismo de seguridad física y lógica.

La emisión, registro y conservación de los certificados por parte de los prestadores de servicios de certificación, como lo señala el artículo 19, se hará dentro del país, y la Secretaría de Economía determinará mecanismos que garanticen que los certificados emitidos por una entidad de certificación no contengan datos que generen confusión a la parte que confía.

No obstante lo anterior, de acuerdo con el artículo 20, la Secretaría podrá autorizar que el resguardo de los datos de creación de la firma electrónica se hagan en el extranjero, en este caso la entidad certificadora deberá asumir los costos que impliquen el traslado de los servidores públicos de la Secretaría para la realización de las auditorías.

Asimismo, el artículo 21 apunta que cualquier cambio de domicilio o modificación del objeto social o estatus de la entidad certificadora deberá ser informado a la Secretaría de Economía, con la finalidad de que ésta verifique si sigue cumpliendo con los requisitos para estar acreditada como tal.

Para el caso de las auditorías, con motivo de visitas de verificación que se le harán a los prestadores de servicios de certificación, el artículo 22 señala que se desahogarán en términos de la Ley Federal de Procedimiento Administrativo, y se podrán practicar de oficio o a petición del titular del certificado, firmante o la parte que confía.

Por último, el artículo 23 menciona que las infracciones y sanciones se aplicarán sin perjuicio de las demás responsabilidades en que puedan incurrir los prestadores de servicios de certificación o su personal. Las sanciones podrán ser temporales o una suspensión definitiva, dependiendo de la gravedad de la infracción, estas se encuentran explicadas en los artículos 24, 25, 26 y 27, los cuales vemos en el siguiente capítulo.

De esta forma, el artículo 28 expone que cuando la entidad certificadora sea suspendida se le revoca su certificado, de manera temporal o definitiva, se le agregará a la lista de certificados revocados y se publicará un extracto de la resolución en el Diario Oficial de la Federación, con la finalidad de que los usuarios verifiquen si la entidad puede o no ejercer sus funciones.

Aunque este reglamento habla detalladamente de algunos aspectos relacionados con las entidades de certificación que no quedan especificadas en el Código de Comercio, otras cuestiones aun quedan poco claras, es por ello que la Secretaría de Economía emitió una serie de reglas generales que terminan por explicar todo lo concerniente a estas entidades, mismas reglas que vemos a continuación.

2.10. Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación.

Las Reglas Generales fueron expedidas por la Secretaría de Economía y publicadas el 10 de agosto de 2004 en el Diario Oficial de la Federación y las últimas reformas fueron publicadas el 5 de marzo de 2007 en el mismo diario, con fundamento en los artículos 102 inciso A) fracción V, 104 fracción IV y VI, 105 y 113 del Código de Comercio y de los artículos 2, 3 párrafo primero, 4 fracción IV y V, 5 segundo párrafo, 6 segundo párrafo, 9, 10 fracción III, 11, 12 y 16 fracción III del Reglamento del Código de Comercio en materia de prestadores de servicios de certificación.

Conformadas por 11 reglas que a su vez se encuentran subdivididas en varias partes, estas reglas fueron emitidas con el propósito de que la Secretaría determinará lo relacionado con los requisitos para acreditarse como entidad de certificación, así como las obligaciones y demás procedimientos que tengan que cumplir estas últimas, y que no quedaron estipuladas en los preceptos que son fundamentos de las reglas.

En lo referente a los elementos humanos, materiales, económicos y tecnológicos con que deben contar las entidades certificadoras o solicitante de acreditación de acuerdo con la regla 2 bis, en el caso de que además de la emisión de certificados preste otros servicios de firma electrónica, como conservación de datos, sellado digital de tiempo y validación de certificados, deberá cumplir para cada servicio adicional lo siguiente:

- Contar con elementos tecnológicos relacionado con los servicios adicionales.
- Proceso de evaluación continua para la adecuada valoración de riesgos a condiciones cambiantes del entorno, respecto de cada servicio.
- Si ya cuenta con acreditación, y solicita su acreditación para otro servicio de firma electrónica, se tendrán por cumplidos los elementos humanos, materiales y económicos.

En cuanto a los elementos humanos, los profesionales jurídicos e informáticos, la regla 2.1 refiere que serán los responsables de aprobar el plan de continuidad de negocios. Por consiguiente, deberán cumplir con algunos requisitos con la finalidad de demostrar que cuentan con los conocimientos necesarios para realizar sus actividades dentro de las entidades de certificación de manera responsable.

La regla 2.1.3.8 explica que a partir del inicio de actividades de la entidad de certificación, esta deberá contar y notificar a la Secretaría en un plazo no mayor de 6 meses que cuenta con la totalidad del personal auxiliar del

profesional de informática, con excepción del Oficial de Seguridad que deberá ser designado desde la solicitud de acreditación.

Asimismo, la regla 2.1.5 determina que la entidad certificadora deberá presentar, y mantener actualizada ante la Secretaría el procedimiento de reclutamiento, selección, evaluación y contratación de sus elementos humanos, así como la forma de corroborar los antecedentes de los mismos.

Además, la regla 2.1.6 señala que todo el personal que maneje información confidencial deberá suscribir un contrato de confidencialidad con el prestador de servicios de certificación, que se extenderá más allá de la vigencia de su contrato laboral o en el caso de ser una empresa externa del contrato de servicios.

Para terminar con lo relacionado a los elementos humanos, la Secretaría de Economía, de acuerdo con la regla 2.1.4, podrá solicitar los exámenes aplicados al personal para verificar sus conocimientos y habilidades.

Por otra parte, la regla 2.2 expone que en cuanto a los elementos materiales la entidad de certificación deberá contar con un espacio físico apropiado para la actividad a realizar, así como controles de seguridad, medidas de protección y políticas necesarias para garantizar la seguridad de áreas destinadas a la realización de un servicio en específico a las que puedan acceder sólo el personal autorizado.

La regla 2.3 refiere que los elementos económicos comprenderán por lo menos, un seguro cuyo monto para cada año será determinado por la Secretaría de Economía, con base a las operaciones comerciales en que sean utilizados los certificados emitidos por la entidad certificadora, pero no será menor a 30 veces el salario mínimo general diario vigente en el Distrito Federal,

si presta otros servicios además de emitir certificados el seguro deberá cubrir la totalidad de ellos.

Finalmente, la regla 2.4 manifiesta que los elementos tecnológicos y sus procedimientos deberán ser compatibles con las normas y criterios internacionales, en materia de políticas de seguridad, declaración de prácticas de certificación, estructura de certificados, análisis de riesgos y amenaza, etc.

Por su parte, la regla 2.4.7 habla de la estructura de los certificados, la cual deberá ajustarse a las siguientes características:

- La estructura de los datos que contenga debe ser compatible con el estándar ISO/IEC 9594-8[85] (el cual establece algunos de los requisitos de seguridad en la áreas de autenticación y otros servicios de seguridad a través de la prestación de un conjunto de marcos en los que se pueden basar los servicios completos), y contener los datos que aparecen en el artículo 108 del Código de Comercio.
- Los algoritmos utilizados para la firma electrónica avanzada deben ser compatibles con los estándares de la industria RFC 3280, Internet X509 *Public Key Infrastructure Certificate and Certificate Revocation List, Profile, R. Housley, W. Polk, W. Ford,* D. Solo, *April* 2002[86] (menciona especificaciones del formato y la semántica de los certificados y lista de revocación de los mismos, al igual que describe los procedimientos para el procesamiento de rutas de certificación en el entorno de Internet, o los que les sustituyan que provean un nivel adecuado de seguridad).
- El tamaño de las claves utilizadas para la generación de la firma electrónica avanzada deberá proveer el nivel de seguridad de 1024 bits para los usuarios y de 2048 bits para las entidades de certificación.

---

[85] ISO, ISO/IEC 9594-8: 2008, [En línea] Disponible: http://www.iso.org/iso/catalogue_detail.htm?csnumber=53372 10 de Octubre 2014 20:08 P.M.

[86] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, [En línea] Disponible: http://www.ietf.org/rfc/rfc3280.txt 10 de Octubre de 2014 20:35 P.M.

- Contendrá la información suficiente para identificar o localizar uno o más sitios de consulta donde se publiquen la notificación de los certificados revocados.

El solicitante, como lo marca la regla 2.5, deberá entregar los documentos que confirmen el cumplimiento de los requisitos para ser acreditado como prestador de servicios de certificación, cuando se trate de documentos públicos en copia certificada o simple, o si son documentos privados en copia simple, o una copia en disco compacto de toda la documentación.

En lo referente a la fianza a la que alude el artículo 102 inciso A) fracción V del Código de Comercio, la regla 3.2 indica que ésta se expedirá a favor de la tesorería de la federación, por el monto mínimo equivalente a 5 mil veces el salario mínimo diario vigente en el Distrito Federal, que incrementará por cada persona física o moral que preste servicios de certificación a nombre o por cuenta del solicitante.

Sin embargo, la regla 3.3 establece que en el caso de que se le acredite para expedir certificados y realizar otros servicios adicionales de firma electrónica, se deberá aumentar el monto antes señalada hasta cubrir todos los servicios.

En el caso de los datos de creación de la firma de la entidad certificadora, la regla 4.2 determina que se generará en el nivel más alto de sus instalaciones con la finalidad de dar certeza y seguridad de toda la información para la creación, y se llevará a cabo bajo supervisión de la Secretaría de Economía.

Ahora bien, en cuanto a la copia del certificado a la que se refiere el artículo 16 del Reglamento del Código de Comercio en materia de prestadores

de servicios de certificación, la regla 5 menciona que debe ser enviada por línea a la Secretaría de Economía en tiempo real, es decir, inmediatamente, salvo que por caso fortuito o de fuerza mayor comprobable, no pueda enviarlo, deberá hacer la réplica en un término de 6 horas.

Además, la entidad de certificación deberá remitir dicha copia en medios ópticos o electrónicos a la Secretaría dentro de las 24 horas siguientes a la expedición del certificado. Asimismo, la entidad deberá cerciorarse de que la copia sea recibida por la Secretaría.

La fecha y hora de emisión del certificado o de la prestación del servicio de firma electrónica, como lo señala la regla 7, se determinará a través de un registro de sellos digitales de tiempo que deberá llevar la entidad certificadora u otra persona física o moral que lo lleve a nombre y a cuenta de la entidad. Pero en cualquier caso el sistema de sellado o estampado de tiempo deberá cumplir con el estándar internacional RFC 3161, Internet X.509 *Public Key Infrastructure Time Stamp* [87] (documento que describe el formato de solicitud de las autoridades de sellado de tiempo y de la respuesta, asimismo establece los requisitos de seguridad para el funcionamiento de estas autoridades).

La Secretaría de Economía, como lo indica la regla 8, verificará que los prestadores de servicios de certificación cumplan con la estructura de certificados establecidos en estas reglas generales, el Código de Comercio, el Reglamento, así como los estándares internacionales, para que en ningún caso, contenga elementos que causen confusión a la parte que confía.

La regla 9 explica que se estará a lo dispuesto en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental para

[87] Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), [En línea] Disponible: https://www.ietf.org/rfc/rfc3161.txt 10 de Octubre de 2014 21:04 P.M.

determinar los casos en que estará a disposición el contenido privado del registro de certificados de la entidad de certificación.

Por último, la regla 10 refiere que si la entidad de certificación decide el cese de manera voluntaria de sus actividades, previo pago de derechos, deberá informar a la Secretaría de Economía el motivo con 45 días de anticipación, para que ésta se cerciore de que cumplió con lo establecido en el artículo 16 del Reglamento y la regla 5 de estas reglas generales.

En conclusión, estas reglas terminan por esclarecer lo relacionado con los elementos humanos, materiales, tecnológicos y económicos, lo referente al monto de la fianza, lo concerniente a los certificados digitales, entre otros aspectos, que ni el Código de Comercio ni el Reglamento precisan, es por ello que ambas legislaciones se remiten a lo determinado en estas reglas generales, por lo cual son parte fundamental de la regulación de los prestadores de servicios de certificación.

2.11. Norma Oficial Mexicana NOM-151-SCFI-2002.

Publicada el 4 de junio de 2002 en el Diario Oficial de la Federación, y expedidas por la Secretaría de Economía, tiene como objetivo establecer los requisitos que se deberán observar para la conservación de mensajes de datos que contengan contratos, convenios o compromisos y que por consecuencia originen el cumplimiento de derechos y obligaciones.

Primeramente, los mensajes de datos podrán ser almacenados en uno o varios archivos diferentes y/o en varias computadoras, en la conservación de estos mensajes intervendrán los siguientes elementos: los prestadores de servicios de certificación para la emisión de la firma electrónica o digital y la constancia que se emita; y los programas informáticos en y con los que se almacenen los mensajes.

Antes de tratar lo referente a la conservación de mensaje de datos, se debe ver el *Front End Comunicaciones*, el cual es descrito en la misma Norma Oficial como un programa desarrollado para manejar las comunicaciones con estructura cliente/servidor, diseñado para aplicaciones que requieren intercambiar datos en tiempo real, es decir, es un mecanismo de enlace entre clientes y servidores. Se encarga de:

a. Autenticar a los clientes que deseen establecer comunicaciones con algún servidor.

b. Notificar la conexión o desconexión de un cliente al servidor adecuado.

c. Notificar a los clientes si un servidor está o no en servicio.

d. Verificar continuamente el estado de los clientes y servidores conectados.

Ahora bien, el esquema de operación del *Front End Comunicaciones* es el siguiente: el programa se encarga de aceptar las conexiones de los clientes, realiza la autentificación de los clientes y servidores, y posteriormente registra y transmite los mensajes de los clientes al servidor y viceversa.

En el *Front End Comunicaciones* los mensajes tiene dos partes: encabezado y cuerpo, debido a que utilizan un protocolo de comunicación abierto. En cuanto al encabezado, la longitud dependerá del destinatario, así si el mensaje es enviado por los clientes y servidores al programa, su longitud será de 4 bytes y tendrá los siguientes campos: destino, instrucciones o procesamiento a realizar y el tamaño del cuerpo del mensaje.

Al contrario, si el mensaje es enviado por el *Front End Comunicaciones* a los servidores, tendrá una longitud de 12 bytes, y se conformará por los campos de: origen, instrucción o procesamiento a realizar, fecha, hora y tamaño del cuerpo del mensaje.

Por otra parte, el cuerpo del mensaje varía de longitud, pero debe respetar el formato que previamente se estableció entre quien lo envía y el que debe ejecutar la acción solicitada. El formato de un mensaje es una secuencia de tipos de datos básicos que describen su contenido, y para facilitar la lectura e interpretación de la secuencia se le asigna un símbolo.

En relación con la conservación de los mensajes de datos, se seguirá un protocolo de comunicación entre el software de almacenamiento y el prestador de servicios de certificación, y se deberá hacer lo siguiente:

1. El usuario generará archivos parciales a partir de sus mensajes de datos, para formar estos archivos se crea un mensaje en formato ASN.1 que contiene: nombre del archivo del sistema de información donde está o estuvo almacenado el contenido del archivo; el tipo del archivo y el contenido del mismo.

2. Con estos archivos parciales se hará un expediente, para conformar este expediente se creará un mensaje ASN.1 que contendrá: el nombre del expediente, que coincidirá con el nombre de identificación en el sistema de información donde esta o estuvo almacenado; un índice; la identificación del operador del sistema de conservación y su firma. El expediente se deberá enviar a la entidad certificadora.

3. El prestador de servicios de certificación generará una constancia en formato ASN.1 que señalará: el nombre del archivo donde se almacena la constancia; el expediente enviado por el sistema de conservación; fecha y hora de creación de la constancia; la identificación de la entidad de certificación y su firma digital. La constancia se deberá registrar en las bases de datos de la entidad certificadora y se enviará una copia del mensaje ASN.1 al usuario.

4. Y el usuario deberá almacenar la constancia como considere conveniente.

Se verificará la autenticidad de la constancia, por medio de los siguientes pasos:

a) Verificar la firma digital del prestador de servicios de certificación.

b) Verificar la firma digital del operador del sistema de conservación.

c) Recalcular el compendio de archivos parciales y cerciorarse de que coincidan con los asentados en el expediente.

Así, esta Norma Oficial Mexicana planteó los principios de la conservación de mensajes de datos por parte de las entidades de certificación, igualmente es la precursora de los cambios que con posterioridad se harían al Código de Comercio en materia de prestadores de servicios de certificación y firmas electrónicas avanzadas.

Entonces, por lo expuesto la regulación de los prestadores de servicios de certificación en nuestro país se desprende de las leyes modelo en materia de comercio electrónico y de firmas electrónicas, aunque no todas las legislaciones se aplican directamente a las entidades de certificación, si les conciernen de manera indirecta, ya que regulan principalmente la función certificadora de estas entidades, y aunado a ello garantizar el derecho de conservación y protección de datos personales.

Pero es precisamente en la normatividad que se le aplica directamente en donde se encuentran las más grandes deficiencias, ya que es en el Código de Comercio donde se permite a estos prestadores de servicios de certificación recibir su acreditación por el simple transcurso del tiempo, sin que pasen por una exhaustiva revisión de sus elementos humanos, tecnológicos, materiales y económicos; lo cual posibilita que no cumplan sus funciones con seguridad, certeza y confiabilidad, y con ello se pone en peligro los datos personales de los comerciantes que solicitan sus servicios y los derechos de los usuarios que confían en el certificado digital, por lo cual se refuerza la idea de que la afirmativa ficta como medio para acreditar a las entidades de certificación debe ser derogado de las legislación comercial, y con ello asegurar que los solicitantes de acreditación pasen por todo el proceso necesario y se

compruebe que cuenta con la infraestructura suficiente para realizar sus funciones.

CAPÍTULO TERCERO.

ENTIDAD DE CERTIFICACIÓN.

Como se ha descrito y justificado las entidades de certificación o prestadores de servicios de certificación o autoridad certificadora es una figura que proporciona seguridad y fiabilidad al comercio electrónico, pues es a través de sus servicios relacionados con la firma electrónica que brindan confianza a los usuarios de ésta y con ello al comercio electrónico.

Es por ello que en este capítulo se precisan algunos aspectos para entender la importancia que tiene esta figura jurídica en relación con la firma electrónica, y sobre todo como ayuda a la realización de actividades comerciales por medios electrónicos.

3.1 Concepto.

Como ya se explicó en el aparatado Prestadores de Servicios de Certificación del Capítulo I de la presente investigación, los prestadores de servicios de certificación son personas físicas o morales o instituciones públicas, que con la debida acreditación, expiden certificados de firma electrónica o prestan algún otro servicio relacionado con esta última.

Ahora bien, ¿quiénes pueden ser entidades de certificación?, pues de acuerdo con lo previsto en el artículo 100 del Código de Comercio, podrán serlo:

a) Los notarios o corredores públicos.

b) Las personas morales de carácter privado.

c) Las instituciones públicas, conforme a las leyes que les son aplicables.

En lo referente a los notarios y corredores públicos, como bien lo señala el artículo anterior, la expedición de certificados no conlleva por sí misma la fe pública, por lo que notarios o corredores podrán extenderlos implicando o no esta última.

De esta forma, es de notar que los certificados digitales que emitan los notarios o corredores públicos en su calidad de prestadores de servicios de certificación podrán estar o no investidos de fe pública, sin que este hecho afecte la valides y autenticidad del certificado ni de su contenido.

Respecto a las personas morales de carácter privado son sociedades legalmente constituidas, que tienen como objeto social:

1. Verificar la identidad de los usuarios y su vinculación con la firma electrónica.
2. Comprobar la integridad y suficiencia del mensaje de datos y verificar la firma electrónica del solicitante.
3. Tener registros de los elementos de identificación del firmante y de la información con la que haya verificado el cumplimiento de fiabilidad de las firmas electrónicas avanzadas y emitir el certificado.
4. Cualquier otra actividad, siempre que no sea incompatible con las anteriores.

Luego, las personas morales de carácter privado que solicitan su acreditación como prestadores de servicios de certificación son sociedades mercantiles legalmente constituidas de acuerdo con las leyes aplicables, que deben tener como objeto social los puntos antes mencionados. Los certificados que emitan estas sociedades como entidad de certificación tendrán el valor que los emitidos por el notario o corredor público.

En el caso de las instituciones públicas, esta son entidades certificadoras siempre que se encuentran facultadas por las leyes que le son aplicables, por

ejemplo la Secretaría de Economía, el Servicio de Administración Tributaria, la Secretaría de la Función Pública, etc. A pesar de ello, deberán cumplir con los mismos requisitos para ser acreditado como prestadores de servicios de certificación que el notario o corredor público y las sociedades.

Por consiguiente, en nuestro país, y de acuerdo a las leyes vigentes, los prestadores de servicios de certificación serán los notarios o corredores públicos, personas morales de carácter privado o instituciones públicas, que estando debidamente acreditadas, proporcionan servicios de expedición de certificados de firma electrónica o cualquier otro que se relacione con la misma, como por ejemplo la conservación de datos o sellado digital de tiempo, etc. Aunque, las instituciones públicas estarán autorizadas a realizar otro tipo de actividades, ya que estas además de estar reguladas de acuerdo con la legislación mercantil, también están reguladas por las leyes que las facultan para realizar actividades de certificación. Pero independientemente de ello, su principal función será la de expedir certificados electrónicos, dichos certificados tendrán la misma validez sin importar que lo expida un fedatario público, una entidad pública o una sociedad mercantil, siempre que estén autorizados para fungir como entidad de certificación.

3.2 Fundamento jurídico.

El fundamento jurídico de las entidades de certificación lo encontramos en el Código de Comercio en su Capítulo III llamado De los Prestadores de Servicios de Certificación del Título Segundo denominado De Comercio Electrónico, ubicado en el Libro Segundo nombrado Del Comercio en General, el cual comprende los artículos 100 al 113.

En los cuales se encuentra insertado lo dispuesto en la Ley Modelo de la CNUDMI sobre firmas electrónicas, estableciendo lo relativo a los sujetos que pueden prestar servicios de certificación, que ya se estudio con exhaustividad

en el Capitulo anterior, las obligaciones que tienen, los requisitos que deberán cumplir para acreditarse como tales, y lo relacionado con el certificado digital.

Aunado a lo establecido en el Código de Comercio, deberán de cumplir con lo estipulado en el Reglamento de dicho código aplicable a los prestadores de servicios de certificación, así como las reglas generales que fueron expedidas por la Secretaría de Economía.

3.3 Naturaleza jurídica.

La naturaleza jurídica de los prestadores de servicios de certificación, como lo menciona el jurista Gabriel Andrés Cámpoli,[88] es considerada mercantil porque aunque su actividad no se encuentra tipificada como acto de comercio, las entidades de certificación tienen su fundamento y nacen de lo estipulado en el Código de Comercio.

Igualmente, tiene naturaleza mercantil en el carácter de auxiliares independientes, en la inteligencia de que estos, de acuerdo con el Doctrinario Raúl Cervantes Ahumada, son: "profesionales que ofrecen sus servicios al público, para auxiliarlo en la celebración de negocios mercantiles"[89]

Por su parte el Maestro Alfredo Morles Hernández señala que son: "personas cuya actividad profesional está dirigida a dispensar su mediación a los comerciantes para facilitarles la conclusión de sus contratos."[90]

La Doctora Elvia Arcelia Quintana Adriano, citada en la Antología de Derecho Mercantil I de la Universidad América Latina, alude que los auxiliares

---

[88] *Vid.* CÁMPOLI, Andrés Gabriel, La firma electrónica en el régimen comercial mexicano, Editorial Porrúa, México, 2004, p. 26.
[89] CERVANTES AHUMADA, Raúl, Derecho mercantil, 3ª edición, Editorial Porrúa, México, 2004, p. 293.
[90] MORLES HERNÁNDEZ, Alfredo, Curso de Derecho Mercantil, Tomo 1, 9ª edición, Editorial Universidad Católica Andrés, Venezuela, 2007, p. 507.

independientes o del comercio son: “todos aquellos que conservan su independencia en el desarrollo de su trabajo, ante el empresario o la negociación. Estas personas son los corredores, contadores públicos, auditores, comisionistas o intermediarios”[91]

El doctrinario Roberto Mantilla Molina[92] menciona que los auxiliares independientes son las personas que no están subordinados a ningún comerciante en particular, que por el contrario realizan actividades para cualquiera que lo solicite.

Por lo tanto, son llamados auxiliares independientes porque no dependen directamente del comerciante sino que prestan sus servicios para ayudar a realizar la actividad comercial en general.

Y en el caso que nos ocupa, los prestadores de servicios de certificación se pueden considerar auxiliares del comercio toda vez que sus servicios auxilian a la realización del comercio electrónico, en específico con relación a la firma electrónica, además de que no dependen del comerciante que contrata sus servicios sino que realizan su actividad de forma independiente. Por ende, las entidades de certificación, al igual que el corredor público, es un intermediario o mediador en las transacciones comerciales entre dos o más partes, que al certificar la identidad del remitente del mensaje de datos genera la confianza necesaria para que el comercio electrónico se lleve a cabo.

En relación con la actividad certificadora de los prestadores de servicios de certificación, si bien no conlleva la fe pública, tiene como finalidad brindar seguridad a las personas que realizan actividades comerciales por medios

---

[91] BECERRA ZAVALA, Roberto (comp.), Antología de Derecho Mercantil I, Editorial Universidad América Latina, México, 2011, p. 2 [En línea] Disponible: http://ual.dyndns.org/Biblioteca/Derecho_Mercantil/Pdf_08.pdf 14 de septiembre de 2014 21:42 P.M.

[92] MANTILLA MOLINA, Roberto L., Derecho Mercantil, 29º edición, Editorial Porrúa, México, 2005, p. 161

electrónicos, ya que al garantizar que la persona que hizo uso de la firma electrónica en un mensaje de datos, es la que posee los datos de creación de la misma y es quien dice ser, proporciona con ello certeza y fiabilidad a la parte que confía en el certificado que se expide.

En conclusión, la naturaleza jurídica de una entidad de certificación es mercantil, aun cuando la actividad que realiza no se encuentre contemplada en el Código de Comercio, ya que nacieron de este Código, y además porque son considerados como auxiliares independientes del comercio, porque los servicios que proporcionan ayuda al comercio electrónico al comprobar la identidad del firmante del mensaje y emitir el certificado digital.

3.4 Requisitos de constitución.

Los requisitos que debe cumplir el solicitante para ser acreditado como prestador de servicios de certificación, se encuentran contemplados en el artículo 102 inciso A) del Código de Comercio, el artículo 5 del Reglamento del Código de Comercio en materia de prestadores de servicios de certificación y en la reglas generales expedidas por la Secretaría de Economía.

En general, los requisitos que deberán cubrir los solicitantes son los siguientes:

1. Solicitar a la Secretaría de Economía la acreditación como prestador de servicios de certificación. En esta solicitud se deberá especificar, si además de ser acreditado para expedir certificados digitales, desea ser acreditado para prestar otros servicios de firma electrónica, como lo son la conservación de datos, el sellado digital de tiempo, la validación de certificados, etc.

De acuerdo con el Registro Federal de Trámites y Servicios[93], la solicitud se hace por medio de escrito libre que debe contener la siguiente información:

- Lugar y fecha de emisión del escrito.
- Debe estar dirigida a la Dirección General de Normatividad Mercantil.
- Nombre del solicitante.
- Nombre del representante legal, si lo nombró.
- Domicilio para recibir notificaciones, teléfono y correo electrónico, así como el nombre de la persona o personas autorizadas para recibirlas.
- Petición expresa de solicitar la acreditación y expedición de su certificado.
- Firma del solicitante.
- Si se trata de persona física, su Clave Única de Registro de Población.(CURP)

2. A la solicitud se deberán adjuntar los siguientes documentos:

a) Los notarios o corredores públicos: copia certificada de la patente, título de habilitación o documento que lo acredite para ejercer la fe pública.

b) Personas morales: copia certificada de su acta constitutiva, póliza u otro instrumento público que acredite su constitución y que su objeto social es el establecido en el artículo 101 del Código de Comercio.

c) Instituciones públicas: copia certificada del instrumento jurídico de su creación o de su acta constitutiva.

3. De igual forma, anexar a la solicitud una carta suscrita por cada persona física que pretenda operar o tener acceso a los sistemas que se utilizaran donde dicha persona manifieste, bajo protesta de decir verdad, que no fue condenado por delito contra el patrimonio de las personas, ni que ha sido inhabilitado para ejercer su profesión, o para desempeñar un puesto de servicio público, en el sistema financiero o para ejercer el comercio, tal como lo

[93] Registro Federal de Trámites y Servicios, Acreditación como Prestador de Servicios de Certificación, [En línea] Disponible: http://187.191.71.208/tramites/FichaTramite.aspx?val=33499 19 de septiembre de 2014 23:28 P.M.

menciona el artículo 5 fracción V del Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación.

4. También, añadir a su solicitud, un escrito en que la entidad de certificación exteriorice su conformidad para ser sujeto a auditoría por parte de la Secretaría de Economía en todo momento. En el caso de que el solicitante pretenda que sus datos de creación de firma electrónica permanezcan resguardados fuera de territorio nacional, deberá pedirlo a la Secretaría y declarar por escrito que se hará cargo de los costos que impliquen el traslado del personal para realizar la auditoria.

5. Entregar junto con la petición el comprobante de pago de derechos, el monto del pago por la acreditación como prestador de servicios de certificación de firma electrónica, con fundamento en el artículo 78 fracción II de la Ley Federal de Derechos, es de doscientos y un mil setecientos treinta y dos pesos y treinta y cuatro centavos en moneda nacional; si la entidad certificadora solicita la acreditación para prestar otros servicios adicionales de firma electrónica la cantidad a pagar, con fundamento en el artículo 78 fracción VI de la Ley Federal de Derechos, es de ciento veintinueve mil novecientos treinta y tres pesos y sesenta y tres centavos en moneda nacional.

6. Deberá contar al momento de la solicitud con los elementos:

A) Humanos: un profesionista jurídico, uno informático y cinco auxiliares de apoyo informático.

El profesional jurídico deberá:

a. Ser licenciado en derecho con título y cédula profesional registrado en la Secretaría de Educación Pública.

b. Demostrar que cuenta con al menos 2 años de experiencia en materia notarial o correduría pública, o en materia mercantil y servicios, procedimientos o actividades relacionadas con la acreditación de personalidad, se acreditará mediante declaración ante fedatario público.

c. Acreditar al menos un año de experiencia, que sea comprobable, en cualquier área del derecho informático o comercio electrónico, se acreditará mediante declaración ante fedatario público.

d. Cumplir con los requisitos señalados en el Código de Comercio y el Reglamento.

e. Comprobar que conoce la operación como usuario de los sistemas informáticos que habrá de utilizar la entidad certificadora, se acreditará por medio de declaración ante fedatario público.

f. Solicitar el examen para encargado de identificación correspondiente, que le aplicará la Secretaría de Economía, dentro de los 45 días siguientes a la presentación de la solicitud de acreditación, previa notificación de la fecha, hora y lugar de aplicación.

El profesional informático, y el personal auxiliar de este, deberán:

a) Ser licenciado o ingeniero informático o afín con título y cédula profesional registrados en la Secretaría de Educación Pública.

b) Tener por lo menos 2 años de experiencia en el campo de la seguridad informática, comprobables mediante declaración ante fedatario público.

c) Contar con diploma en seguridad informática o tener un certificado en esa área como: *GIAC Gold Standard Certificates*[94] (GGSC) (certificado emitido por la *Global Information Assurance Certification*[95] (GIAC) el cual avala que el titular del certificado comprende los conocimientos y habilidades necesarias en la áreas clave de la seguridad informática), *GIAC Security Leadership Certificate*[96] (GSLC) (expedido de igual forma por el GIAC está destinado a los profesionales con responsabilidad gerencial o de supervisión del personal de seguridad informática), CISSP *Certification* el *Certified Information Systems Security Professional*[97] *(*emitido por la *Information System Security Certification Consortium (ISC*^{2}*)* el cual confirma el conocimiento de un individuo

---

[94] *Global Information Assurance Certification, Certifications*, [En línea] Disponible: http://www.giac.org/certifications 11 de Octubre de 2014 13: 11 P.M.
[95] *Ídem.*
[96] *Ídem.*
[97] *Information System Security Certification Consortiu, Credentials*, [En línea] Disponible: https://www.isc2.org/credentials/default.aspx 11 de Octubre de 2014 15: 33 P.M.

en el campo de seguridad de la información) y SSCP *Certification* el *Systems Security Certified Practitioner*[98] (otorgado igualmente por la ISC^2 asegura que el titular del certificado tiene los conocimientos necesarios para proteger los sistemas informáticos contra las amenazas de seguridad), o algún otro que sea equivalente.

d) Cumplir con los requisitos estipulados en el Código de Comercio y en el Reglamento.

Por lo que hace al personal auxiliar del profesional informático, éste estará compuesto por: un oficial de seguridad, un administrador de sistemas, un operador de sistemas, un administrador de bases de datos y un administrador de redes, los cuales deberán:

a. Ser técnicos, licenciados o ingenieros en área informática o afín.

b. Tener por lo menos 4 años de experiencia en el área de informática, comprobable por medio de declaración ante fedatario público. De igual forma tener cuando menos 2 años de experiencia en el campo de la seguridad informática, comprobable de la misma forma.

c. Certificación en manejo de *software* o *hardware* en relación con la seguridad informática.

B) Materiales: deberán contar, por lo menos, con las siguientes características:

- Las áreas y los servicios de manejo de información confidencial requieren procedimientos de control de acceso, y estar supervisados continuamente, con la finalidad de reducir riesgos.
- Las implantaciones de los controles deberán evitar riesgos, daño o pérdida, alteración o sustracción de información
- Los accesos físicos a las áreas de generación de certificados, gestión de revocación de los mismos y áreas de residencia de servicios, deberán estar protegidos por puertas y muros sólidos y firmes, chapas seguras,

[98] *Ídem.*

controles de acceso, sistemas de extinción de incendios, alarmas de seguridad y estar limitado al personal autorizado mediante controles de autenticidad.

- El acceso de visitantes a los espacios con información confidencial, deberá ser autorizada por el Oficial de Seguridad, el visitante deberá portar una credencial y se registrará su actividad con la fecha y hora, tanto de ingreso como de salida.
- El documento de Política de Seguridad Física, que deberá presentarse con la solicitud de acreditación y mantenerse actualizado, contendrá: control de acceso físico; protección y recuperación ante desastres; protección contra robo, forzamiento y entrada no autorizada; medidas de protección en caso de incendio, fallas eléctricas o de telecomunicaciones; procedimiento de actualización para autorización del personal a espacios restringidos.
- Los espacios seguros serán oficinas con gabinetes y chapas seguras, dentro del perímetro de seguridad física.
- En relación a la selección y diseño de las áreas seguras, se tomará en cuenta daños por fuego, sismo, inundación, explosión, desordenes civiles y otras formas de desastres naturales y por causas humanas.
- Los servicios claves estarán lejos de los lugares de acceso y atención al público.
- Las fotocopiadoras y fax estarán ubicados en los espacios seguros, sin comprometer la seguridad ni la confidencialidad.
- El material de desecho deberá ser destruido sin posibilidad de recuperación.
- Las puertas y ventanas deberán estar cerradas en todo momento. Además, contará con un sistema de detección de intrusión física en puertas y ventanas.
- Los servicios de procesamiento de información estarán separados de los demás servicios.
- Deberá contar con procedimientos y prácticas de seguridad para el personal dentro del perímetro de seguridad.

- La seguridad física que proponga el solicitante de acreditación, deberá ser compatible con la normas y criterios internacionales y con el estándar ETSI TS 102 042 – sección 7.4.4 *Physical and Environmental security*[99] – (son especificaciones técnicas emitidas por la *Technical Committee Electronic Signatures and Infrastructures*, esta sección en específico señala que la autoridad certificadora debe asegurar que el acceso físico de sus servicios es controlado y que los riesgos físicos son reducidos al mínimo) e ISO/IEC 17799[100] sección 7, (son Técnicas de seguridad un Código para la práctica de la gestión de la seguridad de la información, en especifico la sección 7 menciona la implementación de controles específicos que pueden ser delegados por el propietario conforme sea apropiado, pero el propietario sigue siendo responsable por la protección apropiada de los activos).

C) Económicos: su capital deberá ser por lo menos el equivalente a una cuarta parte de la inversión requerida para cumplir con los otros tres elementos, y un seguro de responsabilidad civil, cuyo monto será determinado por la Secretaría de Economía con base en el análisis de la operaciones comerciales y mercantiles en que se utilicen los certificados, pero no será menor de 30 veces el salario mínimo general diario vigente en el Distrito Federal, si presta otros servicios además de emitir certificados el seguro deberá cubrir la totalidad de ellos.

D) Tecnológicos: consistentes en el análisis y evaluación de riesgos y amenazas; infraestructura informática; equipo de cómputo y software; política de seguridad de la información; plan de continuidad del negocio y recuperación ante desastres; plan de seguridad de sistemas; estructura de certificados y una lista de los revocados; sitio electrónico; procedimientos que informen de las

---

[99] *Technical Committee Electronic Signatures and Infrastructures, Electronic signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates* [En línea] Disponible: http://www.etsi.org/deliver/etsi_ts/102000_102099/102042/02.02.01_60/ts_102042v020201p.pdf 11 de Octubre de 2014 20: 34 P.M.

[100] Tecnología de la Información-Técnicas de seguridad-Código para la práctica de la gestión de la seguridad de la información [En línea] Disponible: https://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf 11 de Octubre de 2014 21:55 P.M.

características de los procesos de creación y verificación de la firma electrónica avanzada; política de certificados; declaración de prácticas de certificación; modelos de las autoridades certificadoras y registradoras; y plan de administración de claves.

7. Contar con procedimientos definidos y específicos para la tramitación de certificados y medidas que garanticen la seriedad de estos, además de la conservación y consulta de los registros.

8. Contar con una póliza de fianza por el monto mínimo equivalente a cinco mil veces el salario mínimo general diario vigente en el Distrito Federal, en caso de que pida ser acreditado para prestar otro servicio de firma electrónica, además de expedir certificados, deberá ampliar la cobertura de la fianza para cubrir todos los servicios. Esta fianza garantizará el pago de los daños y perjuicios a los usuarios de sus servicios, por el incumplimiento de sus obligaciones que haga la entidad de certificación o por el indebido desempeño de sus funciones. De igual manera, cubrirá los gastos que haga la Secretaría por sustituir a la entidad cuando ésta sea suspendida, inhabilitada o cancelada de sus funciones.

9. Registrar ante la Secretaría de Economía su certificado.

Ahora bien, en cuanto a la tramitación para ser acreditado como prestador de servicios de certificación ésta se llevará de acuerdo a lo dispuesto en la Ley Federal de Procedimiento Administrativo, pero sin perjuicio de esto, el artículo 7 del Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación determina que la Secretaría de Economía deberá:

1. Dentro de los 5 días siguientes a la presentación de la solicitud remitir el nombre, nacionalidad, actividad profesional y domicilio del interesado o de su representante legal, según sea el caso, a las Secretarías de Gobernación, Relaciones Exteriores, Educación Pública, Seguridad Pública, Hacienda y Crédito Público, Comunicaciones y Transportes y de la Función Pública, así como a la Procuraduría General de la República y a las autoridades

locales, municipales y extranjeras, con la finalidad de que evalúen la información en el ámbito de su competencia.

2. Dentro de los 20 días siguientes a la recepción de la solicitud, revisar y evaluar la información y documentación recibida, y en caso que falte alguno de los requisitos prevendrá, por una sola vez, al solicitante para que en el término de 20 días contados a partir de la notificación en ventanilla subsane la deficiencia, si transcurre el plazo y no es subsanada la deficiencia se desechará el trámite.

3. Dentro de los 20 días siguientes a la recepción de la solicitud, realizar una visita al domicilio del solicitante para llevar a cabo una auditoria, y cerciorarse de que cumple con los requisitos.

4. Resolver sobre la procedencia o no de la acreditación como entidad certificadora, dentro de los 45 días siguientes a la presentación de la solicitud, la notificación se hará por ventanilla, y no se podrá otorgar más de una acreditación al mismo solicitante.

5. Y por último publicar en el Diario Oficial de la Federación la acreditación otorgada, en un término de 30 días siguientes a la resolución, lo mismo ocurrirá si la Secretaría no resuelve en el término indicado en el punto anterior.

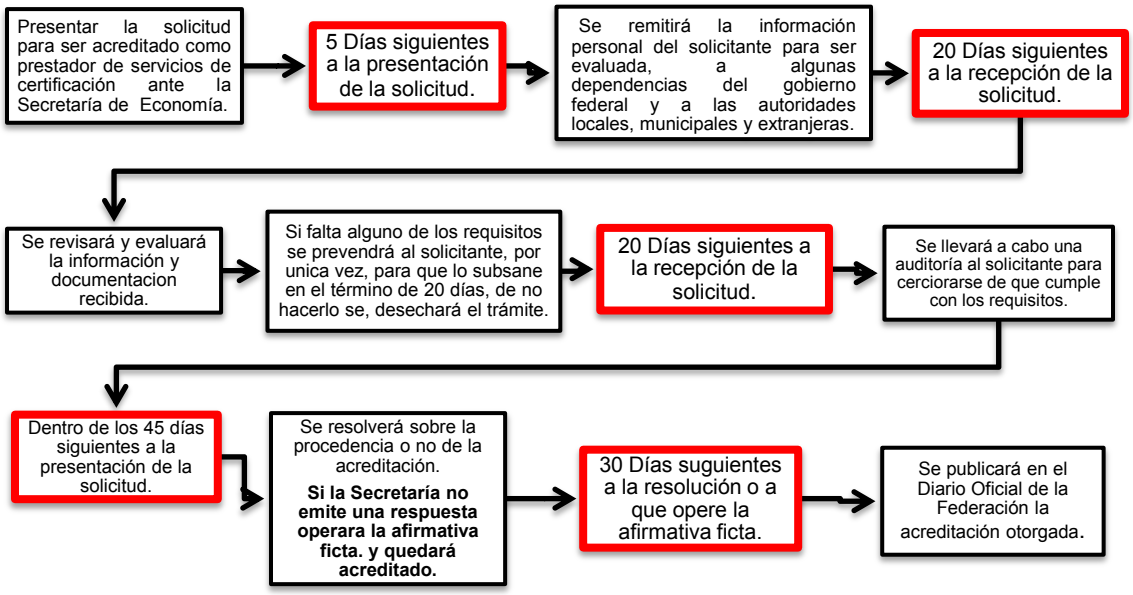

Ilustración 5. Acreditación de Entidades de Certificación.

Así, si los solicitantes cubren todos los requisitos antes explicados no se les podrá negar la petición, se deberá resolver la procedencia o no de la misma dentro de los 45 días siguientes a su presentación, si no se resuelve en este plazo **se tendrá por concedida la acreditación**, esto en conformidad con la dispuesto por el artículo 102 incisos A) y B) del Código de Comercio y el artículo 7 fracción IV del Reglamento de dicho Código en materia de prestadores de servicios de certificación.

3.5 Funciones.

El Doctor Salomón Vargas García[101] postula que la función principal de las entidades de certificación es dar seguridad jurídica y certeza a la firma digital, es decir, su función es autentificar.

Asimismo, la estudiosa Eva Fernández Gómez[102] expone que la principal responsabilidad de la autoridad certificadora es probar que el firmante, a favor del cual se expide el certificado digital, fue reconocido e identificado por la entidad certificadora y es el poseedor de los datos de creación de la firma electrónica.

Por su parte, el doctrinario Alfredo Reyes Kraff[103] menciona que las funciones de los prestadores de servicios de certificación son:

- Identificar a los solicitantes de certificados digitales.
- Expedir certificados de firma electrónica.
- Generar y registrar claves de firma electrónica.
- Almacenamiento en sus sistemas de claves privadas de firma electrónica, siempre que lo autorice el usuario.
- Mantenimiento de las claves vigentes y revocadas.
- Proporcionar servicios de directorio.

---

[101] *Vid.* VARGAS GARCÍA, Salomón, *Op. Cit.* p. 88
[102] *Vid.* FERNÁNDEZ GÓMEZ, Eva, *Op. Cit.* p. 118
[103] *Vid.* REYES KRAFF, Alfredo Alejandro, *Op. Cit.* p. 172

En nuestro país, de acuerdo con el Sistema Integral de Gestión Registral[104] y a la respuesta a la solicitud de información 0001000131414, existen cinco sociedades acreditadas para operar como prestadores de servicios de certificación, las cuales son: Advantage Security, S. de R.L. de C.V., CECOBAN, Edicomunicaciones Mexico S.A. de C.V. y Seguridata S.A. de C.V. las cuales ofrecen los servicios de expedición de certificados digitales, conservación de mensajes de datos y de sellado digital de tiempo; PSC World, S.A. de C.V. solo emite certificados digitales.

Así, a pesar de que los prestadores de servicios de certificación pueden ofrecer otros servicios relacionados con la firma electrónica, sus funciones primordiales serán identificar al solicitante de sus servicios y expedir el respectivo certificado digital, y con ello brindar seguridad a las personas que realizan operaciones comerciales a través de medios electrónicos, y con ello cumplir el propósito con el que fueron creados.

3.6 Obligaciones.

Establecidas en el artículo 104 del Código de Comercio, las obligaciones que tienen los prestadores de servicios de certificación son:

a. Comprobar la identidad de los solicitantes y cualquier otra circunstancia que sea necesaria para la expedición del certificado, podrá hacerlo por si misma o a través de alguna persona física o moral que actué en nombre y por cuenta suyos. Para cumplir con esta obligación podrá utilizar cualquier medio que este permitido por las legislaciones y deberá informar previamente al solicitante de que medios utilizará.

---

[104] Secretaría de Economía, Sistema Integral de Gestión Registral, Prestadores de Servicios de Certificación, [En línea] Disponible: http://www.firmadigital.gob.mx/ 20 de septiembre de 2014 21:23 P.M.

b. Poner a disposición del firmante los dispositivos de generación de los datos de creación y verificación de la firma electrónica.

c. Antes de emitir el certificado, comunicar al solicitante el precio por la expedición del certificado, las condiciones para la utilización del mismo y sus limitaciones, además deberá informarle la forma en que garantizará su responsabilidad.

d. Mantener un registro de certificados, en el cual deberá constar los emitidos y la circunstancias que afecten a la suspensión, pérdida o terminación de la vigencia de los mismos. Se deberá poder acceder a este registro por medios electrónicos, ópticos u otra tecnología; el contenido público deberá estar a disposición de quien lo solicite, pero el contenido privado solo puede estar a disposición del destinatario y de las personas autorizadas por el firmante.

e. Mantener de manera confidencial la información que reciba para realizar sus servicios.

f. Cuando la entidad de certificación decida cesar sus actividades de manera voluntaria, deberá informar a la Secretaría de Economía el motivo de dicho cese con 45 días de anticipación con la finalidad de verificar que se le hayan enviado copia de cada certificado emitido y que obren en su resguardo, para que con posterioridad determine el destino de sus registros y archivos.

g. Cerciorarse de las medidas para evitar la alteración de los certificados y para mantener de manera confidencial los datos personales del firmante, durante el proceso de generación de los datos de creación de la firma electrónica.

h. Hacer declaraciones en relación con sus normas internas y sus prácticas, lo cual deberán dar a conocer a los usuarios de sus servicios y destinatarios.

i. Proporcionarle a la parte que confía en el certificado los medios necesarios para que este pueda determinar:

1. La identidad de la entidad de certificación.

2. Que el firmante, a favor del cual se expidió el certificado, tenía bajo su control los dispositivos y los datos de creación de la firma, y que estos últimos eran validos, en el momento en que se expidió el certificado.

3. El método que se utilizó para identificar al firmante.

4. Las limitaciones de los fines y valores, en relación a los cuales puedan utilizarse los datos de creación de la firma o el certificado.

5. Las limitaciones de las responsabilidades del prestador de servicios de certificación.

6. Si existe un medio para que el firmante de aviso a la entidad certificadora que los datos de creación de la firma han sido controvertidos.

7. Si la entidad ofrece algún servicio de terminación de vigencia del certificado.

Entonces, las obligaciones de los prestadores de servicios de certificación tienen como finalidad que estas entidades emitan certificados digitales de manera eficaz y segura. Además, deberá cumplir con los principios y obligaciones estipulados en la Ley Federal de Protección de Datos Personales en Posesión de Particulares y la Ley Federal de Protección al Consumidor, analizados en el Capítulo anterior, con el objetivo de que se haga un tratamiento adecuado de la información personal proporcionada para emitir el certificado digital así como mantener confidencialidad de la misma, de igual forma para brindar protección a los consumidores en las transacciones comerciales efectuadas a través del comercio electrónico.

Si la autoridad certificadora incumple alguna de las obligaciones antes descritas, previa audiencia y mediante resolución fundada y motivada, se hará acreedora a una sanción que puede ser una suspensión temporal o definitiva de sus actividades, dependiendo de la gravedad de la infracción.

3.7 Facultades.

Los prestadores de servicios de certificación, ya sean notarios o corredores públicos, personas morales de carácter privado o instituciones públicas, se encuentran facultados para expedir certificados digitales de firmas electrónicas.

No obstante lo anterior, también pueden quedar facultados para brindar otros servicios relacionados con la firma electrónica, como lo son el almacenamiento de mensaje de datos o sellado digital de tiempo, etc., pero esto solo en el caso de que el solicitante lo señale en su petición, de lo contrario solo quedará acreditado para expedir certificados.

De igual forma, así como está facultado para expedir los certificados, también está facultado para revocarlos en el caso de que el firmante se lo solicite o su representante o un tercero que se encuentre autorizado para solicitar la revocación.

Es decir, las autoridades certificadoras tienen solo las facultades de expedir certificados electrónicos y de revocarlos, pero en lo que se refiere a las instituciones públicas o las instituciones financieras, estas pueden tener otras facultades de acuerdo con las leyes que les son aplicables.

3.8 Sanciones.

Las sanciones que se impondrán a las entidades de certificación por el incumplimiento de sus obligaciones, se encuentran indicadas en el Capítulo IV del Reglamento del Código de Comercio en materia de prestadores de servicios de certificación, específicamente en los artículos 24 a 27.

Primeramente, veremos lo relativo a la suspensión temporal del ejercicio de sus funciones, que serán:

1) De uno hasta dos meses, como lo manifiesta el artículo 24 del Reglamento, cuando:

a. Omitan determinar e informar a los usuarios si las firmas electrónicas avanzadas que ofrecen cumplen o no los requisitos para ser considerada como tal. Es decir, que los datos de creación de la firma corresponden exclusivamente al firmante; que dichos datos, al momento de la firma, estaban bajo el control exclusivo del firmante; es posible detectar cualquier alteración a la firma electrónica después del momento de firmar; y que se pueda detectar cualquier alteración que sufra la información de un mensaje de datos después de la firma.

b. Deje de cumplir con los requisitos de acreditación.

c. Actúe contrariamente a los procedimientos definidos y especificados para la expedición de certificados.

d. No permita consultar de forma inmediata la validez, suspensión o revocación de los certificados emitidos.

e. No informe al solicitante de sus servicios el precio, condiciones y limitaciones de uso del certificado y la forma en la que garantiza su posible responsabilidad, como lo señalado en la fracción III del artículo 104 del Código de Comercio.

2) De tres hasta cuatro meses, de acuerdo con el artículo 25 del Reglamento, cuando:

a. Reincida en las conductas u omisiones antes citadas.

b. Cambie su domicilio, objeto social o estatus sin dar aviso a la Secretaría de Economía con 15 días de anticipación.

c. Por exceptuar:

- Dar aviso del inicio de sus actividades a la Secretaría de Economía, dentro de los 45 días siguientes al inicio de sus operaciones.

- Enviar a la Secretaría de Economía, las copias de los certificados que emita, de acuerdo con el artículo 16 del Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación.
- Poner a disposición del firmante los datos de creación y verificación de la firma.
- Cumplir con lo dispuesto en el artículo 104, fracción IX del Código de Comercio, es decir no proporciona los medios de acceso al certificado que permitan a la Parte que confía conocer la identidad de la entidad de certificación; que el firmante tenía bajo su control los datos de creación de la firma; el método que se utilizó para identificar al firmante, etc.

3) De cinco hasta seis meses, como lo marca el artículo 26 del Reglamento, cuando:

a. Reincida en las conductas aludidas en el artículo anterior.

b. No cuente con fianza vigente, como lo señala el artículo 12 del Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación y la regla 3.2 de las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación.

c. Provoque la nulidad de un acto jurídico a causa de su negligencia, imprudencia o dolo al expedir un certificado.

d. Omitir notificar a la Secretaría de Economía, de los cambios que pretenda hacer a sus datos que deben ir en el certificado.

Por el contrario, el artículo 27 del Reglamento establece que se sancionará con suspensión definitiva de sus funciones, cuando:

A) Reincida en alguna de las conductas referidas en el artículo 26 del Reglamento.

B) No compruebe la identidad del solicitante y las circunstancias pertinentes para la emisión del certificado.

C) Proporcione documentos o información falsa para obtener su acreditación.

D) Altere o destruya los certificados que expida sin que medie resolución de la autoridad pertinente.

E) Emita, registre o conserve los certificados que expida, fuera del país sin autorización de la Secretaría de Economía, como lo dispone el artículo 20 del Reglamento del Código de Comercio en materia de prestadores de servicios de certificación.

F) Impida efectuar a la Secretaría de Economía las auditorías, a las que se alude en el Código de Comercio y el Reglamento de dicho Código en materia de prestadores de servicios de certificación.

G) Revele los datos de creación de la firma que correspondan a su propio certificado.

H) Difunda sin autorización la información que se le confió o realiza alguna otra conducta que vulnera la confidencialidad de la misma.

En relación con esta última, la Ley Federal de Protección de Datos Personales en Posesión de Particulares señala en su artículo 67 que se impondrá la pena de 3 meses a 3 años de prisión al responsable o tercero autorizado a tratar la información personal proporcionada, que con ánimo de lucro, provoque la vulneración de la seguridad de las bases de datos que son su responsabilidad; asimismo el artículo 68 de la misma ley refiere que se imponen penas de 6 meses a 5 años de prisión al que trate datos personales mediante engaño o aprovechándose del error en que se encuentra el titular de los mismos con la finalidad de obtener un lucro. Estas penas se aplicarán al doble si los datos son sensibles.

Igualmente la Ley Federal de Protección al Consumidor menciona que se sancionará con una multa equivalente a una y hasta dos mil quinientas veces el salario mínimo vigente en el Distrito Federal si los datos proporcionados por los consumidores no se mantienen en completa confidencialidad o si se hace un

mal tratamiento de los mismos, se impondrá la mismas multa si no se brinda una adecuada protección a los derechos de los consumidores al realizar actividades comerciales por medios electrónicos, tal como lo dispone el artículo 128 de dicha ley.

Las sanciones antes expuestas se aplicarán, sin perjuicio de la responsabilidad civil o penal y de las penas que correspondan de acuerdo con los delitos que cometa la entidad de certificación.

El procedimiento para determinar la procedencia o no de las sanciones se llevará acabo de acuerdo con lo estipulado en la Ley Federal de Procedimiento Administrativo, y en caso de que proceda la sanción, se deberá publicar un extracto de la resolución en el Diario Oficial de la Federación.

Por último, si la entidad certificadora es sancionada, inhabilitada o cancelada de sus actividades, todos sus registros y certificados pasarán para su administración a otra autoridad certificadora señalada por la Secretaría de Economía.

Por consiguiente, las entidades de certificación pueden ser fedatarios públicos, instituciones públicas o personas morales de carácter privado cuya finalidad es la de expedir certificados digitales de firma electrónica que autentifiquen la identidad del firmante de un mensaje de datos, aun cuando pueden brindar otros servicios. Estas entidades fueron creadas con el propósito de brindar confianza a los comerciantes y no comerciantes alrededor del mundo para realizar transacciones comerciales a través de redes de comunicación. Es por ello, y debido a la ayuda que prestan al comercio electrónico, que la Secretaría de Economía debe asegurar que cumplen con los elementos tecnológicos, humanos, materiales y económicos necesarios para proporcionar a sus usuarios seguridad informática. Por lo cual no es compatible la idea de que se les permita obtener una acreditación por medio de una afirmativa ficta.

CAPÍTULO CUARTO.

PROPUESTA DE DEROGACIÓN DEL APARTADO B DEL ARTÍCULO 102 DEL CÓDIGO DE COMERCIO VIGENTE.

El comercio electrónico tiene sus ventajas y sus desventajas, y uno de sus más grandes problemas es la seguridad. Es por esta razón, que se crearon nuevas figuras jurídicas que le proporcionan certidumbre al comercio electrónico.

De esta forma, nació la firma electrónica y posteriormente la firma electrónica avanzada, que como quedó explicado en el Capítulo Primero son semejantes, lo que las hace diferentes son las tecnologías con las que son creadas. Sin embargo, por si solas las firmas electrónicas no son suficientes para demostrar la identidad del emisor y destinatario de un mensaje de datos, ya que el hecho de que se plasme una firma en el mensaje de datos no es suficiente garantía para poder asociar el mismo con el firmante.

Para evitar esta circunstancia se crean los prestadores de servicios de certificación o entidades de certificación, quienes son los encargados de emitir certificados digitales que avalan que el firmante es quien dice ser y el único que conoce y posee los datos de creación de la firma electrónica. Pero ¿pueden los usuarios de sus servicios confiar en estos prestadores de servicios de certificación?

En los Capítulos anteriores, se manifiesta la importancia que tienen estos prestadores de servicios de certificación en las transacciones comerciales realizadas por medios electrónicos, no solo por los servicios relacionados con la firma electrónica que prestan éstas entidades sino también por la delicadeza de los datos que manejan al realizar sus funciones, ya que como hemos visto, para poder emitir los certificados requiere de los datos personales de sus usuarios.

Es por ello, que se crearon instrumentos y normas en México, que ya han quedado expuestos con anterioridad, que determinan una serie de estrictos requisitos para acreditar a estas entidades y de esta manera asegurar el eficaz y honesto cumplimiento de sus obligaciones.

Pese a esto, el artículo 102 del Código de Comercio, en el cual se indican las exigencias que debe cumplir el solicitante para ser autorizado para constituirse como prestador de servicios de certificación y emitir certificados digitales, también posibilita que existan entidades de certificación que no los cumplan.

Dicho artículo en su apartado B, disponen que:

Artículo 102.- Los Prestadores de Servicios de Certificación que hayan obtenido la acreditación de la Secretaría deberán notificar a ésta la iniciación de la prestación de servicios de certificación dentro de los 45 días naturales siguientes al comienzo de dicha actividad. […]

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.

Primeramente, el artículo 100 del que habla este inciso es el que estipula quienes podrán, ser considerados prestadores de servicios de certificación, como se señaló en los capítulos anteriores.

Asimismo menciona la aceptación de que se les conceda la acreditación como entidades de certificación a través de una afirmativa ficta o positiva ficta. Entendiendo a esta última, de acuerdo con el jurista David Cienfuegos Salgado como la figura que es: “la consecuencia de la inactividad del órgano

administrativo se traduce en la ficción de considerar que la petición se ha resuelto favorablemente."[105] El mismo autor, cita a la estudiosa Cosculluela Montaner la cual menciona que: "se trata de un acto presunto por el que la administración pública accede a la solicitud de un interesado al no haberla resuelto de forma expresa en el plazo establecido"[106]

En el mismo sentido, el doctrinario Alfonso Nava Negrete[107] explica que en el caso de que exista silencio de la autoridad o la abstención de emitir una resolución en el plazo establecido por parte de la misma, cuando se encuentre contemplado en la ley, se presumirá que la petición fue contestada en sentido afirmativo.

Por su parte, el licenciado Víctor Manuel Alfaro Jiménez expone que es: "la decisión normativa de carácter administrativo por la cual todas las peticiones por escrito de los ciudadanos, usuarios, empresas o entidades que se hagan a la autoridad pública, si no se contesta en el plazo que marca la ley las disposiciones administrativas se consideran aceptadas, bastando para ello conservar la copia del acuse de la solicitud realizada ante la instancia competente."[108]

La Ley Federal de Procedimiento Administrativo, dispone en el artículo 17, primer párrafo que: salvo que en otra disposición legal o administrativa de carácter general se establezca otro plazo, no podrá exceder de tres meses el tiempo para que la dependencia u organismo descentralizado resuelva lo que

---

[105] CIENFUEGOS SALGADO, David, El Derecho de Petición en México, Instituto de Investigaciones Jurídicas UNAM, México, 2004, p. 251. [En línea] Disponible: http://biblio.juridicas.unam.mx/libros/libro.htm?l=1336 12 de Marzo de 2014. 18:37 P.M.
[106] *Ídem.*
[107] *Vid.* NAVA NEGRETE, Alfonso, Derecho Administrativo Mexicano, 3ª edición, Fondo de Cultura Económica, México, 2007, p. 357.
[108] ALFARO JIMÉNEZ, Víctor Manuel, Glosario de términos de Derecho Administrativo [En línea] Disponible: http://www.paginaspersonales.unam.mx/files/358/GLOSARIO_DE_DERECHO_ADMINISTRATIVO.pdf 11 de Marzo de 2014. 19:28 P.M.

corresponda. Transcurrido el plazo aplicable, se entenderán las resoluciones en sentido negativo al promovente, a menos que en otra disposición legal o administrativa de carácter general se prevea lo contrario. A petición del interesado, se deberá expedir constancia de tal circunstancia dentro de los dos días hábiles siguientes a la presentación de la solicitud respectiva ante quien deba resolver; igual constancia deberá expedirse cuando otras disposiciones prevean que transcurrido el plazo aplicable la resolución deba entenderse en sentido positivo.

Por tanto, la afirmativa ficta o positiva ficta es un figura jurídica de acuerdo con la cual el silencio de la autoridad administrativa a una petición en el plazo marcado en la ley tendrá como consecuencia que se entienda que la respuesta fue positiva para el interesado, esto siempre que la ley correspondiente lo indique de esta forma.

Este es el caso del apartado B del artículo 102 del Código de Comercio Vigente, ya que establece que la Secretaría de Economía tiene 45 días siguientes a la presentación de la solicitud para resolverla, de no hacerlo en este plazo operará la afirmativa ficta y el peticionario quedará autorizado como prestador de servicios de certificación.

Entonces, se deduce que dicho numeral permite que existan entidades de certificación que no cumplan con todos los requisitos y operen como tal, ya que sería difícil para la Secretaría de Economía revisar en el término de 45 días que el solicitante cumpla con cada especificación, en relación con sus elementos humanos, materiales, económicos y tecnológicos, además de las restantes exigencias que debe entregar, que plantean tanto el Código de Comercio, como el Reglamento de dicho Código en materia de prestadores de servicios de certificación y las Reglas Generales, los cuales quedaron señalados en los Capítulos precedentes.

Así, al consentir que las entidades de certificación obtengan su acreditación a través de una afirmativa ficta, posibilita que no se brinde seguridad, no solo de los usuarios de sus servicios sino también de las personas que confían en los certificados digitales que avalan una firma electrónica. Ya que si la Secretaría de Economía no se asegura de que el solicitante cubre con los requisitos indicados en la legislación pertinente, no existe la certeza de que las entidades de certificación, autorizadas de esta forma, realicen sus operaciones de manera confiable, diligente y con el equipo tecnológico y personal adecuado.

Es decir, si los prestadores de servicios de certificación no cuentan con la infraestructura adecuada para realizar sus funciones se pondría en peligro el derecho a la conservación y protección de datos personales de los usuarios de sus servicios.

La protección de este derecho es la principal razón del porqué los internautas mexicanos desconfían al realizar transacciones por medios electrónicos, su preocupación recae sobre todo en la poca confianza que tienen al proporcionar sus datos personales o su información bancaria, aunado a esto se encuentra la desinformación de los usuarios de Internet acerca de las alternativas para el resguardo de este derecho. La siguiente gráfica muestra las razones por las cuales los consumidores mexicanos no realizan compras a través de medios electrónicos:

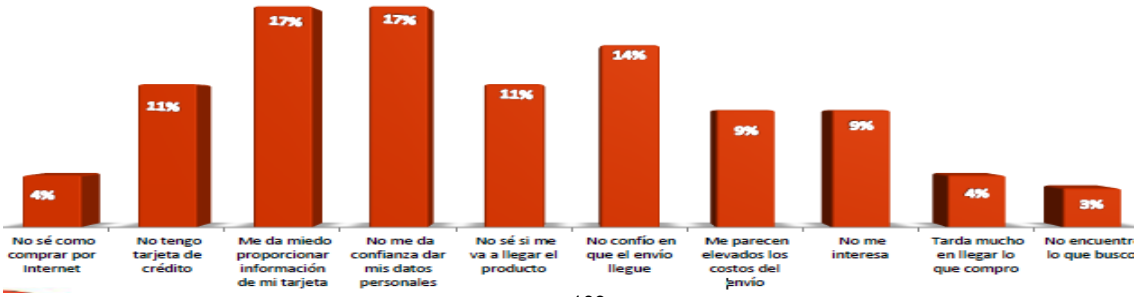

Ilustración 6. Razones de no compra.[109]

[109] JUÁREZ RESEARCH, Renato, Estudio de Comercio Electrónico México 2013, AMIPCI [En línea] Disponible:

Como se observa el 17% de los cibernautas mexicanos refieren que los dos principales motivos por los que no realizan transacciones comerciales a través de Internet son que no les da confianza proporcionar sus datos personales o la información de su tarjeta de crédito, otra razón importante con un 14% es que no confían que el envío llegue, el resto de los porqués se debe a una falta de interés hacia el comercio electrónico o porque no confían en que el producto llegue o no saben cómo llevar a cabo una compra por medio de Internet.

El derecho a la conservación y protección de datos personales, se ve garantizado por la seguridad informática, la cual forma parte de las obligaciones de las entidades de certificación, y que de acuerdo con la Secretaría de Economía[110], abarca tres aspectos importantes:

1. Confidencialidad: se refiere a que la información personal que se les proporciona para la emisión de los certificados no sea leída o copiada por personas que no estén facultadas para ello.
2. Integridad: que los datos personales se mantengan protegidos de ser modificados o borrados, sin la autorización del propietario de los datos.
3. Disponibilidad: la información debe estar accesible en todo momento.

Luego, debido a que los datos personales proporcionados para la expedición de certificados, son archivados de manera digital por los prestadores de servicios de certificación, es necesario que estos cumplan con los tres elementos anteriormente señalados, ya que pueden ser vulnerables de ataques cibernéticos perpetrados por *hackers, cracker y phreacker*, apasionados de la informática, que burlan la seguridad de los sistemas informáticos y roban los datos contenidos en ellos, con la finalidad de cometer algún delito.

---

https://www.amipci.org.mx/estudios/proteccion_de_datos_personales/2012ProtecciondeDatosPersonalesentreUsuariosEmpresasvE-1.pdf 29 de Octubre de 2014 08:40 A.M.

[110] Secretaría de Economía, Seguridad Informática, [En línea] Disponible: http://www.firmadigital.gob.mx/Seguridad.pdf 19 de septiembre de 2014 23:34 P.M.

De acuerdo con la Organización de Estados Americanos[111] en el 2013 se registro un aumento de un 113% en el número de incidentes cibernéticos en México y de acuerdo con los datos preliminares este porcentaje sigue aumentando cada año considerablemente. Asimismo la Organización señala que las violaciones de seguridad cibernética mas denunciados son:

- Uso de *malware* (software utilizado para dañar computadoras o otros dispositivos electrónicos), *phishing* (método de estafa cibernética utilizado para adquirir la información confidencial de usuarios de Internet) *y hackeos* (intrusión no autorizada a computadoras o redes de computadoras).
- Fraudes de comercio electrónico.
- Estafas nigerianas.
- Fraudes de banca electrónica.
- Extorsión.
- Difamación.
- Amenazas.
- Robo de contraseñas.
- Suplantación de identidad.
- Acoso.

Los sectores más afectados por los ataques cibernéticos son: académico, gobierno y privado, la siguiente grafica muestra el porcentaje tomando en cuenta las investigaciones oficiales sobre cibercrimen a petición de la parte afectada:

[111] SULLIVAN, Brian, Tendencias de seguridad cibernética en América Latina y el Caribe, Organización de Estados Americanos, Washington, 2014, p. 68-69 [En línea] Disponible: http://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf 30 de Octubre de 2014 09:36 A.M.

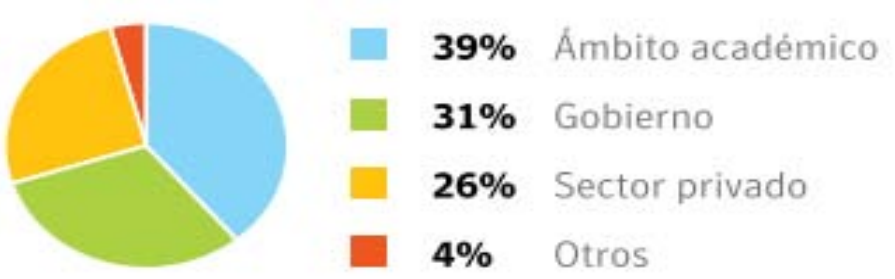

Ilustración 7 Entidades afectadas por los delitos informáticos.[112]

Para evitar que la seguridad informática sea violada las entidades de certificación publican una declaración de prácticas de certificación, en donde detallan el procedimiento que utilizarán, tal y como lo exige la norma, para la emisión de certificados y como se manejará la información personal proporcionada. Igualmente, debe tener planes de contingencia en caso de que su seguridad sea quebrantada, pero si la entidad de certificación no cuenta con un equipo humano profesional y la tecnología apropiada, la confiabilidad que brinda sería cuestionable ya que no existiría la certeza de que cumplen con estas declaraciones.

En relación con esto, en cuanto al tratamiento de los datos personales proporcionados por los titulares de los mismos a las entidades de certificación para la emisión de un certificado digital se debe hacer bajo los principios de: licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad dispuesto en la Ley Federal de Protección de Datos Personales en Posesión de Particulares, analizados en el Capítulo Segundo, los cuales aseguran que la información personal recabada por la autoridad de certificación se llevara a cabo con diligencia y seguridad, sobre todo cuando se trata de datos personales sensibles.

Aunado a esto, en cuanto a su papel dentro del comercio electrónico es la encargada de expedir el certificado digital, que avala la identidad del firmante

[112] Ibídem, p. 68.

del mensaje de datos, y una vez que emite el certificado envía este junto con la clave pública del iniciador al destinatario del mensaje, para lo cual se utilizan métodos de encriptación y la clave privada y la pública, como quedó explicado en el Capítulo Primero.

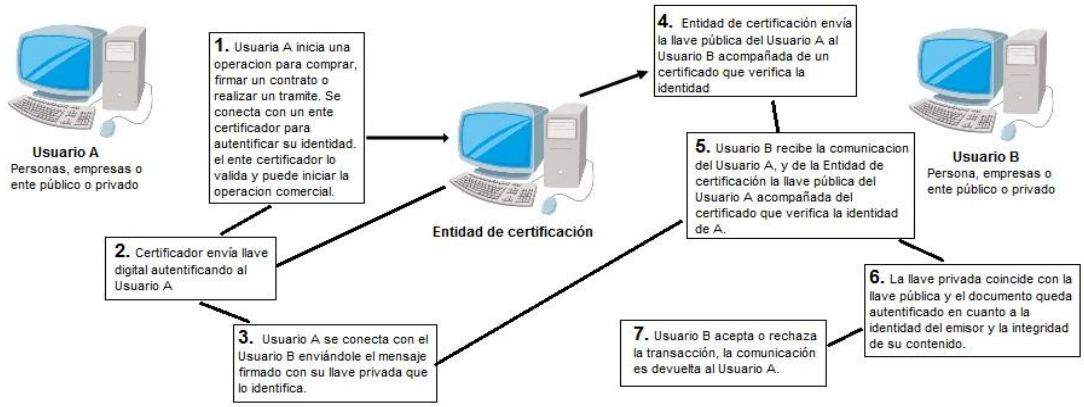

Ilustración 8. Autentificación de firma electrónica.

Pero esta técnica no es completamente confiable, ya que como se utiliza una ecuación matemática para crear las codificaciones cualquiera que conozca de esto e intercepte el mensaje puede descifrarlo. Es por ello que las entidades de certificación deben mostrar especial diligencia al realizar sus funciones, ya que de lo contrario se pondría en peligro la información contenida en el mensaje de datos.

Además, si la autoridad de certificación presta también servicios de conservación de mensajes de datos, debe tener un sistema informático confiable que mantenga protegidos los datos contenidos en estos, ya que el equipo tecnológico se encuentra conectado a el Internet, lo cual lo hace más vulnerable al ataque de cibernéticos.

Es a causa del Internet que se debe tener un mejor control de los prestadores de servicios de certificación, ya que un mal manejo de la información personal de los solicitantes de sus servicios, o la poca

profesionalidad de sus trabajadores, aunado a la carencia de infraestructura tecnológica apropiada, provocarían que su seguridad sea penetrada y los datos contenidos en sus sistemas queden en la red, y una vez que algo es infiltrado en Internet jamás desaparece.

Igualmente, las entidades de certificación por el incumplimiento de su obligación de proporcionar seguridad informática pueden ser sancionadas con una suspensión provisional o definitiva de sus operaciones como lo dispone el Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación; también se pueden hacer acreedores a multas como lo señala la Ley Federal de Protección al Consumidor, o incluso a penas privativas de la libertad, mencionadas en la Ley Federal de Protección de Datos Personales en Posesión de Particulares, sanciones analizadas en el Capítulo Tercero.

Así, la obligación de los prestadores de servicios de certificación de ofrecer seguridad informática es muy importante dentro del comercio electrónico, debido al gran aumento en la comisión de ataques cibernéticos y a la poca confianza que muestran los usuarios de Internet en México para realizar transacciones comerciales por este medio. Luego, la falta por parte de las entidades de certificación de los elementos humanos, tecnológicos y materiales necesarios y adecuados para brindar sus servicios a los comerciantes y no comerciantes pone en peligro el resguardo de la información personal proporcionada por estos últimos a las autoridades certificadoras, y al permitir que estas entidades sean acreditadas por medio de una afirmativa ficta consiente que las mismas no cumplan con la totalidad de los requisitos.

Además, de que existe una incompatibilidad entre lo instaurado en el artículo 102 inciso B del Código de Comercio y lo que se instituye en el Registro Federal de Trámites y Servicios [113] de la Comisión Federal de Mejora

[113] Acreditación como Prestador de Servicios de Certificación, Registro Federal de Trámites y Servicios. [En línea] Disponible:

Regulatoria (COFEMER), ya que de acuerdo con ellos la Dirección de Regulación y Supervisión de los Prestadores de Servicios de Certificación de la Secretaría de Economía, la cual es la responsable del trámite de acreditación de las entidades de certificación, se establece un plazo máximo de 3 meses para dar una respuesta al peticionario con fundamento en el artículo 17 de la Ley Federal de Procedimiento Administrativo. Por lo tanto, es incongruente mantener en la legislación mercantil un precepto que no es cumplido por la autoridad competente, lo cual deriva en otro problema, ya que la Secretaría de Economía debería observar lo señalado en el Código de Comercio Vigente, que es la legislación que regula a las entidades de certificación.

Por todo lo anterior, es que se propone derogar el apartado B del artículo 102 del Código de Comercio Vigente, para que el texto de dicho precepto quede de la siguiente manera:

Artículo 102.- Los Prestadores de Servicios de Certificación que hayan obtenido la acreditación de la Secretaría deberán notificar a ésta la iniciación de la prestación de servicios de certificación dentro de los 45 días naturales siguientes al comienzo de dicha actividad.

A) Para que las personas indicadas en el artículo 100 puedan ser Prestadores de Servicios de Certificación, se requiere acreditación de la Secretaría, la cual no podrá ser negada si el solicitante cumple los siguientes requisitos, en el entendido de que la Secretaría podrá requerir a los Prestadores de Servicios de Certificación que comprueben la subsistencia del cumplimento de los mismos:

I. Solicitar a la Secretaría la acreditación como Prestador de Servicios de Certificación;

---

http://207.248.177.30/tramites/FichaTramite.aspx?val=33499 12 de Marzo de 2014. 20:28 P.M.

II. Contar con los elementos humanos, materiales, económicos y tecnológicos requeridos para prestar el servicio, a efecto de garantizar la seguridad de la información y su confidencialidad;

III. Contar con procedimientos definidos y específicos para la tramitación del Certificado, y medidas que garanticen la seriedad de los Certificados emitidos, la conservación y consulta de los registros;

IV. Quienes operen o tengan acceso a los sistemas de certificación de los Prestadores de Servicios de Certificación no podrán haber sido condenados por delito contra el patrimonio de las personas o que haya merecido pena privativa de la libertad, ni que por cualquier motivo hayan sido inhabilitados para el ejercicio de su profesión, para desempeñar un puesto en el servicio público, en el sistema financiero o para ejercer el comercio;

V. Contar con fianza vigente por el monto y condiciones que se determinen en forma general en las reglas generales que al efecto se expidan por la Secretaría;

VI. Establecer por escrito su conformidad para ser sujeto a Auditoría por parte de la Secretaría, y

VII. Registrar su Certificado ante la Secretaría.

Con la eliminación del apartado B del artículo antes citado, y al hacer las adecuaciones pertinentes en el Reglamento del Código de Comercio en materia de prestadores de servicios de certificación y en las Reglas Generales, se obligaría a la Secretaría de Economía a cerciorarse meticulosamente que el solicitante cumpla los requisitos, aunado a que se seguiría otorgando el plazo de 3 meses para responder a la solicitud de acreditación y que ha seguido hasta ahora la Secretaría, para que la revisión de estos últimos se lleve con la diligencia necesaria, pero sin permitir la acreditación por medio de la afirmativa ficta.

En conclusión, gracias a esta modificación se eliminaría una de las muchas deficiencias que tiene la legislación comercial respecto de los prestadores de servicios de certificación, aunque aún existan varios inconvenientes en la normatividad comercial en relación a el comercio electrónico y los elementos que lo componen, este tipo de comercio aun es joven, además de que con la creación de nuevas tecnologías se actualiza cada día, por lo que le falta un largo camino por recorrer antes de poderse adaptar por completo a la normatividad interna de México, y así hacerlo funcional, confiable, seguro y certero.

CONCLUSIONES.

PRIMERA.- El comercio electrónico es la compra, venta o intercambio de bienes y servicios, además del intercambio electrónico de datos mediante tecnologías de la información y la comunicación, en el cual no existe un contacto físico entre quien ofrece el bien o servicio y quien los demanda, donde se tiene como finalidad obtener un lucro para el iniciador y la satisfacción de una necesidad para el destinatario.

SEGUNDA.- El prestador de servicios de certificación o entidad de certificación es la persona física o moral que emite certificados digitales y que además se encarga de confirmar la identidad del firmante, con respecto a su firma electrónica en un mensaje de datos, y que igualmente puede prestar otros servicios relacionados con la firma electrónica.

TERCERA.- La naturaleza jurídica de las entidades de certificación es puramente mercantil ya que es en las leyes mercantiles donde tienen su fundamento jurídico, específicamente en el Capítulo III del Titulo Segundo del Código de Comercio, además de que son considerados como auxiliares independientes por actuar como intermediario en el comercio electrónico.

CUARTA.- Los notarios y corredores públicos, las personas morales de carácter privado y las instituciones públicas pueden ser acreditados como entidades de certificación por la Secretaría de Economía, siempre que cumplan con los requisitos o por medio de una afirmativa ficta.

QUINTA.- Al realizar la expedición de certificados digitales las entidades de certificación deben cumplir con ciertas obligaciones, entre las cuales las más importantes son: confirmar la identidad del solicitante, mantener un registro de certificados, mantener de manera confidencial la información que reciba para

realizar sus servicios, etc.; ya que si no las cumple será acreedor de una sanción que puede ser la suspensión temporal o definitiva de sus funciones.

SEXTA.- La afirmativa ficta o positiva ficta es un figura jurídica, de acuerdo con la cual el silencio de la autoridad administrativa o la falta de una respuesta de la misma tendrá como consecuencia que se entienda que la respuesta fue positiva para el solicitante, esto siempre que la ley correspondiente lo indique de esta forma.

SÉPTIMA.- La legislación comercial, aun cuando exige una serie de requisitos a los peticionarios para ser acreditados como prestadores de servicios de certificación permite que opere la afirmativa ficta, con lo cual si transcurren 45 días después de entregada la petición sin recibir una contestación de la Secretaría de Economía se tendrá por autorizado al solicitante y podrá comenzar a funcionar como entidad de certificación.

OCTAVA.- El apartado B del artículo 102 del Código de Comercio Vigente al permitir la utilización de la afirmativa ficta en la acreditación de entidades de certificación pone en peligro la seguridad jurídica no solo de los usuarios de los servicios del prestador de servicios de certificación y de sus datos personales, sino también de aquellas personas que confían en el certificado emitido por la entidad de certificación. Esto debido a que no existe certeza de que la entidad cuenta con la infraestructura tecnológica y humana necesaria para brindar un servicio eficaz, responsable y honesto.

NOVENA.- El derecho de conservación y protección de datos personales forma parte de las obligaciones que debe cumplir las entidades de certificación, por lo cual debe hacer un tratamiento adecuado de los datos que recaba con la finalidad de emitir los certificados digitales, por ello si la entidad no cuenta con los elementos humanos y tecnológicos adecuados se pone en peligro este

derecho, al ser acreditada por una afirmativa ficta no se tiene la certeza de que la entidad cumpla con dichos requisitos.

DÉCIMA.- Con la eliminación del aparado B del artículo 102 del Código de Comercio Vigente, y al hacer las correcciones pertinentes, en cuanto al plazo de 45 días para ser acreditado como entidades de certificación, en el Reglamento del Código de Comercio en materia de prestadores de servicios de certificación y en las Reglas Generales, se obligaría a la Secretaria de Economía a cerciorarse meticulosamente que el solicitante cumpla los requisitos marcados en estas legislaciones, y de esta manera brindarle confiabilidad a los prestadores de servicios de certificación, a los usuarios de sus servicios y a la parte que confía en los certificados digitales, además de evitar consecuencias jurídicas y económicas.

DÉCIMA PRIMERA.- Es importante que los prestadores de servicios de certificación garanticen la seguridad informática de los comerciantes y no comerciantes, ya sea que estos últimos actúen como iniciador o destinatario dentro del comercio electrónico, por ello se propone derogar el apartado B del artículo 102 del Código de Comercio Vigente y con ello no permitir que opere la afirmativa ficta, para que el texto de dicho precepto quede de la siguiente manera:

Artículo 102.- Los Prestadores de Servicios de Certificación que hayan obtenido la acreditación de la Secretaría deberán notificar a ésta la iniciación de la prestación de servicios de certificación dentro de los 45 días naturales siguientes al comienzo de dicha actividad.

A) Para que las personas indicadas en el artículo 100 puedan ser Prestadores de Servicios de Certificación, se requiere acreditación de la Secretaría, la cual no podrá ser negada si el solicitante cumple los siguientes requisitos, en el entendido de que la Secretaría podrá requerir a los Prestadores de Servicios de Certificación que comprueben la subsistencia del cumplimento de los mismos:

I. Solicitar a la Secretaría la acreditación como Prestador de Servicios de Certificación;

II. Contar con los elementos humanos, materiales, económicos y tecnológicos requeridos para prestar el servicio, a efecto de garantizar la seguridad de la información y su confidencialidad;

III. Contar con procedimientos definidos y específicos para la tramitación del Certificado, y medidas que garanticen la seriedad de los Certificados emitidos, la conservación y consulta de los registros;

IV. Quienes operen o tengan acceso a los sistemas de certificación de los Prestadores de Servicios de Certificación no podrán haber sido condenados por delito contra el patrimonio de las personas o que haya merecido pena privativa de la libertad, ni que por cualquier motivo hayan sido inhabilitados para el ejercicio de su profesión, para desempeñar un puesto en el servicio público, en el sistema financiero o para ejercer el comercio;

V. Contar con fianza vigente por el monto y condiciones que se determinen en forma general en las reglas generales que al efecto se expidan por la Secretaría;

VI. Establecer por escrito su conformidad para ser sujeto a Auditoría por parte de la Secretaría, y

VII. Registrar su Certificado ante la Secretaría.

FUENTES CONSULTADAS.

ALARCÓN ÁLVAREZ, Enrique de, Diccionario de términos informáticos e internet, 3ª edición, Madrid, Editorial Anaya Multimedia, 2004.

CÁMPOLI, Andrés Gabriel, La firma electrónica en el régimen comercial mexicano, México, Editorial Porrúa, 2004.

CASTRO F., Juan Alberto, (ed.), Comercio Electrónico, Colombia, Editorial Legis, 2005.

CERVANTES AHUMADA, Raúl, Derecho mercantil, 3ª edición, México, Editorial Porrúa, 2004.

DÍAZ BRAVO, Arturo, Contratos mercantiles, 9ª Edición, México, IURE Editores, 2008.

ELÍAS AZAR, Edgar, La contratación por medios electrónicos, México, Editorial Porrúa, 2005.

FERNÁNDEZ GÓMEZ, Eva, Comercio electrónico, Madrid, Editorial McGraw-Hill, 2002.

GONZÁLEZ LÓPEZ, Óscar Rodrigo, Comercio Electrónico, Ediciones Anaya Multimedia, España, 2002.

HUERTA OCHOA, Carla, Las Normas Oficiales Mexicanas en el Ordenamiento Jurídico Mexicano, Boletín Mexicano de Derecho Comparado, número 92, año XXXI, México, mayo-agosto 1998.

Instituto de Investigaciones Jurídicas UNAM, Diccionario Jurídico Mexicano, Tomo 4. P-Z, Editorial Porrúa, México, 2005.

LEÓN TOVAR, Soyla H., La firma electrónica avanzada, 1ª Reimpresión, México, Oxford University Press, 2006.

LEÓN TOVAR, Soyla H., Contratos Mercantiles, México, Editorial Oxford University Press, 2004.

LUCENA CAYUELA, Núria (coord.), Pequeño Larousse, 9ª edición, Editorial Larousse, México, 2003.

MANTILLA MOLINA, Roberto L., Derecho Mercantil, 29º edición, Editorial Porrúa, México, 2005.

MICROSOFT CORPORATION, Diccionario de informática e Internet de Microsoft, 2ª edición, Madrid, Editorial McGraw-Hill, 2005.

MORLES HERNÁNDEZ, Alfredo, Curso de Derecho Mercantil, Tomo 1, 9ª edición, Editorial Universidad Católica Andrés, Venezuela, 2007.

NAVA NEGRETE, Alfonso, Derecho Administrativo Mexicano, 3ª edición, Fondo de Cultura Económica, México, 2007.

PINA VARA, Rafael de, Elementos de Derecho Mercantil Mexicano, 29ª edición, Editorial Porrúa, México, 2003.

QUEVEDO CORONADO, Ignacio F., Derecho Mercantil, 2ª edición, Editorial Pearson, México, 2004.

QUINTANA ADRIANO, Elvia Arcelia (coord.), Diccionario de Derecho Mercantil, Editorial Porrúa, México, 2001.

REYES DÍAZ, Carlos Humberto, (coord.), Temas selectos de comercio internacional, México, Editorial Porrúa, 2008.

REYES KRAFF, Alfredo Alejandro, La firma electrónica y las entidades de certificación, México, Editorial Porrúa, 2003.

TÉLLEZ VALDÉS, Julio, Derecho Informático, 2ª. Edición, México, Ed. McGraw Hill, 1996.

VARGAS GARCÍA, Salomón, Algunos comentarios sobre el comercio electrónico y la correduría pública en México, México, Editorial Porrúa, 2004.

Fuentes electrónicas.

Acreditación como Prestador de Servicios de Certificación, Registro Federal de Trámites y Servicios. http://207.248.177.30/tramites/FichaTramite.aspx?val=33499

ALFARO JIMÉNEZ, Víctor Manuel, Glosario de términos de Derecho Administrativo http://www.paginaspersonales.unam.mx/files/358/GLOSARIO_DE_DERECHO_ADMINISTRATIVO.pdf

Asociación Mexicana de Internet, Glosario de Términos, http://www.amipci.org.mx/?P=glosario

BALTIERRA GUERRERO, Alfredo, La Firma Autógrafa en el Derecho Bancario, Revista de la Facultad de Derecho de México, número 121-122-123, Enero-Junio 1982, http://www.juridicas.unam.mx/publica/librev/rev/facdermx/cont/121/pr/pr3.pdf

BARRETO ZÚÑIGA, Lizbeth Angélica, Evolución de la Firma Autógrafa a la Firma Electrónica Avanzada, Revista Digital Universitaria, mensual, volumen 12, número 3, marzo 2011, http://www.revista.unam.mx/vol.12/num3/art34/art34.pdf

BECERRA ZAVALA, Roberto (comp.), Antología de Derecho Mercantil I, Editorial Universidad América Latina, México, 2011, http://ual.dyndns.org/Biblioteca/Derecho_Mercantil/Pdf_08.pdf

CIENFUEGOS SALGADO, David, El Derecho de Petición en México, Instituto de Investigaciones Jurídicas UNAM, México, 2004, p. 251. http://biblio.juridicas.unam.mx/libros/libro.htm?l=1336

Global Information Assurance Certification, Certifications, http://www.giac.org/certifications

Information System Security Certification Consortiu, Credentials, https://www.isc2.org/credentials/default.aspx Instituto Federal de Acceso a la

Información y Protección de Datos, Guía para instrumentar medidas compensatorias, http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_para_instrumentar_medidas_compensatorias.pdf

Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, http://www.ietf.org/rfc/rfc3280.txt

Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), https://www.ietf.org/rfc/rfc3161.txt

ISO, ISO/IEC 9594-8: 2008, http://www.iso.org/iso/catalogue_detail.htm?csnumber=53372

JUÁREZ RESEARCH, Renato, Estudio de Comercio Electrónico México 2013, AMIPCI https://www.amipci.org.mx/estudios/proteccion_de_datos_personales/2012Proteccionde DatosPersonalesentreUsuariosEmpresasvE-1.pdf

Ley Modelo de la CNUDMI sobre comercio electrónico (1996), Comisión de las Naciones Unidas para el Derecho Mercantil Internacional http://www.uncitral.org/uncitral/es/uncitral_texts/electronic_commerce/1996Model.html

Ley Modelo de la CNUDMI sobre las firmas electrónicas (2001), Comisión de las Naciones Unidas para el Derecho Mercantil Internacional http://www.uncitral.org/uncitral/es/uncitral_texts/electronic_commerce/2001Model_signatures.html

Procuraduría Federal del Consumidor, Comercio Electrónico, última modificación 15 de febrero de 2013. http://www.profeco.gob.mx/internacionales/com_elec.asp

Real Academia Española, Diccionario de la Lengua Española, http://lema.rae.es/drae/?val

Registro Federal de Trámites y Servicios, Acreditación como Prestador de Servicios de Certificación, http://187.191.71.208/tramites/FichaTramite.aspx?val=33499

ROJAS AMANDI, Víctor Manuel, Regulación del Comercio Electrónico en México, Anuario de Derecho de la Universidad Iberoamericana, anual, número 30, México, 2000, http://www.juridicas.unam.mx/publica/librev/rev/jurid/cont/30/cnt/cnt16.pdf

Secretaría de Economía, Misión y visión, http://www.economia.gob.mx/conoce-la-se/mision-y-vision-se

Secretaría de Economía, Seguridad Informática, http://www.firmadigital.gob.mx/Seguridad.pdf

Secretaría de Economía, Sistema Integral de Gestión Registral, Prestadores de Servicios de Certificación, http://www.firmadigital.gob.mx/

SEOANE BALADO, Eloy, La Nueva Era del Comercio: El Comercio Electrónico, Ideaspropias Editorial, España, 2005, http://books.google.com.mx/books?id=evLz521ZVmAC&printsec=frontcover&hl=es#v=onepage&q&f=false

Servicio de Administración Tributaria, Qué es y para qué sirve la firma electrónica avanzada, http://www.sat.gob.mx/sitio_internet/e_sat/tu_firma/60_11498.html

SULLIVAN, Brian, Tendencias de seguridad cibernética en América Latina y el Caribe, Organización de Estados Americanos, Washington, 2014, http://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf

Technical Committee Electronic Signatures and Infrastructures, Electronic signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates http://www.etsi.org/deliver/etsi_ts/102000_102099/102042/02.02.01_60/ts_102042v020201p.pdf

Tecnología de la Información-Técnicas de seguridad-Código para la práctica de la gestión de la seguridad de la información https://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf

Fuentes legislativas.

Constitución Política de los Estado Unidos Mexicanos.

Ley Modelo de la CNUDMI sobre Comercio Electrónico.

Ley Modelo de la CNUDMI sobre Firmas Electrónicas.

Código de Comercio.

Código Civil Federal.

Código Federal de Procedimientos Civiles.

Ley Federal de Protección al Consumidor.

Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Ley Federal sobre Metrología y Normalización.

Ley Federal de Procedimiento Administrativo.

Ley Federal de Derechos.

Ley Orgánica de la Administración Pública Federal.

Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación.

Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación.

Norma Oficial Mexicana 151SCFI.

Anexos.

"2014, Año de Octavio Paz"

SE
SECRETARÍA DE ECONOMÍA

Subsecretaría de Competitividad y Normatividad
Dirección General de Normatividad Mercantil
Dirección de Regulación y Supervisión de los Prestadores de Servicios de Certificación

Oficio No. 316.2014.004609
Asunto: Respuesta a solicitud de Información 0001000131414.

México, D.F., a 23 de septiembre de 2014.

Lic. Gloria Berenice Viruega Landin
Secretaría Técnica del Comité de Información en la Secretaría de Economía.

Me refiero a la solicitud de información número 0001000131414, presentada a través del Sistema de Atención de Solicitudes, mediante el cual requiere, lo siguiente:

> *"...Â¿CUÃ¡NTOS PRESTADORES DE SERVICIOS DE CERTIFICACIÃ³N EXISTEN EN MÃ©XICO Y EN DONDE SE ENCUENTRAN UBICADOS? Â¿CUÃ¡NTOS DE ESTOS PRESTADORES DE SERVICIOS DE CERTIFICACIÃ³N RECIBIERON SU ACREDITACIÃ³N CONFORME A LO DISPUESTO EN EL INCISO B DEL ARTÃCULO 102 DEL CÃ³DIGO DE COMERCIO? Â¿CUÃ¡L ES EL PROCEDIMIENTO QUE REALIZA LA SECRETARÃA DE ECONOMÃA PARA ACREDITAR A LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÃ³N Y CUÃ¡LES SON LOS CRITERIOS QUE TOMAN EN CUENTA PARA CONCEDER LA ACREDITACIÃ³N?..." (sic)*

En atención a la solicitud y derivado de la búsqueda realizada en los archivos que obran en la Dirección General de Normatividad Mercantil, le informo que son 5 los Prestadores de Servicios de Certificación que se encuentran actualmente acreditados por esta Secretaría, los cuales corresponden a:

- ADVANTAGE SECURITY, S. DE R.L. DE C.V., ubicado en, Av. Prolongación Paseo de la Reforma No. 625, despacho 402, Col. Paseo de las Lomas, Santa Fe, Delegación Álvaro Obregón, C.P. 01330, México, D.F.
- PSC WORLD, S.A. DE C.V., ubicado en, Morelos 7, nivel 3, Col. Del Carmen, Delegación Coyoacán, C.P. 04100, México, D.F.
- CECOBAN, S.A. de C.V., ubicado en, Av. Constituyentes No.119, Col. San Miguel Chapultepec, Delegación Miguel Hidalgo. C.P. 11850, México, D.F.
- EDICOMUNICACIONES MEXICO S.A DE C.V., ubicado en, Torre del Ángel, Paseo de la Reforma Nº 350, piso 16-B, Col. Juárez, Delegación Cuauhtémoc, C.P. 06600, México, D.F.
- SEGURIDATA S.A DE C.V., ubicado en, Av. de los Insurgentes No. 2375, 3er piso, Col. Tizapán, Delegación Álvaro Obregón, C.P. 01000, México, D.F.

Ahora bien, en cuanto a las solicitudes respecto de *"...Â¿CUÃ¡L ES EL PROCEDIMIENTO QUE REALIZA LA SECRETARÃA DE ECONOMÃA PARA ACREDITAR A LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÃ³N Y CUÃ¡LES SON LOS CRITERIOS QUE TOMAN EN CUENTA PARA CONCEDER LA ACREDITACIÃ³N?..." (sic),* le comento que esta Dirección General verifica el cumplimiento, para la acreditación como Prestador de Servicios de Certificación, lo expresamente contenido en los artículos 101 y 102 inciso A del Código de Comercio, que a la letra dicen.

> *"...**Artículo 101.-** Los Prestadores de Servicios de Certificación a los que se refiere la fracción II del artículo anterior, contendrán en su objeto social las actividades siguientes:*
> ***I.** Verificar la identidad de los usuarios y su vinculación con los medios de identificación electrónica;*
> ***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.*
> ***Artículo 102.-** Los Prestadores de Servicios de Certificación que hayan obtenido la acreditación de la Secretaría deberán notificar a ésta la iniciación de la prestación de servicios de certificación dentro de los 45 días naturales siguientes al comienzo de dicha actividad.*

A) Para que las personas indicadas en el artículo 100 puedan ser Prestadores de Servicios de Certificación, se requiere acreditación de la Secretaría, la cual no podrá ser negada si el solicitante cumple los siguientes requisitos, en el entendido de que la Secretaría podrá requerir a los Prestadores de Servicios de Certificación que comprueben la subsistencia del cumplimento de los mismos:
***I.** Solicitar a la Secretaría la acreditación como Prestador de Servicios de Certificación;*
***II.** Contar con los elementos humanos, materiales, económicos y tecnológicos requeridos para prestar el servicio, a efecto de garantizar la seguridad de la información y su confidencialidad;*
***III.** Contar con procedimientos definidos y específicos para la tramitación del Certificado, y medidas que garanticen la seriedad de los Certificados emitidos, la conservación y consulta de los registros;*
***IV.** Quienes operen o tengan acceso a los sistemas de certificación de los Prestadores de Servicios de Certificación no podrán haber sido condenados por delito contra el patrimonio de las personas o que haya merecido pena privativa de la libertad, ni que por cualquier motivo hayan sido inhabilitados para el ejercicio de su profesión, para desempeñar un puesto en el servicio público, en el sistema financiero o para ejercer el comercio;*
V. Contar con fianza vigente por el monto y condiciones que se determinen en forma general en las reglas generales que al efecto se expidan por la Secretaría;
VI. Establecer por escrito su conformidad para ser sujeto a Auditoría por parte de la Secretaría, y
VII. Registrar su Certificado ante la Secretaría..."

Así mismo, lo señalado en los artículos 5 y 7 del Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación, que refieren lo siguiente:

***ARTÍCULO 5o.-** Los interesados en obtener la acreditación como Prestador de Servicios de Certificación deberán:*
***I.** Presentar la solicitud de acreditación en los formatos que determine la Secretaría;*
***II.** Adjuntar a la solicitud, según corresponda, lo siguiente:*
a) En caso de los notarios o corredores públicos, copia certificada de la patente, título de habilitación o documento que en términos de la legislación de la materia les acredite estar en ejercicio de la fe pública;

b) En caso de las personas morales, copia certificada de su acta constitutiva, póliza u otro instrumento público, que acredite su constitución de acuerdo con las leyes mexicanas y que su objeto social es el establecido en el artículo 101 del Código de Comercio, y

c) Las instituciones públicas, copia certificada del instrumento jurídico de su creación o, en su caso, copia certificada jurídica aplicable;

III. Comprobar que se cuenta al menos con los siguientes elementos:

a) Humanos.- Un profesionista jurídico, un profesionista informático y cinco auxiliares de apoyo informático;

b) Materiales.- Espacio físico apropiado para la actividad, controles de seguridad, accesos y perímetros de seguridad física, medidas de protección, así como con las políticas necesarias para garantizar la seguridad del área;

c) Económicos.- Capital que comprenderá al menos el equivalente a una cuarta parte de la inversión requerida para cumplir con los elementos humanos, tecnológicos y materiales, y un seguro de responsabilidad civil cuyo monto será determinado por la Secretaría con base en el análisis de las operaciones comerciales y mercantiles en que sean utilizados los Certificados y no será menor al equivalente a treinta veces el salario mínimo general diario vigente en el Distrito Federal correspondiente a un año, y

d) Tecnológicos.- Consistentes en: I).- Análisis y Evaluación de Riesgos y Amenazas, II).- Infraestructura informática, III).- Equipo de cómputo y software, IV).- Política de Seguridad de la Información, V).- Plan de continuidad del Negocio y Recuperación ante Desastres, VI).- Plan de Seguridad de Sistemas, VII).- Estructura de Certificados, VIII).- Estructura de la Lista de Certificados Revocados, IX).- Sitio electrónico, X).- Procedimientos que informen de las características de los procesos de creación y verificación de Firma Electrónica Avanzada, XI).- Política de Certificados, XII).- Declaración de Prácticas de Certificación, XIII).- Modelos de las autoridades certificadora y registradora, XIV).- Plan de administración de claves.

SE
SECRETARÍA DE ECONOMÍA

Oficio No. 316.2014.004609

Los elementos descritos en la presente fracción deberán ajustarse a las especificaciones que determine la Secretaría en las Reglas Generales, a efecto de que las prácticas y políticas que se apliquen garanticen la continuidad del servicio, la seguridad de la información y su confidencialidad;

IV. Contar con procedimientos claros y definidos de conformidad con las Reglas Generales que emita la Secretaría;

V. Adjuntar a la solicitud una carta suscrita por cada persona física que pretenda operar o tener acceso a los sistemas que utilizará en caso de ser acreditado, donde dicha persona manifieste bajo protesta de decir verdad y advertido de las penas en que incurren los que declaran falsamente ante una autoridad distinta a la judicial, de que no fue condenado por delito contra el patrimonio de las personas y mucho menos inhabilitado para el ejercicio de la profesión, o para desempeñar un puesto en el servicio público, en el sistema financiero o para ejercer el comercio;

VI. Contar con una póliza de fianza por el monto y condiciones que se determinan en el presente Reglamento y en las Reglas Generales que al efecto expida la Secretaría;

VII. Acompañar a su solicitud, escrito de conformidad para ser sujeto de auditoría por parte de la Secretaría en todo momento, para que ésta verifique el cumplimiento de los requisitos para obtener y mantener la acreditación como Prestador de Servicios de Certificación; Cuando el interesado pretenda que sus Datos de Creación de Firma Electrónica permanezcan en resguardo fuera del territorio nacional, deberá solicitarlo a la Secretaría. En este caso, el interesado manifestará por escrito su conformidad de asumir los costos que impliquen a la Secretaría el traslado de su personal para efectuar sus auditorías, y

VIII. Registrar ante la Secretaría su Certificado, en los términos que establece el presente Reglamento.

ARTÍCULO 70.- La Secretaría desahogará el trámite para obtener la acreditación como Prestador de Servicios de Certificación en los términos de lo dispuesto por la Ley Federal de Procedimiento Administrativo.

Sin perjuicio de lo anterior, la Secretaría deberá:

I. Remitir dentro de los cinco días siguientes a la recepción de la solicitud el nombre, nacionalidad, actividad profesional, domicilio del interesado o el de su Representante legal según corresponda, a las secretarías de Gobernación, de Relaciones Exteriores, de Educación Pública, de Seguridad Pública, de Hacienda y Crédito Público, de Comunicaciones y Transportes, y de la Función Pública, así como a la Procuraduría General de la República y las autoridades locales o municipales o extranjeras que estime conveniente en atención a los domicilios indicados, para que en el ámbito de su competencia evalúen dicha información;

II. Revisar y evaluar de manera preliminar, dentro de los veinte días siguientes a la recepción de la solicitud, la información y documentación recibida. Cuando de la revisión detecte la falta de cualquiera de los requisitos señalados en el Código de Comercio y este Reglamento, prevendrá al interesado por escrito por única vez, para que subsane la omisión dentro del término de veinte días contados a partir de su notificación en ventanilla. Transcurrido dicho plazo sin que sea desahogada la prevención, se desechará el trámite;

III. Realizar una visita en el domicilio que señaló el interesado, dentro de los veinticinco días hábiles siguientes a la fecha de presentación de la solicitud, a efecto de llevar a cabo una auditoría para comprobar los requisitos para obtener la acreditación como Prestador de Servicios de Certificación que determinan el Código de Comercio y el presente Reglamento;

IV. Resolver dentro de los cuarenta y cinco días hábiles siguientes a la presentación de la solicitud, la procedencia o no de otorgar la acreditación como Prestador de Servicios de Certificación; dicha resolución le será notificada al interesado por ventanilla. La Secretaría no podrá otorgar más de una acreditación al mismo interesado, y

V. Publicar en el Diario Oficial de la Federación las acreditaciones que otorgue en términos del presente artículo, dentro de los treinta días siguientes a la resolución que determine su procedencia. La misma situación se observará en caso de que la Secretaría no resuelva la solicitud del interesado en el plazo de la fracción anterior.

SE
SECRETARÍA DE ECONOMÍA

Subsecretaría de Competitividad y Normatividad
Dirección General de Normatividad Mercantil
Director General Adjunto de Regulación y Supervisión de
Firma Electrónica y Sistemas Registrales

Oficio No. 316.2014.004609

Y de igual forma, todo lo referido en las Reglas Generales a que deberán sujetarse los Prestadores de Servicios de Certificación; por otro lado, es preciso mencionar que esta Dirección General, no cuenta con criterios establecidos, para conceder acreditaciones a los Prestadores de Servicios de Certificación, toda vez que se aboca única y exclusivamente, a lo referido en la normatividad aplicable, como lo es el Código de Comercio, el Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación y las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación.

Cabe mencionar que toda la documentación que requiera, respecto de Prestadores de Servicios de Certificación, podrá encontrarla en la dirección electrónica http://www.firmadigital.gob.mx/, así como en la página http://187.191.71.208/BuscadorTramites/BuscadorGeneralHomoclave.asp, en la cual podrá obtener diversos trámites de los Prestadores de Servicios de Certificación, los cuales, se enlistan, a continuación:

SE-09-027-A, Acreditación como Prestador de Servicios de Certificación.
SE-09-026-A, Autorización de la procedencia para la acreditación de prestador del servicio de certificación de firma electrónica.
SE-09-032, Comunicación de Cese de operaciones del Prestador de Servicios de Certificación.
SE-09-028, Notificación del inicio de actividades como Prestador de Servicios de Certificación.

Se emite el presente, con fundamento en el artículo 44 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, y 22 fracción X, último párrafo del Reglamento Interior de la Secretaría de Economía.

Sin otro particular, reciba un saludo cordial.

Lic. Denise Carla Vázquez Wallach
Directora de Área

C.c.p. Lic. Elsa Regina Ayala Gómez, Directora General de Normatividad Mercantil. Para conocimiento.