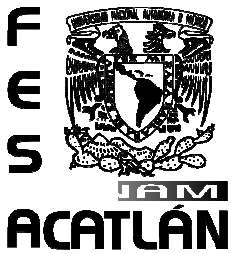
UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES
ACATLAN



Tesis

Responsabilidad derivada de la utilización indebida de un certificado electrónico, por parte de terceros, en el tiempo que transcurre de la solicitud de revocación al otorgamiento de ésta.

Que para obtener el título de
Licenciado en Derecho

Presenta:
Luis Miguel Aragón Hernández

Asesor: Lic. Gerardo Goyenechea Godínez

AGOSTO DE 2008

JUSTIFICACIÓN

La necesidad de generar confianza en las operaciones celebradas por medios electrónicos, ha conducido a la creación de sistemas de seguridad en la comunicación e intercambio de datos. Así nace el Prestador de Servicios de Certificación quien provee de mayor certeza jurídica a un acto en la medida en que expide un certificado electrónico que acredita el vínculo existente entre una firma electrónica y una persona en particular, de manera que esta entidad certifica la validez de una firma electrónica, respondiendo por los daños y perjuicios que pudiere causar por el incumplimiento de sus obligaciones o por el indebido desempeño de sus funciones, asimismo, el titular del certificado asume la responsabilidad de su uso sufriendo los riesgos de la utilización ilegitima originada por su culpa o negligencia.

Sin embargo, en el caso de la revocación de un certificado electrónico surge la incertidumbre de quién responde por el uso indebido del certificado, en el tiempo que transcurre de la solicitud de la revocación al otorgamiento de ésta, pues se debe tomar en cuenta que una vez que la Entidad Certificadora reciba la correspondiente solicitud de revocación, es imprescindible que confirme dicha petición, por lo que necesariamente transcurrirá un intervalo entre la solicitud y la efectiva revocación del certificado, tiempo en el que éste puede ser utilizado.

OBJETIVO

Analizar las causas de responsabilidad de los Prestadores de Servicios de Certificación contempladas en el Código de Comercio, con el propósito de prever la posible utilización indebida de un certificado electrónico, por parte de terceros, en el tiempo que transcurre de la solicitud de revocación al otorgamiento de ésta, de manera que se pueda determinar en que momento el titular del certificado se libera de su responsabilidad y la traslada a la entidad certificadora.

INTRODUCCIÓN

La necesidad de generar confianza en las operaciones celebradas por medios electrónicos, ha conducido a la creación de sistemas de seguridad en la comunicación e intercambio de datos. Así nace la figura del Prestador de Servicios de Certificación quien provee de mayor certeza jurídica a un acto en la medida en que expide un certificado electrónico que acredita el vínculo existente entre una firma electrónica y una persona en particular, de manera que esta entidad responderá por los daños y perjuicios que pudiere causar por el incumplimiento de sus obligaciones o por el indebido desempeño de sus funciones, asimismo el titular del certificado asume la responsabilidad de su uso sufriendo los riesgos de la utilización ilegitima originada por su culpa o negligencia.

Es así que el presente trabajo tiene como objetivo analizar las causas de responsabilidad de los Prestadores de Servicios de Certificación contempladas en el Código de Comercio, con el propósito de prever la posible utilización indebida de un certificado electrónico, por parte de terceros, en el tiempo que transcurre de la solicitud de revocación al otorgamiento de ésta, de manera que se pueda determinar en que momento el titular del certificado se libera de su responsabilidad y la traslada a la entidad certificadora.

Para la consecución de dicho objetivo desarrollamos el siguiente estudio, el cual se conforma de cuatro capítulos que abarcan, de manera general, los siguientes temas.

El primer capítulo titulado “La firma, el documento, la firma electrónica y el documento electrónico” se dedica a la exposición y análisis de los medios convencionales utilizados para la celebración de actos jurídicos como son: la firma y el documento con soporte en papel así como de sus correspondientes equivalentes funcionales, es decir, la firma electrónica y el documento electrónico.

El segundo capítulo denominado “De la Entidad Certificadora o Prestador de Servicios de Certificación” cubre temas que parten de los antecedentes de los Prestadores de Servicios de Certificación en México, hasta los elementos con los que debe contar el PSC para obtener su acreditación por parte de la Secretaría de Economía.

El tercer capítulo lleva por título “Certificado electrónico” en donde se agotan temas que nos permiten conocer el objetivo de la certificación y su diferencia con la fe pública, asimismo, se exponen las clases de certificados electrónicos y casos en que se interrumpen sus efectos jurídicos.

Finalmente, el cuarto capítulo se dedica al estudio de la responsabilidad Civil de los Prestadores de Servicios de Certificación contemplada en el Código de Comercio, lo que permitirá exponer la necesidad de una regulación que contemple una mayor protección para el titular de un certificado electrónico, dado que en el caso del uso indebido de dicho instrumento por parte de terceros, éste terminaría asumiendo todos los riesgos, por lo que se pretende determinar en que momento el titular del certificado se libera de su responsabilidad y la traslada a la entidad certificadora.

ÍNDICE

CAPÍTULO PRIMERO

1. La firma, el documento, la firma electrónica y el documento electrónico

En los últimos años la actualización en materia de tecnologías de información y comunicación ha influido en las diferentes áreas del conocimiento y actividades humanas, fomentando el surgimiento de nuevas formas de trabajar, aprender, comunicar y celebrar operaciones.

La particularidad de estas tecnologías es que utilizan medios electrónicos y la Internet, constituyendo una herramienta ideal para realizar intercambios de todo tipo de información, es así que hoy en día es posible celebrar un acto jurídico a través de la transferencia de datos de un computador a otro sin necesidad de la utilización de documentos con soporte en papel, lo que ha contribuido a eliminar fronteras, ahorro de tiempo y dinero, esto gracias a la facilidad de acceso a los sitios web, permitiendo a los comerciantes y/o empresas llegar de manera eficaz al usuario final y éste a su vez podrá hacer un mejor comparativo de empresas y precios en el mercado.

Lo anterior lo vemos reflejado no sólo en la compraventa de bienes y/o servicios, sino también en el uso de la red para actividades anteriores y posteriores a la venta de éstos, como puede ser la publicidad, búsqueda de información sobre productos, proveedores, garantías de cumplimiento, soporte técnico, sólo por mencionar algunos.

Al respecto, es importante señalar que en México la celebración de actos jurídicos a través del uso de medios electrónicos cuenta con un respaldo normativo que permite su funcionamiento; en efecto, el Código Civil Federal reconoce el uso de medios electrónicos para la celebración de dichos actos, el Código Federal de Procedimientos Civiles les reconoce a los mensajes de datos valor probatorio, el Código de Comercio proporciona un apartado dedicado al Comercio Electrónico en donde se abarcan aspectos que van desde la definición de lo que se entiende por mensaje de datos, firma electrónica, así como la figura del Prestador de Servicios de Certificación, por otra parte la Ley Federal de Protección al Consumidor regula el tratamiento de la información que los consumidores proporcionan a las empresas, así como la información que éstas deben proporcionar al consumidor para que tengan conocimiento de las condiciones a las que estará sujeto el bien o servicio; es así que con el uso de los medios electrónicos, las empresas y los particulares pueden tener total certeza de que las actividades comerciales que están llevando a cabo cuentan con la misma protección como si se celebrarán a través de medios tradicionales, es decir, con soporte en papel.

1.1 Fundamentos metodológicos

Para poder comenzar con el análisis en cuanto a la responsabilidad de los Prestadores de Servicios de Certificación (PSC), se observarán los conceptos de firma y documento, así como la firma electrónica y el documento electrónico, los cuales nos darán la pauta para justificar la relevancia que estas figuras tienen con respecto a la Entidad Certificadora o Prestador de Servicios de Certificación.

1.1.1 Firma

Atendiendo a su significado etimológico, firma proviene del latín "firmare" que quiere decir "afirmar o dar fuerza"[1].

En el derecho mexicano, el único ordenamiento que hace alusión al concepto de firma es el Código Federal de Procedimientos Civiles, al cual nos referiremos más adelante. Por otra parte, en la doctrina encontramos que a la firma se le puede atribuir distintos usos y funciones, que a continuación observaremos.

Mustapich define a la firma como "el nombre escrito por propia mano en caracteres alfabéticos y de una manera particular, al pie del documento al efecto de autenticar su contenido"[2].

Planiol y Ripert señalan que la firma es "una inscripción manuscrita que indica el nombre de una persona que entiende hacer suyas las declaraciones del acto"[3].

Asimismo, Rafael de Pina Vara conceptúa a la firma como la "representación por escrito del nombre de una persona, puesta por ella misma de puño y letra"[4].

De las anteriores definiciones, notamos que el factor común de éstas radica en que en la firma deberá aparecer el nombre de la persona que autorice, autentique o se obligue al acto expresado en un documento, sin embargo, ¿Qué sucede con aquellos documentos en donde la firma que se ha plasmado sea ilegible, o bien la firma se exprese a través de símbolos gráficos?

Al respecto, la Real Academia Española señala que la firma "es el nombre y apellido, o título, que una persona escribe de su propia mano en un documento, para darle autenticidad o para

---

[1] Diccionario jurídico 2000, CD- ROM, Desarrollo Jurídico Copyright 2000, DJ2K - 1010
[2] Mustapich, J.M., Tratado de Derecho Notarial,. citado por Reyes Krafft, Alfredo Alejandro en: La firma electrónica y las entidades de certificación, Porrúa, México 2003, pág. 88.
[3] Planiol y Ripert, Traité Pratique De Droit Civil Francais. Citado por Revidatti, Gustavo Adolfo en : Enciclopedia Jurídica Omeba, "Firma", Argentina, 1987, pág. 290.
[4] De Pina Vara, Rafael, Diccionario de derecho, 27ª ed. Porrúa, México, 1999.

expresar que aprueba su contenido", sin embargo, consideramos que dicha definición se limita ya que a pesar de que acepta la existencia de signos gráficos o símbolos que no necesariamente sean letras, indica que dicha fórmula deberá ir acompañada del nombre o título de la persona que lo suscribe.

Mantilla Molina da otra definición y expresa que la firma es "el conjunto de signos manuscritos por una persona que sabe leer y escribir, con los cuales habitualmente caracteriza los escritos cuyo contenido aprueba"[5]; pero qué sucede en el caso contrario en el que la persona que suscribe un acto jurídico es analfabeta y, por lo tanto, utiliza una seña en particular, como podría ser una "x", ¿Podría tener la "x" valor jurídico?

Ciertamente una persona analfabeta no podrá firmar, no obstante, para ello existen soluciones como la señalada en el Código Civil Federal (CCF) que indica en su artículo 1834 que en el supuesto de que se exija la forma escrita en los contratos, éstos deberán ser suscritos por aquellas personas a las que se les obligue por dicho medio, pero en la segunda parte del citado artículo se prevé que en el caso de que alguna de las partes no pueda o no sepa firmar entonces lo hará otra persona a su ruego, debiendo acompañar a dicha firma la huella digital de aquel que no sabe o no puede firmar. Asimismo, la Ley General de Títulos y Operaciones de Crédito (LGTOC) en su artículo 86 señala un requisito adicional al disponer que en el caso de la letra de cambio, en la cual firma una persona a su ruego, dará fe de ello un corredor público, notario u otro funcionario que tenga fe pública.

En cuanto a la costumbre consistente en estampar la firma de forma ilegible o simplemente plasmar símbolos gráficos sin que junto con ella se contenga el nombre de la persona, dicha forma de estampar la firma no tendría validez, ya que de acuerdo al artículo 204 del Código Federal de Procedimientos Civiles "se entiende por suscripción la colocación, al pie del escrito, de las palabras que, con respecto al destino del mismo, sean idóneas para identificar a la persona que suscribe".

No obstante, existe otra corriente que argumenta que la firma será válida independientemente de la inserción o no de los nombres y apellidos, de manera que se atenderá a la forma en que las personas acostumbren hacerlo. Es así que Planiol señala que no importará si se trata de la reproducción del nombre y apellido de la persona según el estado civil en que se encuentre, sino que se tendrá como válida a aquella que sea "la forma habitual de la cual la persona se sirve para firmar"[6].

---

[5] Ibidem, pág 1453.
[6] Planiol, Traité Élémentaire de Droit Civil. Tomo ll, citado por ACOSTA ROMERO MIGUEL en: Nuevo derecho mercantil, México, ed. Porrúa, 2000, pág. 541.

Segovia expresa que “la firma será válida aún cuando sólo figure ya sea el nombre de la persona, los apellidos de ésta o bien únicamente sus iniciales cuando así sea la costumbre del que suscribe la firma”[7].

Dicha postura es apoyada por Salvat al señalar que “aún cuando el firmante inscribiera el apellido de otra familia en lugar del suyo o el nombre de una tierra de su posesión, tendrá validez si se puede probar que el suscriptor así firma comúnmente los documentos públicos o privados que celebra “[8].

Al respecto el Primer Tribunal Colegiado del Segundo Circuito ha expresado en jurisprudencia respecto a la validez de la firma ilegible del girador de la letra de cambio, argumentando que aún cuando la firma que el girador consigne en la letra sea ilegible, se estará a lo dispuesto por el artículo 29, fracción ll de la LGTOC “Artículo 29.- El endoso debe constar en el título relativo o en hoja adherida al mismo, y llenar los siguientes requisitos: **II.-** La firma del endosante o de la persona que suscriba el endoso a su ruego o en su nombre”, lo anterior según lo expresa la Suprema Corte de Justicia, en virtud de que la ley no exige que la firma del endosante se realice en forma legible[9].

A manera de conclusión diremos que, se entenderá por firma al rasgo o conjunto de rasgos que de forma particular estampa cada persona en un documento con el objeto de autenticar su contenido, asimismo, se tendrá por valida la firma en tanto sea ésta la forma en que la persona, que se ostente como titular de la misma, acostumbre hacerlo independientemente de si es legible, o conste en ella el nombre de la persona o no.

Cabe destacar que la función primordial de la firma es la de ser el instrumento con la que el titular de la misma declara su voluntad, es decir, que asume como propias las manifestaciones, declaraciones o acuerdos que contiene un documento.

1.1.1.1 Tipos de firma

Es de importancia hablar de los tipos de firma debido a que podemos encontrar que ésta puede variar dependiendo del negocio o situación de que se trate, es así que estudiaremos los siguientes casos.

---

[7] Lisandro, Código Civil, nota 1 al artículo 1012, Citado por: SEGOVIA, Código Civil anotado, t.1, notas a los arts. 1012, 1014 y 1192. Citado por REVIDATTI, Gustavo Adolfo en: Enciclopedia Jurídica Omeba, “Firma”, Ob. Cit., pág. 291.
[8] Salvat, Tratado de Derecho Civil Argentino, “Parte General”, T-2, números 2154-2162. Citado por REVIDATTI, Gustavo Adolfo en: Enciclopedia Jurídica Omeba, “Firma”, Ob. Cit., pág. 291.
[9] LETRA DE CAMBIO, FIRMA ILEGIBLE DEL ENDOSANTE. Amparo Directo 727/93. Armando Iturbe Cárdenas, Primer Tribunal Colegiado del Segundo Circuito. Octava Época, Semanario Judicial de la Federación.

1.1.1.1.1 Firma Autógrafa

Se llama autógrafa porque el titular de la misma es quien la plasma de puño y letra, ejecutando, mediante dicho acto, su declaración de voluntad respecto de un documento.

Pero no sólo la firma autógrafa nos sirve para aceptar lo que en un documento se ha consignado, sino también como medio de adjudicarse la autoría de una obra, por ejemplo de una pintura, escultura; o simplemente como protocolo, de manera que una vez más ponemos en evidencia el objeto de la firma en cuanto a que es una afirmación de la individualidad y sobre todo de voluntad, es decir, que es el firmante y no otra persona la que estampa su firma y la voluntad se refiere a que el firmante acepta aquello que en un documento se manifiesta.

1.1.1.1.2 Firma a Ruego

Cuando se da el supuesto de que alguna de las partes no sabe o no puede firmar, lo hará otra en su lugar, incluyendo además la huella digital de aquel que no firmó.

Para Carlos E. González, en su "Teoría General del Instrumento Público", define la firma a ruego como: "la que hace una persona ajena al acto o negocio instrumentado, colocando su propia firma a pedido del imposibilitado que es parte interviniente"[10].

Para que sea posible el uso de la figura de la firma a ruego se requiere cumplir con lo siguientes elementos:

a) Que se trate de un instrumento público. La autenticidad de un instrumento público, su fuerza probatoria, derivada de la presencia del oficial público y la fe pública que provee a dicho instrumento, permite que se firme a ruego, en los casos señalados por la ley.
b) Que una o algunas de las partes no sepa o no pueda firmar.
c) Que otra persona distinta de la impedida o imposibilitada firme por ésta, a su instancia o solicitud.
d) Que la persona del rogado no sea testigo instrumental.

1.1.1.1.3 Firma Autorizada

Es aquella que está reconocida o es autorizada por quien es titular del derecho u obligación acerca del cual se va a celebrar una operación; como por ejemplo, la firma de la persona a la que el titular de una cuenta corriente autoriza para hacer disposiciones de fondos.

[10]González, Carlos E., "Teoría general del instrumento público". Introducción al derecho notarial Argentino y comparado, Buenos Aires, Editorial Ediar, 1953. 478 págs.

1.1.1.1.4 Firma Mancomunada

Es aquella que debe estar acompañada de otra u otras para que el documento a firmar tenga plena validez, por ejemplo, la firma de la persona moral en el que la firma será estampada por las personas físicas, a las cuales los órganos de administración y representación hayan otorgado los poderes o facultades, para obligar a dicha entidad, con su firma, en relación a los términos y limitaciones que dichos órganos acuerden. Asimismo la firma mancomunada se da en una sola obligación cuando hay pluralidad de sujetos acreedores, de deudores o de ambos, y el objeto que se debe pagar se considera dividido en tantas partes cuantos acreedores o deudores haya.

Al respecto, cabe mencionar que una firma solidaria es aquella en la que hay pluralidad de personas vinculadas a un derecho u obligación, en donde cada acreedor puede exigir el todo del objeto, y el deudor debe pagar todo el objeto, no obstante que ese objeto es divisible, física o económicamente, por ejemplo, en una cuenta bancaria en la que hay dos o más titulares, cualquiera de ellos puede, indistintamente, disponer de manera absoluta de la cuenta.

1.1.1.1.5 Firma de Letrado

Es la que, mediante estipulación legal o bien por mandato judicial, se pide a los litigantes para que en determinados trámites procesales, consistentes en peticiones por escrito por parte de éstos, se encuentren debidamente firmadas por el abogado que ejerza el patrocinio del asunto en cuestión.

1.1.1.1.6 Firma sobre documentos en Blanco

Significa el suscribir una firma ya sea en un papel en blanco o bien que se deje un espacio entre el texto y la firma con el objeto de que la otra parte pueda adicionar lo convenido o lo que éste desee.

A lo anterior cabe destacar que de acuerdo a lo dispuesto por el artículo 339 del Código Penal para el Distrito Federal párrafo 2º, se tipificará como causal de delito de falsificación de documentos la conducta en la cual exista un aprovechamiento indebido ya sea de una firma o rúbrica en blanco.

1.1.1.1.7 Rúbrica

La Real Academia de la Lengua define a la rúbrica como “el rasgo o conjunto de rasgos de forma determinada, que como parte de la firma pone cada cual después de su nombre o título, y que a veces va sola, esto es, no precedida del nombre o título de la persona que rubrica”[11].

De la definición anterior podemos señalar que si bien es cierto, la rúbrica suele acompañar a la firma, no es esencial que siempre figuren las dos, de manera que existe la posibilidad de utilizar ya sea la firma o la rúbrica, para suscribir.

1.1.1.2 Características de la firma

1.1.1.2.1 Identificativa

Significa que la firma sirve para identificar quién es el autor de la firma, es decir, asegura la relación jurídica entre el acto firmado y la persona que lo ha firmado, es así que la identidad de la persona nos determina su personalidad a efectos de atribución de los derechos y obligaciones.

1.1.1.2.2 Declarativa

Significa que quien firma conoce y acepta el contenido del documento, al cual se va a obligar; Alfredo Reyes Krafft señala que esta característica consiste en la “asunción del contenido del documento por el autor de la firma, sobretodo cuando se trata de la conclusión de un contrato, en donde la firma es el signo principal que representa la voluntad de obligarse”[12].

1.1.1.2.3 Probatoria

Permite identificar si el autor de la firma es efectivamente aquel que ha sido identificado como tal en el acto de la propia firma, esto mediante el estampado del nombre, rúbrica o de los dos, con lo cual se ostenta ante terceros, de manera que no podrá negar su autoría.

Por su parte, Carnelutti considera que la firma tiene una doble función, es decir: una función indicativa y otra declarativa[13].

---

[11] http://www.rae.es
[12] Reyes Krafft, Alfredo, “La firma electrónica y las entidades de certificación”, Ed. Porrúa, México, 2003, pág. 104.
[13] Carnelutti, Francisco, Estudios sobre la suscripción, citado por Carlos a. Pelosi en “El documento notarial, Ed. Astrea, Buenos Aires, 1997, Pág 67.

a) Indicativa.- No la conocemos en el sentido de la suscripción, sino como una mera indicación del autor, independientemente de la firma.
b) Declarativa.- Es el acto de escribir el propio nombre al pie del documento, asumiendo su autoría, por lo que dicho acto importa una declaración de conformidad con el contenido del documento.

Al respecto señala Carnelutti que no siempre la firma contiene la función declarativa, de manera que puede tener otros fines como la unidad del protocolo[14].

1.1.2 Documento

Ahora estudiaremos el concepto de documento, ello debido a la importancia que éste guarda en relación con la firma, en virtud de que es en el documento donde la firma es estampada.

La palabra documento proviene del latín "documentum" que a su vez proviene de "docere", lo cual significa enseñar o dar a conocer[15].

En cuanto a ello, Rafael de Pina Vara señala que documento es una "representación material idónea para poner de manifiesto la existencia de un hecho jurídico (acontecimiento de la vida independientemente de la voluntad humana, contrato, testamento, sentencia, etc.) susceptible de servir, en caso necesario, como elemento probatorio"[16].

Guillermo Cabanellas menciona que documento es el "escrito, escritura, instrumento con que se prueba, confirma, demuestra o justifica una cosa o, al menos que se aduce para tal propósito"[17].

Para Gómez Orbaneja documento es "toda incorporación o signo material de un pensamiento por signos escritos, bien usuales, bien convencionales"[18].

Ampliando el concepto de documento escrito con una referencia más expresiva al contenido y función del documento, Fausto Moreno lo define como "toda escritura que incorpora, enseña, expresa, constata, publica, prueba declaraciones de voluntad positivas o negativas (de

[14] Ibidem.
[15] Op. Cit., "Documento constitutivo".
[16] De Pina Vara, Rafael, Ob. Cit.
[17] CABANELLAS, Guillermo, "Diccionario Enciclopédico de Derecho Usual, T lll, 21ª ed. Heliasta, Argentina, 1989, pág 307.
[18] Gómez Orbaneja, Derecho Procesal Civil, citado por Carlos A. Pelosi en: "El documento Notarial", Ed. Astrea, Buenos Aires, 1997, pág. 31.

querer, saber o conocer, o bien de no saber, no querer o no conocer), o simplemente hechos y derechos"[19].

La Real Academia Española define al documento como el diploma, carta, relación u otro escrito que ilustra acerca de algún hecho, principalmente de los históricos; o bien como el escrito en que constan datos fidedignos o susceptibles de ser empleados como tales para probar algo.

Al respecto diremos que se entenderá por documento:

- Toda representación gráfica que hace constar hechos, o
- Cualquier objeto que contiene una información que narra, hace conocer o representa un hecho, cualquiera que sea su soporte.

Cabe señalar que entre las reformas realizadas al Código de Comercio, por decreto de 23 de mayo de 2000, en el artículo 89 ya se reconoce al documento electrónico el cual es llamado "mensaje de datos".

1.1.2.1 Elementos del documento

De las nociones que anteceden, podemos determinar los elementos que integran el documento, los cuales son:

1.1.2.1.1 Corporalidad

La representación del hecho en el documento tiene lugar mediante signos gráficos en una cosa, por consiguiente, la corporalidad, es decir, la materia con sus tres dimensiones de longitud, altura y profundidad, como principales características de su aspecto o formato exterior, se integra con:

- La cosa u objeto materia y
- La grafía.

1.1.2.1.2 Autor

El autor es la persona que materializa su pensamiento o voluntad con un soporte físico, cualquiera que éste sea, de manera que el autor "es quien condiciona y da vida al documento"[20].

---

[19] Fausto Moreno, D., Nueva Enciclopedia Jurídica, citado por Carlos A. Pelosi en: "El documento Notarial", Ob. Cit. Pág. 31.
[20] Muñoz Sabté, Luis, Técnica Probatoria, citado por Carlos A. Pelosi en: "El documento Notarial", Ob. Cit . pág 62.

1.1.2.1.3 Contenido

Todo documento debe poseer también un contenido, texto o tenor que exprese o represente el pensamiento del autor, por lo que la ausencia del contenido intelectual "hace perder carácter de documento al *corpus,* como en el caso de una hoja de papel en el que sólo aparece la firma de una persona o la hoja impresa con espacios en blanco"[21], es por ello que el pensamiento del autor debe ser inteligible por la lectura, de ahí que los sujetos del documento son el autor y el destinatario.

1.1.2.2 Clasificación de los documentos

Considerando los aspectos con que se presentan los documentos en la ciencia, es decir, vistos desde los diferentes ángulos en que pueden ser estudiados, sin tocar problemas de orden jurídico y de acuerdo con la fuente de información, Carlos A. Pelosi en "El Documento Notarial"[22] distingue las siguientes clases:

I. Documentos gráficos.- como son los libros, folletos, revistas, hojas sueltas, volantes, manuscritos o impresos, etc.
II. Documentos iconográficos.- Retratos incisiones, diseños, fotografías, mapas geográficos y topográficos, planos ilustraciones, figuras de toda especie, tablas, cuadros.
III. Documentos plásticos.- Monedas, medallas, sellos y todos los objetos originados en relieve metálico o de otras materias plásticas.
IV. Documentos fónicos o auditivos.- Discos, cintas magnéticas y las difusiones y transmisiones del sonido.
V. Documentos visuales.- Filme, microfilme, diapositivas, microfichas, etc.

Los documentos han sido estudiados en profundidad en el mundo jurídico y más concretamente por los profesionistas como medio de prueba, de donde resulta que ciertos objetos o cosas que son documentos para la ciencia en general, no lo son o no lo eran para el proceso.

De manera general, y entre otras clasificaciones, la prueba puede ser:

I. Históricas:
    a. Documentales,
    b. Testimoniales.
II. Críticas;

[21] Pelosi, Carlos A. en: "El documento Notarial", Ed. Astrea, Buenos Aires, 1997, pág. 75.
[22] Ibidem, pág. 27.

a. Presunciones y contraseñas. Ambas actúan por medio del raciocinio porque no representan el hecho, sino que se deducen de ellas.

La función representativa se da en la histórica y tiene virtualidad por acción del hombre que percibe el hecho por los sentidos y lo representa de forma inmediata, creando una cosa (documento) o mediata a través de la memoria (testimonio).

Entre ambas podemos hacer la siguiente distinción:

Testimonio	Documento
Carácter personal	Carácter real. Es una cosa
Noticia viviente o voz viva	Vox mortua
Prueba simple (es la que se crea en el acto del proceso)	Prueba preconstituida (existe con anterioridad)
Representación mediata	Representación inmediata. Se traduce en un objeto exterior
Representación transeúnte	Representación permanente, es decir, que está dada por ese objeto, que fija el hecho histórico

1.1.2.3 Documento Privado

Es el redactado por las partes interesadas, con testigos o sin ellos, pero sin intervención de notario o funcionario público que de fe o autoridad.

El artículo 334 del Código de Procedimientos Civiles para el Distrito Federal señala que son documentos privados los vales, pagarés, libros de cuentas, cartas y demás escritos firmados o formados por las partes o de su orden y que no estén autorizados por escribanos o funcionario competente.

1.1.2.4 Documento Público

En cuanto al documento público tenemos que éste es “el otorgado o autorizado, con las solemnidades requeridas por la ley, por notario, secretario judicial o por funcionario público competente para acreditar un hecho, la manifestación de voluntades y la fecha en que se produce”[23].

El artículo 327 del Código de Procedimientos Civiles para el Distrito Federal, hace mención a los documentos públicos, entre los que se encuentran: los autorizados por un notario, corredor público o por funcionarios con fe pública, así como los documentos que se encuentren en los

[23] Ibidem, pág. 308.

archivos públicos, es así que los documentos públicos hacen prueba plena aún contra tercero por tener reconocimiento del Estado.

Asimismo, el Código de Comercio (CCo) en el artículo 1237 señala que son instrumentos públicos los que están reputados como tales en las leyes comunes, y además las pólizas de contratos mercantiles celebrados como tales en intervención de corredor y autorizados por éste.

Cabe decir que los instrumentos públicos constituyen prueba plena, incluso si se presentan sin que haya citación del colitigante, sin embargo, éste podrá ejercer su derecho de argumentar la falsedad de éstos y pedir que se cotejen con los protocolos y archivos correspondientes, siendo que si se demuestra la inconformidad de dichos documentos, éstos perderán su valor probatorio, de conformidad con lo dispuesto por el artículo 1292 del CCo.

Lo anterior explica una de las ventajas del documento público respecto del privado, dado que el primero constituye prueba plena por si misma a menos que se demuestre su falsedad, en este orden de ideas, queremos decir que el documento público nos brinda mayor seguridad al momento de comprobar determinado hecho, ya que está respaldado por la fe pública, lo cual hace que al documento se le tome por verdadero a primera instancia, esto en tanto no se demuestre lo contrario.

1.2 Mensaje de datos (Documento electrónico)

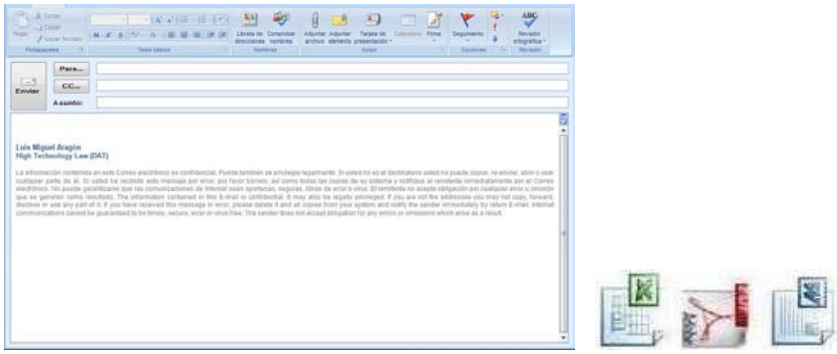
Una vez analizadas las figuras de firma y documento nos centraremos en hablar del mensaje de datos y la firma electrónica, así como otros conceptos relacionados a éstos.

En la legislación mexicana, al documento con soporte en medios electrónicos se le ha denominado como mensaje de datos, lo anterior lo vemos reflejado en el Código de Comercio y en la NOM-151-SCFI-2002, concepto que en términos de unificación de derecho internacional, es adoptado por la Ley de la CNUDMI sobre Comercio electrónico, y que para efectos del presente trabajo nos referiremos al documento electrónico como “mensaje de datos”.

1.2.1 Definición de mensaje de datos

El Código de Comercio en su artículo 89 define al mensaje de datos como “la información generada, enviada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología”.

Asimismo, de acuerdo a lo dispuesto por la Ley Modelo de la CNUDMI sobre Comercio Electrónico, art. 2, inciso a), “por mensaje de datos se entenderá toda información generada, enviada, recibida, archivada o comunicada por medios electrónicos, ópticos o similares” (para los fines del derecho, el término “similar” denota la noción de “equivalente funcional), como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico y el telefax.



El concepto de “mensaje de datos” no se limita a la comunicación sino que pretende también englobar cualquier información consignada sobre un soporte informático que no esté destinada a ser comunicada; así pues, el concepto de “mensaje” incluye el de información meramente consignada.

El término “medios similares” pretende reflejar el hecho de que no se está regulando únicamente las técnicas actuales de comunicación, sino que pretende ser apta para comprender todos los avances técnicos previsibles o imprevisibles.

Asimismo, la definición de “mensaje de datos” está formulada de manera que abarque todo tipo de mensajes generados, archivados o comunicados en forma distinta de documentos con soporte en papel, por ello, al hablar de “medios similares” se incluye cualquier medio de comunicación y archivo de información que se preste a ser utilizado de la manera y por alguna de las funciones desempeñadas por los medios enumerados en la definición.

Por otro lado, la definición de “mensaje de datos” pretende abarcar también el supuesto de la revocación o modificación de un mensaje de datos; si bien es cierto el contenido de un mensaje de datos es invariable, éste puede ser revocado o modificado por otro mensaje de datos.

Como mencionamos al inicio de este capítulo, dentro de las ventajas que podemos encontrar en el uso de mensajes de datos encontramos: el ahorro tanto de dinero como de tiempo, sirve como comprobante fiscal (El Código Fiscal Federal contempla, en el artículo 29, la posibilidad

de emitir comprobantes fiscales digitales por parte de proveedores autorizados por el SAT) y por supuesto sirve como medio de prueba, sólo por mencionar algunos.

Lo anterior porque tenemos una opción más respecto de la forma de documentar los hechos, es así que ya no es necesario contar con grandes espacios para el resguardo de los documentos, sino de un computador en donde almacenar los documentos de forma electrónica, permitiendo un ahorro considerable tanto en el uso de papel como de tinta, espacio y tiempo.

Sin lugar a dudas, uno de los principales aspectos acerca del uso de los mensajes de datos es que puede servir como medio de prueba, tomando en cuenta, para valorar la fuerza probatoria de la información consignada en medios electrónicos, la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas obligadas el contenido de la información relativa y ser accesible para su ulterior consulta. Aunado a lo anterior y como pieza clave para que esto pueda ser una realidad, se tomará en cuenta, para la conservación de los mensajes de datos, lo dispuesto por la Norma Oficial Mexicana NOM-151 SCFI-2002 Prácticas Comerciales – Requisitos que deben observarse para la conservación de Mensajes de Datos, a la cual nos referiremos, con más detalle en el siguiente capítulo.

1.2.2 Nociones Fundamentales

1.2.2.1 Equivalente funcional

La Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) sobre Comercio Electrónico sigue el criterio de los “equivalentes funcionales”, que se basa en el análisis de los propósitos y funciones del requisito tradicional de la presentación de un escrito consignado sobre papel, para determinar la manera de satisfacer sus objetivos y funciones con técnicas electrónicas.

Es decir, el documento con soporte en papel cumple funciones como las siguientes:

- Proporcionar un texto legible para todos;
- Asegurar la inalterabilidad de un mensaje a lo largo del tiempo;
- Permitir su reproducción a fin de que cada una de las partes disponga de un ejemplar del mismo;
- Permitir la autenticación de los datos consignados suscribiéndolos con una firma; y

- Proporcionar una forma aceptable para la presentación de un escrito ante las autoridades públicas y los tribunales.

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

Así pues, se adoptó en la Ley Modelo de la CNUDMI el criterio flexible de "equivalente funcional" que tuviera en cuenta los requisitos de forma, que sirven para dotar a los documentos de papel del grado de fiabilidad, inalterabilidad y rastreabilidad que son aplicables a los documentos consignados sobre papel, de esta forma, el requisito de que los datos se presenten por escrito no debe ser confundido con otros requisitos más estrictos como el de "escrito firmado", "original firmado" o "acto jurídico autenticado".

La Ley Modelo no pretende definir un equivalente informático para todo tipo de documentación de papel, sino que trata de determinar la función básica de cada uno de los requisitos de forma de la documentación sobre papel, con miras a determinar los criterios que, de ser cumplidos por un mensaje de datos, permitirían la atribución a ese mensaje de un reconocimiento legal equivalente al de un documento de papel que haya de desempeñar idéntica función.

La equivalencia funcional, en palabras de Mariliana Rico Carrillo, "se refiere a que el contenido de un documento electrónico surta los mismos efectos que el contenido en un documento en soporte sobre papel"[24], en otras palabras, que la función jurídica que cumple la instrumentación mediante soportes documentales en papel y firma autógrafa respecto de todo acto jurídico, la cumpla igualmente la instrumentación electrónica a través de un mensaje de datos.

La equivalencia funcional implica aplicar a los mensajes de datos un principio de no discriminación respecto de las declaraciones de voluntad, independientemente de la forma en que hayan sido expresadas, en este sentido, los efectos jurídicos deseados por el emisor de la declaración deben producirse con independencia del soporte en papel o electrónico donde conste la declaración.

[24] Mariliana Rico Carrillo, revista Alfa-redi, consultado en http://www.alfa-redi.com, 07 julio 2008.

Rafael Illescas Ortiz, señala que la equivalencia funcional implica “aplicar a los mensajes de datos electrónicos un principio de no discriminación respecto de las declaraciones de voluntad manualmente efectuadas por el mismo sujeto”[25].

Al respecto, el artículo 89 del CCo hace referencia a la figura de la equivalencia funcional al señalar que la firma electrónica produce los mismos efectos jurídicos que la firma autógrafa, la cual además será admisible como prueba en juicio.

1.2.2.2 Neutralidad tecnológica

Consiste en permitir el uso de cualquier medio electrónico en las relaciones jurídicas y no limitarse a alguna tecnología en particular, siempre y cuando ésta ofrezca ciertas características como seguridad y autenticidad.

O. Hance señala que “se trata de dar igualdad de trato a los contratos que tengan soporte informático con relación a aquellos que se consignen en papel, evitando así la ausencia de un régimen general del comercio electrónico”[26].

La Ley Modelo de la CNUDMI sobre Comercio Electrónico refleja el principio de que no debe discriminarse ninguna de las diversas técnicas que pueden utilizarse para comunicar o archivar electrónicamente información, un principio a veces denominado “de neutralidad tecnológica” (A/CN.9/484, pág. 23).

1.2.2.3 No discriminación por falta de acceso a medios electrónicos

Al momento de establecer la normatividad aplicable a las relaciones jurídicas se debe dar oportunidad a aquellas personas que no tienen acceso a los medios electrónicos de realizar determinado acto en papel.

Las palabras “entorno jurídico neutro”, utilizadas en la Ley Modelo, reflejan el principio de la no discriminación entre la información consignada sobre papel y la información comunicada o archivada electrónicamente.

Es así que se le dará igualdad de trato a los actos jurídicos que consten en soporte electrónico con relación a aquellos que se consignen en papel.

---

[25] Rafael Illescas Ortiz “El Comercio Electrónico, fundamentos de derecho y el principio del equivalente funcional”, consultado en http://www.uc3m.es/uc3m/inst/FL/boletin/espanol/pdfdebate/td562.pdf, 10 de julio de 2008.

[26] O. Hance, Leyes y Negocios en Internet, citado por Reyes Krafft, Alfredo Alejandro en: La firma electrónica y las entidades de certificación, Porrúa, México 2003, pág. 107.

1.2.2.4 Autonomía en la voluntad de las partes

Arturo Alessandri define la autonomía de la voluntad como "la libertad de que gozan los particulares para pactar los contratos, y de determinar su contenido, efectos y duración", y señala que esta voluntad es soberana, que el contrato nace del acuerdo de voluntades[27].

Un ejemplo del referido principio, es descrito por Alejandro Loredo A., el cual consiste en que las partes podrán elegir libremente la ley aplicable al contrato electrónico, sin que necesariamente tenga que existir ningún tipo de vinculación entre el ordenamiento seleccionado por las partes y el contrato, favoreciendo la elección de la que más se adapte a la negociación a realizar[28].

Asimismo, las partes podrán convenir el tipo de medios electrónicos a utilizar, para la celebración de actos jurídicos, de manera que no se restrinja su uso a un sistema en particular, cabe señalar que en la práctica se han convenido el uso tanto de documentos con soporte en papel como documentos electrónicos, como convenios (en formato electrónico) posteriores a la celebración de contratos con soporte en papel.

1.2.3 Conceptos relacionados al mensaje de datos

Es de importancia señalar los sujetos que participaran en la generación, envío, recepción y resguardo de la información, lo anterior porque dichos proceso pueden ser llevados a cabo por distintas personas que tengan acceso a un computador y que además tengan acceso a los datos de una persona en particular, es por ello el Código de Comercio señala distintos sujetos y el papel que juegan durante dichas etapas, con la finalidad de poder identificar quien es el iniciador de un mensaje de datos, el destinatario, el intermediario y el carácter vincularte que pueda derivarse.

1.2.3.1 Intercambio Electrónico de Datos (EDI)

Se entiende por EDI a la transmisión electrónica de información de una computadora a otra, estando estructurada la información conforme alguna norma técnica convenida al efecto.

---

[27] Alessandri, Arturo, De los contratos, Centro de Estudios de Derecho Informático, Chile, consltado en http://www.derechoinformatico.uchile.cl/CDA/der_informatico_simple/0,1493,SCID%253D14402%2526ISID%253D507%2526PRT%253D14333,00.html , 10 de julio de 2008.

[28] Loredo, Alejandro A., Contratos telemáticos, naturaleza jurídica en la legislación mexicana, consultado en: http://www.alfa-redi.org/rdi-articulo.shtml?x=7176 10 de julio de 2008.

La Asociación Mexicana de Estándares para el Comercio Electrónico (AMECE) define al EDI o Electronic Data Interchange como el "intercambio electrónico de datos de forma estructurada y estandarizada con la finalidad de ser integrados directamente a los sistemas administrativos sin intervención humana y sin papel de por medio"[29].

Para Claudia Brizzio el EDI "…consiste en un sistema informático que facilita las operaciones comerciales a través de un ordenador, sin necesidad de ningún otro paso intermedio…"[30].

1.2.3.2 Iniciador de un mensaje de datos

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.

1.2.3.3 Destinatario de un mensaje de datos

Aquella persona designada por el emisor para recibir el mensaje de datos, pero que no esté actuando a título de Intermediario con respecto a dicho mensaje.

1.2.3.4 Intermediario de un mensaje de datos

La persona que, actuando por cuenta de otra, envíe, reciba o archive dicho mensaje o preste algún otro servicio con respecto a él.

1.3 Firma Electrónica

1.3.1 Definición

La firma electrónica, técnicamente, es un "conjunto o bloque de caracteres que viajan junto a un documento, fichero o mensaje y que acredita quién es el autor o emisor del mismo, lo que se denomina autenticación, y que nadie ha manipulado o modificado el mensaje en el transcurso de la comunicación, también conocido como integridad"[31].

---

[29] Asociación Mexicana de Estandares para el Comercio Electrónico AMECE, consultado en: http://www.amece.org.mx/amece/faqs/index.php?bnd=3. 10 de julio de 2008.

[30] Barceló, Rosa Julia, Comercio electrónico entre empresarios, la información y prueba del contrato electrónico (EDI), citado por Myrna Elia García Barrera en la Tesis: "La firma Electrónica, nuevo paradigma en el Derecho, Universidad Autónoma de Nuevo León, junio 2005.

[31] Reyes Kraft, Alfredo, consultado en: http://www.alambre.info/2003/12/15/origenes-de-la-firma-electronica, 05 de julio de 2008.

Aquel conjunto de datos, como códigos o claves criptográficas, en forma electrónica, asocia inequívocamente a un documento electrónico que permite identificar a su autor, es decir, que es el conjunto de datos, en forma electrónica, anexos a otros datos electrónicos o asociados con ellos, utilizados como medio para identificar formal y certeramente al autor de un documento.

La firma electrónica, como su nombre lo indica, es el equivalente funcional de la firma manuscrita, la cual es definida por el Código de Comercio en su artículo 89 como: los datos en forma electrónica consignados en un Mensaje de Datos, o adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al Firmante en relación con el Mensaje de Datos e indicar que el Firmante aprueba la información contenida en el Mensaje de Datos, y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio.

1.4 Criptografía

El término Criptografía proviene del griego “kryptos”, ocultar, y “grafo”, texto, lo cual como podemos inferir resulta en el significado “texto oculto”.

La criptografía es el arte o ciencia de cifrar y descifrar información utilizando técnicas matemáticas que hacen posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos.

Con más precisión, cuando se habla de esta área del conocimiento se hace referencia a la criptología, ciencia enfocada tanto al estudio de la disimulación o el cifrado de información, así como a la creación de programas o sistemas que lleven a cabo tales funciones, dicha ciencia involucra diferentes aspectos entre los que se enumeran:

1. La criptografía, la cual se encarga de la disimulación o cifrado de datos, textos o imágenes,
2. La criptofonía que se relaciona con la voz,
3. El criptoanálisis, que estudia los métodos que se utilizan para romper textos cifrados con objeto de recuperar la información original en ausencia de la clave.[32]

1.4.1 Finalidad de la Criptografía

I. En primer lugar, garantizar la confidencialidad de la información contenida en un documento al momento de ser transmitida; y

[32] La Criptografía como elemento de la seguridad informática, consultado en http://bvs.sld.cu/revistas/aci/vol11_6_03/aci11603.htm, 08 de julio de 2008.

II. Asegurar que la información que se envía es auténtica en un doble sentido, es decir:
    a. Que el remitente sea realmente quien dice ser; y
    b. Que el contenido del mensaje enviado, habitualmente denominado criptograma, no haya sido modificado en su tránsito.

En la actualidad, la criptografía no sólo se utiliza para comunicar información de forma segura ocultando su contenido a terceras personas, es así que una de las ramas de la criptografía que más ha revolucionado el panorama actual de las tecnologías informáticas es el de la firma electrónica, tecnología que busca asociar al emisor de un mensaje con su contenido de forma que aquel no pueda posteriormente repudiarlo.

1.4.2 Criptografía aplicada a la firma electrónica

En el caso de la criptografía aplicada a la firma electrónica y al documento electrónico no sólo logra dotar a dichos instrumentos el mismo valor que tradicionalmente se ha dado a sus equivalentes funcionales, sino que con el uso de tal ciencia se busca incrementar la seguridad y disminuir la falibilidad de los documentos que se firman a través de medios electrónicos.

En este orden de ideas, al transformar un documento en texto inteligible podemos observar dos situaciones:

I. Se prevé que éste no sea violado por terceros mediante la intromisión en la computadora de alguna de las partes o por medio de sistemas electrónicos para poder ya sea acceder a la información, a la cual no están autorizados y/o modificarla.
II. Al cumplir con tal objetivo se tiene como resultado un documento que llega a ser incluso más seguro que el firmado de forma autógrafa.

1.4.2.1 Criptosistemas

La palabra criptosistema se refiere a un sistema de encriptación, dicho sistema puede ser simétrico o asimétrico

1.4.2.1.1 Simétrico

La Criptografía Simétrica Implica que las claves para cifrar y descifrar son iguales o que pueden ser calculadas en forma sencilla teniendo solamente una de ellas. En un sistema simétrico tanto la parte que envía como la que recibe deberán compartir el secreto de la clave para cifrar y descifrar lo que haya sido encriptado.

En la Criptografía Simétrica, también conocida como criptografía de clave privada, las dos partes implicadas en una comunicación acuerdan y comparten una clave secreta única, los datos se encriptan y desencriptan utilizando la misma clave[33], para garantizar la seguridad de los datos transmitidos, debe protegerse la clave y sólo debe ser conocida por aquellos que participan en la comunicación.

Criptografía Simétrica

A utiliza la Clave Privada, (misma que comparte con B), para encriptar su mensaje y se lo envía a B

Documento Legible | Llave Privada | Documento encriptado

B recibe el mensaje encriptado y utiliza la Clave Privada (misma que comparte con A)

Llave Privada | Documento encriptado | Documento Legible

El mayor inconveniente de este sistema se presenta en la distribución de la clave entre las partes a comunicarse, es así que la distribución de la clave debe ser por medios seguros ya que de otra forma podría ser interceptada y verse comprometida la privacidad de la información compartida.

De este inconveniente surge, entonces, la necesidad de utilizar un canal seguro para el intercambio o distribución de las claves, esto puede ser resuelto utilizando un sistema de Criptografía Asimétrica.

1.4.2.1.2 Asimétrico

Por otro lado se encuentra el sistema asimétrico, éste consiste en que las claves para cifrar y descifrar son distintas, ello significa que cada una de las partes tiene una clave pública y otra privada, de las cuales la primera es divulgada y la segunda sólo es conocida por el propietario, es así que las partes únicamente compartirán la clave pública.

---

[33] Criptografía simétrica, consultado en: http://www.textoscientificos.com/redes/firewalls-distribuidos/soluciones-seguridad/criptografia, 06 julio 2008.

La Criptografía asimétrica, también conocida como *criptografía de Clave Pública*, se caracteriza por usar un par de claves, llamadas ***Clave Pública*** y ***Clave Privada***. El proceso de uso del par de claves se basa en la aplicación del concepto de función "*unidireccional" con trampa*, es decir, que sólo permite realizar el descifrado al poseedor de la clave secreta (trampa), que de no conocerla, requiere solucionar un problema matemático de un elevado grado de dificultad[34].

En el proceso de comunicación, el receptor crea el par de claves, pública y privada, y distribuye la clave pública libremente a quien desee enviarle información, de manera que la Clave Privada queda en posesión de quien la creó.

En este caso no es problema que un tercero adquiera la clave pública, pues la única forma de descifrar un mensaje encriptado con la misma sólo puede ser descifrado con la Clave Privada que únicamente posee el receptor deseado del mensaje, es decir el titular de la clave privada.

La principal ventaja del cifrado con la clave pública es el incremento de seguridad que proporciona, pues la clave privada nunca es transmitida, ni revelada a persona alguna.

1.4.2.1.2.1 Clave pública

La NOM 151-SCFI-2002 define a la clave pública como "la cadena de bits (es la unidad mínima de información que puede ser procesada por una computadora) perteneciente a una entidad particular y susceptible de ser conocida públicamente, que se usa para verificar las firmas electrónicas de la entidad, la cual está matemáticamente asociada a su clave privada".

La clave pública podrá ser conocida por cualquier persona y sirve para cerciorarse de que el documento firmado a enviarse efectivamente llegue a quien es dueño del tal clave, ya que aún cuando ésta pueda ser conocida por las demás personas sólo el titular de la clave podrá revisar el contenido del documento al utilizar su clave privada que descifrará el mensaje.

Derivado de lo anterior surge la siguiente interrogante ¿Cómo puedo saber que la clave pública pertenece realmente a la persona que se ostenta como titular de la misma? para ello

[34] Ibidem.

existen instituciones que se encargan, entre otras cosas, de autenticar la identidad tanto de quien envía la información como de quien la recibe, dichas instituciones reciben el nombre de Prestadores de Servicios de Certificación (PSC) de quienes hablaremos de forma más detallada en el siguiente capítulo.

1.4.2.1.2.2 Clave privada

De acuerdo con la NOM 151-SCFI-2002, la clave privada es la "cadena de bits conocida únicamente por una entidad, que se usa en conjunto con un mensaje de datos para la creación de la firma digital, relacionada con ambos elementos".

La clave privada es ambivalente, es decir, en el supuesto de ser el destinatario de un documento es lo que se necesita para descifrar la información, por otra parte, en el caso de ser el remitente de un documento que se envíe, se usa para firmar en forma electrónica.

1.4.3 Cifrado de la llave asimétrica o pública

Supuesto en el que A desea enviar un mensaje a B.

- A usa la llave pública de B para encriptar el mensaje que le envía,
- B usa su llave privada para desencriptar el mensaje que le envió A, y
- B verifica la identidad de A con su llave pública.[35]

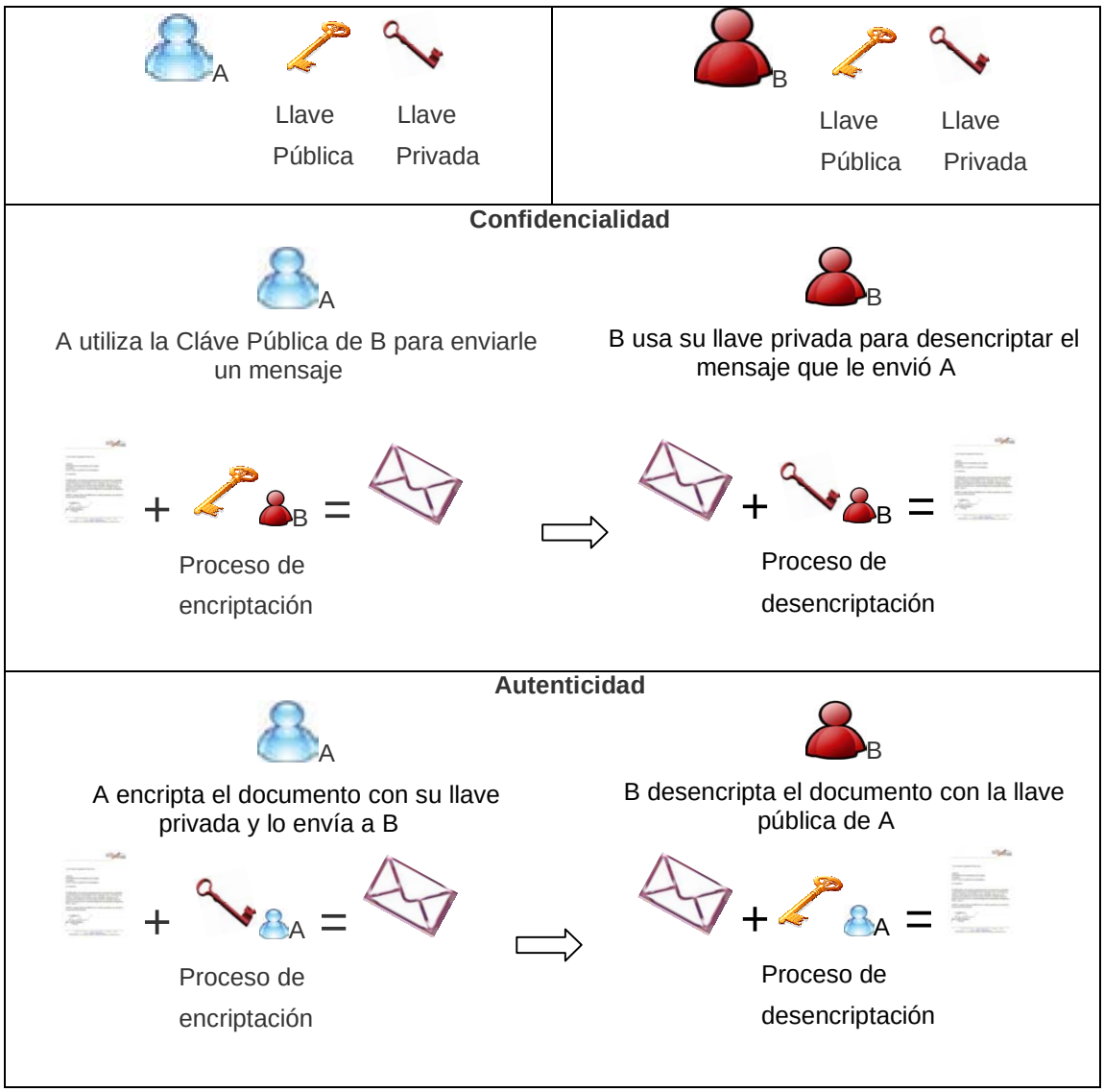
Por otro lado, si A y B desean autenticar un documento, el proceso es al revés.

Supuesto en que A quiere enviar un documento a B, para que éste lo autentique, es decir, para que B pueda comprobar que dicho documento sólo puede provenir de A, este proceso se conoce como "firma digital".

- Cualquier persona que conozca la llave pública de A (todos la conocen) puede desencriptar el documento con esa llave, de manera que existe una llave privada de A y una llave pública de A,
- Es así que A encripta el documento con su llave privada y lo envía a B,
- Por lo que B desencripta el documento con la llave pública de A.[36]

[35] REYES KRAFFT, Alfredo Alejandro, "La firma electrónica y las entidades de certificación", Ed. Porrúa, México 2003, pág 181.
[36] Ibidem.

Criptografía Asimétrica



1.5 Firma electrónica simple

Es una aplicación de *encriptación simétrica* que se basa en el intercambio de una clave entre dos partes, en la cual las personas involucradas deben conocer y utilizar la misma clave y por seguridad mantenerla en secreto, la cual garantiza:

- Confidencialidad (capacidad de mantener un documento electrónico sólo visible al destinatario e inaccesible a todos los demás) y
- Autenticación (reconocimiento y/o compromiso de una persona específica sobre el contenido del documento electrónico).

Algunos ejemplos del uso de firma electrónica simple son:

- Los números de identificación personal (NIP) como llave que se comparte con el banco para hacer transacciones en cajeros automáticos o a través de internet;
- La clave para entrar a la cuenta de correo electrónico (de la que toma parte el prestador del servicio),
- Así como las contraseñas que se utilizan para acceso a otros servicios por internet.

1.6 Firma electrónica avanzada

Se basa en el uso de un juego de claves o llaves, un par de números matemáticamente relacionados, uno para la pública y otro para la privada. Un programa de cómputo los produce y se los proporciona al solicitante, quien puede dar a conocer la primera y debe mantener en secreto la segunda.

Cada clave es la función inversa de la otra, es decir, lo que una clave hace sólo la otra clave puede deshacerlo. Así, para enviar un mensaje privado, el emisor lo encripta (cierra) con la clave pública del receptor y sólo el receptor puede desencriptarlo (abrirlo) con su propia clave privada, que nadie más conoce, de esta forma, la información encriptada con este sistema garantiza la confidencialidad y autenticación.

La Firma Electrónica Avanzada (FEA), además de confidencialidad y autenticación (que proporciona la firma electrónica simple), asegura:

- La integridad del documento (el contenido no puede ser alterado) y
- Al no repudio del mismo (innegable autoría).

La FEA utiliza la función hash para garantizar estas funciones, el hash es una operación matemática que asocia un texto de extensión variable a un número de longitud fija (entre 128 ó 160 bits) que se llama resumen. Si el documento sufre alguna alteración o modificación, por mínima que sea, el hash cambia, reflejando que el documento ya no es el mismo.

Cabe señalar que, las funciones hash no encriptan, sólo comprimen los textos para que el receptor pueda comprobar la integridad del mismo rápidamente. Al aplicar la firma digital, se encripta sólo la función hash y no todo el documento, de esta forma el proceso de desencriptar toma menos tiempo.

Asimismo una firma electrónica avanzada es aquélla que cumple con los requisitos que establece el art. 97 CCo en materia de firma electrónica y que se han considerado imprescindibles para hacer equivalente, de forma absoluta, la firma electrónica y la firma manuscrita.

Estas características son:

I. Los Datos de Creación de la Firma, en el contexto en que son utilizados, corresponden exclusivamente al Firmante;

II. Los Datos de Creación de la Firma estaban, en el momento de la firma, bajo el control exclusivo del Firmante;

III. Es posible detectar cualquier alteración de la Firma Electrónica hecha después del momento de la firma, y

IV. Respecto a la integridad de la información de un Mensaje de Datos, es posible detectar cualquier alteración de ésta hecha, después del momento de la firma.

Es necesario tener en cuenta que el hecho de que la firma electrónica avanzada y la firma manuscrita sean equivalentes implica que un documento electrónico firmado puede ser presentado como una prueba documental en un procedimiento cuyo fin sea dirimir una controversia sobre un hecho documentado por medios electrónicos, lo anterior con fundamento en el art. 210-A del Código Federal de Procedimientos Civiles, el cual establece que “se reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología”, así como los arts. 1205 y 1298-A del Código de Comercio, los cuales también provén de reconocimiento jurídico al mensaje de datos, para ser exhibido como medio probatorio.

Cuando no empleamos una firma electrónica avanzada, tenemos que demostrar, en ese procedimiento, cuestiones como las siguientes:

- Que el remitente verdaderamente escribió el documento,
- Que el documento fue enviado a su destinatario.
- Que el documento fue recibido correctamente.
- Que nadie interceptó y alteró el documento en tránsito.

El empleo de la firma electrónica avanzada supone que será la persona que niegue la validez y eficacia de una firma electrónica, en concreto, la que va a cargar con la prueba

específicamente, es decir, el destinatario de un documento electrónico firmado tendrá que demostrar:

- Que el remitente no escribió el documento.
- Que el documento no llegó al destinatario.
- Que el documento no fue recibido por el destinatario.
- Que el documento fue interceptado y alterado en tránsito.

La principal ventaja de la firma electrónica avanzada sobre otros mecanismos de seguridad, incluida la que hemos denominado firma electrónica "simple", es precisamente su reconocimiento legal, que se plasma en las presunciones a las que hemos hecho referencia.

1.7 Características de la firma electrónica

1.7.1 Integridad

Se refiere a que la información consignada en un documento, amparada con una firma, es la que desde un inicio se introdujo y que no ha sido modificada o borrada.

Ribas Xavier menciona que con esta característica se garantiza que los elementos básicos del negocio, como el precio, la cantidad y las características de lo contratado, entre otras, se considerarán válidos salvo que la parte en desacuerdo demuestre que efectivamente han sido alterados o se han incumplido las normas de seguridad establecidas para garantizar la integridad de la información[37].

1.7.2 Autenticidad

Permite constatar que quien envía el documento es quien así lo ostenta, de manera que es una prueba o garantía de la identidad de quien envía la información.

Ribas Xavier expresa que es un valor necesario y sumamente importante ya que con ella se garantiza a la parte receptora que el documento que recibe fue firmado efectivamente por quien aparece como remitente en el mencionado instrumento[38].

---

[37] Ribas, Xavier, "Propuesta de Directiva sobre Firmas Electrónicas, REDI Revista Electrónica de Derecho Informático, España, consultado en : http://premium.vlex.com/doctrina/REDI-Revista-Electronica-Derecho-Informatico/Propuesta-Directiva-firmas-electronicas/2100-106968,01.html 01 julio 2008.

[38] Ibidem.

1.7.3 No repudio

Tal característica trata acerca de la voluntad de quien suscribe un documento, de manera que implica una imposibilidad para desconocer una transacción una vez realizada.

Ignacio Alamillo explica que esta característica se basa en un anglicismo, el cual quiere decir que una vez que se ha convenido en algo, la persona no puede rechazar lo estipulado[39].

Al respecto, Ribas añade que el no repudio consiste en la presunción de que la firma electrónica fue empleada por quien se ostenta como dueño de la misma, lo cual implica que al dueño de la firma se le tendrá por consentido de aquello que se encuentre estipulado en el documento"[40].

1.7.4 Confidencialidad

Asegura el secreto de la información contenida en el mensaje de datos, a partir de la encriptación del mismo. Reyes Krafft señala que es la garantía de que el contenido de la información se mantiene oculta salvo para el destinatario.

La confidencialidad permite a quien suscriba el documento, al usar la clave pública del destinatario de dicho documento, convertir automáticamente la información en algo incomprensible, denominado criptografía, para cualquiera que no sea el mencionado destinatario.

A manera de conclusión diremos que la firma electrónica cumple con todas las características mencionadas en la firma autógrafa, sin embargo, permite hacerlo en medios electrónicos con seguridad técnica y jurídica. Asimismo, existen dos tipos de firma electrónica, una simple y otra firma electrónica avanzada, ambas tienen diferentes niveles de seguridad, tal y como se observa en el siguiente cuadro:

[39] Alamillo Domingo, Ignacio, "Confianza Digital Basada en Certificados" REDI Revista de Electrónica de Derecho Informático, España, consultado en: http://premium.vlex.com/doctrina/REDI-Revista-Electronica-Derecho-Informatico/Confianza-digital-basada-certificados/2100-107350,01.html, 12 de julio de 2008.
[40] Ribas Xavier, Ob. Cit.

Tabla comparativa[41]

	**Firma Autógrafa**	**Firma Electrónica Simple**	**Firma Electrónica Avanzada**
E l e m e n t o s f o r m a l e s			
La firma como signo personal.	●	●	●
El *animus signandi*, voluntad de asumir el contenido de un documento.	●	●	●
E l e m e n t o s f u n c i o n a l e s			
Identificación	●	●	●
Autentificación	●	●	●
Confidencialidad	X	●	●
Integridad	X	X	●
No repudio	X	X	●

[41]Dr. Alfredo Reyes Kraft, consultado en: http://ciberhabitat.gob.mx/comercio/firma/textos/firma_elecronica.htm, 07 julio 2008.

CAPÍTULO SEGUN

2. De la Entidad Certificadora o Prestador de Servicios de Certificación

La confianza es un elemento imprescindible para que los usuarios utilicen las tecnologías de la Información y Comunicación, y participen animadamente en el intercambio de mensajes de datos, para ello se requiere de un régimen jurídico que refleje seguridad, fomente o incentive su uso, de lo contrario la desconfianza o el recelo sobre el régimen aplicable provocará el abandono de esa figura o hace que ésta quede relegada a segundo plano frente a otra u otras más operativas y seguras.

Es así que, dentro de los actos jurídicos celebrados a través del uso de medios electrónicos encontramos al comercio electrónico, esto es la preparación, el establecimiento y concertación de relaciones comerciales, no estrictamente mercantiles a través de los medios informáticos[42]. No obstante, cabe señalar que el término "contratación a través del uso de medios electrónicos" ha sido también denominada, a veces de manera más confusa, como contratación informática, pues esta última es más bien la que tiene por objeto la transmisión de derechos de propiedad o de uso de un bien informático o la prestación de servicios sobre dichos bienes (ordenadores, programas informáticos, uso y explotación de programas, etc.[43]), entendida la misma como aquella en que los contratos son concluidos a través de medios electrónicos on-line[44], mediante el llamado diálogo de ordenadores, no obstante, la contratación electrónica también comprende la compraventa de bienes y/o servicios, pero la particularidad de esta otra variedad radica en que ésta se ejecuta por vía no electrónica, cuando su objeto debe transportarse materialmente al lugar pactado[45].

Es de importancia destacar que, la materia del presente trabajo también se enfoca en un marco más amplio de la comunicación electrónica, puesto que tal comunicación no sólo es

[42] Al respecto, Ma. Isabel Huerta Viesca y Daniel Rodríguez Ruiz de Villa discrepan de que el comercio electrónico equivalga a la contratación electrónica, pues hay contratación electrónica no comercial, por lo tanto, frente a lo que dice Sala I. Andrés, A. Ma. En "la autoría en las manifestaciones electrónicas" no todo acto realizado por medios electrónicos es comercio electrónico, sino que, como expone Uria, R "Derecho Mercantil", Marcial Pons, Madrid, 2000, pág. 620, en una concepción amplia comprende "…aquellas transacciones comerciales electrónicas, es decir, de compraventa de bienes o prestación de servicios, así como las negociaciones previas y otras actividades ulteriores relacionadas con las mismas, desarrolladas a través de los mecanismos que proporcionan las nuevas tecnologías de la información y comunicación, tales como el correo electrónico, o el World Wide Web, ambas aplicaciones de la Internet o las formas de comercio electrónico surgidas en los años 80 como la basada en el EDI (Electronic Data Interchange). Por tanto, Isabel Huerta Viesca y Daniel Rodríguez Ruiz de Villa comparten la idea de Díaz Brito, F.J. "Contratación electrónica: ¿camino del laberinto?", BICM, núm. 23, enero 2001, pág. 1, acerca de que el comercio electrónico comprende "…una realidad compleja y heterónoma, integrada por diferentes clases de actividades (desde la información y promoción de empresas y productos hasta la venta *on line* de los mismos) con el común denominador de poner en relación el contrato y la contratación con las nuevas tecnologías de la información y la comunicación.

[43] Ma. Isabel Huerta Viesca y Daniel Rodríguez Ruiz de Villa, "Los Prestadores de Servicios de Certificación en la Contratación Electrónica", Ed. Aranzadi, 2001, pág. 52.

[44] Clemente Meoro, M. E. "Algunas consideraciones sobre la contratación electrónica" RdDP, número 4, 2000-1, págs. 59-86.

[45] Ibidem.

contractual sino que va más allá de ésta, gozando de importantes efectos jurídicos en los que la seguridad juega un papel decisivo, como ejemplo de lo anterior podemos decir que cuando se trate de una sociedad y exista acuerdo previo de los afectados, o cuando se les imponga por vía estatutaria el uso de medios electrónicos para efectos de notificaciones para asambleas, será cuando la comunicación electrónica produzca efectos válidos idénticos a la comunicación escrita en papel, esto mediante el envío de mensajes de datos, por el órgano de administración de la sociedad, a través de la Internet[46].

Es por ello que, el Prestador de Servicios de Certificación juega un papel importante en el momento en que quienes contratan a través de medios electrónicos y éstos se encuentren separados geográficamente, como es común, y en donde el uso de la firma electrónica cause incertidumbre en cuanto a la identificación de los obligados, será el PSC quien permita al remitente asegurarse de que el destinatario realmente sea quien reciba el mensaje, y además permitirá al destinatario saber que aquel que le envía el mensaje electrónico es efectivamente quien lo firma. De esta forma, es el Prestador de Servicios de Certificación el encargado de garantizar el intercambio de mensajes de datos a través de comunicaciones electrónicas, lo que permitirá que se desarrolle y fomente su implementación, hasta el punto de que se ha llegado a decir que su existencia es imprescindible para que la firma electrónica sea operativa[47].

De este modo se conseguirá el desarrollo del comercio electrónico, entendiéndose el mismo en sentido lato, para comprender no sólo la contratación por vía electrónica sino también el intercambio de información comercial por la misma vía, de manera que se incluyen tanto las páginas web de simple promoción comercial (con información somera de la empresa propietaria de las mismas), como las denominadas “escaparate electrónico” (con una información más detallada, en la que se incluyen los productos o servicios de la empresa, pero sin permitir la contratación), hasta llegar a las denominadas “tiendas virtuales” (que ofrecen la posibilidad de contratar por vía electrónica, de manera directa o indirecta, sin requerir otras formas de comunicación adicionales entre los contratantes, quienes luego recibirán de manera instantánea o posteriormente los objetos de la contratación, siendo en el primer caso por vía electrónica y en el segundo a través de mensajerías u otros servicios de transportes tradicionales).

En este orden de ideas, se está ante una relación tripartita, en la que una tercera parte, llámese Entidad Certificadora, ha de existir porque los contratantes no están presentes, es decir, actúan a través de una red abierta y pueden no conocerse entre sí previamente, siendo esta tercera parte la que identifica al firmante electrónico y que tiene la fiabilidad que permite que las

[46] El Dr. Alfredo Reyes Kraft define a la Internet como “…un canal mundial de telecomunicaciones informáticas, que está integrado por muchos canales que a se vez, están interconectados entre si…”Ob. Cit., pág. 27.
[47] Alcocer Garau, G. “La firma electrónica como medio de prueba (Valoración jurídica de los criptosistemas de claves asimétricas)”, ACD, núm. , abril 1994, pág. 29.

partes confíen y dota de la imprescindible seguridad a las transacciones celebradas a través de medios electrónicos.

Por todo ello, en la contratación electrónica, se deben asegurar los siguientes puntos:

1. La autenticidad, fiabilidad, integridad e inalterabilidad de los mensajes que circulan a través de la Internet, de forma que no haya duda acerca de quién es el autor (imputabilidad) y cuál es el contenido exacto de un determinado mensaje, sin que haya podido haber errores de transmisión o intervención de terceros, de forma que A no pueda ser suplantado por B, autor del mensaje X, y que B no pueda alterar el contenido inicial del mensaje creado y enviado por A[48]. Nótese, por ejemplo, la importancia que tienen la fiabiliadad de los mensajes electrónicos en la Banca electrónica, pues el riesgo que más le preocupa a la misma es que, ni por azar ni por actuación de un tercero se puede alterar el contenido de la información que se consigne en el mensaje electrónico, de modo que para evitar esto la encriptación se aplica no sólo a lo que es la firma en sí, sino también a todo el mensaje[49].
2. El no rechazo o no repudiación en destino y origen de un mensaje, también denominado irretractibilidad de origen y de destino[50], de forma que A no pueda negar que es el autor del mensaje X y B, destinatario del mismo, no pueda negar haberlo recibido, asimismo no se podrá rechazar la posesión de claves empleadas para la redacción y emisión del mensaje electrónico, puesto que ello es lo que permitirá que exista una prueba de la existencia de la transacción electrónica, vinculante para quienes la efectuaron.
3. La confidencialidad de dicho mensaje, de forma que el contenido del mensaje X enviado por A a B sólo pueda ser conocido por su emisor y por el destinatario y no por terceros ajenos.
4. La perdurabilidad del mensaje electrónico, con el objeto de que su existencia y contenido puedan ser acreditados en el futuro, en caso de aparición de una controversia acerca del mismo. Cuando se trate de la contratación electrónica es evidente que la perdurabilidad es la que permitirá acreditar la existencia y contenido de la relación jurídica en cuestión[51].

---

[48]Martínez Nadal, A., "Aproximación al borrador de propuesta de directiva para un marco común de firma electrónica y proveedores de servicios relacionados", AIA, núm.29, octubre de 1998, pág. 1.

[49] Azofra Vegas, F., "La contratación electrónica bancaria", RDBB, núm. 68, octubre-diciembre de 1997, pags. 1110-1115, citado por Ma. Isabel Huerta Viesca y Daniel Rodríguez Ruiz de Villa, "Los Prestadores de Servicios de Certificación en la Contratación Electrónica", pág. 63.

[50]Ruí-Gallardón, M., "Fe pública y contratación telemática", *Derecho de Internet. Contratación electrónica y firma digital,* Mateu De Ros, R. y J. M. Cendoya Méndez De Vigo (coordinadores), Aranzadi, Pamplona, 1ª reimpresión, 2001, págs. 111-112.

[51]Sanchíz Crespo, C., "Una reflexión acerca de la eficacia probatoria de escritura en el Anteproyecto de LSiv", *presente y futuro del proceso civil,* PICO JUNOY; J.,Barcelona, 1998, págs. 275-282.

Con el logro de los objetivos antes enumerados se incrementará de manera considerable el acceso de las Pequeñas y Medianas Empresas (PYMES) al comercio electrónico, no sólo en la contratación con consumidores (identificado como B2C, e-commerce o C-E EaC[52]) sino también en las contrataciones entre ellas (Business to Business, identificado como B2B, e-business o eprocurement o C-E EaE[53]); y en el ámbito empresarial, servirá para desarrollar las relaciones de los consumidores con la Administración Pública (Business to Administration).

Nótese que cuando se contrata electrónicamente con consumidores, la seguridad de tal contratación no sólo les interesa a éstos, sino también a los comerciantes, quienes querrán saber si aquél con quien contratan no ha empleado una identidad falsa.

A manera de conclusión diremos que, para que esa identificación sea segura es para lo que se atribuye a terceros, ajenos a la contratación electrónica, la función de emitir los certificados, esto es, la certificación electrónica que vincula unos datos de verificación de firma electrónica a un signatario o firmante y que confirma su identidad de forma similar a lo que ocurre con la firma manuscrita respaldada por una identificación oficial, es decir, una credencial del IFE o pasaporte.

2.1 Definición de Prestador de Servicios de Certificación (PSC)

El concepto de Prestador de Servicios de Certificación es definido por el artículo 89 del CCo. al señalar que "…es la persona o institución pública que preste servicios relacionados con Firma Electrónica y que expide los Certificados, en su caso…", de modo que son éstos entes quienes emiten los certificados que permiten confirmar y verificar la identidad de los firmantes de los documentos electrónicos.

En términos de unificación del derecho internacional, compartimos la idea de que el artículo 89 del CCo. contenga el concepto de Prestador de Servicios de Certificación, lo anterior porque podemos encontrar que en la doctrina al PSC también se le llama como "Autoridad Certificadora", "Entidad Certificadora", "Terceras Partes confiables", sólo por mencionar los más comunes.

Asimismo, la Ley de Firma Electrónica Certificada para el Estado de Jalisco y sus municipios en su artículo 3 fracción XIII señala que el Prestador de Servicios de Certificación "es la persona o entidad pública que preste servicios relacionados con la Firma Electrónica Certificada y

[52] Las dos primeras son expresiones anglosajonas de amplia difusión; la última es aportada por Illescas Ortiz, R., "La firma electrónica y el Real Decreto-Ley 14/1999, del 17 de septiembre", DN, núm 109, octubre 1999.
[53] Las dos primeras son expresiones anglosajonas de gran difusión, la última es proporcionada por Illescas Ortiz R., "Entre Europa y la nada (A propósito del Anteproyecto de Ley de Servicios de Sociedad de la Información y de Comercio Electrónico de 29 de septiembre de 2000)" RCE, núm. 11, 2000, págs. 3-33.

que expide certificados electrónicos, previa autorización otorgada por la Secretaría; con la elección de este concepto el legislador ha acertado, no sólo porque refleje el principal objeto de actuación de esta casi nueva Entidad, sino también porque fue el concepto que se encuentra contemplado en el artículo 2, inciso e) de la Ley Modelo de la CNUDMI sobre las Firmas Electrónicas, adoptada el 5 de julio de 2001 (Art 2.- Por "prestador de servicios de certificación" se entenderá la persona que expide certificados y puede prestar otros servicios relacionados con las firmas electrónicas), a nuestro parecer esta última definición denota una concepto más acertado a la figura del PSC, puesto que su principal objeto es el de fungir como tercero de confianza que emite certificados electrónicos, los cuales vinculan la relación que existe entre una llave pública y una persona en particular.

Desde esta perspectiva conceptual, es cierto que también se les podría haber llamado Servidores de Claves, pues, en realidad, uno de los objetos fundamentales de su actividad es crear las claves públicas que se integran en los correspondientes certificados[54].

Por otra parte podemos extraer de la definición normativa del PSC, las siguientes dos funciones:

a).- Una función básica e imprescindible, que es la de la expedición de certificados.
Por tal motivo, el Prestador de Servicios de Certificación actúa como una tercera parte de confianza, que vincula una clave pública, e indirectamente la correspondiente clave privada, a una persona determinada, de forma segura, a través de un certificado electrónico, el cual es un elemento de confianza para los terceros que contraten por medios electrónicos con esa persona, asumiendo el PSC una responsabilidad por la exactitud del certificado[55]. Para que dicho certificado pueda ser empleado por su titular será necesario que el PSC le proporcione la clave privada, así como el correspondiente programa o aplicación informática que se deberá instalar en el ordenador personal del usuario.

b).- Unas funciones adicionales o complementarias, teóricamente no necesarias ni definidoras del PSC, son las de otros servicios en relación con la firma electrónica, como son:

- Conservación de mensajes de datos,
- El sellado de tiempo digital,

[54] Ramos, F., "La firma Electrónica y su normativa", *Otrosí*, núm. 13, marzo 2000, págs. 18-26.
[55] Ormazabal Sánchez, G. "La prueba mediante documento electrónico digitalmente firmado", Act. Civil, 1999-1, pág. 223, citado por Ma. Isabel Huerta Viesca y Daniel Rodríguez Ruiz de Villa, "Los Prestadores de Servicios de Certificación en la Contratación Electrónica", pág. 88.

- Validación de certificados.

Servicios señalados por la Regla 2.bis. del Acuerdo que modifica las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación, publicado el 5 de marzo de 2007 en el DOF.

2.2 Antecedentes del Prestador de Servicios de Certificación en México

Antes de dar continuidad a nuestro estudio sobre la Entidad Certificadora, consideramos de importancia el señalar el primer antecedente de dicha figura en nuestro país, lo anterior porque se puede pensar que el primer antecedente se encuentra en el Código de Comercio, no obstante, como veremos la figura del Prestador de Servicios de Certificación se contempló en otro cuerpo normativo, en el cual se mencionó por primera vez.

Para comenzar señalaremos que, con fecha del 29 de mayo del 2000, se publicó en el DOF, el decreto por el cual se reforman y adicionan diversas disposiciones del Código Civil para el Distrito Federal en Materia Común y para toda la República en Materia Federal, del Código Federal de Procedimientos Civiles, del Código de Comercio y de la Ley Federal de Protección al Consumidor.

En el referido Decreto se reformó el artículo 49 del Código de Comercio, el cual señala lo siguiente:

> **Artículo 49**.- Los comerciantes están obligados a conservar por un plazo mínimo de diez años los originales de aquellas cartas, telegramas, mensajes de datos o cualesquiera otros documentos en que se consignen contratos, convenios o compromisos que den nacimiento a derechos y obligaciones.
>
> Para efectos de la conservación o presentación de originales, en el caso de mensajes de datos, se requerirá que la información se haya mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y sea accesible para su ulterior consulta. **La Secretaría de Comercio y Fomento Industrial emitirá la Norma Oficial Mexicana que establezca los requisitos que deberán observarse para la conservación de mensajes de datos.**

Derivado de lo anterior, con fecha del 4 de junio del 2002, se publicó en el DOF, la Norma Oficial Mexicana **NOM-151-SCFI-2002 Prácticas Comerciales - Requisitos que deben**

observarse para la conservación de mensajes de datos (NOM-151), dando así cumplimiento a lo previsto por el precepto legal antes citado, sin embargo, la referida NOM no pudo entrar en vigor dado que aún no se contaba con la infraestructura para la evaluación de conformidad, es decir, con los lineamientos que permitieran evaluar el cumplimiento de reglamentos o normas técnicas y también, cabe señalar, porque hasta ese momento no existía trámite de persona alguna que pudiera fungir como Prestador de Servicios de Certificación, pues la legislación aplicable aún no existía[56].

Es así como, hasta ese momento, la primera legislación que hace alusión a los PSC, es la propia NOM-151, misma que establece en el numeral 5.1, que "para la emisión de la firma electrónica y/o digital, así como el Prestador de Servicios de Certificación deberán observar los requisitos que la normatividad aplicable señale para su operación".

Por otra parte, el 29 de agosto de 2003, se publicó en el DOF, las reformas y adiciones a diversas disposiciones del CCo en Materia de Firma Electrónica, incorporando así el Título Segundo denominado "Del Comercio Electrónico".

Cabe destacar que, es en este ordenamiento donde una vez más se contempla la figura del PSC y que además se regula su funcionamiento,

2.3 Autoridad Certificadora Raíz de la Secretaría de Economía ACR-SE

La Autoridad Certificadora Raíz de la Secretaría de Economía (ACR-SE) es la instancia de la Secretaría de Economía encargada de certificar la clave pública de las Autoridades certificadoras subordinadas, de acuerdo al CCo. en materia de Prestadores de Servicios de Certificación y sus Reglas Generales, así como de emitir o revocar los certificados de las Autoridades referidas, asimismo, dicha institución se establece para crear y desarrollar una Infraestructura de Llave Pública (PKI) a nivel nacional para el desarrollo del comercio electrónico.

La ACR-SE, a través de la Dirección General de Normatividad Mercantil (DGNM), certificará las claves públicas de las Autoridades Certificadoras que hayan sido acreditadas.

2.3.1 Autoridad Registradora (RA)

La Autoridad registradora (RA), la cual forma parte de la ACR-SE, será la encargada de la autenticación e identificación de las entidades o usuarios finales, verificar la identidad del

[56] En palabras del Lic. Agustín Ríos, Director de R1OS Abogados, Vicepresidente del Comité Jurídico de la AMIPCI y Asesor legal de la APSCE.

solicitante del certificado a favor de éste y de llevar acabo el procedimiento para la emisión y/o revocación de certificados.

2.3.2 Certificación por parte de la ACR-SE

De acuerdo a la estructura jerárquica de certificación, la ACR-SE podrá certificar la clave pública a:

I. La Dirección General de Normatividad Mercantil (DGNM).
   Ésta a su vez podrá certificar las claves públicas de:
   a. Autoridades Certificadoras para Instituciones Públicas Gubernamentales desconcentradas o descentralizadas de la Secretaria de Economía,
   b. Entidades de la Secretaría de Economía,
   c. De Identidad Personal, para funcionarios públicos de la SE y
   d. Para los particulares que realicen trámites ante la SE.

II. El Sistema Integral de Gestión Registral (SIGER).
   Ésta a su vez podrá certificar las claves públicas de:
   a. Los Registros Públicos de Comercio (RPC),
   b. Fedatarios públicos y
   c. A sus respectivos agentes de certificadores del SIGER

III. Prestadores de Servicios de Certificación.
   Que hayan sido acreditadas por la DGNM; estos podrán certificar las claves públicas de:
   a. Personas físicas o
   b. Personas morales.

Solo emitirá otro tipo de certificado digital, en caso de ser necesario para la operación de alguna necesidad de la Secretaría de Economía. Éste deberá ser autorizado por el Comité de Seguridad de la DGNM.

2.4 Estructura jerárquica de la Autoridad Certificadora

La estructura jerárquica de certificación se compone de los siguientes elementos:

I. **Autoridad Certificadora Raíz de la Secretaría de Economía**
   Ofrece servicios de certificación de clave pública de las autoridades certificadoras subordinadas a la SCR-SE. La SE es una institución pública gubernamental establecida para el desarrollo del ámbito comercial, tanto en el Registro Público de Comercio como para el comercio electrónico entre otros.
II. **Autoridades Certificadoras Subordinadas de la ACR-SE**

Serán las personas físicas o morales acreditadas como PSC, Instituciones Públicas Gubernamentales, Direcciones Generales de la Secretaría de Economía, de acuerdo al CCo, RPSC, RGPSC y a la Política de Certificación.

Cabe señalar que, la Política de Certificados, es un conjunto de reglas que indican la aplicabilidad de un certificado a una comunidad y clase de aplicaciones con requerimientos comunes de seguridad. Se entenderá por comunidad a los Prestadores de Servicios de Certificación, Instituciones Públicas Gubernamentales y áreas que integran a la Secretaría de Economía.

III. **Agentes Certificadores de la ACR-SE**

Encargados de emitir los certificados digitales a las entidades subordinadas de la ACR-SE.

IV. **Autoridad Registradora de la ACR-SE**

Será la encargada de la autenticación de documentos e identificación de los solicitantes y titulares del certificado digital de la Autoridad Certificadora, así como de completar el procedimiento definido para la emisión de los certificados.

2.5 Periodo de Validez de los Certificados Digitales para las AC

- El periodo de validez del Certificado Digital de la ACR-SE no será menor a 10 años a partir de su fecha de emisión.

- El periodo de validez de los Certificadores Digitales de las Autoridades Certificadoras Subordinadas no será menor a 10 años a partir de su fecha de emisión.

Cuando se haya superado cuatro quintas partes del tiempo de vida de la ACR-SE, se generará un nuevo certificado digital y en su caso una nueva identidad, a partir de ese momento las nuevas inscripciones se harán firmando certificados con esa nueva identidad, de este modo las Autoridades Certificadoras Subordinadas dispondrán de una quinta parte del tiempo para solicitar nuevos certificados a la nueva entidad.

2.6 Convenciones de nombres

Cada autoridad Certificadora deberá asegurar que su DN (Distinguished Names) sea único, en función de que será el DN que tendrán los certificados que emitan.

El country Name deberá ser “mx”.

2.7 Repositorio o base de datos

Cada AC deberá mantener un repositorio o base de datos con los certificados que emita, de manera que estén disponibles al público a través de un servicio de distribución de certificados.

Asimismo, la ACR-SE mantendrá constancia en las páginas Web habilitadas para tal fin, de los certificados emitidos o revocados por ésta.

2.8 Protocolos

Dentro del sistema de seguridad, para que cualquier usuario pueda confiar en otro usuario se deben establecer ciertos protocolos, los cuales nos sirven para especificar las reglas de comportamiento a seguir.

2.8.1 Protocolos arbitrados

En ellos una Autoridad Certificadora participa en las transacciones para asegurar que las partes actúan de acuerdo a los lineamientos señalados por el protocolo.

2.8.2 Protocolos notariales

En este caso además de garantizar la correcta operación, también permite juzgar si ambas partes actuaron por derecho de acuerdo a la evidencia presentada a través de los documentos aportados por los participantes e incluso dentro del protocolo notarial. En estos casos se añade la firma (digital) del notario a la transacción, pudiendo éste testificar posteriormente, en caso de disputa.

2.8.3 Protocolos Autoverificables

Cada una de las partes puede darse cuenta si la otra actúa deshonestamente durante el transcurso de la operación. La firma digital es un elemento básico de los protocolos autoverificables dado que no requiere de la intervención de una Autoridad Certificadora para determinar la validez de una firma.

2.9 Reforma al Código de Comercio en Materia de Firma Electrónica, publicada el día 29 de agosto de 2003 en el D.O.F.

Si bien es cierto, la legislación mexicana sobre Firmas Electrónicas y Prestadores de Servicios de Certificación se baso en la Ley Modelo de la UNCITRAL sobre Firmas Electrónicas, aprobada en Viena en julio del 2001, tomando en cuenta la experiencia de otras legislaciones (Derecho Internacional) y adecuándolas con las necesidades de México[57].

Es así que, el decreto de reformas al Código de Comercio en materia de Firma Electrónica fue aprobado el 26 de noviembre del 2002 en la Cámara de Diputados por 422 votos a favor y 1 abstención; y fue aprobado por el Senado de la República el 8 de abril del 2003 por unanimidad (85 votos a favor), entrando en vigor 90 días después de su publicación en el DOF (29 de agosto del 2003).

Como habíamos señalado, se adopta básicamente la Ley Modelo sobre firmas Electrónicas de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) y se introduce en la legislación mexicana el concepto de Firma Electrónica Fiable o Avanzada y complementa la parte relativa al Mensaje de Datos, detallando conceptos como: intermediario, acuse de recibo, original, etc.

Al respecto, cabe señalar que, fue adicionado el articulo 89 en donde se define la figura del Prestador de Servicios de Certificación, quien como Tercero confiable (Third Trusted Party) estará investido de la facultad de validar, por su probidad y su tecnología (no estará investido de Fe Pública), el proceso de emisión, identificación y atribución de firmas electrónicas. Asimismo se adicionó al Título Segundo el Capítulo III denominado “De los Prestadores de Servicios de Certificación” señalando los lineamientos que los Notarios, Corredores Públicos, Empresas Privadas o Instituciones Públicas, art. 100 CCo., deberán observar para obtener la acreditación como Entidad Certificadora, dado que sin este trámite no se daría seguridad jurídica a las transacciones comerciales electrónicas, y mediante la revisión que la Secretaría de Economía realiza se verifica que los PSC cuenten con los elementos necesarios para proporcionar un servicio que cumpla con parámetros internacionales, garantizando así al usuario el reconocimiento de su certificado electrónico en territorio nacional y en el extranjero, a fin de que puedan producir efectos jurídicos.

[57] Reyes Krafft, Alfredo Alejandro, “La firma electrónica y las entidades de certificación, Porrúa, México 2003, pág. 80.

2.10 Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación, publicado el 19 de julio del 2004 en el DOF

Con fecha del 19 de julio del 2004 fue publicado en el DOF el Reglamento del Código de Comercio en materia de Prestadores de Servicios de Certificación con el objeto de establecer las normas reglamentarias a las que deben sujetarse las Entidades Certificadoras en materia de firma electrónica y expedición de Certificados para actos de Comercio.

Es de importancia resaltar que, en éste ordenamiento se deja ver la intensión del legislador por hacer hincapié en que se atenderá a los principios de Neutralidad Tecnológica y Compatibilidad Internacional, términos que sin lugar a duda permitirán que México cuente con una Legislación compatible en el ámbito Internacional, de manera que distintos métodos o sistemas para la creación de una firma electrónica podrán ser utilizados.

Por otra parte, es en este Reglamento donde se detalla de manera clara el proceso de acreditación de una Entidad para fungir como PSC, siendo necesario para ello cubrir con los elementos humanos, materiales, económicos y tecnológicos, los cuales serán estrictamente auditados por la Secretaría de Economía a través de la Dirección General de Normatividad Mercantil y que dicho sea de paso, se evaluará atendiendo a lo dispuesto por las Reglas generales a las que deberán sujetarse los Prestadores de Servicios de Certificación.

Es así que aspectos como las medidas a tomar previo inicio de operaciones de un PSC, elementos que deben contemplarse en un certificado digital, así como las infracciones y sanciones en que pueda incurrir un PSC son incluidos en este ordenamiento, y que serán desarrollados a lo largo del presente trabajo.

2.11 Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación, publicadas el 10 de agosto del 2004 en el DOF

En el Decreto con el que se reforman y adicionan diversas disposiciones del Código de Comercio en materia de firma electrónica, publicado en el DOF el 29 de agosto de 2003, en el capítulo III que se adicionó, denominado “De los Prestadores de Servicios de Certificación”, se determina que la Secretaría de Economía coordinará y actuará como Autoridad Certificadora y Registradora respecto de los PSC a los que se refiere dicho capítulo, en donde además se señala que la Secretaría de Economía tiene que determinar algunos de los requisitos y obligaciones señalados en el CCo.

Asimismo, con el objeto de determinar la forma de dar cumplimiento a los elementos humanos, materiales y tecnológicos, la Secretaría de Economía ha expedido las citadas Reglas,

esto con fundamento en el Reglamento del Código de Comercio en materia de PSC, artículo 50, en el cual se menciona que dichos elementos deberán ajustarse a las especificaciones que determine la SE en las Reglas Generales a las que deberán sujetarse los PSC, a efecto de que las prácticas y políticas que se apliquen garanticen la continuidad del servicio, la seguridad de la información y su confidencialidad.

Dentro de los elementos descritos en las Reglas encontramos los siguientes:

I. Humanos; consistentes un en profesionista jurídico, un profesionista informático y cinco auxiliares de apoyo informático.
II. Materiales; comprende un 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.
III. Económicos; será el capital que comprenda al menos el equivalente de 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 de Economía con base en el análisis de las operaciones comerciales y mercantiles en que sean utilizados los certificados y que no será menor al equivalente a treinta veces el salario mínimo general diario vigente en el Distrito Federal, correspondiente a un año
IV. Tecnológicos, consistentes en los documentos donde se compruebe los siguiente:
    a. Análisis y evaluación de riesgos y amenazas,
    b. Infraestructura informática,
    c. Equipo de cómputo y software,
    d. Política de seguridad de la información,
    e. Plan de continuidad del negocio y recuperación ante desastres,
    f. Plan de seguridad de sistemas de la información,
    g. Estructura de certificados,
    h. Estructura de la lista de certificados revocados,
    i. Sitio electrónico,
    j. Procedimientos que informen de las características de los procesos de creación y verificación de Firma Electrónica Avanzada,
    k. Política de certificados,
    l. Declaración de prácticas de certificados,
    m. Modelos de las autoridades certificadora y registradora,
    n. Plan de administración de claves.

2.12 Solicitud de Acreditación para fungir como Prestador de Servicios de Certificación

En principio señalaremos los fundamentos legales que dan origen al trámite de acreditación, los cuales a saber, son los siguientes:

- Artículos 100 y 102, inciso A) del Código de Comercio (reforma publicada en el DOF el 29 de agosto del 2003).
- Artículo 5 del Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación.
- Numerales 1 al 10 de las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación.
- Numerales 3.31 y 5.1 de la Norma Oficial Mexicana NOM-151-SCFI-2002, Prácticas Comerciales-Requisitos que deben observarse para la conservación de mensajes de datos.
- Acuerdo por el que se delegan facultades a la Dirección General de Normatividad Mercantil en Materia de Evaluación de la conformidad de la Norma Oficial Mexicana NOM-151-SCFI-2002, Prácticas Comerciales-Requisitos que deben observarse para la conservación de mensajes de datos, y otros servicios de firma electrónica, competencia de la Secretaría de Economía. (publicado en el DOF el 10 de noviembre del 2005).

El trámite de solicitud para fungir como PSC se inicia mediante la presentación de un escrito en formato libre, haciendo referencia a los siguientes datos:

1) Lugar y fecha de emisión del escrito.
2) Órgano administrativo al que se dirige (Dirección General de Normatividad Mercantil).
3) Nombre del solicitante.
4) Si lo designa, nombre de su representante legal.
5) Domicilio para recibir notificaciones, teléfono y correo electrónico, así como nombre de la persona o personas autorizadas para recibirlas.
6) Petición expresa de solicitar la revisión y evaluación de la información y documentación presentada a fin de que la Secretaría determine si cumple los requisitos para ser acreditado como Prestador de Servicios de Certificación, y listar la documentación que se adjunta a dicha solicitud, así como la indicación de que presenta disco compacto.
7) Solicitud de examen del profesional jurídico encargado de la identificación de los solicitantes de certificados digitales.
8) 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 en la solicitud su conformidad de asumir los costos que impliquen a la Secretaría el traslados de su personal para efectuar sus auditorias.

9) Firma del solicitante.

A dicha solicitud deberá anexarse la siguiente documentación:

- Tratándose de un Notario Público, se adjuntará la Patente o Fiat, y el Corredor Público su Título de habilitación;
- Si se trata de Personas Morales se exhibirá copia certificada de su acta constitutiva, póliza u otro instrumento público, que acredite su constitución de acuerdo a las leyes mexicanas y que su objeto social sea el establecido en el artículo 101 del Código de Comercio.

> **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.

- Asimismo por el tramite y estudio de la solicitud para la acreditación como PSC se exhibirá un pago de derechos por un monto de $32, 829.00.[58]
- 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 manifiesta 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 cargo en el servicio público, en el sistema financiero o para ejercer el comercio.
- Exhibir la póliza de seguro de responsabilidad civil equivalente a treinta veces el salario mínimo general vigente en el Distrito Federal correspondiente a un año y la póliza de seguro contendrá una cláusula que asegure que ésta no será cancelable conforme a los artículos 150 y 150 bis de la Ley sobre el contrato de seguro.

> **Ley sobre el contrato del seguro. Artículo 150.-** El aviso sobre la realización del hecho que importe responsabilidad deberá darse tan pronto como se exija la indemnización al asegurado. En caso de juicio civil o penal,

[58] Monto consultado en la página de la COFEMER, para el trámite de solicitud para fungir como PSC. http://www.cofemer.gob.mx, agosto de 2007.

el asegurado proporcionará a la empresa aseguradora todos los datos y pruebas necesarios para la defensa.

Artículo 150 Bis.- Los seguros de responsabilidad que por disposición legal tengan el carácter de obligatorios, no podrán cesar en sus efectos, rescindirse, ni darse por terminados con anterioridad a la fecha de terminación de su vigencia.

Cabe señalar que aunque en las Reglas no se contempla que se deba incluir la cláusula en que se señale que la póliza no será cancelable, si lo hace la COFEMER en su sitio web en la sección de criterios de resolución del trámite.

- Procedimiento para selección, reclutamiento, evaluación y contratación de personal el cual deberá describir la forma de corroborar los antecedentes del personal antes de contratarlo.
- Escrito de conformidad para ser sujeto de auditoría por parte de la Secretaría de Economía en todo momento durante el proceso de estudio de la solicitud de acreditación como prestador de servicios de acreditación, incluso después de obtenido el dictamen favorable y posteriormente a su acreditación durante la vigencia de la misma. En el escrito deben aceptar que la Secretaría de Economía podrá auxiliarse de algún tercero en el proceso de auditoria al que le darán las mismas facilidades.

Una vez llevada a cabo la revisión de los documentos exhibidos, realizada la auditoria de las instalaciones así como la evaluación de los profesionistas, por parte de la Autoridad, ésta deberá dar respuesta respecto de la petición hecha por el solicitante, para ser acreditado conforme al artículo 100 del CCo. dentro de los 45 días siguientes a la presentación de la solicitud, de lo contrario se tendrá por concedida la acreditación, para ello la Autoridad contará con un plazo máximo de 20 días hábiles para requerirle al particular la información faltante.

Posteriormente, tras haber sido otorgada la acreditación del PSC, éste deberá, en los próximos 10 días a la notificación de la procedencia de la acreditación, exhibir una fianza por un monto mínimo equivalente a cinco mil veces el salario mínimo general vigente en el Distrito Federal, monto que deberá incrementarse por cada persona física o moral adicional que contemple para prestar el servicio de certificación en nombre y por cuenta del solicitante, hecho lo anterior la Autoridad procederá a expedir el certificado respectivo al interesado y lo registrará a efecto de que éste pueda iniciar operaciones, pues la Secretaría de Economía como Autoridad Certificadora y Registradora deberá comprobar la identidad del Prestador de Servicios de Certificación o su representante, para que pueda crear sus datos de identificación de Firma Electrónica.

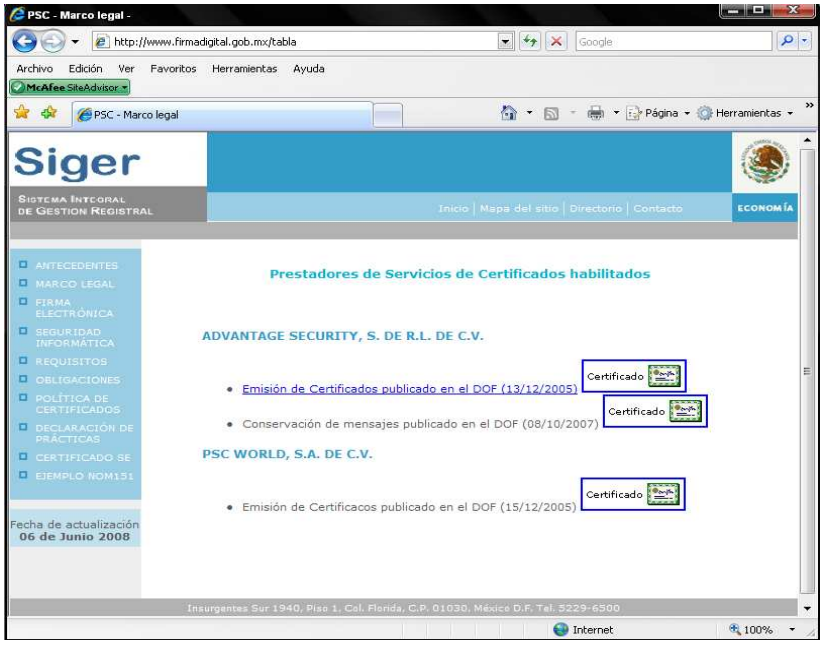
Actualmente en México se cuenta con dos Prestadores de Servicios de Certificación (Advantage Security, S.de R.L. de C.V. y PSCWorld, S.A. de C.V.), los cuales fueron autorizados los días 13 y 15 de diciembre del 2005, respectivamente.

2.13 Prestación de otros servicios de Firma Electrónica

2.13.1 Acuerdo por el que se reforman las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación, publicado el 5 de marzo de 2007 en el D.O.F.

Con la publicación de este acuerdo se pretende dar atención a la exigencia del mercado respecto de la demanda de servicios relacionados con firmas electrónicas. Además de la emisión de certificados electrónicos, se tiene como objetivo regular la conservación de mensajes de datos, la expedición de sellos digitales de tiempo y la validación de certificados. Para ello la Secretaría de Economía modificó las reglas mencionadas, a fin de otorgar mejor certeza jurídica en las acciones de los PSC.

Sin embargo, pese a lo que se pensaba en cuanto a que una vez que una entidad haya obtenido su acreditación para fungir como PSC al mismo tiempo obtendría su acreditación para prestar el servicio de conservación de mensajes de datos y emitir sellos digitales de tiempo, la Dirección General de Normatividad Mercantil ha sostenido el criterio de que ello no es así, pues con la publicación del referido Acuerdo que modifica a las Reglas, se dispone que para ello se tendrá que presentar una solicitud de acreditación para tales efectos[59], con lo cual se estarían creando otras figuras como lo son: PSC para efectos de la NOM-151 y PSC de sellado digital de tiempo.



[59] De conformidad con lo dispuesto por la **Regla 2.bis.** del Acuerdo que modifican a las Reglas generales a las que deberán sujetarse los Prestadores de Servicios de Certificación, la cual señala que "en caso de que el Solicitante de Acreditación refiera en su solicitud, además de la emisión de Certificados, la prestación de otros servicios de firma electrónica, como son la conservación de mensajes de datos, el sellado digital de tiempo y la validación de certificados, conforme lo prevé el artículo 29 del Código de Comercio, se aplicará lo siguiente…"

De manera que, con este Acuerdo se determinan los elementos con los que una entidad debe contar para prestar otros servicios de firma electrónica, trámite que sin lugar a duda es igual de riguroso como el que representa solicitar la acreditación de un PSC para emitir certificados de firma electrónica.

2.13.2 Norma Oficial Mexicana NOM–151–SCFI – 2002 Prácticas comerciales-requisitos que deben observarse para la conservación de mensajes de datos, publicada el 4 de junio de 2002

De acuerdo a lo dispuesto por los artículos 40 de la Ley Federal sobre Metrología y Normalización, así como por el artículo 49 del CCo., la Secretaría de Economía emitirá una Norma Oficial Mexicana que permita dar cumplimiento a la obligación por parte de los comerciantes que utilicen mensajes de datos, para realizar actos de comercio, de conservar por el plazo mínimo de 10 años el contenido de los mensajes de datos en que se hayan consignado contratos, convenios o compromisos que den nacimiento a derechos y obligaciones, y cuyo contenido debe mantenerse integro e inalterado a partir del momento en que se generó por primera vez en su forma definitiva, debiendo ser accesible para su ulterior consulta.

Es así que, con fecha del 17 de agosto del 2001 se dieron por concluidos los trabajos correspondientes al proyecto de la Norma Oficial Mexicana, la **NOM–151–SCFI–2002 Prácticas Comerciales-Requisitos que deben observarse para la conservación de mensajes de datos**. Al respecto la Secretaría de Economía elaboró dicho proyecto de Norma Oficial Mexicana que *establece los requisitos que deben observarse para la conservación de mensajes de datos*, con fundamento en lo dispuesto por el, ya referido, artículo 49 segundo párrafo del CCo.

El viernes 28 de septiembre del 2001, se llevó acabo la reunión 03/2001 del Comité Consultivo Nacional de Normalización de Seguridad al usuario, información comercial y prácticas de comercio, en dicha reunión se aprobó, entre otras cuestiones, la publicación íntegra del Proy-NOM en el DOF.

La publicación se efectuó el día 17 de noviembre del 2001 en el DOF, dicho documento se expidió para consulta pública a efecto de que dentro de los siguientes 60 días naturales, los interesados presentaran sus cometarios ante el Comité Consultivo Nacional de Normalización de Seguridad al usuario, información comercial y prácticas de comercio, para que en los términos de la Ley Federal sobre Metrología y Normalización se consideren en el ceno del comité que lo propuso.

De acuerdo al procedimiento por la Secretaría, los textos una vez aceptados por los grupos de trabajo no podrían sufrir ninguna modificación de ninguna especie. Es así que se solicitó a la Secretaría de Economía, con el objeto de mantener el principio de legalidad en el proceso de elaboración, consulta y publicación de la NOM de referencia, que se establezca un plazo de vigencia. El lunes 18 de marzo se reunió el comité de la NOM para revisar los comentarios y sugerencias presentadas en el periodo de consulta pública. El martes 19 de marzo del 2002 se firmó el texto final de la NOM, el cual fue publicado en el DOF el día 4 de junio del 2002.

Sin embargo, no fue sino hasta el 17 de febrero de 2006 cuando al contar la Secretaría de Economía con la infraestructura necesaria para regular los requisitos que deben observarse para la conservación de los mensajes de datos, entró en vigor la NOM-151-CSFI-2002, con lo cual la Autoridad (Secretaría de Economía a través de la Dirección de Normatividad Mercantil) puede llevar a cabo la evaluación de conformidad para la conservación de mensajes de datos.

Asimismo, el 10 de noviembre del 2006 se publicó en el DOF el acuerdo por el que se delegan facultades a la Dirección General de Normatividad Mercantil en materia de evaluación de la conformidad de la Norma Oficial Mexicana NOM-151-CSFI-2002. Prácticas comerciales – Requisitos que deben observarse para la conservación de mensajes de datos, y otros servicios de firma electrónica, competencia de la Secretaría de Economía, quien entre otras facultades puede recibir, analizar, autorizar y dar respuesta a las solicitudes de evaluación de la conformidad de la NOM-151, incluida la de los programas informáticos para la prestación de los servicios regulados por la misma, sin perjuicio de que estas actividades sean llevadas a cabo por las personas acreditadas de conformidad con la Ley Federal sobre Metrología y Normalización.

Al respecto, el 08 de octubre del 2007 la Secretaría de Economía, por conducto de la Dirección General de Normatividad Mercantil, acreditó a un PSC para prestar el servicio de Conservación de Mensajes de Datos.

Como mencionamos al inicio de este apartado, el objeto de la NOM-151-CSFI-2002 es establecer los requisitos que los comerciantes deben observar para la conservación de los mensajes de datos que consignen datos, convenios o compromisos y que en consecuencia originen el surgimiento de derechos y obligaciones.

Asimismo, se menciona que cuando se pretenda conservar en un medio electrónico, óptico o de cualquier otra tecnología, información derivada de un acto de comercio, que se encuentre en un soporte físico, similar o distinto a aquellos, los comerciantes podrán optar por migrar dicha información a una forma digital y, observar para su conservación, las disposiciones a que se refiere la citada NOM-151-CSFI-2002, lo cual permitirá que la información que dio origen a los actos

jurídicos pueda ser de fácil acceso, además de que representará un ahorro tanto de tiempo, espacio y dinero, al no tener que imprimirlos, destinar espacios para su resguardo y su búsqueda sería más sencilla y organizada.

Por otro lado, la migración de la información deberá ser cotejada por un tercero legalmente autorizado, quien constará que dicha migración se realice íntegra e inalterablemente tal y como se generó por primera vez en su forma definitiva. Es así que, el tercero legalmente autorizado deberá ser una persona física o moral que cuente con la capacidad tecnológica suficiente y cumpla con los requisitos legales aplicables. Cabe señalar que, a la fecha la Dirección General de Normatividad Mercantil no ha determinado si el propio PSC puede fungir como "tercero autorizado", si se requerirá de la intervención de un Notario para la migración de datos o que características deberá tener dicha figura, de tal manera que será necesario conservar el original del documento con soporte en papel para su cotejo con el documento electrónico, lo anterior en tanto se dictan las disposiciones correspondientes ya sea en la NOM-151-CSFI-2002 u otro ordenamiento.

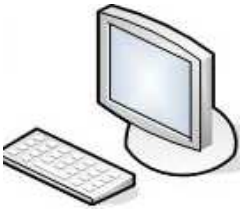
En dicho instrumento se enlista una serie de definiciones necesaria para el mejor entendimiento del lenguaje técnico, tales como: criptografía, firma digital, firma electrónica, mensaje de datos, y Prestador de Servicios de Certificación, mismos que ya hemos detallado a lo largo del presente trabajo.

De la misma forma, también se señalan tres elementos que necesariamente intervendrán en la conservación de los mensajes de datos, los cuales a saber, son los siguientes:

1. Para la emisión de la Firma electrónica y/o digital, así como el Prestador de Servicios de Certificación, deberán observar los requisitos que la normatividad aplicable señale para su operación (Código de Comercio, Reglamento al 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).
2. La constancia emitida por el Prestador de Servicios de Certificación deberá observar los términos establecidos en el Apéndice de la NOM-151.
3. Los programas informáticos en y con los que se almacenan los mensajes de datos.

Generación de constancias Norma Oficial Mexicana NOM–151–SCFI–2002

Documentos



Software

1.-FORMACION DE ARCHIVOS PARCIALES

Para formar un *archivo parcial* se crea un mensaje en formato ASN.1 que contiene:

1. El nombre del archivo del sistema de información en el que está o estuvo almacenado el contenido del archivo.
2. El tipo del archivo.
3. El contenido del mismo.

Archivos parciales ASN1

2.- OBTENCION DE LOS COMPENDIOS O RESUMENES DIGITALES

Se calcula el compendio o resumen digital del *archivo o archivos parciales* resultado del proceso anterior, usando el algoritmo MD5.

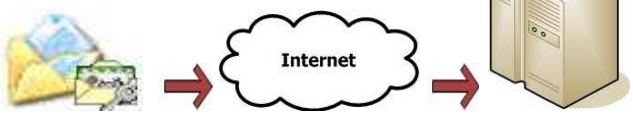
Compendios (Resumen)

3.- INTEGRACION DEL EXPEDIENTE ELECTRONICO

Para conformar un *expediente electrónico* se creará un mensaje ASN.1 que contiene:

1. El nombre del *expediente*.
2. Un índice, que contiene el nombre y el compendio de cada *archivo parcial* que integra el *expediente.*
3. *L*a identificación del operador del sistema de conservación, y
4. Su firma digital.

Expediente firmado por el Usuario



Prestador de Servicios de Certificación

4.- OBTENCION DE LA CONSTANCIA DEL PRESTADOR DE SERVICIOS DE CERTIFICACION

Para la obtención de la *constancia* el sistema de conservación deberá usar el protocolo de aplicación descrito en este apéndice para enviar el *expediente* al prestador de servicios de certificación, quien emitirá una *constancia* en formato ASN.1 y la regresará al sistema de conservación, haciendo uso del mismo protocolo.

El expediente opcionalmente podrá enviarse como un anexo de correo electrónico, siendo aplicables en este caso los protocolos Internet correspondientes.

También podrá usarse la transmisión vía Web siempre que el expediente se reciba como un archivo y siempre que se utilice un directorio protegido por nombre de usuario y contraseña. Para ello, la forma en que lo envíe deberá ser como la siguiente:

```
<form action="url del programa generador de constancias " method="post"
  enctype="multipart/form-data">
    Expediente: <input type="file" name="expediente">
    <input type="submit" value="Obtener Constancia">
</form>
```

La constancia deberá regresar al cliente como un archivo de tipo mime application/octet-stream.

Los MIME Types (Multipupose Internet Mail Extensions) son la manera estándar de mandar contenido a través de la red. Los tipos MIME especifican tipos de datos, como por ejemplo texto, imagen, audio, etc.

El prestador de servicios de certificación podrá recibir, si así lo acuerda con sus clientes, medios físicos conteniendo los archivos correspondientes a los expedientes.

FORMACION DE LA CONSTANCIA

El prestador de servicios de certificación formará una *constancia* en formato ASN.1 (versión 1 de Abstracts Sintax Notation “Notación Abstracta de Sintaxis”) que contendrá:

1. El nombre del archivo en donde está almacenada la *constancia*.
2. El *expediente* enviado por el sistema de conservación.
3. Fecha y hora del momento en que se crea la *constancia*.
4. La identificación del prestador de servicios de certificación y
5. Su firma digital.

Método de verificación de autenticidad

La verificación de la autenticidad de una constancia se realizará por medio del uso de un sistema de verificación que lleve a cabo los pasos siguientes:

1. Verificar la firma digital del prestador de servicios de certificación en la constancia;
2. Verificar la firma digital del operador del sistema de conservación en el expediente contenido en la constancia, y
3. Recalcular el compendio de él o los archivos parciales y verificar que coincidan con los compendios asentados en el expediente.

Es así que, la obligación del comerciante a conservar, por un plazo mínimo de diez años, los originales de aquellos documentos que consignen derechos y obligaciones, podrá ser cumplida no sólo a través del uso de medios tradicionales, es decir, el papel, sino también mediante el uso de mensajes de datos, esto en la medida en que se observe lo dispuesto por la NOM–151–SCFI–2002, pues es en éste ordenamiento donde se precisan los lineamientos que deben seguirse para la conservación de los mensajes de datos.

2.13.2.1 Principales usos de la Norma Oficial Mexicana NOM–151–SCFI–2002

Como ya hemos visto, la NOM–151–SCFI–2002 se refiere a la conservación de mensajes de datos electrónicos que al ser implementada, ofrece múltiples beneficios que pueden segmentarse en tres grandes áreas de oportunidad:

- Beneficios económicos debido al ahorro en costos de operación, disminución de grandes cantidades del uso de papel y otros consumibles, así como la reducción de costos por almacenaje (archivo muerto).
- Beneficios administrativos en cuanto a la aceleración de procesos y tiempos de respuesta, reducción de tiempos en cadenas de logística y carga administrativa; y por último.

- Seguridad al proveer certeza sobre la seguridad física (digital) y legal del documento, otorgando así tranquilidad jurídica al interior como al exterior de la empresa, a departamentos como informática, auditoría o dirección general y a notarios, abogados o administradores de compañías, respectivamente.

Un ejemplo en el que se abarcan las tres áreas, es en el sector financiero, donde se agiliza el enorme volumen de transacciones y se pueden almacenar los documentos de manera electrónica, ahorrando costos. Además se conserva la seguridad jurídica e integridad de la información tal y como lo exige la NOM–151–SCFI–2002.

La certificación de la NOM–151–SCFI–2002 permite el ahorro de dinero y tiempo para procesar y ubicar documentos, aunado a que representa una oportunidad más para que las organizaciones públicas y privadas que tienen dentro de su actividad institucional auditorias y controles financieros y legales, internos o externos, puedan mantenerse a la cabeza de procesos de calidad que las harán ser más rentables y competitivas, al interior y al exterior. Además, en conjunto con el uso de la firma electrónica, se puede cumplir con controles financieros y legales, ya que con esto se garantiza la integridad, privacidad y no repudio de la información.

En un mundo donde las empresas cada vez están más enfocadas en lograr procesos eficientes, de bajos costos, rápidos y con validez jurídica, la aplicación de la NOM–151–SCFI–2002 por las empresas tanto grandes como pequeñas, hará que estas sean cada vez más competitivas. De hecho, la certificación juega un importante papel en las acciones que México realiza en materia de impulso al comercio electrónico como viene contemplado en el Plan Nacional de Desarrollo.

CAPÍTULO TERCERO

3. Certificado electrónico

3.1 Certificación

La certificación es el procedimiento mediante el cual una tercera parte diferente e independiente de las partes a obligarse, asegura por escrito que un producto, proceso o un servicio, cumple con los requisitos especificados, convirtiéndose en la actividad más valiosa en las transacciones comerciales nacionales e internacionales, siendo así un elemento insustituible, para generar confianza en cualquier relación jurídica.

Cabe señalar que, un sistema de certificación es aquel que tiene sus propias reglas, procedimientos y formas de administración para llevar a cabo una certificación de conformidad. Dicho sistema, debe ser objetivo, fiable, aceptado por todas las partes interesadas, eficaz, operativo, y estar administrado de manera imparcial y honesta. Su objetivo primario y esencial es proporcionar los criterios que aseguren a las partes que el producto y/o servicio a adquirir satisface los requisitos pactados.

Todo sistema de certificación debe contar con los siguientes elementos.

- Existencia de Normas y/o Reglamentos.
- Existencia de Laboratorios Acreditados.
- Existencia de un Organismo de Certificación Acreditado.

3.1.1 Beneficios de la Certificación

A nivel nacional

- Ayuda a mejorar el sistema de calidad industrial.
- Protege y apoya el consumo de los productos nacionales.
- Prestigio internacional de los productos nacionales certificados.
- Da transparencia al mercado.

A nivel internacional

- Ayuda los intercambios comerciales por la confianza y la simplificación.
- Protege las exportaciones contra las barreras técnicas.
- Protege la calidad del consumo.

Para los gobiernos

- La certificación asegura que los bienes o servicios cumplen con los requisitos obligatorios relacionados con la salud, la seguridad, el medio ambiente, etc.
- Sirve como medio de control en importaciones y exportaciones.
- Es una herramienta importante en la evaluación de proveedores, en procesos contractuales y para verificar que el bien adjudicado en un proceso contractual sea entregado cumpliendo con los requisitos establecidos en los pliegos de condiciones.

Para la industria

- La certificación permite demostrar el cumplimiento de los requisitos técnicos establecidos en los acuerdos contractuales o que forman parte de las obligaciones legales.

Para el consumidor

- La certificación asegura la adquisición de productos o servicios de buena calidad.
- El consumidor puede acceder a medios donde puede presentar sus reclamos o sugerencias frente a los productos certificados.

Asimismo, el artículo 3 de la Ley Federal sobre Metrología y Normalización, define a la certificación como “el procedimiento por medio del cual se asegura que un producto, proceso, sistema o servicio se ajusta a las normas o lineamientos o recomendaciones de organismos dedicados a la normalización nacionales o internacionales”.

Otro concepto lo podemos tomar del artículo 155 de la Ley del Notariado para el Distrito Federal, al cual señala que “la certificación notarial es la relación que hace el Notario de un acto o hecho que obra en su protocolo, en un documento que él mismo expide o en un documento preexistente, así como la afirmación de que una trascripción o reproducción coincide fielmente con su original…”.

3.1.2 Características de la certificación

Dentro de la certificación se contemplan dos características básicas, las cuales son:

1. Temporal; Se refiere a que el certificado tiene determinado tiempo de vigencia dependiendo de la empresa, producto, proceso servicio o persona y del tercero certificador.

2. Voluntario; se refiere a que en ningún caso existirá una regla u ordenamiento que de manera coercitiva imponga a las partes la obligación de seguir determinados lineamientos;

cabe señalar que, la certificación es sólo solicitada por la parte interesada o por razones de seguridad interna o externa o bien por cumplir con los lineamientos consensuales que el mercado solicita.

3.2 Fe Pública

La fe pública es la garantía que el Estado da en el sentido de que los hechos que interesan al derecho son verdaderos y auténticos, lo anterior porque en la realidad social existen una serie de hechos y actos con relevancia jurídica que, si bien, no todos los ciudadanos pueden presenciar, deben ser creídos y aceptados como verdad oficial.

Por lo que, la fe pública supone exactitud y que lo narrado por el fedatario resulte fiel al hecho por él presenciado y también supone integridad, es decir, que lo narrado bajo la fe pública se ubique en un tiempo y lugar determinado y se preserve en el tiempo sin alteración en su contenido.

En la doctrina podemos encontrar que la fe pública es definida como "la creencia legalmente impuesta y referida a la autoría de ciertos objetos (documentos, monedas, sellos, etc.), o a determinados actos públicos (sentencias, actos administrativos, autorizaciones judiciales), o sobre el hecho de haber ocurrido un comportamiento a acontecer[60], o también como "el imperativo jurídico o coacción que nos obliga a tener por válidos determinados hechos o acontecimientos sin que podamos decidir originalmente sobre su verdad objetiva"[61], tal como lo señala Enrique Giménez Arnau.

Asimismo, de acuerdo a la Ley de la Comisión Estatal de derechos humanos de Jalisco, en su artículo 44, señala que: "se entenderá por fe publica, la facultad de autenticar documentos preexistentes o declaraciones y hechos que tengan lugar o estén aconteciendo en presencia de dichos servidores públicos, sin perjuicio del valor probatorio que se les atribuya, en los términos de este ordenamiento y otras leyes aplicables. Las declaraciones y hechos a que se refiere el párrafo anterior, se harán constar en el acta circunstanciada que al efecto levantará el servidor público correspondiente".

Por otra parte, a la fe pública también se le considera como el imperativo jurídico que impone el Estado a un pasivo contingente universal para considerar cierta y verdadera la

[60] Zinny, Mario Antonio, "El acto notarial (dación de fe)", Ed. Desalma, Buenos Aires, 1990, pp.9, citado por Jorge Ríos Hellig, en "La práctica del Derecho Notarial", 3ª Edición, Ed. Porrúa, México 1998, Pág. 44.
[61] Giménez Arnau, Enrique, "Derecho Notarial", Ediciones Universidad de Navarra EUNSA, pamplona, 1976, 882 págs.

celebración de un acto o el acaecer de un evento que no percibe este contingente por sus sentidos[62].

Abundado más en esta última definición, tenemos que:

1. Imperativo jurídico; se refiere a que es forzoso tener por cierto lo que se contiene en cualquier instrumento emanado por el Estado a través de un fedatario o una Autoridad (documento autentico).
2. Pasivo contingente; se refiere al efecto *erga omnes*, o sea, el carácter de oponible frente a cualquier persona del contenido de un documento autentico.
3. Considerar cierto un acto o hecho; es decir, ya que el notario confecciona el acto, elabora el acuerdo de voluntades y certifica hechos que acaecieron de la manera en que él percibió, el contendido de los documentos se debe tener por cierto y verdadero.
4. Que no percibe por sus sentidos; esto obliga a que el Estado ordene mecanismos en donde se crea en algo que no se ha captado o percibido personalmente.

Todo lo anterior es válido, hasta que no se pruebe su nulidad o falsedad (presunción *juris tantum*) conforme al artículo 156 de la Ley del Notariado para el Distrito Federal (LNDF), que señala:

> **"Artículo 156**.- En tanto no se declare judicialmente la falsedad o nulidad de un instrumento, registro, testimonio o certificación notarial, éstos serán prueba plena de que los otorgantes manifestaron su voluntad de celebrar el acto consignado en el instrumento de que se trate, que hicieron las declaraciones que se narran como suyas, así como de la verdad y realidad de los hechos de los que el Notario dio fe tal como los refirió y de que observó las formalidades correspondientes".

En relación con la validez que un instrumento notarial debe conservar pese a contener un acto declarado judicialmente como nulo, el artículo 162 de la LNDF dispone:

> **Artículo 162**.- El instrumento o registro notarial sólo será nulo:
> I. Si el Notario no tiene expedito el ejercicio de sus funciones en el momento de su actuación;
> II. Si no le está permitido por la Ley intervenir en el acto;

[62] Ríos Hellig, Jorge, "La práctica del Derecho Notarial", 3ª Edición, Ed. Porrúa, México 1998, Pág. 44.

III. Si no le está permitido dar fe del acto o hecho materia de la escritura o del acta por haberlo hecho en contravención de los términos de la fracción II del artículo 45;

III. Si fuere firmado por las partes o autorizado por el Notario fuera del Distrito Federal;

IV. Si ha sido redactado en idioma distinto al español;

V Si no está firmado por todos los que deben firmarlo según esta Ley, o no contiene la mención exigida a falta de firma;

VI. Si está autorizado con la firma y sello del Notario cuando debiera tener nota de "no pasó", o cuando el instrumento no esté autorizado con la firma y sello del Notario.

VII. Si el Notario no se aseguré de la identidad de los otorgantes en términos de esta Ley.

En el caso de la fracción II de este artículo, solamente será nulo el instrumento en lo referente al acto o hecho relativos, pero será válido respecto de los otros actos o hechos que contenga y que no estén en el mismo caso. Fuera de los casos determinados en este artículo, el instrumento o asiento será válido. Cuando se demande la nulidad de un acto jurídico no podrá demandarse al Notario la nulidad de la escritura que lo contiene, si no existe alguno de los supuestos a que se refieren las fracciones anteriores. Sin embargo, cuando se dicte la sentencia que declare la nulidad del acto, una vez firme, el juez enviará oficio al Notario o al Archivo según se trate, para que en nota complementaria se tome razón de ello.

Por otra parte, según el origen de la autoridad, la fe puede ser religiosa o humana. La religiosa es la que proviene de la autoridad de Dios que ha revelado algo a los hombres, y la humana proviene de afirmaciones hechas por el hombre.

Si la fe humana proviene de la autoridad privada, es decir, común, se llama fe privada; a esa clase pertenecen los documentos privados, o sea, firmados por particulares, y que no tienen nada de fe pública si no son reconocidos legalmente ante alguna autoridad. Si el documento, por el contrario proviene o es emitido por una autoridad pública estamos en presencia de un documento público y por lo tanto en un caso de documento que tiene aparejada la fe pública.

3.2.1 Requisitos de la Fe Pública

Ríos Hellig establece un criterio en relación a las circunstancias y características que la fe pública posee, las cuales a saber son las siguientes[63]:

3.2.1.1 Evidencia

Consistente en la relación que existe entre el autor del acto jurídico y el del instrumento notarial, es decir, es la relación entre el quién y el ante quién, el notario narra el hecho propio (certificación) y consta el hecho ajeno, en la certificación el notario concreta su actividad de fedatario, es decir, manifiesta el contenido de su fe pública *originaria*, que versa sobre: fe de la existencia de los documentos relacionados con la escritura, de conocimiento de las partes, de lectura, explicaciones y de otorgamiento de la voluntad.

Por otra parte, Luis Carral y de Teresa[64] distingue los siguientes puntos:

a) En la fase de evidencia, señala que hay aspectos que distinguir entre el autor, el documento y el destinatario. Si nos referimos al autor, se requiere:
    a. Autor
        i. Que sea persona pública
        ii. Que vea el hecho ajeno
        iii. Que narre el hecho propio

    Como se aprecia, no se precisa el acto de fe, sino de conocimiento directo. Se trata del autor, de quien dimana el acto de la fe para el destinatario. El autor jamás produce un acto de fe, pues para él el hecho o el acto es evidente. El acto de fe se requiere para todos los demás entre los que debe surtir efectos ese acto, o sea, para los destinatarios del documento.

b) El acto de evidencia puede producirse llanamente o bien revestido de solemnidad. En el primer caso el acto no tiene fe pública, y en el segundo sí, por haber sido producido dentro de un procedimiento fijado por la ley. Por eso el artículo 26 de la Ley del notariado señala que “la función autenticadora es la facultad otorgada por la Ley al Notario para que se reconozca como cierto lo que éste asiente en las actas o escrituras públicas que redacte, salvo prueba en contrario”. Esto es lo que se llama el “rigor formal” de la fe pública. La evidencia se produce dentro de la solemnidad, es decir, encerrada en un conjunto de garantías legales que aseguran la fiel percepción, expresión y conservación de los hechos históricos.

[63] Ríos Helling, Ob. Cit.
[64] Luis Carral y de Teresa, Ob. Cit.

3.2.1.2 Objetivación

Cosiste en que todo lo percibido debe plasmarse en un instrumento, es decir, todo lo que el notario percibe de manera sensorial o por el dicho de otros, debe constar por escrito dentro de un protocolo.

3.2.1.3 Coetaneidad o simultaneidad

Es la relación entre lo narrado o percibido, su plasmación en el instrumento notarial y su otorgamiento, es una relación temporal entre lo narrado por terceros, lo percibido por éstos o el notario, y su plasmación u otorgamiento en un instrumento notarial.

Luis Carral y de Teresa[65] señala que los requisitos de "evidencia", de "solemnidad" y de "objetivación", deben producirse al mismo tiempo (coetáneamente), esas tres fases, evidencia, ceremonia del acto solemne y su conversión en papel, debe producirse en un sólo acto, pero la coincidencia tiene que darse de acuerdo con ciertas normas de forma previstas por la ley y obligaciones para el fedatario que interviene. Como dichas normas de forma (que son de forma porque se dirigen al autor, fedatario del acto presente) no se concebirían si no se tratara de surtir en el futuro (o sea, las normas de forma se convierten en "normas de prueba"), resulta que aquellas (las normas de forma) son de garantía para el futuro valor probatorio del documento. Dicho en otras palabras, el valor probatorio se alcanza por las garantías de su forma, esto es, por las garantías que acompañan a las fases de evidencia, solemnidad, objetividad y coetaneidad.

3.2.2 Tipos de fe pública

3.2.2.1 Originaria

Este tipo de fe pública se presenta cuando el hecho o el acto del que se debe dar fe fue percibido por los sentidos del notario, la cual se presenta, por ejemplo, cuando el notario asienta una certificación de hechos en sus protocolo o cuando da fe del otorgamiento de un testamento.

3.2.2.2 Derivada

Consiste en dar fe de hechos o escritos de terceros, aquí el notario no ha percibido sensorialmente el acaecer del hecho o el otorgamiento del acto que plasmará en su protocolo. Por

[65] Ibidem.

ejemplo, cuando el notario protocoliza el acuerdo del consejo de administración de una sociedad anónima otorgándole poderes a un tercero.

3.3 Diferencia entre fe pública y certificación

La Fe pública contiene cinco características esenciales:

- Consta documentalmente.
- Proviene del Estado que faculta a un particular (Funcionario público, Notario, etc.)
- Es un imperativo jurídico.
- Es oponible a terceros.
- Será perpetuamente válido, aunque podrá atacarse su autenticidad.

En tanto que la certificación:

- Puede constar o no por escrito, al cual se le denominará certificado.
- Es otorgada por un tercero independiente, quién no estará investido de fe pública y cuya observancia, derivada de su certificación, radicará en el ser aceptada como tal por la confidencialidad, imparcialidad, veracidad y equidad demostrada como organismo certificador.
- En ningún momento conllevará un carácter imperativo; pues su observancia denota un carácter voluntario.
- Al no existir algún elemento coercitivo no podrá ser oponible ante terceros y en todo caso el aceptarlo como válido o no dependerá de las personas interesadas.
- Es de carácter temporal.

Por todo lo anterior, podemos decir a manera de conclusión que la fe pública tiene su origen en la necesidad del Estado de investir a determinadas personas de fe pública para así dar respuesta a la exigencia social de proveer de certeza jurídica a determinados actos. Por otro lado, la certificación es un procedimiento autorregulatorio que carece de un carácter coercitivo, dado que no emana de una entidad investida de fe pública, pero que debido a criterios éticos y consensuales empleados durante el proceso de certificación es considerado un mecanismo válido para dotar de certeza a diversos proceso donde la figura del fedatario no resulta estrictamente necesaria y que por lo tanto puede dejarse al árbitro de organismos de certificación.

3.4 Del Certificado Electrónico

Además del nivel de seguridad que nos ofrece la firma electrónica, existe además otro método con el que estamos seguros se dará una mayor confianza a dicho instrumento, esto

consiste en la certificación realizada por una Entidad certificadora, respecto del documento que haya sido suscrito electrónicamente.

Cabe señalar, que el presente tema es incluido dentro de esta investigación sólo con el ánimo de introducir al lector a una práctica que tiene por objeto dar al documento electrónico, firmado electrónicamente, una mayor fiabilidad y seguridad en su uso, es por ello que nos limitaremos a una mera descripción del tema, ya que tratarlo a fondo significaría realizar un ejercicio de investigación intenso, dado que se tendrían que cubrir distintos aspectos técnicos, lo cual nos alejaría de nuestro tema principal.

La firma manuscrita como tal, a veces necesita de documentación que refuerce la identidad del firmante, un ejemplo palpable de esto lo observamos en algunos trámites bancarios en los cuales además de la firma del signatario se le piden documentos como la credencial para votar o el pasaporte; por otra parte, tratándose de la firma electrónica sucede algo similar, dado que para cumplir con requisitos de tal índole se confeccionó un sistema de certificación como el que a continuación estudiaremos.

3.4.1 Definición de certificado electrónico

La certificación electrónica puede funcionar como el equivalente digital de una identificación, en lo que a la autenticación de personas se refiere, ya que permite que un individuo demuestre que es quien dice ser, es decir, que está en posesión de la clave secreta asociada a su certificado.

Un certificado electrónico o de clave pública, como también es conocido, es un punto de unión entre la clave pública de una entidad y uno o más atributos referidos a su identidad, es así que el certificado garantiza que la clave pública pertenece a la entidad identificada y que dicha entidad posee la correspondiente clave privada.

En la práctica encontramos que a los certificados electrónicos se les denomina comúnmente como: certificados digitales, certificados de clave pública, ID digital o simplemente certificado.

La particularidad de estos certificados es que son emitidos por una Entidad Certificadora para que éstos sean reconocidos jurídicamente, pues dichas Entidades han comprobado ante una Autoridad Certificadora de mayor jerarquía, llámese Secretaría de Economía (en el caso de México), que cuentan con los elementos humanos, materiales, tecnológicos y económicos suficientes para la prestación de los servicios relacionados a la firma electrónica.

Al respecto, Fernando Ramos nos comenta acerca del certificado, explicando que éste consiste en un registro electrónico encargado de testificar que una clave pública corresponde a cierto individuo o ente[66].

Eric Iriarte Ahon, en un plano más técnico, plantea como concepto del certificado el siguiente:

> "denominase certificado digital al documento electrónico generado por una Entidad de certificación, por medio de un sistema criptográfico que valida ciertos aspectos o datos generados electrónicamente".[67]

La Ley 59/2003 de España señala en su artículo 6, que el certificado electrónico "es un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad".

Por otra parte el CCo. en su artículo 89 define al certificado electrónico como "todo Mensaje de Datos u otro registro que confirme el vínculo entre un firmante y los datos de creación de firma electrónica".

En el instrumento denominado "Lineamientos para la homologación de la operación de la Firma Electrónica Avanzada en la Administración Pública Federal" (cuyo propósito principal es la homologación de la operación de la Firma Electrónica Avanzada, evitando la duplicidad o multiplicidad de certificados digitales de firma electrónica asociados a una misma persona y establecer el conocimiento de los mismos que hayan sido emitidos por cada una de las dependencias y entidades)., se manejan dos tipos de certificación, las cuales a saber son las siguientes:

- Certificación cruzada; consiste en el intercambio de certificados digitales de dos o más autoridades certificadoras de un mismo nivel jerárquico y con el fin de establecer el reconocimiento de los certificados digitales emitidos por las mismas.
- Certificación subordinada, consiste en el intercambio de certificados digitales de dos autoridades certificadoras con distinto nivel jerárquico, con el fin de establecer el reconocimiento de los certificados digitales emitidos por las mismas.

---

[66] Ramos Suárez, Fernando, "Cómo aplicar la nueva normativa sobre comercio electrónico", ubicado en: http://www.secretosenred.com/articles/740/1/COMO-APLICAR-LA-NUEVA-NORMATIVA-SOBRE-LA-FIRMA-ELECTRONICA--Primera-Parte/Pagina1.html

[67] Triarte Ahon, Eric, "Firma electrónica y certificado digital. El proyecto peruano", REDI Revista Electrónica de Derecho informático, Perú, ubicado en http://publicaciones.derecho.org/redi/No._14_-_Septiembre_de_1999/9

En consecuencia, con el uso del certificado digital se garantiza que la información intercambiada, a través de dos o más ordenadores, no ha sido robada, alterada, o leída por personas no autorizadas, además de que se podrá evitar que el titular de un certificado niegue haber escrito un mensaje de datos.

En conclusión diremos que un Certificado digital es el equivalente electrónico de un documento de identidad, el cual nos permite identificarnos, firmar y cifrar electrónicamente documentos y mensajes.

Entre sus principales usos, podemos señalar los siguientes:

- Autentificar la identidad del usuario, de forma electrónica, ante terceros.
- Trámites electrónicos ante Organismos Públicos.
- Trabajar con facturas electrónicas.
- Firmar digitalmente e-mails y todo tipo de documentos electrónicos.
- Cifrar datos para que sólo el destinatario del documento pueda acceder a su contenido.

3.4.2 Tipos de certificados electrónicos

Entre los más comunes podemos encontrar los siguientes[68]:

3.4.2.1 Certificado de Servidor:

El certificado tendrá como única finalidad asegurar la existencia y denominación de una entidad en Internet.

Características generales

- Requiere presencia física de la persona o un representante legal de la empresa para acreditar la personalidad de la representación.
- Validación de identidad del servicio con autoridades de registro de nombres de dominio.
- Se registra documentación y firma autógrafa.

Usos típicos

- Autenticación de servidor.
- Comercio electrónico.

[68] Información obtenida de la página web de PSCWorld, consultado en http://www.pscworld.com, 12 de julio de 2008.

3.4.2.2 Certificado de Representación

El certificado tendrá como única finalidad asegurar la existencia y denominación del signatario del certificado. Estos certificados serán emitidos a personas físicas con actividad empresarial o personas morales para garantizar frente a terceros su identidad, autenticidad e integridad de sus mensajes, así como que el representante legal de una empresa manifieste que su representada se encuentra capacitada legalmente para la celebración del acto y acreditar que la personalidad que ostenta y las facultades con que cuenta no le han sido limitadas, modificadas o revocadas.

Características generales

- Requiere de presencia personal de un representante legal de la persona física o moral para acreditar la personalidad de la representada.
- Se registra documentación y firma autógrafa.

Usos típicos

- Comercio electrónico.
- Servicios de suscripción.
- Correo electrónico.
- Autenticación en sitio web.
- Firma de documentación.

3.4.2.3 Certificado Personal

El certificado tendrá como única finalidad asegurar la existencia y denominación del signatario del certificado. Estos certificados serán emitidos a personas físicas para garantizar frente a terceros su identidad, autenticidad e integridad de sus mensajes.

Características generales

- Requiere presencia personal para acreditar la identidad.
- Se registra documentación y firma autógrafa.

Usos típicos

- Comercio electrónico.
- Servicios de suscripción.
- Correo electrónico.
- Autenticación en sitio web.

- Firma de documentos.
- Firma de contratos.

3.4.3 Procedimiento de expedición de un certificado electrónico

De manera general señalaremos el procedimiento a seguir para la expedición de un certificado electrónico, cabe señalar que los trámites de solicitud de certificados digitales se regirán por las Políticas de Certificación autorizadas por la Secretaría de Economía.

Lo anterior con fundamento en el artículo 102 fracción III, el cual dispone que se deberá "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".

En principio se tendrá que ingresar a la aplicación dentro del sitio web del Prestador de Servicios de Certificación, en el cual se cuenta con las instrucciones pertinentes para ingresar exactamente a la aplicación.

Todo solicitante deberá llenar en primer lugar el formulario de solicitud de prestación de servicios de certificación digital (en adelante el formulario), correspondiente al certificado electrónico que desee le sea expedido. El solicitante deberá llenar el formulario de solicitud manifestando su consentimiento a obtener los servicios del PSC, así como a ser registrado como solicitante y como suscriptor en la base de datos de ésta, al respecto, la información proporcionada por el solicitante será resguardada atendiendo a lo dispuesto por el artículo 76 Bis de la Ley Federal de Protección al Consumidor el cual dispone que:

> **ARTÍCULO 76 BIS.-** Las disposiciones del presente Capítulo aplican a las relaciones entre proveedores y consumidores en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología. En la celebración de dichas transacciones se cumplirá con lo siguiente:
> **I.** El proveedor utilizará la información proporcionada por el consumidor en forma confidencial, por lo que no podrá difundirla o transmitirla a otros proveedores ajenos a la transacción, salvo autorización expresa del propio consumidor o por requerimiento de autoridad competente;
> **II.** El proveedor utilizará alguno de los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por el consumidor e informará a éste, previamente a la celebración de la transacción, de las características generales de dichos elementos.

Todo solicitante que sea persona física, deberá acudir de manera personal con el Agente Certificador, presentando junto con el formulario, y además deberá presentar el documento original

de su identificación personal (IFE, Pasaporte, Cédula profesional, Cartilla militar), así como una copia simple.

Para el caso de personas morales, deberá acudir personalmente el representante legal que ostente las facultades legales de la sociedad que representa, además de presentar el instrumento público debidamente certificado ante fedatario público en donde consten las facultades y poderes que no le han sido revocadas hasta la fecha de solicitud del certificado electrónico requerido, asimismo deberá presentar su identificación oficial vigente, y el formulario de prestación de servicios de forma impresa.

Por otra parte, el PSC se reserva el derecho de solicitar documentos adicionales a los anteriores señalados o fotografías certificadas de los mismos, cuando así lo considere necesario para verificar la identidad o cualquier calidad del solicitante.

3.4.4 Verificación de los datos entregados por el solicitante

Recibida la solicitud, el PSC procederá directamente o a través de sus Entidades de Registro, a la verificación de los datos entregados por el solicitante; esta verificación se regirá atendiendo a las siguientes reglas:

1. El Agente Certificador verificará a través de recursos propios:
    1.1. El correcto llenado de todos los campos del formulario.
    1.2. La recepción de todos los documentos originales solicitados.
    1.3. El solicitante conoce y acepta que el PSC se reserva el derecho, pero no tiene la obligación, de investigar todos los hechos y datos que el solicitante le informa hasta donde lo permitan las leyes vigentes. El solicitante colaborará en todo aquello que esté a su alcance para la corroboración de los datos que ha suministrado al PSC.
2. El solicitante acepta que estas medidas pueden incluir, de manera enunciativa mas no limitativa, las siguientes:
    2.1. Entrevistas con el solicitante del certificado electrónico y con los empleados de la empresa que estime convenientes en caso de ser una persona moral.
    2.2. Inspección personal de las instalaciones de la empresa.
    2.3. Verificación de las referencias entregadas por el solicitante.

Si bien es cierto, el PSC no puede garantizar que estos procedimientos de verificación tomen un tiempo determinado, procurará que la verificación sea realizada dentro de un tiempo razonable a la entrega de la documentación por parte del solicitante.

Los contactos y comunicaciones entre el PSC y el solicitante se harán a través del Agente Certificador en la que el solicitante radicó los documentos de solicitud.

Verificados estos datos, el Agente Certificador procederá a dar tramite a la solicitud, enviándola al PSC.

Si el nombre del solicitante coincide exactamente con el nombre de un suscriptor ya existente, el PSC expedirá el certificado electrónico el nuevo solicitante con una aclaración que permita distinguir a los dos suscriptores, salvo que de la información que consta el certificado electrónico se desprenda claramente la identidad de cada uno de ellos.

Por su parte el solicitante asume la obligación de respetar en todo momento y circunstancia los derechos de propiedad intelectual e individual de terceras personas

3.4.5 Rechazo de la solicitud del certificado electrónico

Si el PSC decide rechazar la solicitud de expedición del certificado electrónico, lo notificará por escrito al solicitante del mismo a la dirección que se haya indicado en el formulario, con indicación de los motivos que la provocaron. En caso de que los defectos encontrados sean subsanados, se le otorgará al solicitante del certificado un plazo de quince días hábiles para llevar acabo la subsanación, transcurrido el cual el Agente certificador procederá a confirmar o a revocar por escrito su decisión de manera definitiva.

3.4.6 Publicación del certificado electrónico

De acuerdo con el artículo 104 fracción IV CCo., se deberá mantener un registro de Certificados, en el que quedará constancia de los emitidos y figurarán las circunstancias que afecten a la suspensión, pérdida o terminación de vigencia de sus efectos. A dicho registro podrá accederse por medios electrónicos, ópticos o de cualquier otra tecnología y su contenido público estará a disposición de las personas que lo soliciten, el contenido privado estará a disposición del Destinatario y de las personas que lo soliciten cuando así lo autorice el Firmante, así como en los casos a que se refieran las reglas generales que al efecto establezca la Secretaría;

Al respecto, la lista de certificados es una base de datos o repositorio de acceso público, que se maneja únicamente por personal autorizado y a partir de los ficheros de información generados por el PSC para cada suscriptor.

Aceptado el certificado electrónico, el suscriptor confirma y asume la exactitud del contenido del mismo, con las consiguientes obligaciones que de ello se derivan frente al PSC o cualquier otra parte que confía en el contenido del certificado electrónico.

El llenar el formulario con los datos requeridos bajo protesta de decir verdad, la firma del contrato de suscriptor y el uso del pin y la frase de desafío implica la aceptación de la entrega del certificado electrónico al suscriptor, con todas las consecuencias legales que se deriven en posterior a la entrega.

3.4.7 Verificación de Identidad

Adicional a lo establecido en la parte general concerniente a la certificación, el Agente certificador confirmará la plena identidad en bases de reconocida confiabilidad, es decir, que únicamente se realizará la verificación de la identidad del solicitante antes de la expedición del certificado electrónico, en lo consecuente el suscriptor deberá informar al PSC cualquier cambio en los datos de identidad y de responder frente a terceros por todo perjuicio que el incumplimiento de ésta obligación ocasione.

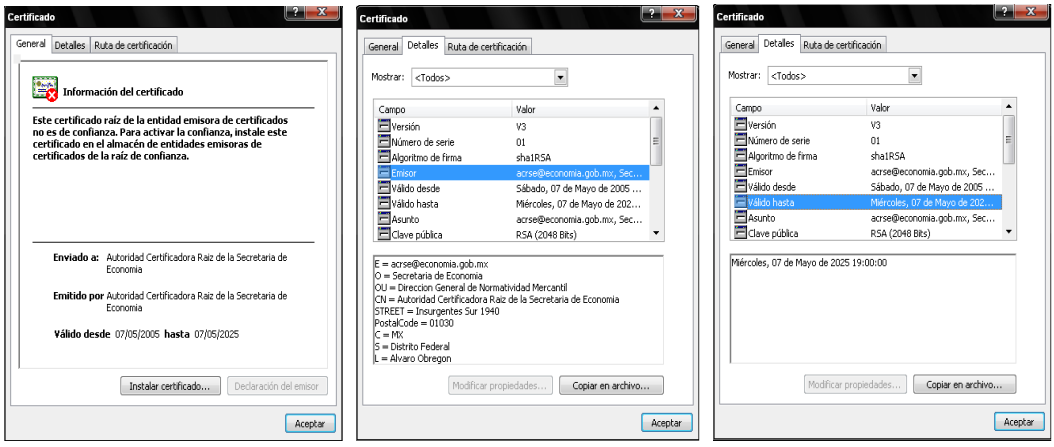
De manera general enumeraremos los requerimientos para la emisión de un certificado electrónico[69]:

Persona Física	Persona moral	Fundamento legal
1.- Llenar el formulario de solicitud de prestación de servicios de certificación digital correspondiente, en el sitio web	1.- Llenar el formulario de solicitud correspondiente, en el sitio web	
2.- El solicitante se deberá presentar de manera física ente el Agente certificador, quien comprobará la identidad de los solicitantes y cualquier otra circunstancia pertinente. El solicitante deberá exhibir: 1. Original y copia simple del su identificación oficial (Credencial IFE, Cédula Profesional, Cartilla Militar, Pasaporte o Documento Migratorio).	2.- Se deberá presentar de forma física el representante legal de la, Entidad objeto de registro, exhibiendo: 1. Original y copia simple de la escritura pública conde consten las facultades legales, 2. Original y copia simple de la identificación oficial del representante. 3. Contrato.	**Art. 104 fr. I CCo.** **I.** Comprobar por sí o por medio de una persona física o moral que actúe en nombre y por cuenta suya, la identidad de los solicitantes y cualesquiera circunstancias pertinentes para la emisión de los Certificados, utilizando cualquiera de los medios admitidos en derecho, siempre y cuando sean previamente notificados al solicitante.

[69] El cuadro que se describe está basado al procedimiento descrito en la página de Advantage Security. http://www.advantage-security.com, 10 de junio de 2008.

2. Contrato. En el mismo acto se firmará el contrato de suscriptor de firma electrónica.	En el mismo acto se firmará el contrato correspondiente de suscriptor de firma electrónica.	**Art. 104 fr. III CCo.** **III.** Informar, antes de la emisión de un Certificado, a la persona que solicite sus servicios, de su precio, de las condiciones precisas para la utilización del Certificado, de sus limitaciones de uso y, en su caso, de la forma en que garantiza su posible responsabilidad;
2.- Se realizará una llamada de seguridad, por parte del personal del PSC, previa a la entrega del certificado digital. Este segundo paso de aprobación también se firma digitalmente y se respalda en la aplicación de control de inscripción del PSC. Al terminar este segundo paso de aprobación se ejecuta la emisión del certificado digital.	2.- Se realizará una llamada de seguridad, por parte del personal del PSC, previa a la entrega del certificado digital. Este segundo paso de aprobación también se firma digitalmente y se respalda en la aplicación de control de inscripción del PSC. Al terminar este segundo paso de aprobación se ejecuta la emisión del certificado digital.	
3.- Entrega de certificado vía correo electrónico.	3.- Entrega de certificado vía correo electrónico.	**Art. 104 fr. II CCo.** **II.** Poner a disposición del Firmante los dispositivos de generación de los Datos de Creación y de verificación de la Firma Electrónica;

3.4.8 Contenido de un certificado digital



Los Certificados, para ser considerados válidos, deberán contener:

I. La indicación de que se expiden como tales;

II. El código de identificación único del Certificado;

III. La identificación del Prestador de Servicios de Certificación que expide el Certificado, razón social, su domicilio, dirección de correo electrónico, en su caso, y los datos de acreditación ante la Secretaría;
IV. Nombre del titular del Certificado;
V. Periodo de vigencia del Certificado;
VI. La fecha y hora de la emisión, suspensión, y renovación del Certificado;
VII. El alcance de las responsabilidades que asume el Prestador de Servicios de Certificación, y
VIII. La referencia de la tecnología empleada para la creación de la Firma Electrónica.

3.4.9 Interrupción de los efectos jurídicos de un cerificado electrónico

Los certificados electrónicos son válidos por un periodo de tiempo, el cual se encuentra determinado en el propio certificado, en donde además se indica la fecha y hora del comienzo de la vigencia y su extinción.

La duración del periodo de validez de los certificados electrónicos no debe ser demasiado extensa, pues en este caso, las claves protegidas se encuentran expuestas a mayores riesgos de ser copiadas, apropiadas o utilizadas ilegítimamente por terceras personas.

Cabe señalar, que una firma electrónica sólo será valida si se expidió dentro del periodo de validez del certificado electrónico correspondiente, de manera que si una firma electrónica es expedida fuera del periodo de validez del certificado, las transacciones celebradas utilizando dicha firma carecen de seguridad jurídica.

Es por ello que, a continuación estudiaremos las causas de terminación de validez de un certificado electrónico contempladas en el CCo. y que a saber son las siguientes:

3.4.9.1 Expiración

El tiempo de vigencia de un certificado no podrá ser superior a dos años, contados a partir de la fecha en que se hubiere expedido, no obstante, antes de que concluya el periodo de vigencia del certificado podrá el firmante solicitar al Prestador de Servicios de Certificación su renovación, art. 109 CCo.

3.4.9.2 Revocación

Por regla general, los certificados electrónicos serán revocados una vez que cumplan el periodo temporal de validez por el cual fueron creados, sin embargo, también cabe la posibilidad de que el certificado sea objeto de una revocación anticipada, generalmente cuando la clave privada ha sido puesta en peligro, ya sea por pérdida o extravío, por lo que puede ser utilizado por terceras personas no autorizadas para fines ilegítimos.

De manera que, la revocación tendrá lugar cuando a solicitud del firmante, el Prestador de Servicios de Certificación otorga el vencimiento anticipado de la vigencia de un certificado electrónico.

Dentro de esta modalidad de terminación de la vigencia también se comprende a:

- La pérdida o inutilización por daños del dispositivo en el que se contenga dicho Certificado.
- Por haberse comprobado que al momento de su expedición, el Certificado no cumplió con los requisitos establecidos en la ley, situación que no afectará los derechos de terceros de buena fe.
- Por resolución judicial o de autoridad competente que lo ordene.

Al respecto, el artículo 17-H del Código Fiscal de la Federación señala que:

Artículo 17-H.- Los certificados que emita el Servicio de Administración Tributaria quedarán sin efectos cuando:

I. Lo solicite el firmante.

II. Lo ordene una resolución judicial o administrativa.

III. Fallezca la persona física titular del certificado. En este caso la revocación deberá solicitarse por un tercero legalmente autorizado, quien deberá acompañar el acta de defunción correspondiente.

IV. Se disuelvan, liquiden o extingan las sociedades, asociaciones y demás personas morales. En este caso, serán los liquidadores quienes presenten la solicitud correspondiente.

V. La sociedad escindente o la sociedad fusionada desaparezca con motivo de la escisión o fusión, respectivamente. En el primer caso, la cancelación la podrá solicitar cualquiera de las sociedades escindidas; en el segundo, la sociedad que subsista.

VI. Transcurra el plazo de vigencia del certificado.

VII. Se pierda o inutilice por daños, el medio electrónico en el que se contengan los certificados.
VIII. Se compruebe que al momento de su expedición, el certificado no cumplió los requisitos legales, situación que no afectará los derechos de terceros de buena fe.
IX. Cuando se ponga en riesgo la confidencialidad de los datos de creación de firma electrónica avanzada del Servicio de Administración Tributaria.

El Servicio de Administración Tributaria podrá cancelar sus propios certificados de sellos o firmas digitales, cuando se den hipótesis análogas a las previstas en las fracciones VII y IX de este artículo.

Cuando el Servicio de Administración Tributaria revoque un certificado expedido por él, se anotará en el mismo la fecha y hora de su revocación. Para los terceros de buena fe, la revocación de un certificado que emita el Servicio de Administración Tributaria, surtirá efectos a partir de la fecha y hora que se dé a conocer la revocación en la página electrónica respectiva del citado órgano.

Las solicitudes de revocación a que se refiere este artículo deberán presentarse de conformidad con las reglas de carácter general que al efecto establezca el Servicio de Administración Tributaria.

3.4.10 Reconocimiento y validez jurídica de certificados electrónicos extranjeros

Para determinar si un Certificado o una Firma Electrónica extranjeros producen efectos jurídicos, o en qué medida los producen, no se tomará en consideración cualquiera de los siguientes supuestos:

I. El lugar en que se haya expedido el Certificado o en que se haya creado o utilizado la Firma Electrónica, y
II. El lugar en que se encuentre el establecimiento del Prestador de Servicios de Certificación o del Firmante.

Es así que, todo Certificado expedido fuera de la República Mexicana producirá los mismos efectos jurídicos en la República Mexicana si presenta un grado de fiabilidad equivalente a los contemplados por el CCo.

A efectos de determinar si un Certificado o una Firma Electrónica presentan un grado de fiabilidad equivalente, se tomarán en consideración las normas internacionales reconocidas por

México y cualquier otro medio de convicción pertinente. Cuando las partes acuerden entre sí la utilización de determinados tipos de Firmas Electrónicas y Certificados, se reconocerá que ese acuerdo es suficiente a efectos del reconocimiento transfronterizo, salvo que ese acuerdo no sea válido o eficaz conforme al derecho aplicable.

3.4.11 Sellado digital de tiempo (Time stamping)

Una Entidad de sellado digital de tiempo es un Prestador de Servicios de Certificación, legalmente autorizado para la prestación del servicio de sellado de tiempo, quien proporciona certeza sobre la preexistencia de determinados documentos electrónicos en un momento dado, cuya indicación temporal junto con el resumen del documento se firman por la Entidad de sellado digital de tiempo.

El sistema de sellado digital de tiempo (Timestamping) es un mecanismo on-line que permite demostrar que una serie de datos electrónicos han existido y no han sido alterados desde un instante específico en el tiempo, en donde una Entidad de sellado digital de tiempo actúa como tercera parte de confianza testificando la existencia de dichos datos electrónicos en una fecha y hora concretos.

Entre los principales usos del sellado digital de tiempo se encuentra la inserción de la hora y fecha exacta a los actos o negocios a celebrar, mismos que comprenden:

- La inserción de estampados de tiempo dentro de firmas digitales para documentos electrónicos, tal como fianzas electrónicas, órdenes de compra, notificaciones de embarque, entre otros.
- Inserción de estampados de tiempo a conjuntos de documentos para contar con una "foto" de ciertas características del documento en el tiempo.
- Acuses de recibo de documentos electrónicos, mejorando la eficiencia de sus transacciones y reduciendo costos de resolución de controversias.

Asimismo, al igual que en el procedimiento de acreditación para un PSC para efectos de la NOM–151–SCFI–2002, en el caso del sellado digital de tiempo, se tendrá que seguir un procedimiento similar al de la citada NOM-151, de manera que el trámite a seguir es el siguiente:

Actividad	Plazo
1.- Presentación de escrito, adjuntando: • Documentos que comprueban los elementos tecnológicos (de acuerdo a las reglas generales) • Póliza del seguro de responsabilidad civil (podrá ser la misma que se exhibe para la NOM–151–SCFI–2002 en tanto se mencione que cubre también el servicio de estampado de tiempo). • Comprobante del pago de derechos por concepto del trámite y estudio de la solicitud para acreditación como PSC de estampado de tiempo, y cuyo monto es de $17,150.00 (Diecisiete mil ciento cincuenta pesos 00/100).	
2.- Observaciones por parte de la Autoridad (requerirá solamente una vez).	20-45 días hábiles
3.- Contestación al requerimiento de la Autoridad.	20 días hábiles
4.- Auditoría para comprobar la seguridad de las instalaciones.	
5.- Acreditación por parte de la Autoridad.	
6.- Exhibir a la SE • Pago de derechos por concepto de la evaluación de la conformidad, cuyo monto es de $105,300.00 (Ciento cinco mil trescientos pesos 00/100). • Fianza, de acuerdo a lo dispuesto por las reglas 3, 3.1 y 3.3 de las Reglas generales y con fundamento en el art. 8 del Reglamento del CCo. en materia de PSC (podrá ser la misma que se exhibe para la NOM–151–SCFI–2002 en tanto se mencione que cubre también el servicio de estampado de tiempo).	10 días hábiles
7.- Publicación de la autorización en el DOF.	30 días a la resolución de acreditación
8.- Notificar a la SE la fecha en que se inicia la operación del servicio de estampado de tiempo.	Dentro de los 45 días naturales al comienzo de dicha actividad

CAPÍTULO CUARTO

4. Responsabilidad derivada de la utilización indebida de un certificado electrónico, por parte de terceros, en el tiempo que transcurre de la solicitud de revocación al otorgamiento de ésta.

En el presente capítulo, con el cual daremos conclusión a nuestro estudio en relación a la responsabilidad que puede derivarse del uso indebido de un certificado electrónico, en particular en el caso de la revocación, plantearemos las hipótesis de responsabilidad en que los Prestadores de Servicios de Certificación pueden incurrir, derivado de las obligaciones y servicios de certificación y que se encuentran regulados en el CCo., lo anterior con el objetivo de que el titular de un certificado electrónico no asuma todas las consecuencias que puedan derivarse de este hecho.

Es así que, las hipótesis de responsabilidad derivadas de la certificación las agruparemos principalmente en tres las cuales, a saber, son las siguientes:

1. Aquellas que son previas a la emisión de un certificado
2. Las derivadas de la certificación, y
3. Aquellas que son consecuencia de la terminación anticipada de la validez de un certificado electrónico.

Para dar inicio a nuestro estudio, comenzaremos con el análisis del concepto de responsabilidad.

4.1 Responsabilidad

El concepto de responsabilidad ha sido objeto de muchas controversias entre juristas, por lo que existen un sinnúmero de teorías que explican sus fundamentos y alcances, prácticamente todos los teóricos del derecho coinciden en señalar que responsabilidad constituye un concepto jurídico fundamental, sin embargo, la noción de responsabilidad no es exclusiva del discurso jurídico.

Para determinar el significado de la palabra responsabilidad es necesario hacer alusión a aquellos usos de “responsabilidad” que están de alguna manera presupuestos a la noción jurídica de responsabilidad.

La voz responsabilidad proviene de “respondere” que significa, “Inter Alia”, es decir, prometer, merecer, pagar, así, “responsalir” significa: “el que responde” (fiador).

En un sentido más amplio “responsum” significa “el obligado a responder de algo o de alguien”, “Respondere” se encuentra estrechamente ligado con “spondere”, la expresión solemne en la forma de la stipulatio, por la cual alguien asumía una obligación.

Otro significado es el que recoge la dogmática jurídica en donde un individuo es responsable cuando de acuerdo con el orden jurídico es susceptible de ser sancionado (H. Kelsen). En este sentido, la responsabilidad presupone un deber, del cual debe responder el individuo, sin embargo, no debe confundirse con él. El deber o la obligación de la conducta que, de acuerdo con un orden jurídico, se debe hacer u omitir; quien la debe hacer u omitir es el sujeto obligado.

La responsabilidad presupone esta obligación, pero no se confunde con ella. La responsabilidad señala quién debe responder del cumplimiento o incumplimiento de tal obligación. La responsabilidad es en ese sentido una obligación de segundo grado, es decir, que aparece cuando la primera no se cumple, esto es, cuando se comete un hecho ilícito. Uno tiene la obligación de no dañar, es responsable del daño el que tiene que pagar por él, de ahí que es responsable de un hecho ilícito (delito). Aquel individuo que debe sufrir las consecuencias de sanción, que el hecho ilícito se imputa. Aquel que sufre la pena de prisión que se impone al homicidio. De la misma forma, aquel que sufre la pena que se impone al robo es el responsable del delito de robo.

Por regla general, el autor del hecho ilícito y el responsable son el mismo individuo, sin embargo, no siempre el responsable de un hecho ilícito es el autor. En efecto puede suceder que un individuo sea el autor del acto ilícito y que otro u otros sean los responsables del mismo, es decir, que otros sean los que deban sufrir las consecuencias de sanción que a ese delito corresponde, de conformidad con una norma jurídica.

Existen dos grandes formas de aplicar la responsabilidad, la llamada responsabilidad por culpa y la conocida como responsabilidad objetiva o absoluta.

En el caso de la primera la aplicación de sanciones al individuo considerado responsable supone “culpa” por parte del autor del hecho ilícito. Esto es, las consecuencias de sanción se aplican al responsable sólo cuando el autor del hecho ilícito tuvo la intención de cometerlo, o bien habiéndolo previsto no lo impidió.

A la responsabilidad objetiva, por el contrario, no le importa la culpa del autor; basta que el hecho ilícito se realice, con o sin culpa del autor, para que se apliquen las consecuencias de

sanción al individuo considerado responsable, esto es, por lo general, el sistema de responsabilidad en los accidentes de trabajo.

4.1.1 Responsabilidad Civil

Algunos autores (De Cupis y Carnelutti)[70] han definido la responsabilidad civil, como la obligación de soportar la reacción del ordenamiento jurídico frente al hecho dañoso. También en términos generales se concibe a la responsabilidad civil como la consecuencia de la violación del deber jurídico de no dañar a nadie.

En el Derecho Romano los daños materiales o de orden moral (golpes heridas, insultos y ofensas al honor) que una persona causaba a otra, constituían el delito de "injuria" siempre que fuera que se realizaran como consecuencia de un comportamiento contrario al Derecho, non jure. Originalmente sólo era reparable el daño patrimonial, único que era "dannum injuria datum" y solamente cuando se causaba por el contacto materia, "corpore corpori datum", independientemente de que el agente obtuviera un lucro, bastara que obrara movido por la intención de dañar o por simple descuido o negligencia.

La responsabilidad civil requiere de la concurrencia de los siguientes elementos:

1. Hecho ilícito
2. La existencia de un daño
3. Un nexo de causalidad entre el hecho y el daño

El concepto de acto ilícito significa que se ha realizado una conducta dolosa o culposa, es decir, que la gente ha obrado con la intención de causar el daño o éste se ha producido por imprudencia, inadvertencia, falta de atención, de cuidado o impericia. En la doctrina francesa el daño causado intencionalmente constituye un delito civil y el que se origina por culpa o negligencia se denomina cuasidelito.

La ilicitud de la conducta es el dato característico de la responsabilidad civil. El daño causado sin justificación alguna, es decir, violando los principios del orden y la justicia en los que se sustenta la convivencia social.

El artículo 1830 del Código Civil Federal CCF postula el concepto de ilicitud declarando: "Es ilícito el hecho que es contrario a las leyes de orden público o a las buenas costumbres", Para

[70] Enciclopedia jurídica Omeba, Ob. Cit.

que proceda la reparación del daño se requiere la prueba de que el demandado ha obrado ilícitamente, sin derecho, por dolo o culpa.

El daño causado por caso fortuito o fuerza mayor que excluyen la culpa o el dolo, no dará lugar a responsabilidad porque no ha podido ser previsto o porque habiendo sido previsto no ha podido ser evitado. Tampoco surge la responsabilidad civil si el daño se ha causado en el ejercicio de un derecho o se produce por el hecho de la víctima. No es imputable al autor material de él.

El segundo elemento de la responsabilidad civil es el daño o menoscabo que sufre una persona en su patrimonio (daño emergente). El daño reparable comprende también la privación de cualquier ganancia lícita que se podría haber obtenido por el cumplimiento de la obligación.

En la actualidad se entiende por daño también la lesión a los bienes no valuables en dinero, por ejemplo, los daños causados sobre la persona en su vida, su intimidad, sus efectos, la salud, etc.

Generalmente se clasifican a esta especie de daños en aquellos que atañen a la persona en su aspecto social (honor, reputación, dignidad, pública consideración, buena fama), los que lesionan a la persona en sus sentimientos, su integridad corporal, su configuración y aspecto físico, el derecho a su imagen, al secreto de su vida intima, etc.

Aunque el daño moral no es susceptible de una reparación pecuniaria, es de justicia que al ofensor se le aplique una sanción como efecto de su conducta ilícita, siendo obligado a pagar al ofendido una suma de dinero por concepto de indemnización compensatoria.

La relación de causalidad es el tercero de los elementos necesarios para que surja la responsabilidad civil. En presencia del efecto (daño) el juzgador debe determinar la causa que produjo el daño y si aquella es imputable al demandado.

El nexo de causalidad entre el hecho ilícito y el daño reparable (que es el daño que interesa al derecho), debe ser entendido como el que consiste en establecer la consistencia de los supuestos necesarios para impulsar las consecuencias del derecho que produce un daño injusto, “non jure”. Como ocurre, por ejemplo, en el caso de la responsabilidad por hechos de terceros, o por el uso de cosas peligrosas en los que la causa material del daño no es decisiva para fijar la obligación de responder por el daño.

Es así que, la reparación del daño consiste en la obligación de restituir o en la de restablecer la situación anterior y, cuando ello no sea posible, en el resarcimiento en dinero por el

equivalente del menoscabo del daño patrimonial causado, en la indemnización de los perjuicios y en el pago de los gastos judiciales, artículo 1915 CCF.

La cuantía de la reparación del daño material o patrimonial será fijada por el juez, de acuerdo con el resultado de la prueba pericial que justiprecie el valor del menoscabo causado por la conducta dañosa.

El artículo 2116 CCF ordena que al fijar el valor y el deterioro de una cosa no se atenderá al precio estimativo o de afectación a no ser que se pruebe que el responsable destruyo o deterioró la cosa con el objeto de lastimar la afección del dueño, el aumento que por estas causas se haga se fijará de acuerdo con el artículo 1916 CCF.

En cuando a la estimación del daño moral, el artículo 1916 CC. dispone que el juez tomando en cuenta las circunstancias del caso, las posibilidades económicas del ofensor y del ofendido, determinará el importe de la compensación a la que tendrá derecho la víctima.

4.1.2 Responsabilidad Penal

La responsabilidad de soportar la consecuencia específica del delito constituye la responsabilidad penal. Esta responsabilidad recae únicamente sobre el delincuente y no debe confundirse con la responsabilidad civil emergente del delito, que propone la obligación de indemnizar a la víctima del mismo, y que tiene carácter accesoria de la anterior, se rige por los principios del derecho civil y puede hacerse efectiva en forma indirecta, sobre terceros que no han intervenido en la ejecución del delito.

La consecuencia específica del delito es la pena, la que sólo puede imponerse al autor o partícipe de un delito que sea penalmente responsable. Para que a un sujeto se le considere penalmente responsable es importante que el delito que se le imputa aparezca configurado con todos los elementos esenciales para su existencia, por lo cual tiene que haber una acción positiva o negativa que pueda atribuirse al sujeto activo como expresión de su responsabilidad, que sea antijurídica (contraria a derecho), típica (que se adecue a una figura delictiva) y que el actor o partícipe sea imputable (capaz de comprender la criminalidad del acto y dirigir sus acciones) y culpable (que su conducta le sea reprochable por no incurrir en el acto ninguna causa de exclusión de la culpabilidad).

Por tanto, la acción (positiva o negativa), la antijuricidad, tipicidad, imputabilidad y la culpabilidad del agente constituyen los presupuestos necesarios de la responsabilidad penal. Esta aparece entonces como una consecuencia del delito, que determina que el sujeto activo deba

cargar con la consecuencia específica del delito, es decir, con la pena que debe soportar como retribución del delito cometido, que la sociedad le impone como reproche por su acto culpable.

Por consiguiente, si no hay acción retribuible al sujeto activo, o ésta no es típica o concurre alguna causa de justificación de imputabilidad o de inculpabilidad no puede haber responsabilidad penal para el agente. Además, la ausencia de alguna de las condiciones objetivas de punibilidad que exija el tipo penal o la concurrencia de alguna excusa absolutoria que excluya la penalidad, produce también como efecto la falta de responsabilidad penal para el sujeto activo, ya que el mismo queda exento de pena en esos casos.

Para Jorge Frías Caballero "la responsabilidad penal es la consecuencia del delito, a la cual se vincula la aplicación de la pena"[71] y debe distinguirse la de culpabilidad, que es un presupuesto de la pena y, por tanto, es el delito mismo en uno de sus aspectos, mientras que la responsabilidad penal está fuera del delito mismo.

4.1.3 Responsabilidad del Estado

Es la obligación que tiene el Estado de proteger jurídicamente a los ciudadanos contra decisiones arbitrarias e ilícitas de la administración pública federal, estatal y de sus funcionarios, indemnizándolos del daño causado mediante una compensación económica que restituye el perjuicio patrimonial e inclusive moral que el Estado ocasione como consecuencia de la actividad administrativa que desempeña en cumplimiento de las funciones que le han sido encomendadas.

En términos generales, el régimen jurídico mexicano acepta la responsabilidad del Estado, pero en forma y extensión tan limitada que debe afirmarse que en la práctica equivale a una falta total de ello. Esta falta de reconocimiento se funda en la idea de soberanía y en el supuesto de que el Estado siempre actúa dentro de los límites del derecho y que por lo mismo, la actividad estatal no puede considerarse ilícita y por tanto dar lugar a responsabilidades patrimoniales cuando menos respecto de actos ejecutados dentro de la atribuciones legales de la administración pública.

La doctrina francesa ha elaborado la doctrina de "la falta en el servicio público", que establece que la misión del Estado es proporcionar servicios a la colectividad, de manera normal, constante y eficiente. Para cumplirlos, el Estado cuenta con ingresos y por lo mismo, no importa quién sea el responsable personal de las faltas. De aquí nace la responsabilidad del Estado de indemnizar al particular a consecuencia de la "falta en el servicio público".

[71] Frías Caballero, Jorge, "Imputabilidad Penal", Ediar, Buenos Aires, 1981.

El Código Civil Federal reconoce de manera expresa la responsabilidad del Estado en el artículo 1928, el cual establece la obligación que tiene el Estado de responder subsidiariamente del daño causado. Otro reconocimiento de la responsabilidad del Estado lo encontramos en el artículo 27 constitucional cuando se refiere a la indemnización por causa de utilidad pública.

4.1.4 Responsabilidad de los servidores públicos

En primer lugar debemos precisar quién puede ser sujeto de este tipo de responsabilidad, es decir, qué debemos entender por servidor público. Al respecto, atendiendo a lo dispuesto por el artículo 108 constitucional, se señalan a los representantes de elección popular, a los miembros de los poderes judiciales federal y del Distrito Federal, funcionarios, empleados y toda persona que desempeñe un empleo, cargo o comisión de cualquier naturaleza en la administración pública. Por otro lado, los gobernadores, diputados y magistrados de los tribunales superiores de justicia, también son sujetos de responsabilidad por violaciones a la constitución, a las leyes federales y por el manejo indebido de fondos y recursos federales; amén de las responsabilidades que los ordenamientos locales pueden establecer en el ámbito de su competencia. A mayor referencia el artículo 2 de la Ley Federal de Responsabilidad de los Servidores Públicos agrega a todas aquellas personas que manejan o apliquen recursos económicos federales.

Por otra parte, la responsabilidad política es la que se hace valer a través del juicio político de responsabilidad, en contra de los funcionarios mencionados en el artículo 110 constitucional. Las causas de procedencia de la pretensión en dicho juicio son los actos u omisiones que redunden en perjuicio de los intereses públicos fundamentales o de su buen despacho, siendo el artículo 7 de la LFRSP en donde se especifican las causas.

La responsabilidad administrativa se exige a todos los servidores públicos por actos u omisiones que afecten la legalidad, imparcialidad y eficiencia que deben observar en el desempeño de sus empleos, cargos o comisiones.

Las diversas causas por las cuales se puede exigir la responsabilidad administrativa están prevista en el artículo 47 de la LFRSP, así como los arts. 50 y 59 del mismo ordenamiento.

4.2 Responsabilidad de los Prestadores de Servicios de Certificación

En lo consecuente iremos desarrollando las hipótesis derivadas de la certificación de firmas electrónicas, y en cada caso describiremos las relaciones jurídicas que pueden suscitarse y los daños por los que puede responder el PSC.

4.2.1 Hipótesis de responsabilidad previas a la emisión del certificado

4.2.1.1 Por creación de la firma electrónica

Es de importancia señalar que, la creación del par de claves que configuran la firma electrónica, es el paso previo a la emisión del certificado electrónico, es por ello que la veracidad del certificado depende en gran medida de los mecanismos técnicos de seguridad con la que fue generada la firma a fin de que ésta no sea obtenida por terceros a través de “ataques” computacionales.

En efecto, si la clave privada se hace accesible a terceros por esta vía, el titular pierde el control exclusivo sobre la firma, situación que puede ocasionar daños tanto al titular del certificado como a los terceros que confían en el certificado, producto de los fraudes que el atacante puede efectuar al suplantar al titular del certificado.

Por lo mismo, en caso de que el PSC en la creación del par de claves, produzca una firma tecnológicamente vulnerable, producto de su negligencia o dolo, el PSC será civilmente responsable por los daños que puedan ocasionarse. Lo mismo, puede decirse en caso de que no se destruyan las claves al momento de entregar la firma al usuario, ello porque la clave puede ser tomada por terceros, lo cual, puede dar pie a fraudes en perjuicio tanto del titular del certificado y de terceros en general.

Por otra parte, respecto del sujeto activo de la acción de indemnización por perjuicios, resulta claro que puede ser tanto el titular del certificado electrónico, quien puede verse obligado al cumplimiento forzado de obligaciones a las cuales ha consentido un tercero, conduciéndolo a un juicio para demostrar que no ha sido él quien ha asumido tal obligación, asimismo podrá ser sujeto activo de la acción el tercero que confía en el certificado quien buscará obtener el cumplimiento de una obligación, en el coste que implica la pérdida del crédito habiendo cumplido con su obligación, el costo de oportunidad de no haber efectuado la operación con otra persona, etc.

4.2.1.2 Por incumplimiento de la obligación de emitir el certificado

La emisión del certificado, es la prestación más elemental a la cual se obliga el PSC al momento de celebrar el contrato de suscriptor de certificado electrónico.

Dicho contrato, es celebrado entre el solicitante del certificado y el PSC, una vez que el PSC o el Agente certificador haya confirmado los datos proporcionados por el solicitante, hecho lo

anterior le es remitido una copia del certificado al solicitante, al manifestar su conformidad, dando así nacimiento al contrato aludido.

Es fácil advertir que esta hipótesis de responsabilidad constituye el incumplimiento total o parcial de la obligación de emitir el certificado, y que producto de ello, pueda provocarse perjuicios al titular del certificado. En principio, tal indemnización sería la devolución del precio pagado por el suscriptor con los respectivos reajustes o penas convencionales.

4.2.2 Hipótesis de responsabilidad derivadas de la certificación, por parte del PSC

4.2.2.1 Responsabilidad por la veracidad de los datos contenidos en certificados emitidos

En este caso nos ubicaremos en el supuesto en el que el certificado emitido contiene datos erróneos en cuanto a la identidad o atributos del titular del certificado, lo cual, en la medida de que se configure un daño efectivo contra una persona y que sea imputable al PSC, podrá generar la obligación de indemnizar.

Sin embargo, la responsabilidad del PSC se configura efectivamente al momento en que se distribuye el certificado, debido a que es a partir de dicho instante en que el certificado se hace accesible al público en general.

Al respecto, cabe señalar que nuestra legislación opta por el sistema de directorios de certificados, de acuerdo a lo previsto por la regla 2.4.13.3.4 de las Reglas generales a las que deberán sujetarse los Prestadores de Servicios de Certificación, en relación con el art. 104 fracción IV CCo. como el medio de distribución de los certificados emitidos por un PSC, de manera que esto revela la íntima relación entre el servicio de directorios y la hipótesis en estudio.

Hecha esta prevención, debemos insistir que, lo esencial para la hipótesis que estamos tratando es el hecho de que la emisión de certificados erróneos surge por la recopilación y comprobación negligente de los datos identificativos y/o de atributos de los solicitantes.

La responsabilidad por la emisión de certificados erróneos, puede tener origen en circunstancias previas a la emisión del certificado o con posterioridad a la misma. Respecto del momento que se trate, estamos en presencia de dos servicios distintos.

En el primer caso estamos en presencia del servicio de registro, mientras que en el segundo, se presenta el servicio de modificación de datos del certificado, por lo que trataremos por separado dichos momentos:

4.2.2.1.1 Por circunstancias previas a la emisión del certificado (Registro de los datos personales del solicitante del certificado digital)

Nos estamos refiriendo al instante en que una persona solicita a un PSC la emisión de un certificado y en que el PSC deberá comprobar la información proporcionada por el solicitante, es decir, hacemos alusión al servicio de registro de los futuros titulares de certificados electrónicos.

Este servicio es una de las formas en que se puede configurar la hipótesis de emisión de certificados erróneos, debido a que los datos recopilados en el servicio de registro de solicitantes de un certificado son los que se expresarán posteriormente al momento de emitir el certificado electrónico.

De este servicio, se deriva la obligación de verificar los datos identificativos o de atributos del solicitante, mismos que se contendrán en el certificado. Dentro de esta obligación se comprende el comprobar la identidad del solicitante, como también la comprobación de la veracidad de los datos suministrados por el solicitante, puesto que éste puede identificarse con documentos falsos con la intención de suplantar a otra persona.

Al respecto, cabe destacar que al PSC se le atribuiría una responsabilidad por incumplimiento a lo estipulado en el contrato (responsabilidad contractual), en cuanto a la correcta comprobación de la identidad del solicitante del certificado electrónico, no obstante, con independencia de lo anterior estamos también ante una responsabilidad penal por parte del solicitante, quien de acuerdo a lo dispuesto por el artículo 244 del Código Penal Federal (CPF), estará incurriendo en el delito de falsificación de documentos.

> **"Artículo 244 CPF**.- El delito de falsificación de documentos se comete por alguno de los medios siguientes:
> **V.-** Atribuyéndose el que extiende el documento, o atribuyendo a la persona en cuyo nombre lo hace: un nombre o una investidura, calidad o circunstancia que no tenga y que sea necesaria para la validez del acto;
> **VIII.-** Expidiendo un testimonio supuesto de documentos que no existen; dándolo de otro existente que carece de los requisitos legales, suponiendo falsamente que los tiene; o de otro que no carece de ellos, pero agregando o suprimiendo en la copia algo que importe una variación substancia".

En efecto, un PSC está obligado a comprobar fehacientemente la identidad del solicitante, de manera que para ello, debe requerir la comparecencia personal y directa del solicitante o de su representante legal si se tratare de una persona jurídica. En caso de no cumplir con esta obligación, esto es, que el PSC no compruebe fehacientemente la identidad del solicitante, compruebe negligentemente su identidad, no requiera la comparecencia personal del interesado o

su representante en caso de ser una persona jurídica, estamos frente a una situación que puede generar daños por la falsedad de los datos contenidos en el certificado en la medida que dichos hechos sean imputables al PSC.

Por otra pare, es necesario observar lo que ha establecido el PSC en sus prácticas de certificación, de las cuales se derivarán sus obligaciones. De esta manera, si un PSC tiene la obligación de comprobar la veracidad de los datos contenidos en el certificado, en particular, la identidad del titular de un certificado, el PSC compromete su responsabilidad si ha actuado dolosa o negligentemente al comprobar los datos del titular al momento de la solicitud del certificado.

Lo antes señalado, es sin perjuicio de la responsabilidad civil que le compete al titular, quien, conforme al art 99 fr. III del CCo. está en la obligación de dar declaraciones exactas y completas respecto de los datos de su identidad personal u otras circunstancias objeto de certificación. La apreciación de esta circunstancia podría ser relevante al momento de justificar la responsabilidad del PSC, esto porque la calidad de la falsificación puede ser tal que exceda la debida diligencia del PSC, además, este acto doloso hace que el uso del certificado constituya un uso fraudulento por parte del titular.

Asimismo, una vez verificados los datos del solicitante y aprobada la emisión del certificado, el PSC remite una copia del certificado al solicitante para que ratifique su contenido manifestando conformidad en el contrato de aceptación del certificado, momento a partir del cual comienza la relación jurídica con el PSC.

Al aceptar el contenido del certificado, el titular tuvo la oportunidad de detectar las inexactitudes de los datos verificados por el PSC, lo que exime de responsabilidad al PSC respecto del titular en caso de que él mismo haya confirmado el contenido del certificado con datos erróneos, debido a que éste necesariamente actuó dolosamente, por ejemplo, el titular del certificado se percató del error pero deliberadamente no manifestó dicha circunstancia o no fue diligente en revisar el contenido del certificado remitido por el PSC.

En lo que respecta al tercero que confía en el certificado cabe anotar que, al confiar en un certificado con datos erróneos, podría configurarse algún perjuicio derivado de la falsa identidad o atributo del titular del certificado, por ejemplo, el tercero que confía en el certificado podría resultar engañado por confiar en un certificado falso como consecuencia de actuaciones del suscriptor quien podría proporcionar datos falsos al PSC, o suplantar la personalidad de un tercero.

Por último, frente a estos servicios proporcionados por el PSC, se pueden derivar perjuicios en contra de terceros, distintos del tercero que confía en el certificado, por ejemplo, aquella a la

que ha suplantado el suscriptor, que también resulte perjudicada por el certificado falso, por daños en su prestigio personal o profesional, gastos de abogados, etc. En dicho caso, esta persona puede actuar contra el suscriptor y, en su caso, en contra del PSC.

Por otra parte, es importante analizar a continuación una hipótesis que podría suscitarse en torno al registro de los solicitantes, nos referimos al hecho de que en dicho servicio medien Entidades Registradoras (ER) o Agentes Certificadores (AR) que se encarguen de la recopilación y verificación de datos del solicitante.

Ante el caso de que producto de su dolo o negligencia haya provocando que el PSC emita certificados con datos erróneos ¿quién debe responder civilmente por la emisión de certificados erróneos frente al suscriptor y terceros?, ¿el PSC o la ER?

Si bien es cierto, la función de la certificación es generar confianza en las transacciones electrónicas, dado que los PSC proveen de confianza de la veracidad de sus certificados conforme a sus prácticas de certificación, son ellos quienes deben hacerse responsables por la falsedad de los certificados que emiten. Sin embargo, ello no obsta a que el PSC posteriormente se dirija en contra de la Entidad registradora por los perjuicios que ha enfrentado al responder pecuniariamente por un hecho ajeno.

4.2.2.1.2 Por circunstancias posteriores a la emisión del certificado (Actualización de los certificados)

En este supuesto, nos encontramos ante las posibles responsabilidades derivadas del servicio de actualización de certificados, en dicho caso, estamos frente a un certificado que ha sido emitido y publicado válidamente, el cual surte todos sus efectos, y que cumple con el requerimiento jurídico de la autenticación de las partes, sin embargo, en esta circunstancia los datos identificativos o de atributos que se certifican han cambiado, por ejemplo, los poderes para representar a una persona jurídica han sido revocados respecto de la persona que consta con dichos poderes en el certificado emitido por el PSC.

Antes del aviso de modificación de datos, el perjuicio que se pudiera derivar de esta omisión es en principio imputable al titular del certificado ya que es él quien debe actuar con la debida diligencia, para que todas las declaraciones que haya hecho en relación con el certificado sean exactas.

Sin embargo, una vez que el PSC ha recibido la solicitud de modificación de los datos contenidos en el certificado, la situación es distinta; al igual que en el servicio de registro, el PSC o

el Agente registrador deberá comprobar la identidad del usuario que solicita el servicio, revisar la veracidad de los datos que presenta para identificarse, comprobar que dicho cambio en los datos identificativos o de atributos del titular se han producido efectivamente, de lo cual responderá en los mismos términos que hemos señalado anteriormente.

No obstante lo anterior, existe una obligación adicional en este caso la cual es relevante frente a la hipótesis de responsabilidad por la emisión de un certificado erróneo, que permite diferenciarla en términos sustantivos del caso anterior. En efecto, en este caso, el certificado se haya emitido y publicado, lo que introduce la necesidad de que la modificación en ciertas circunstancias se haga de manera decisiva. Por ejemplo, si la ampliación de los poderes de representación de una persona no es consignada oportunamente después de efectuada la solicitud de modificación en un certificado de atributos, podrán derivarse perjuicios en contra del titular que, producto del retardo negligente del PSC en la modificación, no pudo celebrar un contrato electrónico dada la negativa de la contraparte de celebrarlo porque en el certificado no constaban los poderes de representación para efectuar la operación, lo cual obligó al titular a viajar al lugar físico donde se encontraba la contraparte para celebrar tal contrato físicamente, con los gastos que implica aquello: pasajes, habitación, alimentos, etc.

Respecto del sujeto activo de la acción de indemnización de perjuicios, puede ser el titular del certificado, los terceros que confían en el certificado, o incluso otros terceros, en términos análogos a las hipótesis de responsabilidad derivadas del servicio de registro detallado con anterioridad.

4.2.2.2 Responsabilidad derivada de la publicación de los certificados en los servicios de directorio

Al tratar la hipótesis de responsabilidad derivada de la emisión de certificados erróneos, consignamos el hecho de que la responsabilidad derivada de este hecho se podía configurar solamente si dichos certificados fueron publicados en el directorio de certificados. Con ello, resaltamos que en la hipótesis de responsabilidad detallada mediaba necesariamente el servicio de directorios, pero que, sin embargo, producto del servicio de directorios se podían configurar otras hipótesis de responsabilidad diversas a la emisión de certificados erróneos relacionados con la gestión de los servicios de registro de solicitantes de un certificado y el servicio de modificación de datos. Son éstas las que veremos a continuación.

La presente hipótesis de responsabilidad, parte de la base que el PSC ha emitido y publicado certificados que no contienen datos erróneos, pero que producto de otros actos u omisiones, dolosas o negligentes del PSC, produce perjuicios a una persona en razón de las

condiciones de seguridad en que debe ser mantenido el servicio de directorios para que sea un medio eficaz, fiable y seguro de distribución de certificados.

En efecto, la seguridad en la conservación de información veraz, la cual será de acceso público, es de vital trascendencia en el sistema de distribución de certificados, ello porque dicha publicación de directorios se hace por medios electrónicos lo que los hace blancos de “ataques” de terceros, con lo cual se puede alterar su contenido, perdiendo la concordancia con los datos que efectivamente contenían los certificados al momento de su emisión o modificación, por ejemplo, el directorio de certificados es alterado por un tercero, quien modifica los datos de un usuario “A”, cambiándolo por la identidad de un tercero “B” lo que le impide efectuar alguna transacción comercial o que producto del mismo ataque se defrauda a un tercero que razonablemente confiaría en un certificado publicado quien contrata con el usuario en atención de tratarse de “B”.

Ahora, en caso de que el PSC haya sido negligente en el mantenimiento y actualización de los mecanismos de seguridad destinados a repeler los ataques de terceros o lisa y llanamente, haya dolosamente permitido la intromisión de éste, debemos concluir que el PSC es responsable civilmente por los daños que se deriven producto del cambio de dichos datos.

Como se advierte, esta hipótesis de responsabilidad se asemeja a las anteriores en la medida de que afecta la veracidad de los certificados, pero que a diferencia de los casos anteriores, la falta de veracidad de dichos certificados es posterior al ingreso de los datos identificativos del titular del certificado y producto de la intromisión de terceros en el servicio de directorios.

Cabe señalar que, la seguridad del sistema de certificados emitidos por el PSC se haya respaldada por la firma electrónica del PSC que se adjunta al certificado, lo cual dificulta que un atacante logre falsificar por completo el certificado, en particular la firma electrónica de PSC, la cual garantiza la integridad del certificado. De hecho, el éxito a este ataque se hace aún más improbable en caso de que la firma del PSC se halle a su vez certificada por una Autoridad Certificada, es decir, la Secretaría de Economía.

Las Reglas generales a las que deberán sujetarse los Prestadores de Servicios de Certificación, prevé esta situación para los PSC acreditados, estableciendo para ellos una serie de obligaciones destinadas a que el PSC cuente con altos niveles de seguridad en la publicación de los certificados.

De esta manera, para que un PSC pueda ser acreditado deberá demostrar que posee los mecanismos técnicos que garanticen la debida seguridad del servicio de directorios frente a ataques de terceros.

En lo relativo al sujeto activo podrán serlo tanto el titular del certificado, el tercero que confía en el certificado, como también un tercero diverso del anterior.

- Respecto de el titular del certificado, podrá verse afectado dado que la integridad del certificado que utiliza para identificarse ha sido alterado, lo cual le impediría en ciertos casos celebrar alguna operación, por ejemplo, el usuario “A”, producto de la alteración del certificado, no puede identificarse frente a terceros dado que la identidad que figura en el certificado es de una persona “B”, lo cual le impide celebrar alguna transacción electrónica.
- Por su parte, el tercero que confía en el certificado puede sufrir también una serie de perjuicios al confiar razonablemente en el certificado, por ejemplo, el tercero cree contratar con un usuario “A”, pero en realidad ha sido defraudado producto de que la identidad que se consignaba en el certificado era falsa.

4.2.2.3 Responsabilidad derivada de los servicios de revocación de los certificados

El presente apartado constituye la parte medular de nuestro trabajo, de manera que tras haber realizado un análisis de la figura del Prestador de Servicios de Certificación ahora nos centraremos en la responsabilidad civil que puede derivarse de la revocación de un certificado electrónico.

La hipótesis de responsabilidad en estudio se funda en la circunstancia de que el titular del certificado ha perdido el exclusivo control de los medios de creación de su firma electrónica, a la cual certifica el PSC, y éste ejecutando este servicio dolosa o negligentemente, ha permitido que un tercero intruso haya utilizado la firma del titular del certificado, perjudicando con ello a una persona.

Como hemos visto, la función del certificado es dar certeza de la identidad de la persona que emite un mensaje. En el caso de la firma electrónica, el certificado electrónico opera como un modo de distribución seguro de la clave pública de la firma del emisor. En el certificado se provee de certeza de que el par de claves están bajo el control exclusivo del titular y de la correspondencia de la clave pública con la clave privada lo que permite identificar (autenticar) a la persona que firma, así como otros atributos que posea.

Cabe señalar que, el sistema de seguridad en que interactúan la firma electrónica y el certificado electrónico se basa en que la clave privada del emisor se halle bajo su exclusivo control, permitiendo que únicamente éste sea la persona posibilitada de emitir la firma certificada. En caso de perderse dicho control exclusivo (sea por extravío, robo, creación de un par de llaves de una firma poco segura, etc.), el sistema cae debido que existe la posibilidad de que un tercero pueda hacer uso de la clave privada, suplantando la identidad del usuario, derivándose así graves daños al titular y terceros que confían en el certificado. De esta manera, el certificado deja de proveer de certeza jurídica respecto de la identidad de las personas, toda vez que la relación exclusiva entre un par de claves con determinada persona deja ser de hecho efectiva; de aquí surge la necesidad del sistema de revocación de certificados como un medio de hacer frente a estos hechos, privando de validez al certificado.

Esta hipótesis se encuentra prevista en el ya citado artículo 109 fracción II del CCo, en el que el PSC procede a revocar un certificado previa solicitud del firmante, o por la persona física o moral representada por éste o por un tercero autorizado. Ahora bien, la motivación de esta solicitud puede deberse a la pérdida del control exclusivo de la clave privada.

Por su parte, el artículo 99 fracción I del CCo, dispone que el firmante deberá actuar con la debida diligencia y establecer los medios razonables para evitar la utilización no autorizada de los datos de creación de la firma.

De manera que, un supuesto de responsabilidad especialmente complejo y problemático es el derivado de la revocación de un certificado, lo que plantea la necesidad de delimitar y atribuir responsabilidades a los distintos sujetos implicados (PSC, titular del certificado y tercero usuario que confía en el mismo) en las distintas fases del proceso de revocación.

La emisión, distribución y uso de un certificado, junto con la eventual revocación o suspensión del mismo, hasta su expiración, generan unas relaciones de naturaleza contractual o extracontractual, entre los diversos sujetos implicados, que plantean la necesidad de establecer, delimitar y clarificar sus respectivos derechos, obligaciones y cargas, así como sus eventuales responsabilidades.

Se trata de una cuestión de esencial importancia y, sin embargo, confusa en la fase inicial de desarrollo, comercial y legal de los PSC, pues plantea numerosas cuestiones tales como la naturaleza de la responsabilidad, los sujetos frente a los que responde, la eventual existencia de limitaciones de uso, garantías de responsabilidad, etc.

Ciertamente, el tema de las responsabilidades derivadas de las prácticas de los Prestadores de Servicios de Certificación es una cuestión esencial, pues los titulares y los usuarios de certificados, especialmente si son consumidores, no pueden participar en un mercado cuyas condiciones económicas y legales no son claras, y de igual forma, tampoco lo harán las empresas.

De ahí la necesidad de establecer y delimitar claramente el régimen de responsabilidad derivado de la emisión y utilización de certificados, teniendo en cuenta que la clarificación de derechos, obligaciones y responsabilidades debería servir a los intereses de todas las partes implicadas en el comercio electrónico, no sólo los del PSC, sino también los del titular y el tercero usuario del certificado.

Al respecto, el núcleo principal de la regulación de la responsabilidad del PSC se encuentra en el art. 104 del CCo. el cual enlista una serie de obligaciones propiamente derivadas de la actividad de certificación del PSC, las cuales a saber son las siguientes:

Artículo 104.- Los Prestadores de Servicios de Certificación deben cumplir las siguientes obligaciones:

1) Comprobar por sí o por medio de una persona física o moral que actúe en nombre y por cuenta suyos, la identidad de los solicitantes y cualesquiera circunstancias pertinentes para la emisión de los Certificados, utilizando cualquiera de los medios admitidos en derecho, siempre y cuando sean previamente notificados al solicitante;
2) Poner a disposición del Firmante los dispositivos de generación de los Datos de Creación y de verificación de la Firma Electrónica;
3) Informar, antes de la emisión de un Certificado, a la persona que solicite sus servicios, de su precio, de las condiciones precisas para la utilización del Certificado, de sus limitaciones de uso y, en su caso, de la forma en que garantiza su posible responsabilidad;
4) Mantener un registro de Certificados, en el que quedará constancia de los emitidos y figurarán las circunstancias que afecten a la suspensión, pérdida o terminación de vigencia de sus efectos. A dicho registro podrá accederse por medios electrónicos, ópticos o de cualquier otra tecnología y su contenido público estará a disposición de las personas que lo soliciten, el contenido privado estará a disposición del Destinatario y de las personas que lo soliciten cuando así lo autorice el Firmante, así como en los casos a que se refieran las reglas generales que al efecto establezca la Secretaría;
5) Guardar confidencialidad respecto a la información que haya recibido para la prestación del servicio de certificación;
6) En el caso de cesar en su actividad, los Prestadores de Servicios de Certificación deberán comunicarlo a la Secretaría a fin de determinar, conforme a lo establecido en las reglas generales expedidas, el destino que se dará a sus registros y archivos;

7) Asegurar las medidas para evitar la alteración de los Certificados y mantener la confidencialidad de los datos en el proceso de generación de los Datos de Creación de la Firma Electrónica;
8) Establecer declaraciones sobre sus normas y prácticas, las cuales harán del conocimiento del usuario y el Destinatario, y
9) Proporcionar medios de acceso que permitan a la Parte que Confía en el Certificado determinar:
   a) La identidad del Prestador de Servicios de Certificación;
   b) Que el Firmante nombrado en el Certificado tenía bajo su control el dispositivo y los Datos de Creación de la Firma en el momento en que se expidió el Certificado;
   c) Que los Datos de Creación de la Firma eran válidos en la fecha en que se expidió el Certificado;
   d) El método utilizado para identificar al Firmante;
   e) Cualquier limitación en los fines o el valor respecto de los cuales puedan utilizarse los Datos de Creación de la Firma o el Certificado;
   f) Cualquier limitación en cuanto al ámbito o el alcance de la responsabilidad indicada por el Prestador de Servicios de Certificación;
   g) Si existe un medio para que el Firmante dé aviso al Prestador de Servicios de Certificación de que los Datos de Creación de la Firma han sido de alguna manera controvertidos, y
   h) Si se ofrece un servicio de terminación de vigencia del Certificado.

Lo anterior con relación en los arts. 110 y 111 del CCo., que señalan:

Artículo 110.- El Prestador de Servicios de Certificación que incumpla con las obligaciones que se le imponen en el presente Capítulo, previa garantía de audiencia, y mediante resolución debidamente fundada y motivada, tomando en cuenta la gravedad de la situación y reincidencia, podrá ser sancionado por la Secretaría con suspensión temporal o definitiva de sus funciones. Este procedimiento tendrá lugar conforme a la Ley Federal de Procedimiento Administrativo.

Artículo 111.- Las sanciones que se señalan en este Capítulo se aplicarán sin perjuicio de la responsabilidad civil o penal y de las penas que correspondan a los delitos en que, en su caso, incurran los infractores.

Es así que, el régimen general de responsabilidad de todo prestador de servicios de certificación se deriva de la falta de observancia a lo dispuesto por referido art. 104 del CCo.

Por otra parte el art. 13 del Reglamento al Código de Comercio en materia de Prestadores de Servicios de Certificación señala que la fianza que otorgue el Prestador de Servicios de

Certificación, se podrá hacer efectiva, cuando éste cause daños o perjuicios a los usuarios de sus servicios por incumplimiento de sus obligaciones o por el indebido desempeño de sus funciones. Su monto también se aplicará para cubrir los gastos que erogue la Secretaría, por actuar en sustitución del Prestador de Servicios de Certificación, cuando éste sea suspendido, inhabilitado o cancelado en su ejercicio.

Como es sabido, la revocación de un certificado tiene su origen en la puesta en peligro de la clave privada, normalmente en caso de pérdida o extravío de la misma, lo cual exige la finalización anticipada del periodo de validez del certificado, pues es posible el uso ilegítimo de la clave de la firma por parte de un tercero que, en principio, en virtud de la apariencia generada por el certificado, serían atribuidos al titular del mismo, ocasionando un serie de obligaciones que se atribuirían al titular del certificado.

Desde el punto de vista técnico, el PSC tiene la obligación de contar con un sistema de revocación seguro e inmediato, no obstante, en el ámbito jurídico existe la necesidad de delimitar los derechos, obligaciones, cargas y responsabilidades de las distintas personas implicadas, en el supuesto de que durante la revocación surjan otros eventos que causen daños y perjuicios a las partes.

Como es sabido, el efecto de la revocación es que el certificado revocado deviene inválido de forma anticipada, de manera que la invalidez anticipada de un certificado por revocación del mismo implica el desarrollo temporal de una serie de hechos y acciones, desde la puesta en peligro, en su caso, de la clave privada (causa fundamental de revocación), hasta el conocimiento por parte de terceros del hecho de la revocación.

Estas diversas fases del desarrollo temporal del proceso de revocación, inevitables desde el punto de vista material, por razones físicas y técnicas, plantean, desde el punto de vista jurídico, importantes e interesantes interrogantes respecto de la responsabilidad de los distintos sujetos implicados (titular, entidad y terceros) en los diversos periodos del mismo.

Pues, en efecto, si el certificado es utilizado en algún momento después de la puesta en peligro de la correspondiente clave privada, para verificar una firma electrónica, esa clave privada puede no estar ya bajo el control de la parte (el titular legítimo) que el usuario del certificado cree y espera conforme al contenido inicial del certificado, sino que puede que se encuentre en manos de un tercero que haga de ella un mal uso, del que podrían derivarse importantes perjuicios para el usuario del certificado y/o el legítimo titular de la clave privada.

La cuestión es quién acaba asumiendo o respondiendo por esos perjuicios, pues podría tener que asumirlos el tercero que confía en el certificado, o bien podría responsabilizarse al legítimo titular de la clave privada (el titular del certificado), o incluso a la propia entidad de certificación. La determinación de la responsabilidad no es cuestión nada fácil, especialmente desde el momento en que las situaciones de las diferentes partes cambian en los diversos momentos de proceso de revocación.

Supongamos que la revocación se produce por pérdida de la clave privada, ¿quién responde del mal uso de la clave privada antes de que nadie, ni siquiera el titular del certificado, tenga conocimiento del compromiso de la misma?, ¿y quién responde una vez que se ha pedido la revocación pero esta no ha sido recibida, confirmada, decidida o anunciada por la entidad de certificación?

La revocación de un certificado en la hipótesis que estudiamos consta de una serie de momentos, los cuales son relevantes a fin de distribuir las responsabilidades, dado que, no en todos los instantes es el PSC responsable civilmente por el servicio de revocación.

Dichas etapas pueden resumirse de la siguiente manera:

4.2.2.3.1 La seguridad de la clave se ha visto comprometida y es utilizada por un tercero, para suplantar al suscriptor, quie todavía no conoce del peligro, o conociéndolo todavía no lo ha notificado al PSC, solicitando la revocación del certificado

En este momento, parece razonable sostener que el PSC no debe responder civilmente de los perjuicios que se produzcan al tercero que confía en el certificado o al mimo titular, dado que aún no se haya en condiciones de prestar el servicio de revocación debido a que desconoce de la puesta en peligro de la clave, de manera que no se puede esperar en ese momento actuación alguna por parte del PSC, en la medida en que aún no se le ha solicitado la revocación, por lo que la responsabilidad en este caso será en principio del titular del certificado electrónico.

Del tercero que confía en el certificado no se puede esperar ni presumir que conozca la puesta en peligro de la clave privada, por lo que la revocación no sólo no ha sido publicada, sino que ni siquiera ha sido decidida por la entidad de certificación e incluso puede que la puesta en peligro de la clave privada que la motiva no sea conocida todavía por el titular del certificado.

No parece razonable oponer a los terceros que confían con el certificado una circunstancia que no ha provocado todavía la revocación del correspondiente certificado. Este principio doctrinal encuentra respaldo legal en el ya citado art. 104 fracción IV del CCo., el cual dispone que el PSC

tendrá por obligación “Mantener un registro de Certificados, en el que quedará constancia de los emitidos y figurarán las circunstancias que afecten a la suspensión, pérdida o terminación de vigencia de sus efectos. A dicho registro podrá accederse por medios electrónicos, ópticos o de cualquier otra tecnología y su contenido público estará a disposición de las personas que lo soliciten, el contenido privado estará a disposición del Destinatario y de las personas que lo soliciten cuando así lo autorice el Firmante, así como en los casos a que se refieran las reglas generales que al efecto establezca la Secretaría”.

Por tanto, la simple puesta en peligro no tiene efectos frente a terceros, es necesaria no sólo la comunicación a la entidad certificadora sino la publicación de la revocación para que esta sea oponible.

De esta forma, la solución del art. 104 fracción IV del CCo. da respaldo legal a la consideración de que los sistemas de comunicación de revocación no han de tener una función meramente informativa, sino que, si se pretende que introduzcan seguridad en el sistema de certificados, la suya ha de ser una función informativa cualificada, de la que se puedan derivar determinados efectos jurídicos en función de la apariencia así generada, pues la responsabilidad de la entidad de certificación frente a terceros tiene también su origen y fundamento en la apariencia creada por ella y en la que aquellos confían.

4.2.2.3.2 El PSC ha recibido la solicitud de revocación, sin embargo, en el periodo que medía entre la verificación de la solicitud de revocación y la adopción de ésta por parte del PSC, un tercero suplanta al titular del certificado, realizando múltiples operaciones

En este momento, una vez que ha tenido conocimiento de la puesta en peligro de la clave privada, el titular del certificado solicita al PSC la revocación de su clave comprometida, sin embargo, un tercero la utiliza, suplantando al suscriptor, durante el periodo que media entre la petición de revocación del suscriptor, la adopción de ésta y la eliminación del registro de certificados válidamente emitidos por el PSC.

Cabe notar que, en el periodo en que el PSC decide revocar y eliminar el certificado de la firma comprometida del registro de certificados válidamente emitidos, el tercero que suplanta al titular del certificado puede realizar múltiples operaciones provocando graves perjuicios al titular mismo y a los terceros que confían en el certificado. Incluso, por más diligente y rápido que sea el PSC en la revocación del certificado, existirá necesariamente un lapso en el que el tercero intruso pueda causar dichos perjuicios.

Por ejemplo, si el servicio de revocación se realiza en una hora desde la solicitud de revocación (lo que demuestra un servicio sorprendentemente eficiente) el tercero cuenta con ese lapso para provocar fraudes y perjuicios con la suplantación del titular del certificado.

En esta hipótesis, es admisible concluir que el PSC es civilmente responsable frente al usuario y el tercero que confía en el certificado, por las actuaciones dolosas o negligentes al momento de prestar el servicio de revocación, sin embargo, a fin de determinar las posibles responsabilidades que el PSC debiera soportar, es importante tener en cuenta dos factores:

1. La relación con la verificación de la identidad del solicitante de la revocación. En efecto, lo primero que el PSC debe efectuar es dicha verificación dado que es posible que dicha solicitud sea falsa, por ejemplo, la persona que efectúa la solicitud no sea efectivamente el titular del certificado, lo cual produce perjuicios al titular como consecuencia de la revocación de su certificado.
2. El segundo factor que debe considerase es la rapidez con el cual el PSC debe dar curso a la revocación y eliminación del registro de certificados válidamente emitidos; este hecho, permitirá determinar al juez si el PSC fue o no lo suficientemente diligente al prestar este servicio. Lo anterior no obsta a que el PSC se comprometa a ciertos estándares de rapidez en la revocación, lo cual ciertamente facilitará la función del juez.

Creemos que estos factores se deben apreciar de la misma manera en que tratamos al ver la responsabilidad derivada de la emisión de certificados erróneos, sin perjuicio de que la urgencia en este caso pueda apreciarse más estrictamente dado lo sensible que es el tiempo en esta hipótesis.

Se trata, por tanto, de distribuir el riesgo entre el titular del certificado y la entidad certificadora. En principio, el titular, como hemos visto en el periodo anterior, asume, de entrada, la responsabilidad derivada del mal uso de la clave privada, de forma similar al titular de una tarjeta de crédito. No obstante, igual que en el sistema de tarjetas de crédito, el titular del certificado habría de poder liberarse de esa responsabilidad procediendo a comunicar la pérdida a la entidad de certificación y solicitando la revocación del certificado.

Ello sería una carga del titular, una actuación que ha realizar si quiere liberarse de esa responsabilidad inicial, trasladándola al PSC; en caso contrario, deberá asumir las consecuencias que por falta de actuación se deriven, es decir, seguirá siendo responsable del posible mal uso de la clave privada. El problema que se plantea es que, entre la comunicación y la revocación efectiva (y su publicación) existe, inevitablemente, un periodo temporal más o menos largo, que provoca la incertidumbre de quién responde durante el mismo.

Es, en suma, el problema de determinar en qué momento exactamente el titular se libera de su responsabilidad inicial y la traslada al PSC, problema también existente, aunque quizás no de forma tan acusada, en el sistema de tarjetas de crédito. Pues téngase en cuenta, en efecto, que una vez recibida la correspondiente solicitud, es imprescindible que la entidad de certificación confirme la solicitud de revocación, por lo que inevitablemente transcurrirá un intervalo materialmente inevitable entre la recepción de la solicitud y la decisión de revocación, y entre la decisión y la efectiva publicación de la revocación.

Las soluciones posibles al respecto son diversas: en principio, cabe optar por que el responsable sea el titular, que no se vería liberado de responsabilidad hasta la publicación de la revocación; puede optarse por considerar más razonable que sea la entidad de certificación la que afronte el mayor riesgo por mal uso de la clave privada durante este periodo; o bien cabe considerar como elemento clave si la entidad de certificación actuó con la celeridad necesaria, cuestión que dependería de los usos del comercio, pero que es difícil cuando no hay usos y la tecnología varía rápidamente.

La mayoría de iniciativas legislativas en la materia no resuelven de forma correcta el tema de la distribución de riesgos durante el proceso de revocación del certificado. En algunos casos no abordan la cuestión, y si lo hacen parecen limitarse a la distribución de riesgos frente a terceros (que aparece conectada a la efectiva publicación de la revocación), pero no a la cuestión de la transmisión del riesgo entre titular y entidad de certificación, que prácticamente no ha sido contemplada.

Por su parte, la Ley de Utah (Utah Digital Signature Act), en su art. 46-3-307 2) "Revocación de un certificado" establece que "una autoridad de certificación con licencia confirmará la petición de revocación y revocará el certificado dentro del día hábil siguiente después de recibir tanto la petición escrita del suscriptor como una evidencia razonablemente suficiente para confirmar la identidad y la representación de la persona solicitante". Conforme al art. 46-3-307 6), dos días después de que el suscriptor solicite la revocación por escrito y proporcione a la autoridad de certificación emisora información razonablemente suficiente para confirmar la petición, y pague cualquier tasa requerida contractualmente, se producirán los efectos de la revocación, cabe entender también que frente a terceros.

El art. 46-3-307 2) establece, por tanto, un plazo de un día para que la autoridad de certificación proceda a revocar un certificado, y el art. 46-3-307 6) establece un periodo de dos días para la revocación de un certificado electrónico.

No obstante, obsérvese que del tenor literal de estos preceptos parece desprenderse que el cómputo del plazo de un día (o, en su caso, de dos) no es desde la recepción de la petición sino desde la confirmación de la petición por parte de la autoridad, y la aportación de pruebas para esa confirmación parece configurarse además como una carga del solicitante. De forma que, en caso de que la autoridad de certificación no reciba evidencias razonablemente suficientes para la confirmación de la identidad del solicitante, no se iniciará el cómputo del plazo de un día, ni tampoco el de dos, previsto en los arts. 46-3-307 (2 y 46-3-307 (6 como solución a la falta de celeridad de las entidades de certificación, con lo que puede dilatarse excesivamente, e incluso indefinidamente, la decisión de revocación efectiva.

En suma, las distintas soluciones y propuestas legislativas intentan resolver esta cuestión exigiendo genéricamente diligencia en la actuación de la entidad de certificación, una vez recibida la petición de revocación, con el problema de determinar entonces cuando existe esa diligencia, cuestión que habría de resolverse según los usos que se vayan estableciendo y teniendo en cuenta la evolución de la tecnología, llegando incluso en algunos casos (Utah) a concretar un plazo temporal transcurrido el cual se traslada a la entidad de certificación la responsabilidad, de forma que, mientras tanto, sigue asumiendo la responsabilidad el titular.

No obstante, entendemos que, en la zona de penumbra planteada en este periodo, cabrían otras soluciones más satisfactorias, a las que podrían llegar las partes implicadas por la vía contractual, y entendiendo por ello cualquier norma legal al respecto de naturaleza dispositiva. Pues téngase en cuenta que en el intervalo físicamente inevitable entre la recepción de la solicitud y la decisión de revocación, durante el que se debe confirmar la petición, cabe entender que la entidad de certificación, mientras actúe diligentemente, quizá no sea la que deba asumir todavía el riesgo, aunque parece que tampoco deba serlo el titular, que ha actuado diligentemente solicitando la revocación, por lo que quizá sería uno de los supuestos adecuados para establecer *una responsabilidad mancomunada..*

4.2.2.3.3 Efectiva revocación y eliminación de certificados en el directorio de certificados

En este periodo, el PSC ha procedido a revocar el certificado, pero dado el sistema de comunicación a los terceros que confían en el certificado, puede acontecer que éstos aún no tengan conocimiento de la revocación y eliminación del certificado de las listas de certificados válidamente emitidos. Esto nos obliga a estudiar los sistemas de comunicación que puede adoptar el PSC.

1. Sistema de comunicación periódica de revocaciones (renovaciones periódicas de las listas de certificado válidamente emitidas).

En este sistema, las listas de certificados válidamente emitidas se van renovando cada cierto tiempo, en dicho caso, el tercero que confía en el certificado no conocerá de la revocación hasta que se efectúe la eliminación del certificado, lo cual será hasta la siguiente renovación periódica de la lista de certificados válidamente emitidos.

Es así que, la revocación es solamente oponible al tercero que confía en el certificado cuando ha sido removido de las listas de certificados válidamente emitidos. Como ello aún no ha ocurrido, un tercero podría verse perjudicado al confinar de buena fe en un certificado pudiendo exigir al PSC las indemnizaciones pertinentes.

2. Sistema de revocación inmediata (Sistema de renovación inmediata de las listas de certificados válidamente emitidos)

En este caso, el PSC habiendo adoptado la decisión de revocar el certificado y eliminar el certificado de la lista, procede inmediatamente a renovar y publicar la nueva lista de certificados válidamente emitidos habiendo eliminado el certificado revocado, a partir de ahí, la revocación se hace oponible a terceros, de manera que quien confíe en el certificado posteriormente lo hará bajo su propio riesgo.

Si se opta por este sistema de comunicación de las revocaciones, desaparece el lapso de tiempo que estamos tratando, por lo que la hipótesis de responsabilidad para este lapso temporal se limita al sistema de renovación periódica de las listas de certificado válidamente emitidos.

En definitiva, para determinar la responsabilidad del PSC habrá de estarse primeramente a dilucidar el modelo de comunicación de los certificados por el cual se regula el PSC, sólo siendo procedente una hipótesis de responsabilidad en este periodo bajo el modelo de renovación periódica de certificados válidamente emitidos. Ahora, el PSC se hace responsable únicamente en el caso de que, producto del retardo doloso o culpable de la renovación periódica de los certificados en la cual se elimina el certificado revocado, se derivan perjuicios contra el titular del certificado (que obró diligentemente) o el tercero que confía, producto de las actuaciones de los terceros intrusos que se hayan en control de la firma del titular.

a) El certificado revocado ha sido efectivamente eliminado del directorio de certificados válidamente emitidos.

En este último periodo debe descartarse toda clase de responsabilidad por parte del PSC, dado que el certificado ha dejado de ser confiable y es oponible a terceros, por lo que el riesgo de

asumir daños se traslada a los propios terceros que negligentemente confíen en un certificado de esta clase.

Respecto del sujeto activo de la acción de indemnización de perjuicios en las hipótesis descritas, debemos concluir que podrán ser el titular del certificado y el tercero que confía en el certificado. Sin embargo, la titularidad de dicha acción variará según el momento en que se halle la revocación. De esta manera, el titular del certificado no podrá ejercer esta acción en el periodo que abarca entre la pérdida del control exclusivo de la clave privada y la solicitud de revocación. Por otra parte, debe descartarse al titular del certificado así como al tercero que confía para que puedan dirigirse contra el PSC una vez que éste ha procedido a eliminar el certificado revocado de la lista de los certificados válidamente emitidos.

4.2.2.3.4 Necesidad de la existencia de un servicio de sellado digital de tiempo, para distribuir las responsabilidades en la revocación de los certificados

Hemos señalado que, el problema temporal en la revocación reviste especial trascendencia al momento de determinar las responsabilidades de los actores implicados en la revocación de un certificado ya que como hemos visto, las responsabilidades se van distribuyendo conforme a los periodos en que se divide la revocación.

En efecto, no es la misma responsabilidad la que asiste al PSC cuando el usuario ha perdido el control exclusivo de su clave, no comunicando aún de tal hecho al PSC, que cuando el PSC ha recibido la solicitud de revocación. Ahora, en caso de no sellarse temporalmente los mensajes firmados y certificados electrónicamente, es imposible acreditar con certeza qué mensajes fueron emitidos al momento previo de la solicitud de revocación y qué mensajes fueron emitidos con posterioridad a la solicitud de revocación, lo cual impide determinar quiénes son los llamados a responder civilmente.

Además, el sellado digital de tiempo es una herramienta fundamental para determinar la responsabilidad de las partes conforme al criterio de “perentoriedad”, ya que sin la existencia de un sellado digital de tiempo, se pone en serio riesgo a las partes implicadas (tanto el afectado como el PSC) de probar que el PSC ha obrado o no con debida diligencia.

Por otra parte, en caso de las responsabilidades que puede tener el usuario del certificado frente a terceros por los mensajes emitidos, es importante el Sellado Digital de tiempo para evitar responsabilidades por los contratos firmados con clave revocada dado que, éste al no tener medio para probar la fecha en que la oferta del contrato fue remitido, podría verse en la imposibilidad de demostrar que esta oferta fue no emitida por éste, para lo cual ciertamente serviría el hecho de

demostrar que en dicho instante el PSC había revocado el certificado que respaldaba su firma producto de que él había perdido el control exclusivo de su clave privada al momento en que se celebró tal contrato.

4.2.2.3.5 Obligación del PSC de informar a la Secretaría de Economía del cese voluntario de operaciones

Dicha obligación de informar a la Secretaría de Economía, acontece por tres situaciones, las cuales desarrollaremos a continuación:

a) En caso del cese voluntario de las actividades del PSC.

Esta obligación es contemplada por el art. 104 fracción VI del CCo., el cual prescribe que en caso de cesar en su actividad los Prestadores de Servicios de Certificación deberán comunicarlo a la Secretaría de Economía a fin de determinar conforme a lo establecido por las Reglas generales expedidas, el destino que se dará a sus registros y archivos.

Al respecto, en las Reglas generales, numeral 10, se. señala que el Prestador de Servicios de Certificación que en términos del artículo 104 fracción VI quiera cesar de manera voluntaria su actividad, previo pago de derechos, tiene que informar el motivo de dicho cese con cuarenta y cinco días de anticipación a la Secretaría de Economía a efecto de que la misma se cerciore que se ha cumplido con lo establecido en el artículo 16 del Reglamento del Código de Comercio en materia de prestadores de Servicios de Certificación y el apartado 5., 5.1. y 5.2. de las Reglas generales en cuanto a que el PSC deberá enviar en línea, mediante el procedimiento que establezcan las Reglas Generales que expida la Secretaría, una copia de cada certificado que generen.

De manera que, en el caso de cesar voluntariamente en su actividad, los Prestadores de Servicios de Certificación deberán comunicarlo previamente a la SE y deberán transferir los datos de sus certificados a otro Prestador de Servicios de Certificación, en la fecha en que el cese se produzca.

Esta obligación tiene por objeto que el titular del certificado tome las medidas pertinentes a fin de evitar que la cancelación del certificado le produzca perjuicios o decidir que su certificado sea traspasado a otro PSC. Al respecto analizaremos los siguientes puntos:

b) En caso de la cancelación de la acreditación e inscripción del prestador en el registro de prestadores acreditados

Esta obligación de informar es para los PSC acreditados que han perdido tal calidad, de manera que la cancelación de la acreditación e inscripción del PSC en el registro de prestadores acreditados como se advierte, es consecuencia de una serie de hechos graves que hacen que la prestación en las condiciones que requiere la ley para el PSC, han sido incumplidos.

c) En caso de suspensión del PSC

La trascendencia de la obligación de informar de la situación expuesta, se relaciona con el hecho de que el certificado pierde su validez anticipadamente (temporalmente en el caso de la suspensión).

De esta pérdida de validez, sea permanente o temporal, el usuario del certificado puede sufrir menoscabos en su patrimonio dado que el periodo de validez del certificado ha sido acortado por causas ajenas a la voluntad del titular, lo que importa en principio un incumplimiento negligente del contrato por parte del PSC. Asimismo, se hará responsable por la oportuna comunicación de las circunstancias aludidas, dentro de los plazos que para este efecto establece la ley a fin de que el titular pueda determinar el destino de su certificado en los dos primeros casos, o que esté al tanto del hecho de la suspensión para prever daños.

CONCLUSIONES Y PROPUESTA.

PRIMERA.- El Código de Comercio establece los requisitos que las personas deberán cumplir y someter a evaluación ante la Secretaría de Economía, con el propósito de que sus elementos humanos, materiales, económicos y tecnológicos sean adecuados para garantizar la prestación de sus servicios, así como la seguridad de la información y su confidencialidad, y cuyo cumplimiento implicaría la acreditación, por parte de la referida Autoridad, a través de la Dirección General de Normatividad Mercantil, como Prestador de Servicios de Certificación.

SEGUNDA.- Los cuerpos normativos que complementan al Código de Comercio en cuanto a la regulación de la figura del Prestador de Servicios de Certificación (PSC) son: el Reglamento al Código de Comercio en materia de Prestadores de Servicios de Certificación, las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación y la Norma Oficial NOM-151-CSFI–2002, Prácticas Comerciales – Requisitos que deben observarse para la conservación de mensajes de datos, de donde se derivan los fundamentos para la existencia de tres tipos de Prestadores de Servicios de Certificación, los cuales a sabes son: el PSC de firma electrónica, PSC para efectos de la NOM-151(conservación de mensajes de datos) y PSC de Sellado Digital de Tiempo (Timestamping Authority).

TERCERA.- Los principios fundamentales que imperarán en el uso las tecnologías de la información y comunicación serán el de neutralidad tecnológica, autonomía de las partes y equivalente funcional, figuras que permitirán la existencia de una armonización jurídica en cuanto al uso de los medios electrónicos, no sólo en el derecho doméstico sino también a nivel de derecho internacional.

La particularidad de estas tecnologías es que utilizan medios electrónicos y la Internet, constituyendo una herramienta ideal para realizar intercambios de todo tipo de información, es así que hoy en día es posible celebrar un acto jurídico a través de la transferencia de datos de un computador a otro sin necesidad de la utilización de documentos con soporte en papel, lo que ha contribuido a eliminar fronteras, ahorro de tiempo y dinero, esto gracias a la facilidad de acceso a los sitios web, permitiendo a los comerciantes y/o empresas llegar de manera eficaz al usuario final y éste a su vez podrá hacer un mejor comparativo de empresas y precios en el mercado.

CUARTA.- Aspectos como la forma escrita, la firma y original podrán ser representados mediante un mensaje de datos, al cual no se le podrá negar efectos jurídicos, validez o fuerza obligatoria, de acuerdo a lo establecido por el artículo 89 bis del Código de Comercio.

Al respecto, el concepto de “mensaje de datos” no se limita a la comunicación sino que pretende también englobar cualquier información consignada sobre un soporte informático que no esté destinada a ser comunicada; así pues, el concepto de “mensaje de datos” incluye el de información meramente consignada.

QUINTA.- Una firma electrónica avanzada (FEA) es aquélla que cumple con los requisitos que establece el CCo en materia de firma electrónica y que se han considerado imprescindibles para hacer equivalente, de forma absoluta, la firma electrónica y la firma manuscrita, lo anterior porque cuenta con características tales como integridad, autenticidad, no repudio y confidencialidad.

Es necesario tener en cuenta que el hecho de que la firma electrónica avanzada y la firma manuscrita sean equivalentes implica que un documento electrónico firmado puede ser presentado como una prueba documental en un procedimiento cuyo fin sea dirimir una controversia sobre un hecho documentado por medios electrónicos.

SEXTA.- El certificado electrónico funciona como el equivalente digital de una identificación, en lo que a la autenticación de personas se refiere, ya que permite que un individuo demuestre que es quien dice ser, es decir, que está en posesión de la clave secreta asociada a su certificado.

La particularidad de estos certificados es que son emitidos por un PSC para que éstos sean reconocidos jurídicamente, pues dichas Entidades han comprobado ante una Autoridad Certificadora de mayor jerarquía, llámese Secretaría de Economía, que cuentan con los elementos humanos, materiales, tecnológicos y económicos suficientes para la prestación de los servicios relacionados a la firma electrónica, cabe señalar que la facultad de certificar por parte de los PSC no conlleva fe pública por sí misma, no obstante, los notarios y corredores públicos podrán llevar a cabo certificaciones que impliquen o no la fe pública tanto en documentos con soporte en papel como en archivos electrónicos.

SÉPTIMA.- En el comercio electrónico, así como en cualquier otra relación jurídica en el que se haga uso de medios electrónicos, será un Prestador de Servicios de Certificación quien, como tercero de confianza, proveerá de certeza jurídica respecto de la identidad de las personas mediante la expedición de un certificado electrónico que vincule la identidad de una persona en particular con su firma electrónica.

Es así que, el Prestador de Servicios de Certificación juega un papel importante en el momento en que quienes contratan a través de medios electrónicos, y éstos se encuentren

separados geográficamente, como es común, y en donde el uso de la firma electrónica cause incertidumbre en cuando a la identificación de los obligados, será el PSC quien permita al remitente asegurarse de que el destinatario realmente sea quien reciba el mensaje, y además permitirá al destinatario saber que aquel que le envía el mensaje electrónico es efectivamente quien lo firma. De esta forma, es el Prestador de Servicios de Certificación el encargado de garantizar el intercambio de mensajes de datos a través de comunicaciones electrónicas, lo que permitirá que se desarrolle y fomente su implementación, y que dicho está de paso, es una figura imprescindible para que la firma electrónica sea operativa.

OCTAVA.- La Autoridad Certificadora Raíz de la Secretaría de Economía (ACR-SE) es la instancia de la Secretaría de Economía encargada de certificar la clave pública de las Autoridades Certificadoras Subordinadas, de acuerdo al CCo en materia de Prestadores de Servicios de Certificación y sus Reglas Generales, así como de emitir o revocar los certificados de las Entidades referidas, Asimismo, dicha institución se establece para crear y desarrollar una Infraestructura de Llave Pública (PKI) a nivel nacional para el desarrollo del comercio electrónico.

La ACR-SE, a través de la Dirección General de Normatividad Mercantil (DGNM), certificará las claves públicas de las Entidades Certificadoras que hayan sido acreditadas, de manera que la Secretaría de Economía es la máxima Autoridad a nivel jerárquico de las Entidades Certificadoras.

NOVENA.- La Norma Oficial Mexicana NOM-151-CSFI–2002, permite dar cumplimiento a la obligación por parte de los comerciantes que utilicen mensajes de datos, para realizar actos de comercio, de conservar por el plazo mínimo de 10 años el contenido de los mensajes de datos en que se hayan consignado contratos, convenios o compromisos que den nacimiento a derechos y obligaciones, y cuyo contenido debe mantenerse integro e inalterado a partir del momento en que se generó por primera vez en su forma definitiva, debiendo ser accesible para su ulterior consulta.

Asimismo, cuando se pretenda conservar en un medio electrónico, óptico o de cualquier otra tecnología, información derivada de un acto de comercio, que se encuentre en un soporte físico, similar o distinto a aquellos, los comerciantes podrán optar por migrar dicha información a una forma digital y, observar para su conservación, las disposiciones a que se refiere la citada NOM-151, al respecto se menciona en dicho instrumento que la migración de la información deberá ser cotejada por un “tercero legalmente autorizado”, quien constará que dicha migración se realice íntegra e inalterablemente tal y como se generó por primera vez en su forma definitiva. Sin embargo, a la fecha la Dirección General de Normatividad Mercantil no ha determinado si el propio PSC puede fungir como “tercero autorizado”, si se requerirá de la intervención de un Notario para la migración de datos o qué características deberá tener dicha figura, de tal manera que será

necesario conservar el original del documento con soporte en papel para su cotejo con el documento electrónico, lo anterior en tanto se emitan las disposiciones correspondientes.

DÉCIMA.- Un supuesto de responsabilidad especialmente complejo y problemático, derivado de las prestación de los servicios de un PSC, es el de la revocación de un certificado electrónico, lo que plantea la necesidad de delimitar y atribuir responsabilidades a los distintos sujetos implicados (PSC, titular del certificado y tercero usuario del mismo) en las distintas fases del proceso de revocación.

Lo anterior porque la emisión, distribución y uso de un certificado, junto con la eventual revocación o suspensión del mismo, hasta su expiración, generan unas relaciones de naturaleza contractual o extracontractual, entre los diversos sujetos implicados, que plantean la necesidad de establecer, delimitar y clarificar sus respectivos derechos, obligaciones y cargas, así como sus eventuales responsabilidades.

De ahí la necesidad de establecer y delimitar claramente el régimen de responsabilidad derivado de la emisión y utilización de certificados, teniendo en cuenta que la clarificación de derechos, obligaciones y responsabilidades debería servir a los intereses de todas las partes implicadas en el comercio electrónico, no sólo los del PSC, sino también los del titular y el tercero usuario del certificado.

DÉCIMA PRIMERA.- El núcleo principal de la regulación de la responsabilidad del PSC, en cuanto a la emisión de certificados así como la suspensión y revocación de los mismos, se encuentra contemplada en el art. 104 fr. IV y IX del CCo, en relación con el artículo 109 del CCo, mismos que se limitan a responsabilizar al PSC por la efectiva publicación de los listados en los que se haga constar dichas circunstancias de los certificados.

No obstante, no se contempla el supuesto en el que una vez que ha tenido conocimiento de la puesta en peligro de la clave privada, el titular del certificado solicita al PSC la revocación de su clave comprometida, intervalo en el que un tercero no autorizado la utiliza, suplantando al suscriptor, durante el periodo que media entre la petición de revocación del suscriptor, la adopción de ésta y la eliminación del registro de certificados válidamente emitidos por el PSC, de donde se deriva la interrogante acerca de quién responde por dicha situación,de manera que el titular del certificado terminaría asumiendo todas las consecuencias derivadas del uso de su certificado, dado que el problema que se plantea es que, entre la solicitud de revocación y efectiva revocación (y su publicación) existe, inevitablemente, un periodo temporal, que provoca la incertidumbre de quién responde durante el mismo.

PROPUESTA

A fin de que los titulares de los certificados electrónicos no se vean desprotegidos en cuanto al uso indebido, por parte de terceros, de su certificado, en el momento que media entre la solicitud de revocación al otorgamiento de ésta por parte del PSC, se plantea una responsabilidad mancomunada, en donde se distribuya el riesgo entre el titular del certificado y la entidad certificadora.

Para ello tomaremos en cuenta los siguientes factores:

3. La verificación de la identidad del solicitante de la revocación, titular del certificado; y
4. La rapidez con el cual el PSC debe dar curso a la revocación y eliminación del registro de certificados válidamente emitidos; este hecho, permitirá determinar al juez si el PSC fue o no lo suficientemente diligente al prestar este servicio.

Se trata, por tanto, de distribuir el riesgo entre el titular del certificado y la entidad certificadora. En principio, el titular, asumiría la responsabilidad del uso indebido de su certificado hasta el momento en que lo hace del conocimiento de la entidad certificadora de la puesta en peligro de su llave privada, solicitándole su revocación.

Ello sería una carga del titular, una actuación que ha de realizar si quiere liberarse de esa responsabilidad inicial, trasladándola al PSC; en caso contrario, deberá asumir las consecuencias que por falta de actuación se deriven, es decir, seguirá siendo responsable del posible mal uso de la clave privada.

Cabe señalar que, para la verificación de la identidad del titular del certificado el PSC podrá solicitar al titular del certificado los elementos razonablemente suficientes que le permitan al PSC tener plena convicción respecto de la información que le ha sido proporcionada, de manera que pueda confirmar la identidad y la representación de la persona solicitante, como el contrato de suscriptor, identificación oficial, carta membretada dónde se haga formal solicitud de la revocación de su certificado (en el caso de las empresas que solicitan certificados para sus colaboradores, siendo esta una práctica muy común en la que la empresa respalda el envío de dicha solicitud).

Una vez que el PSC reciba formal solicitud por parte del titular del certificado, tendrá lugar un intervalo de tiempo del que el PSC dispondrá para realizar la verificación correspondiente de que el titular es realmente quien solicita la revocación y no otra persona, lapso en el que ambas partes tendrán una responsabilidad mancomunada, dado que por una parte el titular del certificado

tuvo la responsabilidad de dar un adecuado cuidado al resguardo de su clave privada, y por la otra el PSC deberá dar cumplimiento al servicio que presta respecto de la suspensión anticipada de la validez de un certificado electrónico que emite, tiempo que a nuestra consideración sería de 12 a 24 horas.

Transcurrido dicho plazo, se le trasladaría la responsabilidad al PSC, pues la solicitud de revocación ya ha tenido lugar, asimismo ha transcurrido un periodo razonable en el que el PSC pudo verificar la identidad del solicitante de la revocación.

Bibliografía

1) Acosta Romero Miguel, Nuevo Derecho Mercantil, Ed, Porrúa, México, 2000.
2) Alcocer Garau, G. “La firma electrónica como medio de prueba (Valoración jurídica de los criptosistemas de claves asimétricas)”, ACD, núm. , abril 1994, pág. 29.
3) Barceló, Rosa Julia, Comercio Electrónico entre empresarios. La formación y prueba del contrato electrónico (EDI), Tirant lo blanch. Valencia 2000.
4) Barrera Graf, Jorge, Instituciones de Derecho Mercantil. 2ª ed., Porrúa. México, 2003.
5) Bejarano Sánchez, Manuel, Obligaciones Civiles, 5ª ed., Oxford, México, 1999.
6) Carral y de Teresa, Luis, Derecho Notarial y Derecho Registral, 15ª ed., Porrúa, México, 1998.
7) Cabanellas, Guillermo, “Diccionario Enciclopédico de Derecho, Ed. Heliasta, Argentina, 1989.
8) Cervantes Ahumada, Raúl, Derecho Mercantil, 1er curso, Porrúa, 2ª ed., Herrero, México, 2002.
9) Clemente Meoro, M. E. “Algunas consideraciones sobre la contratación electrónica” RdDP, número 4, 2000-1, págs. 59-86.
10) De J. Tena, Felipe, Derecho Mercantil Mexicano, 19ª ed., México, 2001.
11) De Pina Vara, Rafael, Derecho Mercantil Mexicano, 28ª ed., Porrúa, México, 2002.
12) Enciclopedia Jurídica Omeba, Argentina, 1987.
13) Frías Caballero, Jorge, “Imputabilidad Penal”, Ediar, Buenos Aires, 1981.
14) García Rodríguez, Salvador, Derecho Mercantil, 7ª ed., Porrúa, México, 2003.
15) García Joaquín, Curso de Derecho mercantil, Tomo 1, 9ª ed., Porrúa, México, 1990.
16) Giménez Arnau, Enrique, “Derecho Notarial”, Ediciones Universidad de Navarra EUNSA, Pamplona, 1976, 882 págs.
17) González, Carlos E., “Teoría general del instrumento público”. Introducción al derecho notarial Argentino y comparado, Buenos Aires, Editorial Ediar, 1953. 478 págs.
18) González Lara, Cipriano, Teoría General del Proceso, 9ª ed., Oxford, México, 2000.
19) Gutiérrez y Gonzáles, Ernesto, Derecho de las Obligaciones, Ed Porrúa, México, 2002.
20) Illescas Ortiz, R., “La firma electrónica y el Real Decreto-Ley 14/1999, del 17 de septiembre”, DN, núm 109, octubre 1999.
21) Illescas Ortiz R., “Entre Europa y la nada (A propósito del Anteproyecto de Ley de Servicios de Sociedad de la Información y de Comercio Electrónico de 29 de septiembre de 2000)” RCE, núm. 11, 2000, págs. 3-33.
22) Mantilla Molina, Roberto, Derecho Mercantil, 29ª ed., Porrúa, México, 2001.
23) Ma. Isabel Huerta Viesca y Daniel Rodríguez Ruiz de Villa, “Los Prestadores de Servicios de Certificación en la Contratación Electrónica”, Ed. Aranzadi, 2001, pág. 52.
24) Martínez Nadal, A., “Aproximación al borrador de propuesta de directiva para un marco común de firma electrónica y proveedores de servicios relacionados”, AIA, núm.29, octubre de 1998, pág. 1.

25) Quevedo Coronado, Ignacio, Compendio de Derecho Mercantil Mexicano, 19 ed., Addison Wesley de México, México, 1998.
26) Quintana Adriano, Elvia Arcelia, Ciencia del Derecho Mercantil, Porrúa, México 2002.
27) Quintana Adriano, Elvia Arcelia, Derecho Mercantil, Mc Mraw Hill Interamericanas, México 1997º
28) Pelosi, Carlos A., El documento notarial, Buenos Aires, Ed. Astrea, 1997.
29) Rábago, José Félix, Introducción a las Redes Locales, 1ª ed., Anaya Multimedia Americana, México, 1995.
30) Reyes Krafft, Alfredo Alejandro, La Firma Electrónica y las Entidades de Certificación, Porrúa, México; 2003.
31) Ríos Helling , Jorge, La Práctica del Derecho Notarial, Ed. Mc Graw Hill, México, 1998.
32) Smith, Rpb, Traducción Martínez, Miguel Ángel, Comercio Electrónico, 1ª ed., Parson Education, México, 2001.
33) Ruí-Gallardón, M., "Fe pública y contratación telemática", *Derecho de Internet. Contratación electrónica y firma digital,* Mateu De Ros, R. y J. M. Cendoya Méndez De Vigo (coordinadores), Aranzadi, Pamplona, 1ª reimpresión, 2001, págs. 111-112.
34) Sanchíz Crespo, C., "Una reflexión acerca de la eficacia probatoria de escritura en el Anteproyecto de LSiv", *presente y futuro del proceso civil,* PICO JUNOY; J., Barcelona, 1998, págs. 275-282.
35) Soriano, Ramón, compendio de la teoría General del Derecho, 2ª ed., Ariel, España, 1993.

Legislación

1) Constitución Política de los Estados Unidos Mexicanos
2) Código de Comercio
3) Ley General de Títulos y Operaciones de Crédito
4) Código Civil Federal
5) Código Federal de Procedimientos Civiles
6) Código Fiscal Federal
7) Código Civil Para el Distrito Federal
8) Código Penal para el Distrito Federal
9) Ley del Notariado para el Distrito Federal
10) Ley de Firma Electrónica Certificada para el Estado de Jalisco y sus municipios
11) Ley de la Comisión Estatal de derechos humanos de Jalisco
12) Reglamento del Código de Comercio en materia de Prestadores de Servicios de Certificación
13) Decreto por el que se reforman y adicionan diversas disposiciones del Código Civil para el Distrito Federal, del Código Federal de Procedimientos Civiles, del Código de Comercio y de la

Ley Federal de Procedimientos al Consumidor del 23 de mayo de 2000 (D:O: 29 de mayo de 2000).

14) Norma Oficial Mexicana NOM-151-SCFI-2002, Prácticas comerciales-Requisitos que deben observarse para la conservación de mensajes de datos, publicada el 4 de junio del2002 en el D.O.F.

15) Lineamientos para la homologación de la operación de la Firma Electrónica Avanzada en la Administración Pública Federal.

Jurisprudencia

1) Suprema Corte de Justicia de la Nación: http://www.scjn.gob.mx

Páginas Web

1) Alessandri, Arturo, De los contratos, Centro de Estudios de Derecho Informático, Chile, consultado en http://www.derechoinformatico.uchile.cl/CDA/der_informatico_simple/0,1493,SCID%253D14402%2526ISID%253D507%2526PRT%253D14333,00.html

2) Asociación Mexicana de Estándares para el Comercio Electrónico AMECE, consultado en: http://www.amece.org.mx/amece/faqs/index.php?bnd=3.

3) Asociación Mexicana de Internet
http://www.amipci.org.mx

4) Comisión de las Naciones Unidas para el Derecho Mercantil Internacional
http://www.uncitral.org/

5) Comisión Federal de Mejora Regulatoria
http://www.cofemer.gob.mx

6) Comisión Intersecretarial de Gobierno Electrónico
http://www.cidge.gob.mx/

7) Loredo, Alejandro A., Contratos telemáticos, naturaleza jurídica en la legislación mexicana, consultado en: http://www.alfa-redi.org/rdi-articulo.shtml?x=7176

8) Prestador de Servicios de Certificación “Advantage Security”
http://www.advantage-security.com

9) Prestador de Servicios de Certificación “PSC World”
http://www.pscworld.com

10) Rafael Illescas Ortiz, “El Comercio Electrónico”, fundamentos de derecho y el principio del equivalente funcional, consultado en:
http://www.uc3m.es/uc3m/inst/FL/boletin/espanol/pdfdebate/td562.pdf.

11) Ramos Suárez, Fernando, “Cómo aplicar la nueva normativa sobre comercio electrónico”, consultado en: http://www.secretosenred.com/articles/740/1/COMO-APLICAR-LA-NUEVA-NORMATIVA-SOBRE-LA-FIRMA-ELECTRONICA--Primera-Parte/Pagina1.html
12) REDI Revista de Electrónica de Derecho Informático, España. http://premium.vlex.com/doctrina/REDI-Revista-Electronica-Derecho-Informatico/Confianza-digital-basada-certificados/2100-107350,01.html
13) Revista de derecho informático Alfa-redi.
http://www.alfa-redi.com.
14) Real Academia Española
http://www.rea.es
15) Secretaría de Economía
    a. http://www.economia.gob.mx
    b. http://www.firmadigital.gob.mx
    c. http://www.siger.gob.mx/
16) Triarte Ahon, Eric, “Firma electrónica y certificado digital. El proyecto peruano”, REDI Revista Electrónica de Derecho informático, Perú, consultado en http://publicaciones.derecho.org/redi/No._14_-_Septiembre_de_1999/9

Otras Fuentes

1) Ley Modelo de la CNUDMI sobre Comercio Electrónico
2) Ley Modelo de la CNUDM sobre Firma Electrónica
3) Ley 59/2003, del 19 de diciembre sobre firma electrónica, España.
4) Ley sobre mensajes de datos y firmas electrónicas. Venezuela.
5) Ley de Utah sobre Firma Electrónica (Utah Digital Signature Act)
6) Política de Certificados de la Autoridad Certificadora Raíz de la Secretaría de economía.
7) Declaración de Prácticas de Certificación de la Autoridad Certificadora Raíz de la Secretaría de Economía.