TEMA II

INFORMÁTICA JURÍDICA DEL DERECHO NOTARIAL Y DEL DERECHO REGISTRAL

Coordinador Internacional
NOT. JOSÉ ANTONIO MÁRQUEZ GONZÁLEZ (MÉXICO)

Ponente
NOT. CARLOS ALEJANDRO DURÁN LOERA (D.F.)

Revista de Derecho Notarial Mexicano, núm. 121, México, 2007.

ÍNDICE

Revista de Derecho Notarial Mexicano, núm. 121, México, 2007.

Revista de Derecho Notarial Mexicano, núm. 121, México, 2007.

TEMA II

INFORMÁTICA JURÍDICA DEL DERECHO NOTARIAL Y DEL DERECHO REGISTRAL

NOTARIO Carlos ALEJANDRO DURÁN LOERA

FIRMA DIGITAL Y FIRMA ELECTRÓNICA AVANZADA.

ANTECEDENTES

Cronología de la Firma Electrónica en México

A continuación se enlistan algunos de los pasos más significativos del historial del marco jurídico que tiene que ver con este interesante tema:

Mayo 2000. Mensajes de Datos. Se reforman y adicionan diversas disposiciones del Código Civil, el Código Federal de Procedimientos Civiles, el Código de Comercio y la Ley Federal de Protección al Consumidor, así como de la Ley Federal de Procedimiento Administrativo

Septiembre 2000. Registro Público de Comercio. Se estipula el modo de operación del registro mediante un sistema (SIGER), utilizado por los fedatarios públicos autorizados.

Noviembre 2001. Conservación de Mensajes de Datos NOM-151. En ella se establecen los requisitos que deben observarse para la conservación de mensajes de datos.

Enero 2002. Procedimientos Administrativos por medios electrónicos. Se establecen las disposiciones que deberán observar las dependencias de la Administración Publica Federal, para la recepción de promociones y resoluciones administrativas definitivas a través de medios de comunicación electrónica.

Revista de Derecho Notarial Mexicano, núm. 121, México, 2007.

Abril 2003. Ley de Firmas Electrónicas. Se reforman y adicionan diversas disposiciones del Código de Comercio, en materia de Firma Electrónica.

Agosto 2003. Ley de la Firma Electrónica Avanzada. En esta ley se establecen los parámetros generales para la aceptación y uso de la firma digital en el país, definiéndose las instancias a cargo de las cuales estarán los procesos relacionados con los sectores mercantil, financiero y gubernamental.

Enero 2004. Factura Electrónica. Se declara que las personas que tengan certificado de firma electrónica avanzada y lleven su contabilidad en sistema electrónico, podrán emitir comprobantes en documento digital y con sello digital, debiendo incorporar en los documentos los requisitos de identificación establecidos en el CFF.

Julio 2004. Reglamento de Código de Comercio en Materia de Prestadores de Servicio de Certificación. Se establecen las disposiciones y los requisitos técnico y jurídicos para darse de alta y para operar como PSC en el sector comercial,

Fuentes inspiradoras del Proyecto de Ley

- Ley modelo de la UNCITRAL (Agencia de Naciones Unidas para universalización del Derecho)
- Directiva de la Unión Europea
- Consultas con los órganos y representantes del sector

FIRMA DIGITAL

Es la transmisión de mensajes telemáticos, un modo criptográfico que asegura su integridad así como la identidad del remitente.

El procedimiento utilizado para firmar digitalmente un mensaje es el siguiente: el firmante genera mediante una función matemática una huella digital del mensaje.

Esta huella digital se encripta con clave privada del firmante, y el resultado es lo que se denomina firma digital la cual se enviara adjunta al mensaje original. De esta manera el firmante va a estar adjuntando al documento una marca que es única para ese documento y que sólo él es capaz de producir.

El receptor del mensaje podrá comprobar que el mensaje no fue modificado desde su creación y que el firmante es quién dice serlo a través del siguiente procedimiento: en primer término generará la huella digital de mensaje recibido, luego desencriptará la firma

Revista de Derecho Notarial Mexicano, núm. 121, México, 2007.

digital del mensaje utilizando la clave pública del firmante y obtendrá de esa forma la huella digital del mensaje original; si ambas huelas digitales coinciden, significa que el mensaje no fue alterado y que el firmante es quien dice serlo.

Descripción

El concepto de firma digital nació como una oferta tecnológica para acercar la operatoria social usual de la firma ológrafa (manuscrita) al marco de lo que se ha dado en llamar el ciberespacio o trabajo de redes.

Consiste en la transformación de un mensaje utilizando un sistema descifrado asimétrico de manera que la persona que posee el mensaje original y la clave pública del firmante, pueda establecer de forma segura, que dicha transformación se efectuó utilizando la clave privada correspondiente a la pública del firmante, y si el mensaje es el original o fue alterado desde su concepción.

Las transacciones comerciales y el hecho de tener que interactuar masiva y habitualmente por intermedio de redes de computadoras le dio lugar al concepto. Pero solo después de que los especialistas en seguridad y los juristas comenzaran a depurarlo alcanzó un marco de situación como para ocupar un lugar en las actuaciones entre personas, ya sea jurídicas o reales.

El fin de la firma digital, es el mismo de la firma ológrafa; y es por eso que a través de la legislación se intenta acercarla, exigiéndose ciertos requisitos de validez.

El papel es el medio de almacenamiento, y el mecanismo es alguno de los tipos de impresión posibles (tinta, láser, manuscrito etc.). Esta cualidad física le da entidad al documento, contiene sus términos sus conceptos y sentidos de una manera perdurable, y al ser un elemento físico cualquier alteración dejará "señales" identificables.

FIRMA ELECTRÓNICA

Se entenderán los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información contenida en el mensaje de datos".

Tomando en cuenta los conceptos anteriormente expuestos, la FIRMA DIGITAL o FIRMA ELECTRONICA es un conjunto de datos asociados a un mensaje que permite asegurar la identidad del firmante y la integridad del mensaje.

Cuando la ley exija la firma de una persona, el requisito quedará cumplido... si se utiliza una forma electrónica que, a la luz de todas las circunstancias del caso..., sea tan fiable como resulte apropiado a los fines para los cuales se genera o comunicó ese mensaje...

En todo caso la presunción de fiabilidad de la firma electrónica, admitirá prueba en contrario: esto sin perjuicio de la posibilidad de que cualquier persona: a) demuestre de cualquier manera... la fiabilidad de una firma electrónica; o b) aduzca pruebas de que una firma electrónica no es fiable.

Firma electrónica avanzada

El convencimiento de la inseguridad tecnológica de internet respecto de la autenticidad de los "mensajes de datos" trasmitidos a través de la Red planean en toda la normativa de firma electrónica entre ellas, a la hora de indicar que para confirmar la identidad de la persona que firma electrónicamente.... se utilizarán certificados, y de aquí, "las firmas electrónica avanzada"; dentro de las cuales, la equivalencia jurídica con la manuscrita, se reservaría a las firmas electrónicas avanzadas relacionadas con un certificado reconocido y creadas mediante un depósito seguro de creación de firma.

La firma electrónica avanzada es una especie de firma electrónica que cumple los requisitos de creación y funcionalidad. En cuanto a su creación, la directiva requiere que haya sido creada utilizando medios que el firmante puede mantener bajo su exclusivo control. Exigencia que coordinándose con otros preceptos permite afirmar que se trata de una firma electrónica creada con un nivel de seguridad tecnológica verificable, al tratarse de un "programa informático configurado o un aparato informativo configurado que sirve para aplicar los datos de creación de firma" y referido exclusivamente a una persona, según se define al:

Firmante: Persona que esta en posesión de un dispositivo de creación de firma y que actúa en su propio nombre o en el de la entidad o persona física o jurídica a la que representa.

Dispositivo seguro de creación de firma y se requiere para la existencia de la "firma electrónica avanzada basada en un certificado

reconocido, que es aquel que cumple los requisitos de calificación tecnológica, solvencia económica, eficacia de sus servicios y credibilidad de su actividad, como son:

a) La indicación de que el certificado se expide como certificado reconocido
b) La identificación del proveedor de servicios de certificación y el Estado en que está establecido
c) El nombre y los apellidos del firmante o un seudónimo que conste como tal
d) Un atributo específico del firmante, en caso de que fuera significativo en función de la finalidad del certificado.
e) Los datos de verificación de firma que correspondan a los datos de creación de firma bajo control del firmante
f) Una indicación relativa al comienzo y fin del período de validez del certificado
g) El código identificativo del certificado.
h) La firma electrónica avanzada del proveedor de servicios de certificación que expide el certificado.
i) Los limites de uso del certificado, si procede y
j) Los limites del valor de las transacciones para las que puede utilizarse el certificado, si procede.

En nuestra legislación esta regulado en el Código de Comercio en el Capítulo II "DE LAS FIRMAS". En dicho Código se menciona por los siguientes artículos que son de interés para nuestro tema:

Artículo 96.-Las disposiciones del presente Código serán aplicadas de modo que no excluyan, restrinjan o priven de efecto jurídico cualquier método para crear una Firma Electrónica.

Artículo 97.- Cuando la ley requiera o las partes acuerden la existencia de una firma en relación con un Mensaje de Datos, se entenderá satisfecho dicho requerimiento si se utiliza una Firma Electrónica que resulte apropiada para los fines para los cuales se generó, o comunicó ese Mensaje de Datos.

La Firma Electrónica se considerará Avanzada o Fiable si cumple por lo menos los siguientes requisitos:

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

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

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

Revista de Derecho Notarial Mexicano, núm. 121, México, 2007.

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.

Lo dispuesto en el presente artículo se entenderá sin perjuicio de la posibilidad de que cualquier persona de cualquier otra manera la fiabilidad de una Firma electrónica; o presente pruebas de que una Firma Electrónica es Fiable.

Artículo 98.- Los Prestadores de Servicios de Certificación determinarán y harán del conocimiento de los usuarios si las Firmas Electrónicas Avanzadas o Fiables que les ofrecen cumplen o no los requerimientos dispuestos en las fracciones I al IV del artículo 97.

La determinación que se haga, con arreglo al párrafo anterior, deberá ser compatible con las normas y criterios internacionales reconocidos.

Lo dispuesto en el presente artículo se entenderá sin perjuicio de la aplicación de las normas del derecho internacional privado.

Artículo 99.-El Firmante deberá:

I.- Cumplir las obligaciones derivadas del uso de la Firma Electrónica;

II.- Actuar con diligencia y establecer los medios razonables para evitar la utilización no autorizada de los Datos de Creación de la Firma;

III.-Cuando se emplee un Certificado en relación con una Firma Electrónica, actuar con diligencia razonable para cerciorarse de que todas las declaraciones que haya hecho en relación con el Certificado, con su vigencia, o que hayan sido consignadas en el mismo, son exactas.

Diferencias entre firma electrónica y firma electrónica avanzada

- Firma Electrónica (autentifica la identidad de la persona, es como "mostrar" nuestra cédula de identidad, para que se confirme quien soy).
- Firma electrónica Avanzada (autentifica la identidad, pero además permite llevar a cabo transacciones comerciales avanzadas y contratos, es como ir a la Notaria, pero además se confirma ante el Notario la legalidad de la transacción o relación)

La diferenciación entre ambas clases de firmas está hecha en función de la protección legal que ellas producen.

Los efectos jurídicos que ella produce son consecuencia de ser un medio apto al que se le atribuye la cualidad de contener la voluntad de la persona.

Por ejemplo, offline, yo puedo firmar un contrato con un sujeto, ambos lo firmamos y ponemos nuestra firma, La ley protege ese contrato. Sin embargo, si ese mismo contrato, además es legalizado ante un Notario, la ley lo protege más aún, puesto que tiene una autentificación mayor que el primero, por tanto, en cuanto a lo penal también es diferente.

Identidad y Personalidad de la Firma Digital

El artículo 90 del Código de Comercio menciona que para presumir sin un mensaje de datos proviene del emisor se debe usar "medios de identificación, tales como claves o contraseñas del Emisor". Dicha contraseña es la firma electrónica avanzada.

En el DECRETO DE REFORMAS AL CÓDIGO DE COMERCIO EN MATERIA DE FIRMA ELECTRÓNICA, de fecha 26 de noviembre del 2002 y publicado en el Diario Oficial el 29 de agosto de 2003, basado en la Ley Modelo de Firmas Electrónicas de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional se introduce la Figura de Prestador de Servicios de Certificación, quien como tercero confiable tendrá la facultad de validar, por su integridad y su tecnología, el proceso de emisión, identificación y atribución de firmas electrónicas, entre ellos encontramos a los Notarios, Corredores, Empresas Privadas e Instituciones Públicas y como Autoridad Registradora Central a la Secretaría de Economía (además de Banco de México y la Secretaría de la Función Pública)

La firma electrónica avanzada supone un avance sumamente importante en la manera en que se llevan a cabo las operaciones vía Internet debido a que en menos tiempo se pueden realizar toda clase de contratos transacciones etc. . Pero todo esto que a primera vista parece ideal, produce en el usuario de dicho servicio una inseguridad, que se genera debido a que dichos documentos pueden ser interceptados, descifrados y prestarse para realizar incontables fraudes, lo cual nos lleva a hacernos el siguiente cuestionamiento, ¿Como comprobar la identidad y personalidad de dicha firma?

Una firma debe determinar el vínculo que tiene una persona con el acto jurídico que se esta realizando, su consentimiento, determina su personalidad, así como sus derechos y obligaciones sobre el convenio de que se trata.

Revista de Derecho Notarial Mexicano, núm. 121, México, 2007.

Todo esto son cualidades que la firma electrónica debe cumplir con el fin de dar validez al acto. Elíaz Azar en su obra La Contratación por Medios Electrónicos, menciona que "para tener certidumbre en la identidad de las partes y su vinculación al contenido no son atributo de cualquier documentación electrónica sino que se restringe a los confiables jurídicamente por ser fiables tecnológicamente; es decir, de la figura de la firma electrónica avanzada, peculiarizada porque los datos de creación de firma estaban bajo el control del signatario en el momento de su generación y los mismos pertenecen en exclusiva al firmante.

Es decir que la firma tendrá identidad y personalidad si es creada por uno de los "confiables jurídicamente", estos cerciorándose en el momento de la creación de que la persona tenga la capacidad para celebrar actos jurídicos y que compruebe mediante distintos documentos (ej. Acta de nacimiento, credencial de elector etc.) que es quien dice ser, y una vez creada la firma se destruye el archivo y solo el signatario es el que tendrá un único archivo y su clave personal.

Documento Electrónico

No se puede negar validez legal a un documento por el simple hecho de ser electrónico, máxime que hay ahora medios para certificar su autenticidad. Es imperante cambiar nuestra concepción acerca papel como única materia para celebrar contratos.

La noción de documento electrónico no queda restringida a aquel instrumento asentado en un registro magnético del ordenador, sino que comprende cualquier otro soporte electrónico (como el fax)

Desde luego, que su eficacia probatoria está supeditada a la autenticidad que emane del mismo. Para ello, es necesario determinar que el documento no ha sufrido alteraciones. De allí la importancia de los sistemas de seguridad que impidan su alteración.

Ello nos lleva a la cuestión de la firma digital (o firma electrónica), entendiéndose por tal todos aquellos datos electrónicos utilizados como medio para identificar al autor de un documento, a través de métodos criptográficos que permiten codificar la información mediante una clave secreta, la que actúa a modo de "Notario" que da fe de la identidad del firmante.

Corresponde asignarles a los documentos nacidos de las nuevas tecnologías, el mismo valor al de los instrumentos tradicionales para

Revista de Derecho Notarial Mexicano, núm. 121, México, 2007.

el Derecho Civil, en la medida que la firma pueda ser atribuida a su signatario.

El principio del que debe partir una regulación jurídica sobre el documento electrónico y firma electrónica, es que el documento firmado electrónica o digitalmente tiene la misma validez y eficacia que un documento tradicional, en soporte en papel, debidamente firmado.

El tratamiento por medios informáticos permite la sustitución del soporte en papel del documento por un nuevo soporte contenido en un medio electrónico, el documento puede serlo tanto si se encuentra sobre un papel o sobre cualquier otro soporte apto según su naturaleza.

Podemos decir que el documento en soporte electrónico, informático y telemático es un documento con las mismas características, en principio y en cuanto a su validez jurídica, que cualquier otro de los que tradicionalmente se aceptan en soporte de papel, tal como lo ha declarado el artículo 210-A del Código Federal de Procedimientos Civiles.

El documento electrónico o informático, se concibe como un medio de expresión de la voluntad con efectos de creación, modificación o extinción de derechos y obligaciones por medio de la electrónica, informática y telemática.

No deberá rechazarse la existencia del contrato electrónico y su autenticidad por el simple hecho de no estar firmado de puño y letra por los contratantes, ya que en estos casos, la firma puede suplirse por otros medios de identificación como son el uso de claves secretas y sistemas criptológicos.

La Firma Electrónica consiste en un método de encriptación o de clave pública, que establece un par de claves asociadas a un sujeto, una pública y otro privada; la clave privada nos va permitir la perfecta identificación de su emisor objeto de la autenticidad de la Firma Electrónica a través de mensajes de datos.

De conformidad con el articulo 89 del Código de Comercio se define al Mensaje de Datos como: "La información generada, enviada, recibida o archivada por medios electrónicos, ópticos o cualquier otra tecnología."

Cuando queramos establecer una comunicación segura con otra parte basta con encriptar el mensaje con la clave pública para que a su recepción sólo el sujeto que posee la clave privada pueda leerlo.

En las reformas publicadas en el Diario Oficial de la Federación el 29 de mayo del año 2000, las operaciones de comercio electró-

Revista de Derecho Notarial Mexicano, núm. 121, México, 2007.

nico se reconoce el valor jurídico de los documentos electrónicos, la equivalencia de la firma electrónica con la firma autógrafa, la participación de los Notarios y Corredores Públicos en los proceso de emisión de certificados digitales y la obligatoriedad de su incorporación al Registro Público de Comercio."

El problema del original

Muchas son las dudas que tienen las personas sobre si un documento electrónico es confiable o no. Por eso en este punto expondremos las características que ofrece la ley, acerca de si un documento que es enviado o elaborado por vía electrónica es original.

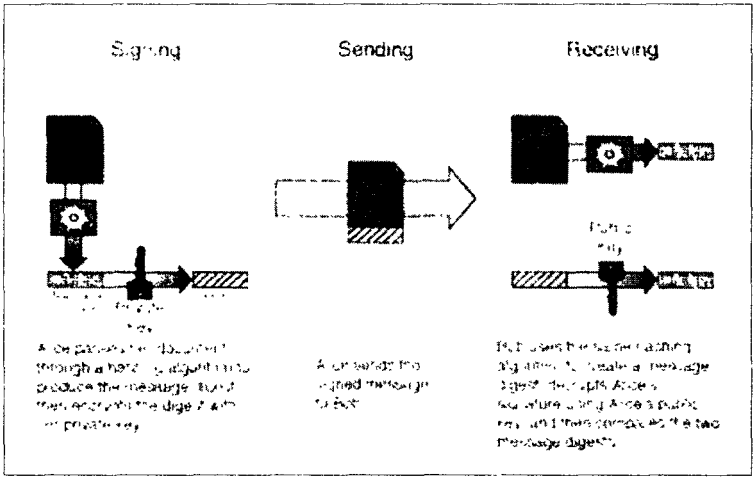
Tenemos en este momento grandes problemas acerca de ello, por que según la definición del mensaje de datos contenida en el articulo 89 del Código de Comercio nos muestra solo un requisito para ser original, precisamente que sea por medios electrónicos o cualquier tecnología, así mismo la Ley del Notariado para el Distrito Federal en su articulo 97 párrafo primero dice: "...considerándose como documento original para el cotejo no solo el documento publico o privado que así lo sea, si no también su copia certificada por Notario o por autoridad legítimamente autorizada para expedirla y las impresiones hechas vía electrónica o con cualquier otra tecnología. De aquí tenemos el entendido que cualquier documento impreso por cualquier vía electrónica y a su vez cualquier mensaje de datos recibido en algún ordenador serán siempre originales. El problema radica en la verdadera autentificación, es por eso que los documentos electrónicos serán certificados por un servidor publico, esto para darle fuerza al documento y valga con tal fuerza que hasta pueda ser usado como prueba en una litis, esta facultad de certificar documentos electrónicos la obtienen los servidores y fedatarios públicos que cumplan con los requisitos del articulo 5 del Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación.

Con esto vemos que falta especificar, que documentos deben ser originales y cuales no, en cuanto a impresiones; por que podría ser que no toda persona actúe de buena fe y así perjudique a otra. Por otro lado la certificación de un documento por vía electrónica es muy segura ya que para validar una certificación se deben contener las especificaciones del articulo 108 del Codigo de Comercio y a su vez el articulo 109 nos indica cuando y en que circunstancias dejaran de ser validos los certificados. Un punto mas que debemos

Revista de Derecho Notarial Mexicano, núm. 121, México, 2007.

apuntar es que la información del certificado estará cifrada o encriptada por medio de códigos y las personas autorizadas tendrán llaves para abrirlos con esta seguridad y con esta certificación muy pronto se podrán hacer cualquier tipo de operaciones por medio del ciber espacio.

Este diagrama muestra como se hace una certificación digital.



Certificaciones cruzadas

Las certificaciones cruzadas como lo establece el Lineamiento segundo del la fracción segunda de los Lineamientos para la Homologación de la Operación de la Firma Electrónica Avanzada en la Administración Publica Federal: es el intercambio de certificados digitales de dos o mas autoridades certificadas de un mismo nivel jerárquico y con el fin de establecer el reconocimiento de los certificados digitales emitidos por las mismas.

Esta definición es enfocada a un solo sector pero lo que debemos tomar del concepto anterior es que las certificaciones de datos son intercambios de certificados digitales de una o mas autoridades entendiéndose que si una autoridad certifica un documento en Roma con su firma digital y una autoridad lo Recibe en México lo podrá recibir y confiar en su validez, esto esta contemplado en el articulo 114 del Código de Comercio fracción segunda: " II II. El lugar en

Revista de Derecho Notarial Mexicano, núm. 121, México, 2007.

que se encuentre el establecimiento del Prestador de Servicios de Certificación o del Firmante.

Todo Certificado expedido fuera de la República Mexicana producirá los mismos efectos jurídicos en la misma que un Certificado expedido en la República Mexicana si presenta un grado de fiabilidad equivalente a los contemplados por este Título.

Toda Firma Electrónica creada o utilizada fuera de la República Mexicana producirá los mismos efectos jurídicos en la misma que una Firma Electrónica creada o utilizada en la República Mexicana si presenta un grado de fiabilidad equivalente.

A efectos de determinar si un Certificado o una Firma Electrónica presentan un grado de fiabilidad equivalente para los fines de los dos párrafos anteriores, se tomarán en consideración las normas internacionales reconocidas por México y cualquier otro medio de convicción pertinente.

Cuando, sin perjuicio de lo dispuesto en los párrafos anteriores, las partes acuerden entre sí la utilización de determinados tipos de Firmas Electrónicas y Certificados, se reconocerá que ese acuerdo es suficiente a efectos del reconocimiento transfronterizo, salvo que ese acuerdo no sea válido o eficaz conforme al derecho aplicable."

Con esto podemos observar que podemos hacer transacciones de toda índole desde cualquier parte del mundo y sobre todo con seguridad gracias a las autoridades Certificadoras que con su Firma Electrónica le dan fiabilidad al documento que Certifican y que es valido en muchas partes del mundo.

La apostilla electrónica

El concepto de la apostilla tradicional o documental como hasta hoy la conocemos nació en el mundo jurídico a partir del Convenio de La Haya de 1961, sobre la Eliminación del Requisito de la Legalización de Documentos Públicos Extranjeros, con el fin de suprimir el requisito de la legalización de documentos para que los mismos tuvieran fuerza legal y pudieran causar validamente todos sus efectos jurídicos en otro país. Con este fin surge la idea de la apostilla para que con este documento se tuvieran como válidos sin necesidad de legalización los documentos provenientes de un Estado firmante en otro Estado firmante destinatario de dicho documento. Todo esto tiene lugar debido a los avances tecnológicos que han tenido como una realidad el incremento de las relaciones tanto de los Estados mismos como de los particulares de un Estado con los particulares de otro Estado.

Revista de Derecho Notarial Mexicano, núm. 121, México, 2007.

Con estos antecedentes y debido a que el desarrollo tecnológico avanza a pasos agigantados así como las relaciones entre Estados y particulares de distintos Estados nos hemos visto en la necesidad de abarcar diversos temas como el de la apostilla electrónica con el fin de dar certeza jurídica para todos los Estados parte de la Convención de que las transacciones, contratos y demás documentos electrónicos surgidos en un Estado se reconozcan como válidos en otro Estado receptor de los mismos y debido a esto se llevo a cabo una revisión al Convenio de La Haya de 1961, sobre la Eliminación del Requisito de la Legalización de Documentos Públicos Extranjeros, en la cual se toma como conclusión que dicha Convención no solo no cierra las puertas a la idea de la apostilla electrónica sino que con el contexto en el que nace pugna la misma Convención realizando una interpretación correcta y contextuada a estar abierta a las nuevas tecnologías por lo cual concluyo que si el documento electrónico se reconoce como válido y eficaz en los Estados parte así mismo este Estado debiera reconocer con el texto actual de la Convención la validez y eficacia de la apostilla electrónica como medio de certeza de los documentos electrónicos que se realizan en su Estado.

PREGUNTAS

1.- SE RECONOCEN EN SU PAÍS LAS FIRMAS DIGITALES?

Si, principalmente en el Código de Comercio Capítulo II. "De las Firmas", del, en su última reforma publicada en el Diario Oficial de la Federación el 26 de Abril de 2006 así como en el Código Fiscal de la Federación en los Artículos 71 en adelante, así como en legislaturas estatales como la Ley de Firma Electrónica del Estado de Guanajuato, así como en el Código Civil Federal.

ARTÍCULO 1803.- EL CONSENTIMIENTO PUEDE SER EXPRESO O TACITO, PARA ELLO SE ESTARA A LO SIGUIENTE:

SERA EXPRESO CUANDO LA VOLUNTAD SE MANIFIESTA VERBALMENTE, POR ESCRITO, POR MEDIOS ELECTRONICOS, OPTICOS O POR CUALQUIER OTRA TECNOLOGIA, O POR SIGNOS INEQUIVOCOS.

2.- SE RECONOCEN EN SU PAÍS LAS FIRMAS ELECTRÓNICAS AVANZADAS?

Revista de Derecho Notarial Mexicano, núm. 121, México, 2007.

Por su parte el artículo 17-D del Código Fiscal de la Federación (CFF) señala que cuando las disposiciones fiscales obliguen a presentar documentos, éstos deberán ser digitales y contener una FEA del autor, salvo los casos que establezcan una regla diferente.

3.- SE RECONOCE EL MENSAJE DE DATOS COMO DOCUMENTO?

El mensaje de datos como información generada, enviada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología es considerado como documento electrónico, por lo que tiene la misma validez y eficacia que un documento tradicional; lo que permite la sustitución del soporte en papel por un nuevo soporte contenido en un medio electrónico, el documento puede serlo tanto si se encuentra sobre un papel o sobre cualquier otro soporte apto según su naturaleza.

4.- SE ESTABLECE EL CONCEPTO DE ORIGINAL?

El concepto como tal no lo define ningún cuerpo legal en México, lo único que nos menciona son los documentos que se pueden establecer como originales, claro que por medio de la interpretación lo podemos deducir así es como se establecen cuales son considerados como originales de acuerdo al criterio de cada Autoridad Certificadora.

5.- SE RECONOCEN LAS CERTIFICACIONES ELECTRÓNICAS CRUZADAS?

Cierto es que falta una perfección en el campo del Derecho Informático; pero aunque el campo es primitivo se esta trabajando arduamente en cada país y como se ha podido observar, México se ha unido a esta tecnología mundial y tan es así que lo ha legislado y con ello forma parte del mundo del Derecho Informático.

La informática jurídica del derecho notarial y del derecho registral

INCISO III
VALOR PROBATORIO DEL DOCUMENTO INFORMÁTICO

3.1 El valor probatorio; carga de la prueba; ejecutividad.

Podemos iniciar este epígrafe preguntándonos: ¿cuál es el valor probatorio del documento electrónico? ¿Se puede considerar documento público o documento privado? ¿Tiene o no fuerza ejecutiva?

Partiendo del axioma "los juicios se ganan o se pierden por las pruebas" en nuestro sistema codificado de tipo latino, la prueba más

Revista de Derecho Notarial Mexicano, núm. 121, México, 2007.

importante es el documento público. Los códigos de procedimientos civiles, mercantiles, penales, etcétera, son los que determinan cuál es un documento público y cuál uno privado. En nuestra legislación el Código Federal de Procedimientos Civiles establece:

Art. 129. Son documentos públicos aquellos cuya formación está encomendada por la ley, dentro de los límites de su competencia, a un funcionario público revestido de la fe pública, y los expedidos por funcionarios públicos, en el ejercicio de sus funciones.

La calidad de públicos se demuestra por la existencia regular, sobre los documentos, de los sellos, firmas u otros signos exteriores que, en su caso, prevengan las leyes.

Por su parte el Código de Procedimientos Civiles para el Distrito Federal dispone:

Art. 327. Son documentos públicos:

I. Las escrituras públicas, pólizas y actas otorgadas ante notario o corredor público y los testimonios y copias certificadas de dichos documentos;

II. Los documentos auténticos expedidos por funcionarios que desempeñen cargo público, en lo que se refiere al ejercicio de sus funciones;

III. Los documentos auténticos, libros de actas, estatutos, registros y catastros que se hallen en los archivos públicos, o los dependientes del Gobierno Federal, de los Estados, de los Ayuntamientos o del Distrito Federal;

IV. Las certificaciones de las actas del estado civil expedidas por los Jueces del Registro Civil, respecto a constancias existentes en los libros correspondientes;

V. Las certificaciones de constancias existentes en los archivos públicos expedidas por funcionarios a quienes competa;

VI. Las certificaciones de constancias existentes en los archivos parroquiales y que se refieran a actos pasados antes del establecimiento del Registro Civil, siempre que fueren cotejadas por notario público o quien haga sus veces con arreglo a derecho;

VII. Las ordenanzas, estatutos, reglamentos y actas de sociedades o asociaciones, universidades, siempre que estuvieren aprobadas por el Gobierno Federal o de los Estados, y las copias certificadas que de ellos se expidieren;

VIII. Las actuaciones judiciales de toda especie;

IX. Las certificaciones que expidieren las bolsas mercantiles o mineras autorizadas por la ley y las expedidas por corredores titulados con arreglo al Código de Comercio;

X. Los demás a los que se les reconozca ese carácter por la ley.

Revista de Derecho Notarial Mexicano, núm. 121, México, 2007.

Por exclusión, son privados los documentos que no reúnen las condiciones previstas en las disposiciones anteriormente transcritas (Artículo 327).

Como se desprende de lo anterior, el documento electrónico no está incluido dentro de la enumeración y definición de los documentos públicos o privados. El documento electrónico lo podemos catalogar como una prueba autónoma que el Código de Comercio lo regula en el artículo 1298-A al decir:

Se reconoce como prueba los mensajes de datos. Para valorar la fuerza probatoria de dichos mensajes, se estimará primordialmente la fiabilidad del método en que haya sido generada, archivada, comunicada o conservada.

El documento electrónico así como la firma electrónica son reconocidos en la legislación mexicana por las siguientes leyes: Ley de Instituciones de Crédito (Art. 52); Ley del Mercado de Valores (Art. 91); Ley Aduanera (Art. 36); Ley Federal de Protección al Consumidor (Arts. 1º fr. VIII, 24 fr. IX bis y 76 bis); Ley Federal de Derechos de Autor (Arts. 101-114, 123); Ley de Adquisiciones Arrendamientos y Servicios del Sector Público (Arts. 26, 27, 56, 65 y 67); Ley de Obras Públicas y Servicios relacionados con las mismas (Arts. 27, 28, 31, 33, 83 y 85); Código Civil Federal (Arts. 1803, 1834 bis); Reglamento Interior del Registro Agrario Nacional (Art. 106); Código de Comercio (Arts. 20 bis, 25,26, 30 bis, 89-94 y 1298-A) y Código Federal de Procedimientos Civiles (Art. 210-A)

El documento público se caracteriza por tener pleno valor probatorio; valor que sólo puede ser destruido por vía de acción, la cual debe ser intentada ex profeso para su nulidad y su validez no puede hacerse valer por las excepciones presentadas. También tiene fuerza ejecutiva, es decir, cuando una deuda es reconocida notarialmente, la acción de pago se puede intentar y pedir al juez el embargo precautorio sin necesidad de esperarse a la sentencia ejecutoriada e iniciar un incidente de ejecución.

En cambio, toda vez que el documento electrónico no es público, no cuenta con estas características y por lo tanto no tiene fuerza ejecutiva y vale como prueba autónoma (Art. 1298-A)

INCISO IV

4.1 CONTEXTO LEGAL DEL DERECHO INFORMÁTICO

Principios doctrinales del derecho informático

La doctrina en general, considera que los principios fundamentales de la contratación electrónica son:

Revista de Derecho Notarial Mexicano, núm. 121, México, 2007.

- Autonomía de la voluntad
- Libre competencia;
- Neutralidad tecnológica;
- Reciprocidad o compatibilidad internacional;
- Principio de equivalencia funcional, y
- Buena fe, inherente a todo el derecho internacional.

La Ley Española pretende dar seguridad y confianza al establecer que la contratación electrónica debe apoyarse en los principios de:

Autenticidad: asegurar que aquel con quien se contrata es quien dice ser. Hay que garantizar la identidad del interlocutor.

Integridad: busca la garantía de que el mensaje es idéntico en su contenido y formato. Asegurar la exactitud.

Confidencialidad: tiende a garantizar la privacidad del mensaje. Asegurar que nadie no autorizado accede al mismo. Es decir, que no pueda ser manipulado por terceras personas ajenas al emisor del mensaje.

No repudiación: asegurar que ninguna de las partes pueda negar haber enviado o recibido el mensaje; es decir, que el mensaje no podrá ser rechazado, salvo pacto de desistimiento. También es conocido como principio de inobjetabilidad.

En términos generales en las legislaciones, en mayor o menor medida, adoptan los principios antes enunciados, lo que proporciona una armonía en las diversas legislaciones que regulan el comercio electrónico.

Es importante que esta especie de código de conducta se adapte a las leyes de los diferentes países para igualar la firma y el documento electrónico.

Contexto legal

Respecto de los principios anteriormente enumerados, en la legislación mexicana el artículo 89 en su segundo párrafo dispone:

> Las actividades reguladas por este Título se someterán en su interpretación y aplicación a los principios de neutralidad tecnológica, autonomía de la voluntad, compatibilidad internacional y equivalencia funcional del Mensaje de Datos en relación con la información documentada en medios no electrónicos de la Firma Electrónica en relación con la firma autógrafa.

Limitaciones legales de la tecnología electrónica

En nuestro país, dentro del Código de Comercio, se encuentra el Título Segundo "Del Comercio Electrónico" que se divide en los

Revista de Derecho Notarial Mexicano, núm. 121, México, 2007.

siguientes capítulos "De los Mensajes de Datos"; "De las Firmas"; "De los Prestadores de Servicios de Certificación"; y, "Reconocimiento de Certificados y Firmas Electrónicas Extranjeros". En relación con la actividad notarial, el problema que existe en estas disposiciones es que el prestador del servicio electrónico es una empresa que requiere de una millonaria inversión, tanto por la concesión expedida por la Secretaría de Economía como por los implementos físicos y humanos exigidos, en donde el notariado es un agente certificador dependiente de la empresa y no como en otros países donde los colegios o cámaras notariales son los que prestan este servicio.

Necesidad de reformas a los códigos civiles, *códigos de comercio*, códigos de procedimientos civiles y leyes *del notariado*

Códigos Civiles: En México existen más de 30 códigos civiles que rigen a cada uno de los Estados de la República y un código federal. La mayoría de los códigos estatales resultan anacrónicos en materia electrónica, sin embargo, el código federal establece, cuando trata el consentimiento, artículos 1803, 1804 y 1811 que la voluntad puede expresarse por medios electrónicos, óptico o cualquier otra tecnología. El Código de Comercio, en tratándose de Registro Público de Comercio, el artículo 20 en su parte correspondiente establece:

El Registro Público de Comercio operará con un programa informático y con una base de datos central interconectada con las bases de datos de sus oficinas ubicadas en las entidades federativas. Las bases de datos contarán con al menos un respaldo electrónico.

Mediante el programa informático se realizará la captura, almacenamiento, custodia, seguridad, consulta, reproducción, verificación, administración y transmisión de la información registral.

Las bases de datos del Registro Público de Comercio en las entidades federativas se integrarán con el conjunto de la información incorporada por medio del programa informático de cada inscripción o anotación de los actos mercantiles inscribibles, y la base de datos central con la información que los responsables del Registro incorporen en las bases de datos ubicadas en las entidades federativas.

El programa informático será establecido por la Secretaría. Dicho programa y las bases de datos del Registro Público de Comercio, serán propiedad del Gobierno Federal.

En caso de existir discrepancia o presunción de alteración de la información del Registro Público de Comercio contenida en la base de datos de alguna entidad federativa, o sobre cualquier otro

Revista de Derecho Notarial Mexicano, núm. 121, México, 2007.

respaldo que hubiere, prevalecerá la información registrada en la base de datos central, salvo prueba en contrario.

Por lo que se refiere al comercio electrónico como ya se comentó en el párrafo anterior, cuenta con un título especial y en materia de arbitraje, también establece las comunicaciones electrónicas como medio de contratar y sustanciar el arbitraje.

Los códigos de procedimientos civiles y penales todavía no tratan este medio de prueba.

La Ley del Notariado tampoco ha incursionado en el medio electrónico, por lo que su regulación, es necesaria y de pronta actualización.

Leyes electrónicas *especiales*

El título correspondiente en el Código de Comercio sobre "Del Comercio Electrónico" que ya fue comentado, su reglamento y acuerdos de la Secretaría de Economía.

Introducción

Para iniciar daremos un breve vistazo a la Teoría General de los Sistemas (TGS), con esto, buscamos que nuestros temas; Perfeccionamiento del contrato electrónico, Registro Público electrónico y Protección del consumidor. Sean reflexionados bajo la estructura básica de la Teoría General de los Sistemas que tiene la bondad (¡afortunadamente!) de facilitarles la compresión de nuestras exposiciones.

Teoría general de los sistemas

Esta teoría surgió con los trabajos del alemán Ludwig von Bertalanffy, publicados entre las décadas de 1950 – 1960.

La TGS busca producir teorías y formulaciones conceptuales que tengan aplicación en la realidad empírica.

Se fundamenta en tres premisas básicas:

1.- Los sistemas existen dentro de sistemas: cada sistema existe dentro de otro más grande.

2.- Los sistemas son abiertos: Los sistemas abiertos se caracterizan por un proceso de cambio con su entorno (que son los otros sistemas), recibe y descarga algo en los otros sistemas, generalmente en los contiguos.

(Cuando el intercambio cesa, el sistema se desintegra, esto es, pierde sus fuentes de energía.)

Revista de Derecho Notarial Mexicano, núm. 121, México, 2007.

3.- Las funciones de un sistema dependen de su estructura
Ejemplos: Para el sistema Jurídico; Constitución, Códigos, Leyes.
Para los sistemas biológicos: ejem. ; los tejidos musculares se contraen porque están constituidos por una estructura celular que permite contracciones.

Definición de Sistema

(Si bien existe una multitud de definiciones, para efecto de ser prácticos señalamos dos)
Sistema es un todo organizado y complejo; Es un conjunto o combinación de cosas o partes que forman un todo complejo o unitario
Su propósito u objetivo: todo sistema tiene uno o algunos propósitos.
Los elementos (u objetos), así como también las relaciones, se ajusta en una distribución que trata siempre de alcanzar su objetivo
En cuanto a su constitución, pueden ser físicos o abstractos:
Los Sistemas físicos o concretos: son los compuestos por equipos, maquinaria, objetos y cosas reales.
Los Sistemas abstractos: están compuestos por conceptos, ideas planes, hipótesis.
En cuanto a su naturaleza, pueden ser cerrados o abiertos:
Sistemas abiertos: estos presentan un intercambio con el ambiente, a través de entradas y salidas.
Intercambian energía y materia con el ambiente.
Son adaptativos para sobrevivir.
Su estructura es óptima cuando el conjunto de elementos del sistema se organiza, aproximándose a una operación adaptativa.
Entendiendo adaptabilidad como un continuo proceso de aprendizaje y de auto-organización.
Los Sistemas cerrados: estos no presentan intercambio con el medio ambiente que los rodea. No reciben ningún recurso externo y nada producen que sea enviado hacia fuera. En rigor, no existen sistemas cerrados.
Algunos de los principales parámetros de los sistemas son:
La Entrada, el insumo o impulso (input): es la fuerza de arranque del sistema, que provee el material o la energía para la operación del sistema.
El Procesamiento, procesado o transformación (throughput): es el fenómeno que produce cambios, es el mecanismo de conversión de las entradas en salidas o resultados.

La Salida, producto o resultado (output): es la finalidad para la cual se reunieron los elementos y las relaciones del sistema.

Los resultados de un proceso son las salidas, las cuales deben ser coherentes con el objetivo del sistema.

Los resultados de los subsistemas son intermedios. Los resultados de los sistemas son finales

La Retroalimentación, retro- información (feedback): es la función de retorno del sistema que tiende a comparar la salida con un criterio preestablecido, manteniéndola controlada dentro de su criterio o estándar.

El Ambiente: es el medio que envuelve externamente el sistema y está en constante interacción con el sistema.

La supervivencia de un sistema depende de su capacidad de adaptarse, cambiar y responder a las exigencias y demandas del ambiente externo.

El Sistema Abierto

El sistema abierto, es influenciado por el medio ambiente y a su vez influye sobre él, alcanzando un equilibrio dinámico en ese sentido.

La categoría más importante de los sistemas abiertos son los sistemas vivos, de estos, nuestro interés y enfoque están dirigidos hacia los sistemas sociales/jurídicos.

Como dijimos el sistema abierto interactúa constantemente con el ambiente en forma dual, o sea, lo influencia y es influenciado.

El sistema puede crecer, cambiar, adaptarse al ambiente y hasta reproducirse bajo ciertas condiciones del ambiente.

Es propio del sistema abierto competir con otros sistemas.

La Regeneración de las partes: Para que el sistema sobreviva debe regenerarse en sus partes, para así, sobrevivir en conjunto.

La Organización de las funciones; La organización se requiere en el sistema para tener un control y una buena toma de decisiones.

En un ambiente de constante cambio es necesario que en el sistema existan la investigación, la planeación y el desarrollo, aspectos que son necesarios para que el sistema pueda hacer ajustes.

Así que se puede decir:

Que el sistema abierto es un conjunto de partes en interacción constituyendo un todo sinérgico, orientado hacia determinados propósitos y en permanente relación de interdependencia con el ambiente externo.

A continuación mencionamos:

Algunas características y premisas de las organizaciones sociales como sistema abierto

La organización debe ser abordada como un sistema funcional, diferenciándolo de un sistema social mayor por sus propiedades esenciales y únicas.

El sistema esta organizado con el fin primero de alcanzar un determinado tipo de metas sistemáticas.

Interdependencia de las partes: El cambio en alguna de las partes del sistema, afectará a las demás.

Estado firme u homeostasis: la organización puede alcanzar el estado firme, solo cuando se presenta dos requisitos, la uni- direccionalidad y el progreso.

Este progreso es el mejoramiento que se efectúa para alcanzar la condición propuesta con un esfuerzo relativamente menor y mayor precisión.

Los sistemas sociales, al contrario de otras estructuras, no tienen limitación de amplitud. Las organizaciones sociales están vinculadas a un mundo de seres humanos, recursos materiales, Leyes y otros.

Los sistemas sociales necesitan entradas de producción y de mantenimiento;

Las entradas de producción son las importaciones de energía, procesadas para proporcionar un resultado productivo.

Las entradas de mantenimiento son las importaciones de energía que sustentan al sistema

Esta doctrina, dicta que Los sistemas sociales necesitan fuerzas de control (como El Fedatario Público) para reducir la variabilidad e inestabilidad de las acciones humanas.

Y como último punto menciona que las funciones, normas y valores son componentes principales del sistema social

Conclusión

De acuerdo a este esquema de pensamiento el Fedatario Público se interrelaciona con los individuos e instituciones como una fuerza motora INDEPENDIENTE que ejerce la Fe publica de manera Única en cada caso .

Entre otras funciones (desde el punto de vista de la TGS) el Fedatario desempeña un papel importante en el sistema social, que es el de reducir la variabilidad e inestabilidad de las acciones humanas.

Revista de Derecho Notarial Mexicano, núm. 121, México, 2007.

Su interacción con el sistema social refuerza la confianza y certidumbre de la sociedad.

No queremos dejar de mencionar que el fin que persigue esta introducción es que reflexionemos sobre el marco legal del comercio electrónico en México relacionándolo con los puntos mencionados de la TGS.

En México se inicia en el año 2000 la formación de las bases jurídicas para regular el comercio electrónico, estos cambios prevén también el uso de cualquier otra tecnología, esta iniciativa se plasma en las reformas a los:

Código de Comercio
Código Civil
Código Federal de Procedimientos Civiles y a la ;
Ley Federal de Protección al Consumidor.

La dinámica de los ajustes jurídicos necesarios para enfrentar los cambios en este rubro en México podrán ser comprendidos con mayor facilidad una vez que veamos los temas presentados como un todo dinámico e interrelacionado, iniciaremos con:

Perfeccionamiento del contrato

En nuestra legislación encontramos plasmado el concepto " perfeccionamiento", en el Código de Comercio (C.C.), en su Artículo 80 que dice; " los convenios y contratos mercantiles celebrados por correspondencia, telégrafo, o mediante el uso de medios electrónicos, ópticos o de cualquier otra tecnología, quedarán perfeccionados desde que se reciba la aceptación de la propuesta".....

El Contrato queda perfeccionado----- si se entiende como tal, el momento exacto en el que el contrato nace a la vida jurídica---- en el último instante en que la oferta es aceptada sin modificación alguna: Existen en la doctrina cuatro sistemas o teorías que gobiernan el momento preciso de la perfección del contrato:

A) Declaración.
B) Expedición
C) Recepción
D) Conocimiento o información

Con relación a los contratos electrónicos independientemente de la naturaleza civil o mercantil del contrato, así como del ámbito de

Revista de Derecho Notarial Mexicano, núm. 121, México, 2007.

aplicación, nacional ó internacional, el momento de perfeccionamiento del contrato vendrá determinado por la teoría de la recepción.

Para llegar a este punto del "perfeccionamiento" la ley señala una serie de requisitos o " ruta" a seguir antes de llegar a la aceptación.

Este proceso; Envío, recepción, verificación, y finalmente la aceptación o perfeccionamiento, involucra una serie de definiciones de conceptos (destinatario, emisor, firma electrónica, etcétera) utilizados en este proceso, mismas que se encuentran al final de este documento en "Definición de Conceptos".

El proceso

La Expedición o Envío

¿En qué momento se considera que ha sido enviado el mensaje?

"se tendrá por expedido cuando ingrese en un Sistema de Información que no esté bajo el control del Emisor o del Intermediario." (Art. 91 bis C. C.)

Con respecto al lugar de expedición del mensaje el Art. 94 del C. C. establece que se tendrá como lugar de origen el establecimiento principal o la residencia habitual del emisor.

Recepción

El Artículo 91 del C. C., señala que esta recepción está determina en : "el momento de su ingreso en el sistema designado por el destinatario", si no hubiere este sistema, la recuperación, de este mensaje por medio de otro sistema (no designado) se toma como el momento de recepción.

En lo referente al lugar de recepción del mensaje el Art. 94 del C. C dicta que será el establecimiento principal o residencia habitual del destinatario

Verificación de la Autenticidad

El Artículo 90 del C. C., señala que para no tener dudas de que el mensaje de datos proviene del emisor; el destinatario debe asegurarse que es autentico, utilizando medios de identificación antes convenidos (como; claves ó contraseñas.)

Continua en el 90 bis, aclarando que se puede dar como cierto el mensaje si el destinatario aplicó el procedimiento acordado pre-

Revista de Derecho Notarial Mexicano, núm. 121, México, 2007.

viamente con el emisor, para establecer sin duda que proviene de este (el emisor.)

En el caso contrario, se da como falso; si el destinatario conoce que el mensaje de datos no proviene del emisor, o bien al aplicar el método de identificación convenido resulta que no es autentico (no proviene del emisor.)

Acuse de Recibo del Mensaje

Este aviso de haber recibido el mensaje es abordado en el Artículo 92 del C. C., que señala que cuando el emisor solicita este acuse y ambos no han acordado una forma o método para efectuarlo, el destinatario lo podrá hacer comunicándose de cualquier forma con el emisor o bien, este acuse, se dará por recibido si el destinatario efectúa algún acto que indique que ha recibido dicho mensaje.

En el caso de que el emisor condicione el recibir este acuse y no sea así, (en un plazo fijado o razonable) no se dará el efecto.

Si existe entre ambos el acuerdo de un acuse de recibo el emisor debe indicar de manera tácita que; el efecto, esta condicionado a este acuse.

Para recibirlo se puede acordar un plazo o esperar un tiempo razonable (esto último, de acuerdo a la naturaleza del negocio.)

En el caso de que el emisor no haya recibido este acuse en el tiempo acordado, se lo informará al destinatario pudiendo fijar un nuevo plazo para recibirlo. Una vez recibido se sabe que el mensaje llegó.

El Efecto

En su Artículo 95 del C.C., señala que una vez que se tiene la certeza de que el mensaje es valido, sin errores e único, el destinatario puede actuar en consecuencia.

Der. Completar los requisitos para que un acto civil, especialmente un contrato, tenga plena fuerza jurídica.

La Conservación del Mensaje y su integridad

Los comerciantes estás obligados a conservar por un plazo mínimo de diez años el mensaje de datos, este, debe mantenerse integro entendiendo por integro que esta ..."completo e inalterado independientemente de los cambios que hubiere podido sufrir el

Revista de Derecho Notarial Mexicano, núm. 121, México, 2007.

medio que lo contiene" (Art. 49 y 93, 93 bis C.C.), la Secretaría de Comercio emite la Norma Oficial Mexicana para la conservación de mensajes de datos, que se encuentra en el Anexo 1, (NOM-151-SCFI-2002, Prácticas comerciales-Requisitos que deben observarse para la conservación de mensajes de datos.)

El Fedatario Público y el Mensaje de Datos

Se establece (Art. 93 C.C. tercer párrafo) .... "que cuando la Ley exija que un acto jurídico se otorgué en instrumento ante Fedatario Público, éste y las partes obligadas podrán, a través de mensajes de datos, expresar los términos exactos en que las partes han decidido obligarse, en cuyo caso el Fedatario Público deberá hacer constar en el propio instrumento los elementos a través de los cuales se atribuyen dichos mensajes a las partes y conservar bajo su resguardo una versión íntegra de los mismos para su ulterior consulta, otorgando dicho instrumento de conformidad con la legislación aplicable que lo rige."

Equivalencia entre el mensaje de datos y la firma autógrafa

El proceso que vimos someramente es posible a la equivalencia que la Ley hace entre el mensaje de datos y la firma autógrafa utilizada por cientos de años, la Ley mexicana lo define en su C. C. de la siguiente manera:

El Código de Comercio en su Art. 89, confiere una equivalencia funcional entre el mensaje de datos y la información documentada en medios no electrónicos, así como entre la firma electrónica en relación con la autógrafa.

Por lo que este mensaje tiene un efecto jurídico de validez o fuerza obligatoria (Art. 89 bis, C.C. .)

Y podrá ser tomado como medios de prueba en una controversia judicial (Art. 1205 C.C.) . Siempre que sea atribuible a algunas de las partes (Art. 93, C.C.).

Estimando principalmente lo confiable del método con que ha sido generado, comunicado y archivado o conservado (Art. 1298- A, C.C.)

En Nuestra Legislación El Código de Federal de Procedimientos Civiles y el Código Civil Federal son parte fundamental en la estructura jurídica del mensaje de datos.

Revista de Derecho Notarial Mexicano, núm. 121, México, 2007.

Código Federal de Procedimientos Civiles

En el Código Federal de Procedimientos Civiles encontramos en el año 2000 la inclusión del Artículo 210-A, donde se consigan : "que se reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología". En su segundo párrafo aclara que para valorar la fuerza probatoria de este tipo de información, como principio fundamental valorará la seguridad del método con que ha sido generado, comunicado, recibido y/o archivado el mensaje (o información), por ultimo señala, que en caso necesario debe ser posible atribuir a las personas obligadas, el contenido de la información, por lo tanto, debe ser factible de acceder a esta información en cualquier momento. n el momento que se puede acceder a esta información, como se ve en el tema " Derecho informático y protección al consumidor" en el caso de las Leyes mexicanas se cuenta con una Norma Oficial para las prácticas comerciales, los requisitos que deben observarse para la conservación de mensajes de datos. (Véase Anexo 1)

Código civil federal

A la par de las reformas y adiciones al Código Federal de Procedimientos Civiles se llevaron al mismo tiempo las reformas y adiciones al Código Civil Federal

En su Artículo 1803, dice; "El consentimiento puede ser expreso o tácito, para ello se estará a lo siguiente: en su Fracción I indica que esta voluntad será patente, clara, ya sea si se manifiesta verbalmente, por escrito, por medios electrónicos, ópticos u otros signos inequívocos.

Artículo 1805; nos dicta que si se ha utilizando algún medio electrónico para un ofrecimiento sin fijar un plazo para la respuesta y esta no se hace de inmediato, el que ofrece queda desligado.

El Artículo 1811 En su segundo párrafo encontramos que si la propuesta y aceptación es efectuada a través de un medio electrónico, óptico o cualquier otra tecnología no requiere de estipulaciones previas entre los contratantes para que produzca efectos.

Artículo 1834 bis; encontramos una gran similitud de este, con el tercer párrafo del Artículo 93 del C. C., donde señala que el mensaje es una vía de comunicación. Y en el Código Civil Federal (Art.1834 bis) permite generar, enviar, recibir, archivar o comunicar la información que contenga los términos en que las partes han decidido obligarse, utilizando medios electrónicos.

Revista de Derecho Notarial Mexicano, núm. 121, México, 2007.

Definición de conceptos

En su Titulo Segundo "De comercio electrónico"; Capítulo I; " De los mensajes de datos" en el Artículo 89 señala que la actividad que regula, esta sometida a los principios de autonomía de la voluntad, neutralidad tecnológica, compatibilidad internacional.

Define los conceptos utilizados en el comercio electrónico :

Certificado: Todo Mensaje de Datos u otro registro que confirme el vínculo entre un Firmante y los datos de creación de Firma Electrónica.

Datos de Creación de Firma Electrónica: Son los datos únicos, como códigos o claves criptográficas privadas, que el Firmante genera de manera secreta y utiliza para crear su Firma Electrónica, a fin de lograr el vínculo entre dicha Firma Electrónica y el Firmante.

Destinatario: La persona designada por el Emisor para recibir el Mensaje de Datos, pero que no esté actuando a título de Intermediario con respecto a dicho Mensaje.

Emisor: Toda persona que, al tenor del Mensaje de Datos, haya actuado a nombre propio o en cuyo nombre se haya enviado o generado ese mensaje antes de ser archivado, si éste es el caso, pero que no haya actuado a título de Intermediario.

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

Firma Electrónica Avanzada o Fiable: Aquella Firma Electrónica que cumpla con los requisitos contemplados en las fracciones I a IV del artículo 97. que son:

(Art. 97 C.C.) La Firma Electrónica se considerará Avanzada o Fiable si cumple por lo menos los siguientes requisitos:

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

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

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

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

Revista de Derecho Notarial Mexicano, núm. 121, México, 2007.

En aquellas disposiciones que se refieran a Firma Digital, se considerará a ésta como una especie de la Firma Electrónica.

Firmante: La persona que posee los datos de la creación de la firma y que actúa en nombre propio o de la persona a la que representa.

Intermediario: En relación con un determinado Mensaje de Datos, se entenderá toda persona que, actuando por cuenta de otra, envíe, reciba o archive dicho Mensaje o preste algún otro servicio con respecto a él.

Mensaje de Datos: La información generada, enviada, recibida o archivada por medios electrónicos, ópticos o cualquier otra tecnología.

Parte que Confía: La persona que, siendo o no el Destinatario, actúa sobre la base de un Certificado o de una Firma Electrónica.

Prestador de Servicios de Certificación: La persona o institución pública que preste servicios relacionados con Firmas Electrónicas y que expide los Certificados, en su caso.

Secretaría: Se entenderá la Secretaría de Economía.

Sistema de Información: Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma Mensajes de Datos.

Titular del Certificado: Se entenderá a la persona a cuyo favor fue expedido el Certificado.

Protección del consumidor

(Medios Electrónicos)

En México la Procuraduría Federal de Consumidor Institución que depende de la Secretaría de Comercio, es la entidad que lleva a la vida diaria el precepto constitucional que prohíbe el cobro de precios exagerados en bienes y servicios y todo lo que constituya una ventaja indebida ordenando que las leyes fijen las bases para los precios máximos en materias o productos necesarios para la economía nacional o el consumo popular. (Art. 28)

En pocos años, internet se ha convertido en una de las fuentes de información y medio de comunicación más importante del mundo.

La naturaleza de las redes digitales y las tecnologías de computación que intervienen en el mercado electrónico crearon en México (como en otros países) la necesidad de construir las bases de un marco legal de protección del consumidor.

Es importante revisar algunos aspectos como son:

Contexto económico

De acuerdo con el estudio de la Asociación Mexicana de Internet, A.C. que llevo a cabo en el 2005 (Estudio de la AMIPCI Internet en México 2005). Al cierre de 2005 existían 17.1 millones de usuarios de Internet en nuestro país.

Con una base de 6.3 millones de "Pcs" con conexión a Internet, de las cuales el 58% se encuentran en los hogares y 42% en las empresas. De los usuarios el 9 % realizó una compra por Internet en los últimos 30 días. En el 2004 las ventas totales del Comercio electrónico en México alcanzaron la cifra de 210 millones de dólares.

En cuanto a los servicios financieros en línea, los datos de la Comisión Nacional Bancaria y de Valores (CNBV) reportan, que de enero a diciembre de 2005, el número de transacciones totales ascendió a 288 mil 657. Esto fue un incremento superior al 110% de las operaciones reportadas en 2004.

Directrices

Creemos que las Directrices de la OCDE emitidas en su declaración de 1998 sirven como marco para el desarrollo de la exposición.

(Declaración Ministerial sobre Protección del Consumidor en el contexto del Comercio Electrónico del 8 y 9 de octubre de 1998)

Directrices:

Sus principios generales buscan la protección efectiva y transparente, aclarando que ésta no sea menor al nivel de protección que asegura otras formas de comercio. Como recordamos en México a través de las leyes que hemos citado se reconoce la igualdad jurídica en ambas esferas.

Sugiere que los gobiernos, proveedores, consumidores y sus representantes trabajen en conjunto para conseguir esa protección. Para determinar qué cambios serían necesarios para abarcar las especiales circunstancias del comercio electrónico.

Identificación adecuada

Señala que los proveedores no harán uso de las características especiales del comercio electrónico para ocultar su identidad o ubicación real, o para evitar cumplir con los estándares de protección del consumidor y/o los mecanismos de aplicación de esta protección.

Revista de Derecho Notarial Mexicano, núm. 121, México, 2007.

Información sobre los bienes y servicios

Para lograr esto, los proveedores deben facilitar a los consumidores la información correcta y de fácil acceso que describa los bienes o servicios ofrecidos, lo suficiente, para permitir que los consumidores realicen una decisión informada sobre la conveniencia o no de efectuar la transacción.

Información sobre la transacción

Se debe proporcionar a los consumidores una amplia información sobre los términos, condiciones y costos asociados con la transacción,

Tal información deberá ser clara, correcta, fácilmente accesible y proporcionada de tal manera que le dé a los consumidores la oportunidad de tener elementos suficientes para su decisión antes de realizar la transacción.

El lenguaje debe ser claro al explicar las condiciones y términos de la transacción.

Cuando sea aplicable se mantendrá un registro de tal información.

Se recomienda que esta información contenga lo siguiente:

1.- Los costos totales a cobrar; (desglosando los impuestos y otros costos)

2 .- Los plazos de entrega o cumplimiento del servicio.

3.- Los términos, condiciones y métodos de pago.

4.- Las restricciones, limitaciones o condiciones de la compra (tales como el requisito de aprobación de la misma por parte de los padres o tutores, restricciones geográficas o de tiempo)

5.- Información sobre la existencia de servicios de posventa.

6.- Instrucciones de uso, incluyendo alertas de seguridad y cuidado de la salud.

7.- Los detalles y condiciones sobre la retractación, cancelación, retorno, cambio, terminación y/o reembolso.

8.- Debe indicar la moneda aplicable a la transacción.

9.- Las garantías disponibles.

Proceso de confirmación

El fin de este proceso es evitar las ambigüedades y conferir certeza en el intento por parte del consumidor de realizar una transacción.

Revista de Derecho Notarial Mexicano, núm. 121, México, 2007.

Antes de finalizar la transacción el consumidor puede identificar en forma precisa, las claves, métodos y otros elementos acordados antes de adquirir los bienes o servicios.

En este paso debe existir la posibilidad de corregir cualquier error.

Se debe mantener un completo y exacto archivo de la transacción.

Una vez cumplido el proceso el consumidor podrá expresar un consentimiento informado.

El pago

Los mecanismos de pago deben ser seguros y fáciles de utilizar, con sistemas que eviten cobros fraudulentos o no autorizados.

La OCDE insiste en que en la medida que esta herramienta sea cada vez más sólida aumentará la confianza del consumidor.

Resolución de conflictos

La resolución de conflictos debe contar con un sistema que sea apropiado y efectivo, con un marco legal que asegure una protección efectiva y transparente al consumidor

Se debe difundir la información sobre los aspectos más relevantes de las leyes de protección del consumidor así como de las vías de solución de conflictos.

Privacidad

Este tipo de comercio debe realizarse respetando los datos personales del consumidor, es decir el prestador de bienes y servicios no pueden difundirlos.

Con respecto a los mensajes comerciales usados tan comúnmente en este medio, si los consumidores no desean recibir este tipo de mensajes, la elección debe ser respetada.

Educación

Exhorta a las instituciones educativas y a los medios de comunicación a utilizar las herramientas que les son propios para educar a los consumidores y proveedores, acerca de las técnicas novedosas que hacen posible la comunicación a través de la red global.

Revista de Derecho Notarial Mexicano, núm. 121, México, 2007.

Un vez que hemos visto estos aspectos pasamos a Ley Federal de Protección al Consumidor de nuestro país:

Esta Ley es adicionada y modificada junto con el marco legal complementario (que hemos visto en la ponencia " Perfeccionamiento)

En el año 2000 inician estos cambios y continúan en 2004.

En el año 2000

Se reforma y adiciona quedando de la siguiente manera :

En el Artículo 1 de esta Ley indica que protege al consumidor en las transacciones efectuadas a través del uso de medios convencionales, electrónicos, ópticos o de cualquier otra tecnología. (DOF 29-05-2000, reformada DOF 04-02-2004)

Señala que el objetivo de la Procuraduría (Art. 24) es la de promover y proteger los derechos del consumidor respecto de las transacciones que celebren a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología" (Fracción IX adicionada DOF 29-05-2000)

En este mismo año(2000) se le adicionó el Capítulo VIII bis:

"De los Derechos de los Consumidores en las transacciones efectuadas a través del uso de Medios Electrónicos, Ópticos o de cualquier otra tecnología.

Que contiene un solo Artículo el 76 bis., con VIII fracciones.

Este Artículo regula las relaciones entre consumidores y proveedores que utilizan en sus transacciones los medios electrónicos, señalando que se debe cumplir con lo que se establece en sus fracciones de la I a la VII:

(DOF 29-05-2000)

La Fracción I se refiere a que la información que posee el proveedor sobre el consumidor es confidencial prohibiendo su difusión.

La Fracción II señala que el proveedor debe utilizar elementos técnicos de seguridad para brindar confidencialidad al consumidor informándole a este ultimo sobre las características generales de los elementos de seguridad utilizados, antes de la transacción.

En la fracción III se ordena al proveedor que proporcione todos los datos necesarios para que el consumidor pueda localizarlo en caso de que así lo desee; teléfono, dirección, correo electrónico, etc.

La IV señala que el proveedor debe evitar prácticas comerciales engañosas.

Su Fracción V establece que el proveedor esta obligado a informar de forma minuciosa los costos y formas de pago del bien o servicio ofrecidos por el. En la VI se señala que el proveedor debe respetar las decisiones del consumidor sobre la cantidad y calidad del producto ofrecido, así como sobre recibir avisos comerciales.

La Fracción VII, prohíbe al proveedor el uso de acciones de publicidad o ventas que no sean claras, señalando en especial a la población vulnerable; como son los niños, ancianos y enfermos. Obligándolo a incorpora mecanismos de advertencia cuando la información no sea apta para esta población. Esta Fracción (VII) fue reformada en el año 2004. (DOF 04-02-2004)

En el Capítulo X: De los contratos de adhesión, en el Artículo 86 BIS, se refiere a que estos contratos (los de adhesión) puedan ser emitidos por el proveedor y aceptados por el consumidor vía electrónica. Este Artículo fue adicionado el año 2000 (DOF 05-06-2000) y reformado el año 2004, (DOF 04-02-2004)

Año 2004

Prohíbe (Art., 10) de manera tacita cualquier acción que atente contra la libertad, seguridad o integridad personal de los consumidores así como la de prestar servicios adicionales a los a no solicitados o aceptados ya expresamente, ya fueren por escrito o por vía electrónica. (DOF 04-02-2004)

ARTÍCULO 17.- En la publicidad que se envíe a los consumidores se deberá indicar el nombre, domicilio, teléfono y, en su defecto, la dirección electrónica del proveedor; de la empresa que, en su caso, envíe la publicidad a nombre del proveedor, pudiendo pedir al proveedor por medio de la Procuraduría F. del C. no ser molestado con publicidad que no desea.

Párrafo reformado DOF 04-02-2004

Para ilustrar hacia donde deben ir encuazados los esfuerzos de nuestro quehacer es muy ilustrativo el siguiente cuadro:

Revista de Derecho Notarial Mexicano, núm. 121, México, 2007.

CARACTERÍSTICAS DE LOS SITIOS MEXICANOS DE COMERCIO ELECTRÓNICO
Información obtenida en visitas directas a 114 sitios entre el 30 de marzo y el 28 de abril de 2004

		Porcentaje del total de sitios visitados que cuentan con:
IDENTIDAD DEL VENDEDOR	Domicilio	86.8
	Correo electrónico	74.6
	Número telefónico	94.7

		Porcentaje del total de sitios visitados que cuentan con:
INFORMACIÓN SOBRE LA TRANSACCIÓN	Descripción detallada de bienes o servicios	100
	Costos totales	96.5
	Moneda aplicable a la transacción	98.2
	Plazos de entrega	78.9
	Condiciones de devolución, reembolso y cancelación	50.9
	Ayuda en caso de dudas para consultar la página	80.7
	Corrección de errores en la orden de compra	78.1

		Porcentaje del total de sitios visitados que cuentan con:
POLÍTICAS DE PRIVACIDAD	Políticas explícitas de privacidad o de seguridad	38.6
	Especifica para qué utilizarán la información proporcionada por el usuario	38.6
	Especifica quiénes van a tener acceso a esa información	34.2

		Porcentaje del total de sitios visitados que cuentan con:
SEGURIDAD DEL SITIO	Para datos personales	45.6
	Para datos financieros*	77.1

* Porcentaje de sitios que utilizan tarjeta de crédito como forma de pago.
Fuente: Asociación Mexicana de internet, A. C.; estudio de la AMIPCI Internet en México 2005

Revista de Derecho Notarial Mexicano, núm. 121, México, 2007.

De esta información se puede inferir que del total de sitios visitados la gran mayoría disponen de información clara sobre la identidad del vendedor.

En el rubro "información sobre la transacción" vemos que en las condiciones de devolución, reembolso y cancelación, son menos los que lo cumplen.

Las políticas de privacidad no son instrumentadas por la mayoría de sitios y en cuanto a seguridad se presta mayor atención a la financiera.

A manera de Conclusión podemos decir que:

Estos cambios en Ley están orientados a cubrir los desafíos que presenta el comercio electrónico debido a su dinámica tecnológica.

Como sabemos este tipo de comercio por sus características técnicas suponen un continuo estudio e investigación continuo de los cambios que se den en este campo para poder abordar de forma adecuada los temas relacionados con la protección del consumidor en el contexto de este comercio.

Entidades certificadoras

Objetivo

Siguiendo la línea de difundir al máximo el uso de la firma electrónica es necesario crear una empresa privada, pública o colegio profesional para crear su propia autoridad de certificación o disponer de una autoridad de registro para la gestión de sus certificados electrónicos. La propuesta es que en un futuro no muy lejano en América se generen los certificados notariales, que sean emitidos ante notario tanto a personas físicas como morales, el notario, realizaría la correspondiente verificación de identidad, quedando ésta, reflejada en el certificado que emita el colegio profesional en este caso se propone que realizando modificaciones a la ley mexicana pueda emitir dicho certificado la asociación nacional del notariado mexicano.

La NOM-151-SCFI-2002 establece los requisitos que deben observarse para la conservación del contenido de mensajes de datos que consignen contratos, convenios o compromisos y que en consecuencia originen el surgimiento de derechos y obligaciones.

Campo de aplicación

La NOM-151-SCFI-2002 es de observancia general para los comerciantes que deban conservar los mensajes de datos en que se consignen contratos, convenios o compromisos que den nacimiento a derechos y obligaciones, así como para todas aquellas personas con quienes los comerciantes otorguen o pacten dichos contratos, convenios o compromisos.

Ejemplos:

Facturas
Pagarés
Contratos, otros.
Archivos parciales
Formación de los archivos parciales
Obtención de los compendios o resúmenes digitales
Expediente Electrónico
Integración del expediente electrónico
Constancia del Prestador de Servicios de Certificación
Obtención de la constancia del Certificador
Formación de la constancia
Método de verificación de autenticidad

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

El nombre del archivo del sistema de información en el que está o estuvo almacenado el contenido del archivo,

El tipo del archivo, y

El contenido del mismo; con el objetivo de guardar la relación lógica que existe entre estos tres elementos

Integración del expediente electrónico

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

El nombre del expediente, que debe de coincidir con el nombre con el que se identifica en el sistema de información en donde está o estuvo almacenado,

Un índice, que contiene el nombre y el compendio de cada archivo parcial que integra el expediente,

La identificación del operador del sistema de conservación, y

Su firma digital de acuerdo a la definición correspondiente en la presente Norma Oficial Mexicana.

Obtención de la constancia del prestador de servicios de certificación

Para la obtención de la constancia el sistema de conservación deberá usar el protocolo de aplicación descrito en el 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

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

Formación de la constancia

El Prestador de Servicios de Certificación formará una constancia en formato ASN.1 que contendrá:

El nombre del archivo en donde está almacenada la constancia.

El expediente enviado por el sistema de conservación,

Fecha y hora del momento en que se crea la constancia,

La identificación del prestador de servicios de certificación y

Su firma digital de acuerdo a la definición correspondiente de esta Norma Oficial Mexicana.

Método de verificación de autenticidad

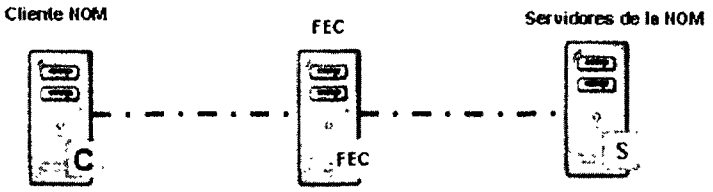
La verificación de la autenticidad de una constancia se realizará por medio del uso de un sistema de verificación que lleve a cabo los pasos siguientes:

Verificar la firma digital del Prestador de Servicios de Certificación en la constancia;

Verificar la firma digital del operador del sistema de conservación en el expediente contenido en la constancia, y

Recalcular el compendio de él o los archivos parciales y verificar que coincidan con los compendios asentados en el expediente.

COMPONENTES DE LA ARQUITECTURA NOM



El modelo básico de operación se compone de tres tipos de servidores o elementos:

Cliente
Front End de Comunicaciones (FEC)
Servidor NOM

Cliente

El Cliente genera, a partir de sus mensajes o archivos originales de datos los archivos parciales necesarios para hacer con ellos un expediente el cual enviará al Servidor NOM.

La Solicitud de conexión por parte del Cliente ante el Servidor NOM, se establece a través del FEC

FEC - Front end de comunicaciones

El FEC es un mecanismo de enlace entre clientes y servidores.

Se encarga de aceptar las conexiones de los clientes, autenticar y, en caso de que el servicio al que se deseen conectar se encuentre en operación, avisar a éste último de la conexión del cliente.

En este esquema los clientes no establecen comunicación directa con el servidor, en lugar de ello envían sus mensajes a través del FEC, éste los toma y los entrega al servidor adecuado.

Del mismo modo, el FEC recibe los mensajes del servidor y los entrega al cliente indicado por éste.

Servidor NOM

El Servidor NOM forma parte de la infraestructura del Prestador de Servicios de Certificación

Emite la constancia

Importancia

Existen diferentes leyes, normas y regulaciones que obligan a almacenar la información de los procesos de negocio por diferentes

períodos de tiempo, por lo que es de vital importancia al transcurrir este tiempo (5, 10, 15 0 20 años), tener bien identificado el archivo fuente y su respectiva constancia en caso de presentarse una controversia legal ante un juzgado, mismo que exigirá como fuerza probatoria la validación de que el documento original no ha sido modificado en el tiempo.

Importancia

Los archivos fuentes normalmente son generados y almacenados por diferentes aplicaciones y en diferentes repositorios entre los que se encuentran las Bases de Datos, sistemas LDAP, sistemas de archivos, etc. SeguriNOM cuenta con dos opciones clientes para la selección de los archivos fuentes y generación de los expedientes, la primera consiste en una interfaz gráfica cuyo proceso se realiza manualmente y la segunda consiste en un proceso automático a través de la integración de API's.

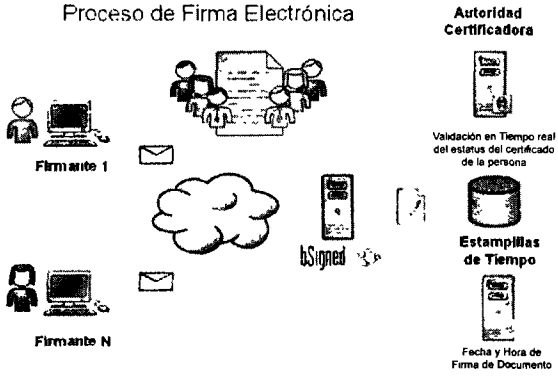
Esquema comercial

El esquema comercial consiste en:
Adquisición de certificados
Pago de una renta mensual

Un pago a mes vencido por las transacciones realizadas o precompra de un paquete de transacciones.

Se anexa al presente trabajo las Reglas Generales a las que deberán sujetarse los prestadores de servicios de certificación:

En México es el **Gobierno Federal** a través de la **Secretaría de Economía** quien acredita a los prestadores de servicios para certificación digital y el proceso que se sigue en una firma electrónica se gráfica con la siguiente representación.



A continuación anexo las las reglas que expidió el Gobierno Federal y que por si solas se explican.

Reglas generales a las que deberán sujetarse los prestadores de servicios de certificación

(Publicadas en el Diario Oficial de la Federación el 10 de agosto de 2004)

Al margen un sello con el Escudo Nacional, que dice:
Estados Unidos Mexicanos.-
Secretaría de Economía.

FERNANDO DE JESUS CANALES CLARIOND, Secretario de Economía, con fundamento en lo dispuesto por los artículos 102 inciso A) fracción V, 104 fracciones IV y VI, 105 y 113 del Código de Comercio, artículos 2o., 3o. primer párrafo, 4o. fracciones IV y V, 5o. segundo párrafo, 6o. segundo párrafo, 9o., 10 fracción III, 11, 12, y 16 fracción III del Reglamento del Código de Comercio en materia de Prestadores de Servicios de Certificación, y

CONSIDERANDO

Que el Plan Nacional de Desarrollo 2001-2006 establece que dentro del proceso de globalización corresponde al Estado promover las condiciones para la inserción competitiva de México en el nuevo orden económico mundial. Por lo que se promoverán todas las reformas necesarias para que la economía funcione mejor, los mercados sean más eficaces y se reduzca el poder de mercado de monopolios y oligopolios. Asimismo se buscará aumentar y extender la competitividad del país, la competitividad de las empresas, la competitividad de las cadenas productivas y la competitividad de las regiones. Lo anterior implica regulación apropiada, disponibilidad oportuna y eficaz de infraestructura económica para el desarrollo, fomento de capacidades para el trabajo productivo de clase mundial, desarrollo tecnológico y científico para la nueva economía; todo ello en el marco de una moderna cultura laboral y empresarial;

Que el Decreto por el que se reforman y adicionan diversas disposiciones del Código de Comercio en Materia de Firma Electrónica, publicado en el Diario Oficial de la Federación el 29 de agosto de 2003, en el capítulo III que se adiciona denominado: "De los Prestadores de Servicios de Certificación", determina que la Secretaría de Economía coordinará y actuará como autoridad certificadora, y registradora, respecto de los Prestadores de Servicios de Certificación a los que se refiere dicho capítulo, en ese mismo capítulo se señala

Revista de Derecho Notarial Mexicano, núm. 121, México, 2007.

que la Secretaría de Economía tiene que determinar algunos de los requisitos y obligaciones solicitados en el Código de Comercio, y Que el Reglamento del Código de Comercio en materia de Prestadores de Servicios de Certificación, publicado en el Diario Oficial de la Federación el 19 de julio de 2004, señala que los elementos humanos, materiales, económicos y tecnológicos, así como el monto y condiciones de la fianza y demás procedimientos con los que tiene que cumplir el Prestador de Servicios de Certificación, serán determinados por la Secretaría de Economía, he tenido a bien expedir las siguientes:

REGLAS GENERALES A LAS QUE DEBERAN SUJETARSE LOS PRESTADORES DE SERVICIOS DE CERTIFICACION

1. En la aplicación de las presentes Reglas Generales se estará a las definiciones a que se refiere el artículo 89 del Código de Comercio y se entenderá por Reglamento al Reglamento del Código de Comercio en materia de Prestadores de Servicios de Certificación. Unidad de Asuntos Jurídicos Dirección de Legislación

2. Conforme a lo dispuesto por el artículo 102 inciso A) fracciones II y III del Código de Comercio y la fracción III del artículo 5 del Reglamento, la Secretaría tendrá por satisfechos los elementos humanos, materiales, económicos y tecnológicos y procedimientos a que se refieren dichas disposiciones, por parte de un Solicitante de Acreditación como Prestador de Servicios de Certificación, en adelante el Solicitante de Acreditación, y por un Prestador de Servicios de Certificación ya acreditado, en los términos siguientes:

2.1.- Elementos humanos

Los profesionales jurídico e informático, serán responsables de aprobar el plan de continuidad del negocio que señalan las presentes Reglas Generales. El grado académico, los cursos con los que deben contar los profesionales jurídico, informático, así como el personal auxiliar del profesional informático y los requisitos que deben cumplir serán al menos los siguientes:

2.1.1. El profesional jurídico deberá:

2.1.1.1. Ser licenciado en derecho o abogado con título y cédula profesional registrados en la Secretaría de Educación Pública;

2.1.1.2. Demostrar al menos dos años de experiencia en materia notarial o de correduría pública, o en materia mercantil y servicios, procedimientos o actividades relacionadas con la acreditación de la personalidad;

Revista de Derecho Notarial Mexicano, núm. 121, México, 2007.

2.1.1.3. Acreditar al menos un año de experiencia comprobable en actividades relacionadas con cualquier área del derecho informático o comercio electrónico;

2.1.1.4. Cumplir con el requisito establecido en el artículo 102 inciso A) fracción IV del Código de Comercio y el artículo 5 fracción V del Reglamento;

2.1.1.5. Comprobar que conoce la operación como usuarios de los sistemas informáticos que habrá de utilizar el Solicitante de Acreditación y el Prestador de Servicios de Certificación, y

2.1.1.6. Solicitud de examen para encargado de identificación correspondiente, mismo que aplicará la Secretaría dentro de los cuarenta y cinco días siguientes a la presentación de la solicitud del Solicitante de Acreditación, previa notificación de fecha, hora y lugar en el que se aplicará el mismo.

2.1.1.7. Los requisitos de los apartados del 2.1.1.2. al 2.1.1.5. podrán acreditarse con declaración ante fedatario público en la cual el profesionista jurídico manifieste bajo protesta de decir verdad y advertido de las penas en que incurren los que declaran falsamente ante una autoridad distinta a la judicial, que cumple con cada uno de los requisitos y que incluya los datos de las empresas o instituciones y fechas en las que adquirió la experiencia, sus cargos y las actividades y funciones desempeñadas.

2.1.2. El profesional informático deberá:

2.1.2.1. Ser licenciado o ingeniero en área Informática o afín, con título y cédula profesional registrados en la Secretaría de Educación Pública; Unidad de Asuntos Jurídicos Dirección de Legislación.

2.1.2.2. Comprobar al menos dos años de experiencia en el campo de seguridad informática con declaración ante fedatario público en la cual el profesionista informático manifieste bajo protesta de decir verdad y advertido de las penas en que incurren los que declaran falsamente ante una autoridad distinta a la judicial, que cumple con la misma y que incluya los datos de las empresas o instituciones y fechas en las que adquirió la experiencia, sus cargos y las actividades y funciones desempeñadas. Además, deberá contar con diploma en seguridad informática o, en su caso, tener alguna certificación en esta área como: "GIAC Gold Standard Certificates (GGSC), GIAC Security Leadership Certificate (GSLC), CISSP Certification y SSCP Certification" o equivalentes.

2.1.2.3. Cumplir con el requisito establecido en el artículo 102 inciso A) fracción IV del Código de Comercio y el artículo 5 fracción V del Reglamento.

Revista de Derecho Notarial Mexicano, núm. 121, México, 2007.

2.1.3. El Personal Auxiliar del Profesional Informático estará conformado por:

2.1.3.1. Un Oficial de Seguridad;

2.1.3.2. Un administrador de sistemas;

2.1.3.3. Un operador de sistemas;

2.1.3.4. Un administrador de bases de datos, y

2.1.3.5. Un administrador de redes.

2.1.3.6. El personal indicado en los apartados 2.1.3.2 a 2.1.3.5 deberán:

2.1.3.6.1. Ser técnico, licenciado o ingeniero en área Informática o afín;

2.1.3.6.2. Tener experiencia comprobable en el área de informática de cuando menos cuatro años, con declaración ante fedatario público en la cual el personal auxiliar del profesionista informático, a excepción del Oficial de Seguridad manifiesten cada uno bajo protesta de decir verdad y advertido de las penas en que incurren los que declaran falsamente ante una autoridad distinta a la judicial, que cumple con la misma y que incluya los datos de las empresas o instituciones y fechas en las que adquirió la experiencia, sus cargos y las actividades y funciones desempeñadas, así como las cartas de las empresas o instituciones públicas en donde la haya adquirido;

2.1.3.6.3. Comprobar experiencia en el campo de la seguridad informática de cuando menos dos años, con declaración ante fedatario público en la cual el personal auxiliar del profesionista informático, a excepción del Oficial de Seguridad manifiesten cada uno bajo protesta de decir verdad y advertido de las penas en que incurren los que declaran falsamente ante una autoridad distinta a la judicial, que cumple con la misma y que incluya los datos de las empresas o instituciones y fechas en las que adquirió la experiencia, sus cargos y las actividades y funciones desempeñadas, así como las cartas de las empresas o instituciones públicas en donde la haya adquirido.

2.1.3.6.4. Acreditar al menos una certificación en manejo de software o hardware referente a seguridad informática.

2.1.3.7. El Oficial de Seguridad será responsable del diseño, implantación, cumplimiento de los procedimientos y prácticas de seguridad en las instalaciones y deberá acreditar:

2.1.3.7.1. Los requisitos exigidos en el apartado 2.1.2. Unidad de Asuntos Jurídicos Dirección de Legislación.

2.1.3.8. A partir del inicio de operaciones en los términos previstos por el Reglamento, el Prestador de Servicios de Certificación deberá contar y notificar a la Secretaría, en un plazo no mayor a

seis meses, que cuenta con la totalidad del personal auxiliar del profesional informático, salvo el caso del Oficial de Seguridad que deberá estar designado desde el momento de la solicitud de acreditación y podrá ser el propio Profesional Informático.

2.1.4. La Secretaría, a efecto de verificar los conocimientos y habilidades de los elementos humanos de un solicitante de acreditación o de un Prestador de Servicios de Certificación, podrá requerir los exámenes que se hayan aplicado a dicho personal. Asimismo, en el caso del profesional informático y sus auxiliares se constatará que la elaboración y alcance de dichos exámenes sea compatible con el estándar ISO 17799, además en el caso del Oficial de Seguridad deberá ser compatible con el estándar ETSI TS 102 042.

2.1.5. El Solicitante de Acreditación y el Prestador de Servicios de Certificación, presentará y mantendrá actualizado ante la Secretaría, el procedimiento que utilizarán para reclutar, seleccionar, evaluar y contratar al personal a que se refieren las presentes Reglas Generales, el cual deberá describir la forma de corroborar los antecedentes del personal antes de contratarlo.

2.1.6. El Prestador de Servicios de Certificación deberá suscribir con el personal que maneje información confidencial un contrato de confidencialidad que se extienda más allá de la vigencia del contrato laboral del empleado o de servicios en caso de una empresa externa.

2.2.- Elementos Materiales y sus procedimientos:

En atención al dinamismo del avance tecnológico y la necesidad de preservar la seguridad física y lógica en la prestación del servicio de certificación, los elementos materiales que deberán estar en disposición del Solicitante de Acreditación y del Prestador de Servicios de Acreditación y los procedimientos aplicables en este ámbito, deberán contener como mínimo las características siguientes:

2.2.1. Las áreas y los servicios en los cuales se maneja información confidencial requerirán procedimientos de controles de acceso, deberán estar supervisados continuamente, a efecto de reducir al mínimo los riesgos.

2.2.2. Las implantaciones de los controles deberán evitar riesgo, daño o pérdida, de los activos, alteración o sustracción de información.

2.2.3. Los accesos físicos a las áreas de generación de certificados, gestión de revocación de certificados y área de residencia de servidores, deberán estar protegidas con puertas y muros sólidos y firmes, chapas seguras, controles de acceso, sistemas de extinción de incendios y alarmas de seguridad, y se encontrarán limitados sólo al personal autorizado mediante controles de autenticación de

Revista de Derecho Notarial Mexicano, núm. 121, México, 2007.

por lo menos dos factores para asegurar que no habrán accesos no autorizados. Los servicios compartidos por otra entidad distinta al Prestador de Servicios de Certificación o por personal de éste no dedicado al servicio de certificación, deberán estar fuera del perímetro de seguridad.

2.2.4. El acceso de visitas a las áreas con información confidencial deberá ser autorizado por el Oficial de Seguridad. El visitante deberá portar una credencial en todo momento para identificarse. Se deberá registrar toda actividad que realice el visitante con la fecha y hora de ingreso y salida. Unidad de Asuntos Jurídicos Dirección de Legislación.

2.2.5. Un documento que se denominará "Política de Seguridad Física", a que se sujetará la prestación del servicio, el cual será presentado por el Solicitante de Acreditación con su solicitud y que el Prestador de Servicios de Certificación deberá mantener actualizado. El documento denominado "Política de Seguridad Física" deberá contemplar y desarrollar por lo menos los siguientes aspectos:

2.2.5.1. Control de acceso físico;

2.2.5.2. Protección y recuperación ante desastres;

2.2.5.3. Protecciones contra robo, forzamiento y entrada no autorizada a los espacios físicos;

2.2.5.4. Medidas de protección en caso de incendio, contra fallas de servicios eléctricos o de telecomunicaciones.

2.2.5.5. Un procedimiento de actualización para autorización de acceso al personal a las áreas restringidas.

2.2.6. Las áreas seguras deben ser oficinas cerradas dentro del perímetro de seguridad física, contener mobiliario con gabinetes y chapas seguras.

2.2.7. Para la selección y el diseño de áreas seguras se debe tomar en cuenta la posibilidad de daños por fuego, sismo, inundación, explosiones, desórdenes civiles, y otras formas de desastres naturales y causadas por el hombre.

2.2.8. Todos los servicios claves deberán situarse alejados de las áreas de acceso y atención al público.

2.2.9. Los dispositivos como fax y fotocopiadoras deberán ubicarse dentro de las áreas seguras que así lo requieran, siempre bajo control para no comprometer la seguridad ni la confidencialidad de la información.

2.2.10. Todo material de desecho deberá ser destruido sin posibilidad de recuperación antes de desecharlo.

2.2.11. Las puertas y ventanas deberán estar siempre cerradas y aseguradas, instalando protecciones internas o externas en las mismas.

2.2.12. Deberá contarse con sistemas de detección de intrusión física en puertas y ventanas del perímetro de seguridad. Aquellas salas desocupadas que estén dentro del perímetro de seguridad, deberán tener activado el sistema de detección de intrusos todo el tiempo.

2.2.13. La gestión de los servicios de procesamiento de información deberá estar físicamente separada del resto de los servicios.

2.2.14. Deberán establecerse procedimientos y prácticas de seguridad para el personal dentro del perímetro de seguridad, que contemplen por lo menos lo siguiente:

2.2.14.1. El personal deberá conocer y entender los procedimientos y prácticas de seguridad dentro del perímetro de seguridad;

2.2.14.2. Las áreas vacías deberán cerrarse y revisarse periódicamente llevando una bitácora de tal revisión;

2.2.14.3. El personal de soporte que no es parte del personal del Solicitante de Acreditación o del Prestador de Servicios de Certificación, deberá acceder a las áreas restringidas sólo en caso necesario y si es autorizado por el Profesional Informático o el Oficial de Seguridad, además de ser acompañado por personal que sí lo esté;

Unidad de Asuntos Jurídicos Dirección de Legislación.

2.2.14.4. No se deberá permitir dentro del perímetro de seguridad equipo de grabación, audio o video, con excepción del propio equipo de seguridad; y de comunicaciones.

2.2.14.5. Las actividades sin supervisión dentro de las áreas seguras deberán definirse para evitar problemas de seguridad, y prevenir actividades contrarias al servicio;

2.2.14.6. La recepción de insumos y la salida de basura deberán estar controladas y separadas del área de procesamiento de la información, para evitar accesos no autorizados;

2.2.14.7. Los requerimientos de seguridad para las áreas de atención a clientes se determinarán a partir del Análisis y Evaluación de Riesgos y Amenazas a que se refieren las presentes Reglas Generales;

2.2.14.8. El personal que acceda a las áreas externas de recepción de insumos y de desechos deberá estar controlado. Se deberá contar con los mecanismos que impidan que el personal no autorizado acceda a través de estas áreas al perímetro de seguridad;

2.2.14.9. Los procedimientos y prácticas para inspeccionar el material que ingrese, en busca de potenciales peligros antes de ser trasladados desde las áreas externas a las áreas de uso;

2.2.14.10. El equipo instalado deberá estar protegido para reducir las amenazas;

Revista de Derecho Notarial Mexicano, núm. 121, México, 2007.

2.2.14.11. Contar con respaldo de sistemas no interrumpible de energía eléctrica, y con planta de . energía eléctrica de emergencia para asegurar la continuidad del servicio de certificación;

2.2.14.12. El cableado eléctrico y de datos de los servicios de información confidencial deberá ser compatible con los estándares vigentes en la materia y protegidos contra daños e intervenciones;

2.2.14.13. Las líneas eléctricas no deberán interferir el funcionamiento del cableado de datos;

2.2.14.14. Contar con el personal o los contratos de mantenimiento requerido para garantizar la continua disponibilidad e integridad de los equipos, de acuerdo a las especificaciones y periodos recomendados por los fabricantes;

2.2.14.15. Evitar que equipos, información y software salgan de los perímetros de seguridad sin autorización.

2.2.14.16. Evitar que el equipo portátil contenga información confidencial. Si hay alguna razón que justifique equipos portátiles que contengan información confidencial o procesos críticos de la operación o información de los usuarios de los certificados, éstos nunca deberán salir del perímetro de seguridad designado;

2.2.14.17. Evitar que los equipos sean reutilizados o queden en desuso conteniendo información confidencial;

2.2.14.18. Los discos duros, disquetes y demás medios de almacenamiento de información magnético u óptico que ya no se utilicen deberán ser destruidos antes de salir del perímetro de seguridad;

2.2.14.19. Establecer un mecanismo para registrar el mal funcionamiento, fallas, mantenimientos preventivos y correctivos, de los equipos sensibles para la operación del servicio;

Unidad de Asuntos Jurídicos Dirección de Legislación.

2.2.14.20. Adoptar la política de "escritorio limpio y pantalla limpia" enfocados a evitar riesgos de acceso no autorizado, pérdidas o daños a la información durante o fuera del horario de trabajo.

2.2.15. La Seguridad Física propuesta por el Solicitante de Acreditación y el Prestador de Servicios de Certificación, deberá ser compatible con las normas y criterios internacionales y al menos con el estándar ETSI TS 102 042 -sección 7.4.4 Physical and Environment security- e ISO/IEC 17799 sección 7.

2.3.- Elementos económicos:

Los elementos económicos con que deberá contar el Solicitante de Acreditación y el Prestador de Servicios de Certificación comprenderán al menos:

2.3.1. El seguro, cuyo monto aplicable para cada año será determinado por la Secretaría con base en un análisis de las operaciones

comerciales y mercantiles en las que sean utilizados los Certificados, monto que se dará a conocer mediante publicación en el Diario Oficial de la Federación.

2.4.- Elementos tecnológicos y sus procedimientos. Los elementos tecnológicos y sus procedimientos garantizarán la continuidad del servicio, por lo que deberán ser compatibles con las normas y criterios internacionales, en atención a lo siguiente:

2.4.1. Análisis y Evaluación de Riesgos y Amenazas.

El Solicitante de Acreditación o el Prestador de Servicios de Certificación deberá elaborar un documento denominado Análisis y Evaluación de Riesgos y Amenazas, en el que desarrolle los apartados y aspectos que a continuación se indican:

2.4.1.1. Realizar un estudio que identifique los riesgos e impactos que existen sobre las personas y los equipos, así como recomendaciones de medidas para reducirlos;

2.4.1.2. Implementación de medidas de seguridad para la disminución de los riesgos detectados o riesgos mínimos;

2.4.1.3. Proceso de evaluación continua para adecuar la valoración de riesgos a condiciones cambiantes del entorno;

2.4.1.4. Determinar un proceso equivalente o adoptar el descrito en los documentos siguientes: "Risk Management Guide for Information Technology Systems, Special Publication 800-30. Recommendations of the National Institute of Standards and Technology, October 2001", "Handbook 3, Risk Management, Version 1., Australian Communications Electronic Security Instruction 33 (ACSI 33)", o aquellos que les sustituyan.

2.4.2. Infraestructura informática:

Deberá incluir al menos lo siguiente:

2.4.2.1. Una Autoridad Certificadora;

2.4.2.2. Una Autoridad Registradora;

2.4.2.3. Depósitos para: Datos de Creación de Firma Electrónica del Prestador de Servicios de Certificación y su respaldo, certificados y Listas de Certificados Revocados (LCR) basadas en un servicio de Protocolo de Acceso de Directorio de Peso ligero (LDAP) o equivalente y un Protocolo de Estatus de Certificados en Línea (OCSP);

2.4.2.4. Los procesos de administración de la Infraestructura;

Unidad de Asuntos Jurídicos Dirección de Legislación.

2.4.2.5. Un manual de Política de Certificados;

2.4.2.6. Una Declaración de Prácticas de Certificación, y

2.4.2.7. Los manuales de operación de las Autoridades Certificadora y Registradora.

2.4.3. Equipo de cómputo y software:

2.4.3.1. Por lo menos un servidor de misión crítica para la Autoridad Certificadora y la Autoridad Registradora, contemplando otro servidor de las mismas características para redundancia por seguridad.

2.4.3.2. Un servidor de misión crítica, contemplando redundancia por seguridad, para LDAP, LCR y OCSP.

2.4.3.3. Una computadora para almacenar el sistema de administración de la Infraestructura que se opera.

2.4.3.4. Un Sistema de Sello o Estampado de Tiempo, para insertar fecha y hora de emisión de los certificados, con las especificaciones y en los términos del apartado 7 de las presentes Reglas.

2.4.3.5. Un dispositivo de alta seguridad que sea compatible con el estándar FIPS-140 nivel 3, contemplando redundancia por seguridad, para almacenar los Datos de Creación de Firma Electrónica del Prestador de Servicios de Certificación.

2.4.3.6. Un enlace mínimo de 512 Kilo Bytes, contemplando redundancia con un enlace de al menos 256 Kilo Bytes a Internet.

2.4.3.7. Un ruteador, contemplando redundancia por seguridad.

2.4.3.8. Un muro de fuego (firewall), contemplando redundancia por seguridad.

2.4.3.9. Un sistema de monitoreo de red.

2.4.3.10. Un sistema confiable de antivirus.

2.4.3.11. Herramientas confiables de detección de vulnerabilidades.

2.4.3.12. Sistemas confiables de detección y protección de intrusión.

2.4.3.13. Las computadoras personales e impresoras necesarias para la prestación del servicio.

2.4.4. Política de seguridad de la información.

La Política de Seguridad deberá constar por escrito y cumplir con los siguientes requisitos:

2.4.4.1. Ser congruente con el objeto del Prestador de Servicios de Certificación;

2.4.4.2. Los objetivos de seguridad determinados deberán ser, claros, generales y no técnicos y resultado del Análisis y Evaluación de Riesgos y Amenazas;

2.4.4.3. Estar basada en las recomendaciones del estándar ISO 17799 sección tres;

2.4.4.4. Contar con los manuales de Política General y los necesarios para establecer políticas específicas;

2.4.4.5. Con base en el Análisis y Evaluación de Riesgos y Amenazas deberán identificarse los objetivos de seguridad relevantes y las amenazas potenciales relacionadas a los servicios suministrados, así como las medidas a tomar para evitar y limitar los efectos de tales riesgos y amenazas; Unidad de Asuntos Jurídicos Dirección de Legislación.

2.4.4.6. Describir las reglas, directivas y procedimientos que indiquen cómo son provistos los servicios y las medidas de seguridad asociadas;

2.4.4.7. Señalar el periodo de revisión y evaluación de la Política de Seguridad;

2.4.4.8. Ser consistente con la Declaración de Prácticas de Certificación y con la Política de Certificados a que se refieren las presentes Reglas Generales;

2.4.4.9. Incluir un proceso similar al descrito en: Internet Security Policy: A Technical Guide, by the National Institute of Standards and Technologies (NIST).

2.4.5. Plan de Continuidad del Negocio y Recuperación ante Desastres.

2.4.5.1. El Solicitante de Acreditación y el Prestador de Servicios de Certificación deberán elaborar y presentar un Plan de Continuidad del Negocio y Recuperación ante Desastres, que describa cómo actuará en caso de interrupciones del servicio. El Plan deberá ser mantenido y probado periódicamente, y describir los procedimientos de emergencia a seguir en al menos los siguientes casos:

2.4.5.1.1. Afectación al funcionamiento de software en el que se basarán los servicios del Prestador de Servicios de Certificación;

2.4.5.1.2. Incidente de seguridad que afecte la operación del sistema en el que se basan los servicios del Prestador de Servicios de Certificación;

2.4.5.1.3. Robo de los Datos de Creación de Firma Electrónica del Prestador de Servicios de Certificación;

2.4.5.1.4. Falla de los mecanismos de auditoría;

2.4.5.1.5. Falla en el hardware donde se ejecuta el producto en el que se basarán los servicios del Prestador de Servicios de Certificación;

2.4.5.1.6. Mecanismos para preservar evidencia del mal uso de los sistemas.

2.4.5.2. En el Análisis y Evaluación de Riesgos y Amenazas se considerará el impacto que sufrirá el negocio, en caso de interrupciones no planificadas.

Revista de Derecho Notarial Mexicano, núm. 121, México, 2007.

2.4.5.3. El Plan de Continuidad del Negocio y Recuperación ante Desastres deberá ser compatible con las normas y criterios internacionales, al menos con los lineamientos descritos en el estándar ISO 17799 sección 11 o el estándar ETSI TS 102 042 sección 7.4.8, o los que les sustituyan. Además deberá ser coherente con los niveles de riesgo determinados en el Análisis y Evaluación de Riesgos y Amenazas y seguirá un proceso similar al descrito en: NIST ITL Bulletin June 2002, Contingency Planning Guide for Information Systems; NIST Special Publication 800-34, Contingency Planning Guide for Information Systems, June 2002; y NIST Special Publication 800-30 Risk Management Guide, u otros textos posteriores equivalentes.

2.4.6. Plan de Seguridad de Sistemas.

Los solicitantes de acreditación o los Prestadores de Servicios de Certificación deberán contar con un Plan de Seguridad de Sistemas coherente con la Política de Seguridad de la Información, que describa los requerimientos de seguridad de los sistemas y de los controles a implantar y cumplir; así como delinear las responsabilidades y acceso de las personas a los sistemas.

2.4.6.1. El Plan de Seguridad de Sistema incorporará:

Unidad de Asuntos Jurídicos Dirección de Legislación.

2.4.6.1.1. La Política de Seguridad de la Información, seguridad organizacional, control y clasificación de activos, administración de operaciones y comunicaciones, control de accesos, desarrollo y mantenimiento de sistemas, seguridad del personal, seguridad ambiental y física que sean compatibles con los señalados por la norma ISO 17799;

2.4.6.1.2. Los mecanismos y procedimientos de seguridad propuestos que se aplicarán en todo momento;

2.4.6.1.3. La forma en que se garantizará el logro de los objetivos de la Política de Certificados y la Declaración de Prácticas de Certificación. En caso de claves criptográficas, la manera en que se efectuará su administración;

2.4.6.1.4. Las medidas de protección del depósito público de certificados y de información privada obtenida durante el registro.

2.4.6.2. Implantación del Plan de Seguridad de Sistemas.

2.4.6.2.1. El Solicitante de Acreditación y el Prestador de Servicios de Certificación, verificarán que operaciones, procedimientos y mecanismos permitan alcanzar sus objetivos y lograr el riesgo mínimo determinado en el Análisis y Evaluación de Riesgos y Amenazas, así como los controles de los aspectos mencionados en el apartado;

2.4.6.1.1. La capacidad de administrar las instalaciones debe ser acorde con el Plan de Seguridad de Sistemas.

2.4.6.2.2. La Implantación del Plan debe garantizar el logro de los objetivos de la Política de Certificados y la Declaración de Prácticas de Certificación, el cual debe de ser compatible por lo menos con las secciones 4 a 10 del estándar ISO 17799, o las que le sustituyan.

2.4.7. Estructura de Certificados.

2.4.7.1. La estructura de datos del Certificado debe ser compatible con el estándar ISO/IEC 9594-8; además de contener los datos que aparecen en el artículo 108 del Código de Comercio, para ser considerados como válidos.

2.4.7.2. Los algoritmos utilizados para la Firma Electrónica Avanzada deben ser compatibles con los estándares de la industria RFC 3280. Internet X509 Public Key Infraestructure Certificate and Certificate Revocation List (CRL) Profile (Obsoletes 2459), R. Housley, W. Polk, W. Ford, D. Solo, April 2002, o los que les sustituyan que provean un nivel adecuado de seguridad tanto para la firma del Prestador de Servicios de Certificación como del usuario.

2.4.7.3. En el caso de las claves utilizadas para la generación de una Firma Electrónica Avanzada, su tamaño deberá proveer el nivel de seguridad de 1024 bits para los usuarios y de 2048 bits para los Prestadores de Servicios de Certificación. Deberán utilizar funciones hash conforme a estándares de la industria, actuales y que provean el adecuado nivel de seguridad para este tipo de firmas tanto del Prestador de Servicios de Certificación como del usuario.

2.4.7.4. Contendrán referencia o información suficiente para identificar o localizar uno o más sitios de consulta donde se publiquen las notificaciones de revocación de los certificados y al menos los que indican estas Reglas Generales.

2.4.8. Estructura de la Lista de Certificados Revocados (LCR).

2.4.8.1. La estructura e información de la Lista de Certificados Revocados deberá ser compatible con la última versión del estándar ISO/IEC 9594-8 o la que le sustituya, e incluir por lo menos la siguiente información:

Unidad de Asuntos Jurídicos Dirección de Legislación.

2.4.8.1.1. Número de serie de los certificados revocados por el emisor con fecha y hora de revocación;

2.4.8.1.2. La identificación del algoritmo de firma utilizado;

2.4.8.1.3. El nombre del emisor;

2.4.8.1.4. La fecha y hora en que fue emitida la Lista de Certificados Revocados;

2.4.8.1.5. La fecha en que emitirá la próxima Lista de Certificados Revocados que no podrá exceder de veinticuatro horas, con independencia de mantener el Protocolo de Estatus de Certificados en Línea (OCSP);

2.4.8.1.6. La Lista de Certificados Revocados deberá ser firmada por el Prestador de Servicios de Certificación que la haya emitido, con sus Datos de Creación de Firma.

2.4.9. El solicitante de acreditación y el Prestador de Servicios de Certificación deberán señalar un sitio electrónico de alta disponibilidad con mecanismos redundantes o alternativos de conexión y de acceso público a través de Internet que permitirá a los usuarios consultar los certificados emitidos de forma remota, continua y segura compatible con el estándar ISO/IEC 9594-8 o el que le sustituya, a efecto de garantizar la integridad y disponibilidad de la información ahí contenida. En dicho sitio se incluirá la Política de Certificados y la Declaración de Prácticas de Certificación.

2.4.10. El solicitante de acreditación y el Prestador de Servicios de Certificación definirán procedimientos que informen de las características de los procesos de creación y verificación de Firma Electrónica Avanzada, así como aquellos que aplicarán para dejar sin efecto definitivo los certificados.

2.4.11. Política de Certificados

2.4.11.1. El solicitante de Acreditación y el Prestador de Servicios de Certificación deberán establecer una Política de Certificados conforme a la cual se establecerá la confianza del usuario en el servicio;

2.4.11.1.1. Asegure su concordancia con la Declaración de Prácticas de Certificación y los procedimientos operacionales;

2.4.11.1.2. Permita la interoperabilidad con los Prestadores de Servicios de Certificación ya acreditados y con la Secretaría de Economía;

2.4.11.1.3. Indique a quién se le puede otorgar un Certificado y cómo se aplicará el proceso de registro, y que se deberá verificar en forma fehaciente la identidad del usuario. Cuando se trate de un certificado que habrá de ser utilizado para generar Firma Electrónica Avanzada deberá describir la forma en que se precisarán los propósitos, objetivos y alcances del Certificado y sus limitaciones. Asimismo, se deberán describir las obligaciones que contrae el Prestador de Servicios de Certificación y el usuario en la emisión y utilización del Certificado;

Revista de Derecho Notarial Mexicano, núm. 121, México, 2007.

2.4.11.1.4. Dé a conocer las medidas de privacidad y de protección de datos que se aplicarán en materia de Firma Electrónica Avanzada. La Política de Certificados será pública;

2.4.11.1.5. Deberá establecer bajo qué circunstancias se puede revocar un Certificado y quiénes pueden solicitarlo;

2.4.11.1.6. Tendrá que ser compatible por lo menos con el estándar ETSI TS 102 042 o el que le sustituya.

2.4.12. Declaración de Prácticas de Certificación Unidad de Asuntos Jurídicos Dirección de Legislación.

2.4.12.1. En la Declaración de Prácticas de Certificación, que deberá elaborar y mantener actualizado el solicitante de acreditación y el Prestador de Servicios de Certificación, determinarán:

2.4.12.1.1. Los procedimientos de operación para otorgar certificados y el alcance de aplicación de los mismos;

2.4.12.1.2. Las responsabilidades y obligaciones del Prestador de Servicios de Certificación y de la persona a identificar. Particularmente desarrollará aquellas inherentes a la emisión, revocación y expiración de certificados;

2.4.12.1.3. La vigencia de los certificados. Y una vez otorgada la acreditación por la Secretaría, la fecha de inicio de operaciones;

2.4.12.1.4. Detalladamente el método de verificación de identidad del usuario que se utilizará para la emisión de los certificados;

2.4.12.1.5. Procedimientos de protección de confidencialidad de la información de los solicitantes;

2.4.12.1.6. Un procedimiento para registrar la fecha y hora de todas las operaciones relacionadas con la emisión de un Certificado y conservarlas de manera confiable;

2.4.12.1.7. Los procedimientos que se seguirán en los casos de suspensión temporal o definitiva del Prestador de Servicios de Certificación y la forma en que la administración de los certificados emitidos pasarán a la Secretaría o a otro Prestador de Servicios de Certificación, en el caso, de suspensión definitiva;

2.4.12.1.8. Las medidas de seguridad adoptadas para proteger sus Datos de Creación de Firma Electrónica;

2.4.12.1.9. Los controles que se utilizarán para asegurar que el propio usuario genere sus Datos de Creación de Firma Electrónica, autenticación de usuarios, emisión de certificados, revocación de certificados, auditoría y almacenamiento de información relevante;

2.4.12.1.10. La Declaración de Prácticas de Certificación deberá ser compatible por lo menos con el estándar ETSI TS 102 042 y el RFC 3647 o el que le sustituya.

2.4.13. Modelo Operacional de la Autoridad Certificadora;

2.4.13.1. El solicitante de acreditación y el Prestador de Servicios de Certificación deberán definir su Modelo Operacional de la Autoridad Certificadora conforme al cual operará y prestará sus servicios al fungir como autoridad certificadora a efecto de lograr confiabilidad e interoperabilidad, que desarrollará los apartados siguientes:

2.4.13.1.1. Cuáles son los servicios prestados;

2.4.13.1.2. Cómo se interrelacionan los diferentes servicios;

2.4.13.1.3. En qué lugares se operará;

2.4.13.1.4. Qué tipos de certificados se entregarán;

2.4.13.1.5. Si se generarán certificados con diferentes niveles de seguridad;

2.4.13.1.6. Cuáles son las políticas y procedimientos de cada tipo de certificado, y

2.4.13.1.7. Cómo se protegerán los activos.

2.4.13.2. El Modelo Operacional de la Autoridad Certificadora deberá contener un resumen que incluya:

2.4.13.2.1. Contenido del documento;

Unidad de Asuntos Jurídicos Dirección de Legislación.

2.4.13.2.2. La historia del posible Prestador de Servicios de Certificación, y

2.4.13.2.3. Relaciones comerciales con proveedores de insumos o servicios para sus operaciones.

2.4.13.3. El Modelo Operacional de la Autoridad Certificadora deberá comprender los siguientes aspectos:

2.4.13.3.1. Interfaces con las Autoridades Registradoras;

2.4.13.3.2. Implementación de elementos de seguridad;

2.4.13.3.3. Procesos de administración;

2.4.13.3.4. Sistema de directorios para los certificados;

2.4.13.3.5. Procesos de auditoría y respaldo, y

2.4.13.3.6. Bases de Datos a utilizar.

2.4.13.4. El Modelo Operacional de la Autoridad Certificadora deberá considerar la Política de Certificados, la Declaración de Prácticas de Certificación, la Política de Seguridad de la Información y el Plan de Seguridad de Sistemas por lo que se refiere a la generación de claves.

2.4.13.5. El Modelo Operacional de la Autoridad Certificadora deberá incluir los requerimientos de seguridad física del personal, de las instalaciones y del módulo criptográfico.

2.4.14. Modelo Operacional de la Autoridad Registradora.

Revista de Derecho Notarial Mexicano, núm. 121, México, 2007.

2.4.14.1. El solicitante de acreditación y el Prestador de Servicios de Certificación deberán definir su Modelo Operacional de la Autoridad Registradora conforme al cual operará y prestará sus servicios con su autoridad registradora a efecto de lograr confiabilidad e interoperabilidad, que desarrollará los apartados siguientes:

2.4.14.1.1 Cuáles son los servicios de registro que se prestarán;

2.4.14.1.2 En qué lugares se ofrecerán dichos servicios, y

2.4.14.1.3 Qué tipos de certificados generados por la Autoridad Certificadora se entregarán.

2.4.14.2. El Prestador de Servicios de Certificación deberá ofrecer los mecanismos para que el propio usuario genere en forma privada y segura sus Datos de Creación de Firma Electrónica. Deberá indicar al usuario el grado de fiabilidad de los mecanismos y dispositivos utilizados.

2.4.14.3. El Modelo Operacional de la Autoridad Registradora deberá comprender los siguientes aspectos:

2.4.14.3.1. Interfaces con Autoridad Certificadora;

2.4.14.3.2. Implementación de dispositivos de seguridad;

2.4.14.3.3. Procesos de administración;

2.4.14.3.4. Procesos de auditoría y respaldo;

2.4.14.3.5. Bases de Datos a utilizar;

2.4.14.3.6. Privacidad de datos, y

2.4.14.3.7. Descripción de la seguridad física de las instalaciones.

2.4.14.4. El Modelo Operacional de la Autoridad registradora deberá establecer el método para proveer de una identificación unívoca del usuario y el procedimiento de uso de los Datos de Creación de Firma Electrónica.

2.4.15. Plan de Administración de Claves.

2.4.15.1. El solicitante de acreditación y el Prestador de Servicios de Certificación deberán definir su Plan de Administración de Claves conforme al cual generará, protegerá y administrará sus claves criptográficas, respecto de los apartados siguientes:

2.4.15.1.1. Claves de la Autoridad Certificadora;

2.4.15.1.2. Almacenamiento, respaldo, recuperación y uso de los Datos de Creación de Firma Electrónica de la Autoridad Certificadora del Prestador de Servicios de Certificación;

2.4.15.1.3. Distribución del certificado de la Autoridad Certificadora;

2.4.15.1.4. Administración del ciclo de vida del hardware criptográfico que utilice la Autoridad Certificadora;

2.4.15.1.5. Dispositivos seguros para los usuarios.

2.4.15.2. Los procedimientos implantados de acuerdo al Plan de Administración de Claves, deberán garantizar la seguridad de las claves en todo momento, aun en caso de cambios de personal, componentes tecnológicos, y demás que señalan las presentes Reglas Generales.

2.4.15.3. El Plan de Administración de Claves deberá establecer como requerimiento mínimo el utilizar aquellas con longitud de 1024 bits para los usuarios y de 2048 bits para los Prestadores de Servicios de Certificación.

2.4.15.4. El Prestador de Servicios de Certificación, su autoridad certificadora y registradoras, utilizarán dispositivos seguros para almacenar sus Datos de Creación de Firma Electrónica, compatibles como mínimo con el estándar FIPS-140 nivel 3 en sus elementos de seguridad e implantación de los algoritmos criptográficos estándares, o el que le sustituya.

2.4.15.5. El Plan de Administración de Claves tendrá que ser compatible por lo menos con el estándar ETSI TS 102 042 sección 7.2 -Generación de la clave de la Autoridad Certificadora, Almacenamiento, Respaldo y Recuperación de la clave de la Autoridad Certificadora, Distribución de la clave pública de la Autoridad Certificadora, uso de clave de la Autoridad Certificadora, fin del ciclo de vida de la clave de la Autoridad Certificadora y Administración del ciclo de vida del Hardware criptográfico-, o el que le sustituya.

2.5. El Solicitante de Acreditación y el Prestador de Servicios de Certificación, deberán proporcionar a la Secretaría, la documentación con la que acredite el cumplimiento de los requisitos previstos en el Código, el Reglamento o en las presentes Reglas Generales conforme a lo siguiente:

2.5.1. Tratándose de documentos públicos en copia certificada o en copia simple con el original para cotejo, o

2.5.2. Tratándose de documentos privados en copia simple, y

2.5.3. Una copia en disco compacto de toda la documentación presentada.

3. Para los efectos del artículo 102, inciso A), fracción V del Código, las condiciones a que se sujetará la fianza que otorgarán los solicitantes que obtengan su acreditación en términos del artículo anterior, previo al inicio del ejercicio de sus funciones como Prestadores de Servicios de Certificación, serán conforme a lo siguiente:

3.1. Una vez resuelta la procedencia de la solicitud de acreditación, en términos de la fracción IV del artículo 7 del Reglamento,

el interesado deberá presentar la fianza de compañía debidamente autorizada a favor de la Tesorería de la Federación, en el término establecido en el artículo 8 del mencionado Reglamento:

3.1.1. Tratándose de un notario o corredor públicos, por un monto equivalente a cinco mil veces el salario mínimo general diario vigente en el Distrito Federal;

3.1.2. Tratándose de personas morales de carácter privado o instituciones públicas, por el monto resultante de multiplicar cinco mil veces el salario mínimo general diario vigente en el Distrito Federal por cada persona física de su personal, o integrante de una persona moral distinta que se contemple para efectos del artículo 104 fracción I del Código dentro de la acreditación para prestar el servicio de certificación en nombre y por cuenta del solicitante conforme al artículo 104 fracción I del Código;

3.2. Cuando la fianza tenga que ser otorgada por un notario o corredor público, la Secretaría podrá acordar que se otorgue de manera solidaria por parte de los colegios o agrupaciones de notarios o corredores públicos.

4. Para los efectos del artículo 10 del Reglamento, la Secretaría a través de sus servidores públicos comprobarán la identidad del solicitante de acreditación o del Prestador de Servicios de Certificación o su representante, utilizando cualquiera de los medios admitidos en derecho.

4.1. Tratándose de la identificación del representante de un Prestador de Servicios de Certificación que sea persona moral privada o institución pública, éste deberá acreditar su personalidad y la legal existencia de su representado a la Secretaría.

4.2. El Prestador de Servicios de Certificación generará sus Datos de Creación de Firma Electrónica, en el nivel de seguridad más alto de sus instalaciones, a fin de dar certeza y seguridad a todos los elementos necesarios para la creación de los mismos y bajo la supervisión de la Secretaría, en dicha generación se podrá utilizar cualquier tecnología por lo que el procedimiento técnico variará de acuerdo a la que se utilice, lo anterior a fin de cumplir con el principio de neutralidad tecnológica.

5. Para los efectos de los artículos 113 del Código y 16 del Reglamento, el procedimiento para obtener la copia de cada Certificado generado por un Prestador de Servicios de Certificación, será mediante envío en línea de cada Certificado a la Secretaría, lo cual será en tiempo real, es decir, se enviará una copia de cada certificado inmediatamente después del momento de expedición de los

Revista de Derecho Notarial Mexicano, núm. 121, México, 2007.

Certificados generados por el Prestador de Servicios de Certificación en su autoridad certificadora.

5.1. En el caso que el Prestador de Servicios de Certificación por caso fortuito o de fuerza mayor debidamente comprobado a la Secretaría, no pudiese llevar a cabo el envío a que se refiere el apartado anterior, el Prestador de Servicios de Certificación deberá hacer la réplica por cualquier medio en un término no mayor a seis horas.

5.2. Además del envío en línea de la copia de los Certificados, el Prestador de Servicios de Certificación remitirá dicha copia a la Secretaría en medios ópticos o electrónicos dentro de las veinticuatro horas siguientes a la generación de los Certificados, a fin de garantizar redundancia del procedimiento técnico descrito en el apartado 5 anterior de estas Reglas Generales.

5.3. El Prestador de Servicios de Certificación deberá cerciorarse que la Secretaría recibió la copia de cada certificado.

6. Para los efectos del artículo 108 fracción III del Código y 17 fracción III del Reglamento, los datos de acreditación ante la Secretaría observarán los siguientes elementos.

6.1. El Certificado emitido por el Prestador de Servicios de Certificación debe contener los datos que aparecen en el artículo 108 del Código de Comercio, para ser considerado válido.

6.2. Los certificados emitidos por el Prestador de Servicios de Certificación deberán contener la dirección electrónica de la Secretaría, en donde se podrá consultar la Lista de los Certificados Revocados de Prestadores de Servicios de Certificación.

7. Para los efectos del artículo 108 fracción VI del Código y 18 del Reglamento, la fecha y hora de emisión del Certificado se determinará conforme a lo siguiente:

7.1. El Prestador de Servicios de Certificación deberá llevar un registro del Sistema de Sello o Estampado de Tiempo que se sincronizará con el de la Secretaría, para asegurar la fecha y la hora de la emisión de los certificados generados por el Prestador de Servicios de Certificación.

7.2. El Sistema de Sello o Estampado de Tiempo deberá cumplir por lo menos con el estándar internacional Internet X.509 Public Key Infrastructure Time Stamp y considerar el RFC 3161.

7.3. El Prestador de Servicios de Certificación deberá asegurar en todo momento el enlace del Sistema de Sello o Estampado de Tiempo con el de la Secretaría.

Revista de Derecho Notarial Mexicano, núm. 121, México, 2007.

7.4. El Sistema de Sello o estampado de tiempo podrá ser del propio Prestador de Servicios de Certificación o de una persona física o moral que lo lleve en nombre y por cuenta del Prestador de Servicios de Certificación.

8. Para efectos del artículo 19 del Reglamento, la Secretaría verificará que los Prestadores de Servicios de Certificación cumplan con la estructura de certificados referida en las presentes Reglas Generales en los apartados 2.4.7. al 2.4.7.4., así como con los estándares internacionales, el Código de Comercio, el Reglamento y estas Reglas Generales, con el objetivo de asegurar que los certificados emitidos por los Prestadores de Servicios de Certificación, en ningún caso, contengan elementos que puedan generar confusión en la Parte que Confía.

9. Para los efectos del artículo 104 fracción IV del Código de Comercio, los casos en que estará a disposición el contenido privado del Registro de Certificados de un Prestador de Servicios de Certificación se sujetarán a lo dispuesto por la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

10. El Prestador de Servicios de Certificación que en términos del artículo 104 fracción VI, quiera cesar de manera voluntaria su actividad, previo pago de derechos tiene que informar el motivo de dicho cese con cuarenta y cinco días de anticipación a la Secretaría a efecto de que la misma se cerciore que se ha cumplido con lo establecido en el artículo 16 del Reglamento y el apartado 5, 5.1 y 5.2 de las presentes Reglas Generales.

11. Abreviaturas utilizadas en las presentes Reglas Generales.

11.1 GIAC-Global Information Assurance Certification.

11.2 GGSC GIAC Gold Standard Certificates.

11.3 GSLC-GIAC Security Leadership Certificat.

11.4 CISSP-Certified Information Systems Security Professionals.

11.5 SSCP-System Security Certified Practitioner.

11.6 ISO-International Organization for Standardization.

11.7 ETSI TS-European Telecommunications Standards Institute.

11.8 EIA/TIA-Electronic Industries Alliance/Telecommunications Industry Association.

11.9 ISO/IEC-International Organization for Standardization/International Electrotechnical Commission.

11.10 NIST-National Institute of Standards and Technology.

11.11 ACSI-Australian Communications Electronic Security Instruction.

11.12 LCR-Lista de Certificados Revocados.

Revista de Derecho Notarial Mexicano, núm. 121, México, 2007.

11.13 LDAP-Protocolo de Acceso de Directorio de Peso ligero.
11.14 OCSP-Protocolo de Estatus de Certificados en Línea.
11.15 FIPS-Federal Information Processing Standards.
11.16 RFC-Request for Comments.
11.17 TCP/IP Transmission Control Protocol/Internet Protocol.
11.18 IPSEC-Internet Protocol Security.

TRANSITORIOS

PRIMERO.- Las presentes Reglas entrarán en vigor al día siguiente de su publicación en el Diario Oficial de la Federación.

SEGUNDO.- Estas Reglas estarán sujetas a cambios y a una revisión anual de la Secretaría de Economía, debido a los constantes cambios en la industria, a los estándares, normas y criterios internacionales reconocidos para prestar el servicio de certificación.

México, D.F., a 4 de agosto de 2004.- El Secretario de Economía, Fernando de Jesús Canales Clariond.- Rúbrica.

CUESTIONARIO:

Se plantearón las siguientes preguntas respecto del tema de las Entidades Certificadoras:

1.- ¿Quién es la autoridad certificante en su país?
2.- ¿Quién es la autoridad registradora en su país?
3.- ¿Cuál es el procedimiento de expedición de certificados?
4.- ¿Cual es su contenido?
5.- ¿Cuáles son las causas de cancelación?
6.- ¿Cuáles son las causas de revocación?
7.- ¿Cuáles son las causas de extinción?
8.- ¿Cuáles son las responsabilidades de la Autoridad Certificante?
9.- ¿Cuáles son las responsabilidades de la Autoridad Registradora?
10.- ¿Cuál es la vigencia del certificado?
11.- ¿Existen diferentes tipos de certificado?

A todas estas preguntas corresponde una respuesta en sentido negativo dado que en México no existen aún las figuras de la Autoridad Certificante ni de la Autoridad Registradora.