



UNIVERSIDAD NACIONAL  
AUTÓNOMA DE  
MÉXICO

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

---

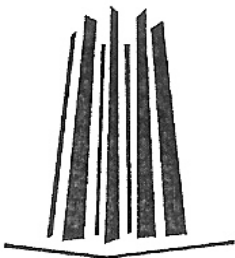
FACULTAD DE ESTUDIOS SUPERIORES

ARAGÓN

**VENTAJAS Y DESVENTAJAS DE LA FIRMA  
ELECTRÓNICA AVANZADA**

**EN LA MODALIDAD DE SEMINARIO DE TITULACIÓN  
COLECTIVA**

**T E S I N A**  
QUE PARA OBTENER EL TÍTULO DE:  
LICENCIADO EN DERECHO  
P R E S E N T A:  
**OLIVERA GARCIA ROSA**



MEXICO, ARAGON

2006



Universidad Nacional  
Autónoma de México

Dirección General de Bibliotecas de la UNAM

**Biblioteca Central**



**UNAM – Dirección General de Bibliotecas**  
**Tesis Digitales**  
**Restricciones de uso**

**DERECHOS RESERVADOS ©**  
**PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL**

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

## AGRADECIMIENTOS

A mis padres Enriqueta y Joaquín por el amor, la confianza, apoyo incondicional que siempre me han dado y en honor a su lucha y sacrificio.

Con admiración y respeto.

A mis hermanos Ana y Tony por su cariño y apoyo en todos los momentos de mi vida.

A Braulio por sus consejos, paciencia, dedicación, apoyo y por el amor que me alimenta día a día.

A mis amigos Elidet, Lorena, Cesar, Edgar; Carlos y Esteban que estuvieron conmigo brindándome su amistad incondicional en los buenos y malos momentos.

Alicia: gracias por todo

A mi hija Melissa por las constantes alegrías y ganas de salir adelante que día a día me da.

A todos los que de alguna manera contribuyeron a mi meta.

A la familia Franco Favila por su gran apoyo y cariño.

A la UNAM por permitirme ser parte de ella y en especial a la FES ARAGON.

A mis asesores por el apoyo y confianza depositados en mí.

# VENTAJAS Y DESVENTAJAS DE LA FIRMA ELECTRÓNICA AVANZADA

## Í N D I C E

INTRODUCCIÓN.....	I
-------------------	---

### CAPÍTULO PRIMERO GENERALIDADES

	<b>Pág</b>
1.1 Internet.....	1
1.2 Internet en México.....	4
1.3 Correo electrónico.....	6
1.4 Criptografía.....	7
1.5 Certificado.....	10
1.6 Ley modelo sobre las firmas electrónicas de la Comisión de las Naciones Unidas para el Derecho Mercantil.....	12

### CAPÍTULO SEGUNDO ENTORNO LEGAL.

2.1 Código Civil Federal.....	15
2.2 Código Federal de Procedimientos Civiles.....	17
2.3 Código de Comercio.....	18
2.4 Ley Federal de Protección al Consumidor.....	26
2.5 Código Fiscal de la Federación.....	26

**CAPÍTULO TERCERO  
VENTAJAS Y DESVENTAJAS DE  
LA FIRMA ELECTRÓNICA**

3.1	Firma autógrafa.....	35
3.2	Firma electrónica.....	39
3.3	Firma electrónica avanzada.....	42
3.3.1	Contribuyentes que pueden utilizar la firma electrónica avanzada.....	44
3.3.2	Características de la firma electrónica avanzada.....	45
3.3.3	Requisitos de la firma electrónica avanzada.....	46
3.3.4	Entidades certificadoras.....	48
3.3.5	Métodos criptográficos.....	53
3.4	Ventajas y desventajas de la firma electrónica avanzada.....	56
	<b>CONCLUSIONES.....</b>	<b>62</b>
	<b>ANEXOS.....</b>	<b>65</b>
	<b>BIBLIOGRAFÍA.....</b>	<b>67</b>

## INTRODUCCIÓN

En los últimos tiempos el avance de la tecnología ha ido aumentando con más fuerza repercutiendo en nuestra vida diaria, hemos observado avances tecnológicos que han transformado las actividades del hombre; tal es el caso del Internet que ha tenido un gran auge en el mundo entero; como consecuencia de esto hay la necesidad de regular los actos jurídicos que se realizan por este medio.

En lo que respecta a la materia fiscal en el título primero, del Código Fiscal de la Federación también se adicionó un capítulo denominado “de los medios electrónicos” en el que se establece una nueva figura “La firma electrónica avanzada” la cual es el tema primordial de nuestra tesina.

El uso de la firma electrónica en la presentación de declaraciones, avisos, solicitudes y todos los documentos digitales ahorra tiempo y recursos en beneficio de los contribuyentes y al mismo fisco, ya que el contribuyente no tiene que trasladarse a las oficinas correspondientes para realizar sus trámites.

Nuestra tesina se encuentra dividida en tres capítulos que tienen como finalidad estudiar las ventajas y desventajas que este reciente método trae como resultado.

En nuestro primer capítulo daremos de manera general algunos conceptos de los medios electrónicos que son necesarios para nuestro estudio.

En el segundo capítulo abordaremos el marco jurídico aplicable en México a la firma electrónica; nos remitiremos al Código Civil del Distrito Federal, Código de Procedimientos civiles para el Distrito Federal, Código de Comercio, Ley Federal de Protección al Consumidor y las recientes reformas del Código Fiscal de la Federación en relación a los medios electrónicos, principalmente a la firma electrónica.

En nuestro tercer y último capítulo haremos referencia a la firma electrónica en particular, sus elementos, sus funciones así como los requisitos a seguir para la obtención de la misma.

Por último debemos mencionar que la presente tesina se desarrollo a través del método inductivo.

## **CAPÍTULO PRIMERO**

### **GENERALIDADES**

En este primer capítulo trataremos de manera general algunos conceptos que nos ayudarán a comprender mejor el tema de la presente tesina.

#### **1.1 Internet**

En los últimos años, la humanidad ha tenido grandes avances tecnológicos en comunicación e información que han sido determinantes para su evolución, y es el caso del Internet que se está formando en uno de los adelantos tecnológicos con mayor impacto en nuestra sociedad.

Actualmente existen muchos conceptos y definiciones del vocablo Internet: en términos generales Internet, es el canal mundial de telecomunicaciones informática, que se esta integrando por muchos canales a su vez, están interconectados entre sí, lo cual lo convierte en el medio de comunicación más veloz de toda la historia de la humanidad”<sup>1</sup>.

El Internet es una red mundial que agrupa a miles de computadores alrededor del mundo y por esta razón que se ha denominado al Internet como “red de redes”. Una red esta

---

<sup>1</sup> REYES KRAFFT, Alfredo Alejandro. La firma electrónica y las entidades de certificación, Porrúa, México, 2003, p27.



formada por dos o más computadoras conectadas que interactúan entre sí con la finalidad de comunicar a sus usuarios.

El uso de estas redes ha hecho posible consultar información de un computador que se encuentra a corta distancia con otro que esté al otro lado del mundo. Es increíble el hecho de que hasta hace algunos años era improbable pensar que dos personas que habitaran en extremos opuestos pudieran tener comunicación al mismo tiempo por medio del internet. El internet no tiene fronteras.

“Internet se define como un conjunto de computadoras conectadas entre sí. La única diferencia que existe entre una red de computadoras instalada en una empresa (intranet) e internet es la importancia que esta última tiene, ya que conectada a millones de computadoras en todo el mundo. De hecho, cualquier compañía puede conectar su Intranet internet y permite que sus empleados tengan acceso a esta última.”<sup>2</sup>

Como podemos darnos cuenta, esta última definición es más técnica pues se refiere a la conexión física de los equipos.

De lo expuesto entendemos que el internet es una red de computadoras conectadas entre sí a nivel mundial, permitiendo que una enorme cantidad de usuarios se comuniquen entre ellos y

---

<sup>2</sup> RATIA MENDOZA, Alberto, Declaración por medios electrónicos, calidad e información, México, 2000, p.18.

tengan acceso a la información que ellos deseen de la forma más rápida que existe. Cabe señalar que esos fines van más allá de la comunicación, ya que este medio permite en la actualidad el comercio y el cumplimiento de ciertas obligaciones jurídicas.

Para conectarse a internet es necesario tener un modem, el cual traduce las señales digitales de la computadora en señales analógicas, que pueden ser enviadas a través de líneas telefónicas estándar.

El internet nos ofrece varios servicios, pero el más popular y difundido es el *Word Wide Web*, lo que conocemos como *www*; que es un conjunto de documentos en computadoras de todas partes del mundo interrelacionados; cabe mencionar que estos documentos también cuentan con gráficos, audio y algunos otros con video.

Algunas veces el término *web* se utiliza para el internet en general, pero los términos se refieren a cosas diferentes. EL Internet es tecnología, el *web* es información.

La *web* utiliza el protocolo *http (hiper text transfer protocol)* y permite a los usuarios acceder a información contenida en cualquier computadora de la red, a través de un programa llamado navegador.

El navegador es una aplicación cliente de *software* para la red que sirve como interfase que utiliza para navegar a través del mundo de la información de la web; como es el Internet Explorer de Microsoft o *Navigator* de *Netscape*.

También es necesario un proveedor de conexión a internet. En la actualidad existen varios proveedores. Por ejemplo Terra, Google; Yahoo, etc.

### **1.1 Internet en México.**

El internet en la actualidad está muy avanzado en nuestro país; sin embargo, anteriormente no era así ya que fue hasta 1989 que México se conecta a internet por primera vez con la conexión del Instituto Tecnológico y de Estudios Superiores Monterrey (ITESM campus Monterrey) se conecta a la Universidad de Texas en San Antonio (*UTSA*) específicamente a la escuela de Medicina. Una línea analógica a 9600bps.

En este mismo año se conecta la Universidad Nacional Autónoma de México (UNAM), vía satélite de 56 *kbps* con el instituto de Astronomía de la ciudad de México con el Centro Nacional de Investigación Atmosférica (NCAR) de *Boulder* Colorado en los Estados Unidos.

En enero de 1992 surge MEXNET, integrada por el ITESM, La universidad de Guadalajara, LANA, CIQA, Universidad de

Guanajuato, Universidad Veracruzana, Instituto de Ecología, Universidad Iberoamericana e Instituto Tecnológico de Mexicali.

En el mes de junio de ese mismo año MEXNET establece una salida digital de 56 *kbps* al *backbone* (columna vertebral) de Internet.

En 1993 el Consejo Nacional de Ciencia y Tecnología (CONACYT) se conecta a internet mediante un enlace satelital al NCAR.

Es en este mismo año cuando la UAM se establece como primer NAP al intercambiar tráfico entre dos diferentes redes.

Para finales de 1993 ya existían algunas redes establecidas en el país: Red ITESM, Red UNAM, Red total CONACYT, BAJAnet, SIRACYT.

En diciembre de 1995 se crea el centro de información de redes de México (NIC-México), el cual se encarga de la administración y coordinación de los recursos de internet asignados a México tales como la administración y delegación de los nombres de dominio ubicados bajo "mx".

En el año de 1996, ciudades como Monterrey, N.L; registran cerca de 17 enlaces contratados con Telmex para uso privado. En este mismo año, el INFOTEC, crea el centro de tecnologías avanzadas cuyo objetivo es desarrollar servicios de contenido de

valor agregado en internet y todos aquellos que se desarrollan con nuevas tecnologías de internet y multimedia. En este año nace la sociedad de internet, Capitulo México, una asociación internacional no gubernamental, para la coordinación global y cooperación en internet. A finales del año la apertura en empresas de comunicaciones y conexiones de telefonía de larga distancia provoca un auge momentáneo en las conexiones a internet. Empresas como AVANTEL y alestra-AT&T ahora compiten con TELMEX.

En 1997 existen mas de 150 proveedores de acceso a internet (ISP's) que brindan su servicio en el territorio mexicano, ubicados en los principales centros urbanos.

Para el 2003 existen más de 180 proveedores de acceso a internet (ISP's) que brindan sus servicios en el territorio mexicano, ubicados en los principales centros urbanos: Ciudad de México, Guadalajara, Monterrey, Chihuahua, Tijuana, Puebla, Mérida, Nuevo Laredo, Saltillo por mencionar algunos.

### **1.3 Correo electrónico (e-mail).**

El correo electrónico es una aplicación de internet que funciona utilizando el protocolo *Simple Mail Transfer Protocol*, y permite intercambiar mensajes electrónicos en segundos, con cualquier persona, en cualquier parte del mundo, que también obtenga una dirección de correo electrónico.

El correo electrónico tiene la ventaja de poder enviar y recibir mensajes en segundos y contestarlos selectivamente, a la hora que uno quiera; esta función de internet tiene la mayor cobertura; y por último, no hay cargos de larga distancia por comunicarse con personas de otros países, ya que sólo se cobra la llamada local al conectarse con el proveedor de acceso a internet.

#### **1.4 Criptografía.**

La palabra criptografía proviene del griego *Kriptos*, secreto, y *graphos*, escribir; por lo que se define a ésta como el arte de escribir con clave secreta o de un modo enigmático<sup>3</sup>.

Criptografía es el conjunto de reglas matemáticas para cifrar información.

Criptografía “es la ciencia de mantener en secreto los mensajes, el texto original, o texto puro es convertido en un equivalente en código, llamado *criptotexto (ciphertex)* vía un algoritmo de encriptación. El *criptotexto* es decodificado (desencriptado) al momento de su recepción y vuelve a su forma de texto original”<sup>4</sup>.

La protección de la información que se persigue en criptografía se lleva a cabo borrando su forma. Se llama cifrado (o

---

<sup>3</sup> Diccionario de la real Academia de la Lengua Española, Tomo II, Décimo novena edición, planeta, p 381

<sup>4</sup> REYES KRAFFT Alfredo Alejandro. La firma electrónica y las entidades de certificación. Porrúa, México, 2003.,178.

transformación criptográfica) a una transformación de texto original (llamado también texto inicial o texto claro) que lo convierte en el llamado texto cifrado o criptograma. Análogamente, se llama descifrado a la transformación que permite recuperar el texto original a partir del texto cifrado.<sup>5</sup>

Las firmas numéricas se crean y verifican utilizando la criptografía, la rama de las matemáticas aplicadas que se ocupa de transformar mensajes en formas aparentemente ininteligibles y devolverlas a su forma original. Las firmas numéricas utilizan lo que se denomina “criptografía de clave pública”, que con frecuencia se basa en el empleo de funciones algorítmicas para generar dos “claves” diferentes, pero matemáticamente relacionadas entre sí (por ejemplo, grandes números producidos utilizando una serie de fórmulas matemáticas aplicadas a números primos). Una de esas claves se utiliza para crear una firma numérica o transformar datos en una forma aparentemente ininteligible, y la otra para verificar una firma numérica o devolver el mensaje a su forma original. El equipo y los programas informáticos que utilizan dos de esas claves se suelen denominar en conjunto “criptosistemas” o, más concretamente, “criptosistemas asimétricos” cuando se basan en el empleo de algoritmos asimétricos.<sup>6</sup>

---

<sup>5</sup> PINO CABALLERO Gil, Introducción a la criptografía, segunda edición, Alfaomega Ra Ma, México, 2003, p.7

<sup>6</sup> PEREZ CHAVEZ Capero Fol, Firma electrónica avanzada, documentos, digitales y comprobantes electrónicos, Tax editores, México, 2005, p.20.

La criptografía posee dos métodos diferentes: los de transposición y los de sustitución. En los primeros el orden habitual de las letras que integra el mensaje se altera mediante diversos procedimientos, a fin de que el texto resultante sea ilegible. El mecanismo puede por ejemplo, consistir en colocar la segunda letra debajo de la primera, la cuarta bajo la tercera y así sucesivamente.

A continuación se enlistarán aquellos algoritmos criptográficos más usados en la actualidad y que gozan de una gran seguridad. Todos y cada uno de ellos poseen uno o más propósitos.

- a) **Encriptación:** Se usan simplemente para encriptar comunicación. Tanto el emisor como el receptor encriptan y decriptan el mensaje usando el mismo algoritmo.
  
- b) **Firmas Digitales:** Existen muchos algoritmos de firma electrónica. Todos ellos son algoritmos de clave pública con información secreta para firmar documentos e información pública para verificar las firmas. Muchas veces al proceso de firmado se le llama encriptar con una clave privada y la verificación se le llama desencriptar con una clave pública.
  
- c) **Hashing y Digest:** Un algoritmo de *hashing* es una función matemática que toma una cadena de longitud variable y



la convierte a una cadena de longitud fija. Es una manera de obtener una huella digital de los datos. Si se necesita verificar un archivo que pertenece a cierta persona se manda un valor de *hashing* para comprobarlo. Esto es muy usado en transacciones financieras. El algoritmo de *hashing* genera un valor para el mensaje.

- d) *Digest* es la representación del texto en forma de una cadena de dígitos, creado con una fórmula de *hashing* de una sola dirección. El encriptar un digest de un mensaje con una clave privada, genera una firma digital.

De lo anterior se desprende que la criptografía sólo se refiere al uso de los códigos, los cuales nos sirve para salvaguardar los intereses jurídicos en diversas situaciones, es decir, la criptografía tiene como finalidad el de proporcionar comunicaciones seguras ya que nos brinda confidencialidad y seguridad jurídica, esto es porque mientras nuestros mensajes están en su recorrido, nadie pueda leerlos.

## **1.5 Certificado**

La firma electrónica requiere para su funcionamiento contar con un certificado reconocido lo que no ocurre con las firmas manuales, ya que tienen una asociación intrínseca con una persona física determinada. En la Firma Electrónica Avanzada se

observa un juego de claves usado para crear la firma y no tienen una asociación intrínseca con nadie

El certificado permite la verificación de que una clave pública dada pertenece indudablemente a un determinado sujeto. Un certificado por sí solo no es más que una certificación electrónica que vincula unos datos de verificación de la firma a un signatario y confirma su identidad.

El Certificado tiene como primordial función unir un par de claves con la firma de un determinado suscriptor, asociar la identidad de una persona determinada a una clave pública concreta

La Ley modelo sobre las firmas electrónicas de la Comisión de las Naciones Unidas para el Derecho Mercantil nos menciona definiciones que son importantes; de acuerdo al artículo 2, inciso b) y c), nos establece lo siguiente:

Para los fines de la presente Ley:

*b)* Por Certificado se entenderá todo mensaje de datos u otro registro que confirme el vínculo entre un firmante y los datos de creación de la firma

c) Por Prestador de Servicios de Certificación se entera la persona que expida certificados y puede prestar otros servicios relacionados con las firmas electrónicas.

En resumen, los certificados de firma electrónica sirven para asegurar la veracidad de la clave pública perteneciente al propietario del certificado. Como se observa, los certificados digitales o de firma electrónica son en realidad un documento firmado digitalmente por una entidad conocida como autoridad certificadora. En el documento así firmado esta una liga entre un sujeto particular y su llave pública

## **1.6 Ley modelo sobre las firmas electrónicas de la Comisión de las Naciones Unidas para el Derecho Mercantil**

Por lo que respecta a este tema señalaremos sólo algunos conceptos que esta ley nos indica, ya que en el desarrollo de la presente tesina seguiremos haciendo referencia a esta ley.

**Concepto de firma electrónica.**- Según el artículo 2o., inciso a, de la Ley Modelo de la CNUDMI sobre las Firmas Electrónicas, por “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 este último aprueba la información recogida en el mensaje de datos.

**Concepto de certificado.-** De acuerdo con el artículo 2o., inciso b, de la Ley Modelo de la CNUDMI sobre las Firmas Electrónicas, por “certificado” se entenderá todo mensaje de datos u otro registro que confirme el vínculo entre un firmante y los datos de creación de la firma.

**Concepto de mensaje de datos.-** De conformidad con el artículo 2o., inciso c, de la Ley Modelo de la CNUDMI sobre las Firmas Electrónicas, por “mensaje de datos” se entenderá la información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax.

**Concepto de firmante.-** Por “firmante” se entenderá la persona que posee los datos de creación de la firma y que actúa por cuenta propia o por cuenta de la persona a la que representa. Ello, según el artículo 2o., inciso d, de la Ley Modelo de la CNUDMI sobre las Firmas Electrónicas.

**Concepto de prestador de servicios de certificación.-** De acuerdo con el artículo 2o., inciso e, de la Ley Modelo de la CNUDMI sobre las Firmas Electrónicas por “prestador de servicios de certificación” se entenderá la persona que expide certificados y puede prestar otros servicios relacionados con las firmas electrónicas

**Concepto de parte que confía.**- De conformidad con el artículo 2o., inciso f, de la Ley Modelo de la CNUDMI sobre las firmas Electrónicas, por “parte que confía” se entenderá la persona que pueda actuar Sobre la base de un certificado o de una firma electrónica.

Como podemos darnos cuenta, la ley modelo nos da definiciones muy concretas y claras que nos permiten entender mejor el tema.

## **CAPÍTULO SEGUNDO**

### **ENTORNO LEGAL.**

En el presente capítulo se dan a conocer los diversos ordenamientos legales en los que se encuentra regulada la Firma electrónica, los cuales veremos de manera general.

#### **2.1 Código Civil Federal**

El Código Civil Federal en su artículo 1803 nos establece que el consentimiento puede ser expreso o tácito y nos menciona lo siguiente:

- I. será expreso cuando la voluntad se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos; y
- II. el tácito resultará de hechos o de actos que lo supongan o que autoricen a presumirlo, excepto en los casos en que por ley o por convenio la voluntad debe manifestarse expresamente.

Este artículo nos muestra la posibilidad de que las partes puedan manifestar su voluntad por medios electrónicos.

El artículo 1811 del presente código menciona que: “tratándose de la propuesta y aceptación hechas a través de medios electrónicos, ópticos o de cualquier otra tecnología no se requerirá de estipulación previa entre los contratantes para que produzca efectos.”

En lo que respecta al artículo 1834 del Código Civil, cuando se exija la forma escrita para el contrato, los documentos relativos deben ser firmados por todas las personas a las cuales se imponga esa obligación. Si alguna de ellas no puede o sabe firmar, lo hará otra a su ruego y en el documento se imprimirá la huella digital del interesado que no firmó.

Para tal efecto, el artículo 1834-Bis del referido Código Civil indica que “los supuestos previstos por el artículo anterior se tendrán por cumplidos mediante la utilización de medios electrónicos, ópticos o de cualquier otra tecnología, siempre que la información generada o comunicada en forma íntegra, a través de dichos medios, sea atribuible a las personas obligadas y accesible para su ulterior consulta.

En los casos en que la ley establezca como requisito que un acto jurídico deba otorgarse en instrumento ante fedatario público, éste y las partes obligadas podrán generar, enviar, recibir, archivar o comunicar la información que contenga los términos exactos en que las partes han decidido obligarse, mediante la utilización de medios electrónicos, ópticos o de cualquier otra tecnología, en cuyo caso, el fedatario público deberá hacer constar en el propio instrumento, los elementos a través de los cuales se atribuye dicha información a las partes y conservar bajo su resguardo una versión íntegra de la misma para su ulterior consulta, otorgando dicho instrumento de conformidad con la legislación aplicable que lo rige.

## **2.2 Código Federal de Procedimientos Civiles.**

En el Código Federal de Procedimientos Civiles se reconoce como prueba la información generada y que conste en medios electrónicos. También se le da validez de original a esa información.

“El Art 210—A. Se reconoce como prueba de información generada o comunicada que conste en medios electrónicos, ópticos o cualquier otra tecnología.

Para valora la fuerza probatoria de la información a que se refiere el párrafo anterior, se estimará primordialmente la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas obligadas el contenido de la información relativa y ser accesible para su ulterior consulta

Cuando la ley requiera que un documento sea conservado y presentado en su forma original, ese requisito quedará satisfecho si se acredita que la información generada, comunicada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología, se ha mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y ésta pueda ser accesible para su ulterior consulta”.

Lo anterior obliga a las partes en conflicto y a los jueces a proporcionar medios idóneos para la reproducción de la probanza y que además sean valoradas conforme a derecho y no a criterio de los jueces.



### **2.3 Código de Comercio.**

De acuerdo con el artículo 80 del Código de Comercio, los convenios y contratos mercantiles que se celebren 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 o las condiciones con que ésta fuere modificada.

Por otra parte, en los artículos 89 al 114 del citado Código, se regulan los aspectos relacionados con el comercio electrónico, de los cuales, a nuestro juicio, destacan los siguientes:

El Código de Comercio, título segundo, denominado “Del Comercio Electrónico”, regirá en toda la República Mexicana en asuntos del orden comercial, sin perjuicio de lo dispuesto en los tratados internacionales de los que México sea parte.

En los actos de comercio y en la formación de los mismos podrán emplearse los medios electrónicos, ópticos o cualquier otra tecnología. Para efectos del Código de Comercio, se deberán tomar en cuenta las definiciones siguientes:

*Certificado:* Todo mensaje de datos u otro registró 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 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.

El artículo 97 señala que *Firma Electrónica Avanzada o fiable:* es Aquella firma electrónica que cumpla con los requisitos siguientes:

1. Los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante;
2. Los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante;
3. Es posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma, y
4. 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.

En aquellas disposiciones que se refieran a la firma digital, se considerará a ésta como una especie de 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 SE.

**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.

No se negarán efectos jurídicos, validez o fuerza obligatoria a cualquier tipo de información por la sola razón de que esté contenida en un mensaje de datos.

Se presumirá que un mensaje de datos proviene del emisor si ha sido enviado:

- a) Por el propio emisor;
- b) Usando medios de identificación, tales como claves o contraseñas del emisor o por alguna persona facultada para actuar en nombre del emisor respecto a ese mensaje de datos, o

c) Por un sistema de información programado por el emisor o en su nombre para que opere automáticamente.

Conforme a lo anterior, siempre que se entienda que el mensaje de datos proviene del emisor, o que el destinatario tenga derecho a actuar con arreglo a este supuesto, dicho destinatario tendrá derecho a considerar que el mensaje de datos recibido corresponde al que quería enviar el iniciador, y podrá proceder en consecuencia. El destinatario no gozará de este derecho si sabía o hubiera sabido, de haber actuado con la debida diligencia, o de haber aplicado algún método previamente acordado, que la transmisión había dado lugar a un error mensaje de datos recibido

Cuando la ley exija la forma escrita para los actos, convenios o contratos, este supuesto se tendrá por cumplido tratándose de mensaje de datos, siempre que la información en él contenida se mantenga íntegra y sea accesible para su ulterior consulta, sin importar el formato en el que se encuentre o represente.

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

En los casos en que la ley establezca como requisito que un acto jurídico deba otorgarse en instrumento ante fedatario público, 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.

Sin perjuicio de lo dispuesto en el artículo 49 del Código de Comercio, cuando la ley requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho respecto a un mensaje de datos:

- a) Si existe garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma, y
- b) De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona a la que se deba presentar.

Para tales efectos, se considerará que el contenido de un mensaje de datos es íntegro, si éste ha permanecido completo e inalterado independientemente de los cambios que hubiere podido sufrir el medio que lo contiene, resultado del proceso de comunicación, archivo o presentación. El grado de confiabilidad requerido será determinado conforme a los fines para los que se

generó la información y de todas las circunstancias relevantes del caso.

Las disposiciones del Código de Comercio serán aplicadas de modo que no excluyan, restrinjan o priven de efecto jurídico cualquier método para crear una firma electrónica.

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 con los requisitos antes mencionados.

Lo dispuesto en este número se entenderá sin perjuicio de la posibilidad de que cualquier persona demuestre de otra manera la fiabilidad de una firma electrónica, o presente pruebas de que una firma electrónica no es fiable.

De conformidad con el 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 el 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.

El artículo 99 señala que 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.

El firmante será responsable de las consecuencias jurídicas que deriven por no cumplir oportunamente con las obligaciones previstas en este número, y

Responder por las obligaciones derivadas del uso no autorizado de su firma, cuando no hubiere obrado con la debida diligencia



para impedir su utilización, salvo que el destinatario conociere de la inseguridad de la firma electrónica o no hubiere actuado con la debida diligencia.

El Código de Comercio también hace referencia a los servicios de certificación, quienes son prestadores de servicios de certificación, y sus obligaciones. Así como los requisitos del certificado y cuando dejara de surtir efectos.

### **2.1.1 Ley Federal de Protección al Consumidor.**

En la Ley Federal de Protección al Consumidor se incluye la protección al consumidor por las operaciones realizadas a través de medios electrónicos.

Con los cambios anteriores a la Ley Federal de Protección al Consumidor, se observó un avance significativo en materia de comercio electrónico. Sin embargo, los comerciantes no podían facturar por medios electrónicos, ya que las facturas no eran aceptadas por las autoridades fiscales.

### **2.1.2 Código Fiscal de la Federación.**

Como hemos visto en las leyes antes mencionadas, en México no existe un apartado específico en donde sea regulada la Firma Electrónica, sólo hablan de ella, al igual que en el presente código.

El título I segundo capítulo del Código Fiscal de la Federación se denomina “De los medios electrónicos” y comprende los siguientes artículos. 17-C, 17-D, 17-E, 17-F, 17-G, 17-H, 17-I, 17-J. entre los cuales se encuentra regulada la Firma Electrónica Avanzada; a continuación veremos los artículos referentes a la Firma Electrónica Avanzada.

“Artículo 17-C Tratándose de contribuciones administradas por organismos fiscales autónomos, las disposiciones de este código en materia de medios electrónicos sólo serán aplicables cuando así lo establezca la ley de la materia.”

“Artículo 17-D Cuando las disposiciones fiscales obliguen a presentar documentos, éstos deberán ser digitales y contener una firma electrónica avanzada del autor, salvo los casos que establezcan una regla diferente. Las autoridades fiscales, mediante reglas de carácter general, podrán autorizar el uso de otras firmas electrónicas.”

Para los efectos mencionados en el párrafo anterior, se deberá contar con un certificado que confirme el vínculo entre un firmante y los datos de creación de una firma electrónica avanzada, expedido por el Servicio de Administración Tributaria cuando se trate de personas morales y de los sellos digitales previstos en el artículo 29 de este Código, y por un prestador de servicios de certificación autorizado por el Banco de México cuando se trate de personas físicas. El Banco de México publicará en el Diario

Oficial de la Federación la denominación de los prestadores de los servicios mencionados que autorice y, en su caso, la revocación correspondiente.

En los documentos digitales, una firma electrónica avanzada amparada por un certificado vigente sustituirá a la firma autógrafa del firmante, garantizará la Integridad del documento y producirá los mismos efectos que las leyes otorgan a los documentos con firma autógrafa, teniendo el mismo valor probatorio.

Se entiende por documento digital todo mensaje de datos que contiene información o escritura generada, enviada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología.

Los datos de creación de firmas electrónicas avanzadas podrán ser tramitados por los contribuyentes ante el Servicio de Administración Tributaria o cualquier prestador de servicios de certificación autorizado por el Banco de México.

Cuando los datos de creación de firmas electrónicas avanzadas se tramiten ante un prestador de servicios de certificación diverso al Servicio de Administración Tributaria, se requerirá que el interesado previamente comparezca personalmente ante el Servicio de Administración Tributaria para acreditar su identidad. En ningún caso los prestadores de servicios de certificación autorizados por el Banco de México podrán emitir un certificado

sin que previamente cuenten con la comunicación del Servicio de Administración Tributaria de haber acreditado al interesado, de conformidad con las regias de carácter general que al efecto expida. A su vez, el prestador de servicios deberá informar al Servicio de Administración Tributaria el código de identificación único del certificado asignado al Interesado.

La comparecencia de las personas físicas a que se refiere el párrafo anterior, no podrá efectuarse mediante apoderado o representante legal. Únicamente para los efectos de tramitar la firma electrónica avanzada de las personas morales de conformidad con lo dispuesto en el artículo 19-A de este Código, se requerirá el poder previsto en dicho artículo.

La comparecencia previa a que se refiere este artículo también deberá realizarse cuando el Servicio de Administración Tributaria proporcione a los Interesados los certificados, cuando actúe como prestador de servicios de certificación.

Los datos de Identidad que el Servicio de Administración Tributaria obtenga con motivo de la comparecencia, formarán parte del sistema integrado de registro de población, de conformidad con lo previsto en la Ley General de Población y su Reglamento, por lo tanto dichos datos no quedarán comprendidos dentro de lo dispuesto por los artículos 69 de este Código y 18 de la Ley Federal de Transparencia y Acceso a la información Pública Gubernamental”.

El presente artículo en sus dos últimos párrafos hace referencia a la vigencia de los certificados, pero este tema lo veremos más adelante en nuestro tercer capítulo.

El Artículo 17-E nos menciona que cuando los contribuyentes remitan un documento digital a las autoridades fiscales, recibirán el acuse de recibo que contenga el sello digital.

“Artículo 17-F El Servicio de Administración Tributaria podrá proporcionar los siguientes servicios de certificación de firmas electrónicas avanzadas:

1. Verificar la Identidad de los usuarios y su vinculación con los medios de identificación electrónica.

- II. Comprobar la integridad de los documentos digitales expedidos por las autoridades fiscales.

- III. Llevar los registros de los elementos de identificación y de vinculación con los medios de identificación electrónicos de los firmantes y, en su caso, de la representación legal de los firmantes y de aquella información con la que haya verificado el cumplimiento de fiabilidad de las firmas electrónicas avanzadas y emitir el certificado.

IV. Poner a disposición de los firmantes los dispositivos de generación de los datos de creación y de verificación de firmas electrónicas avanzadas o sellos digitales.

V. Informar, antes de la emisión de un certificado a la persona que solicite sus servicios, de las condiciones precisas para la utilización del certificado y de sus limitaciones de uso.

VI. Autorizar a las personas que cumplan con los requisitos que se establezcan en reglas de carácter general, para que proporcionen los siguientes servicios:

a) Proporcionar Información sobre los certificados emitidos por el Servicio de Administración Tributaria, que permitan a terceros conocer:

1) Que el certificado fue emitido por el Servicio de Administración Tributaria.

2) Si se cuenta con un documento suscrito por el firmante nombrado en el certificado en el que se haga constar que dicho firmante tenía bajo su control el dispositivo y los datos de creación de la firma electrónica avanzada en el momento en que se expidió el certificado y que su uso queda bajo su exclusiva responsabilidad.

3) Si los datos de creación de la firma eran válidos en la fecha en que se expidió el certificado.

- 4) El método utilizado para identificar al firmante.
- 5) Cualquier limitación en los fines o el valor respecto de los cuales puedan utilizarse los datos de creación de la firma o el certificado.
- 6) Cualquier limitación en cuanto al ámbito o el alcance de la responsabilidad del Servicio de Administración Tributaria.
- 7) Si se ofrece un servicio de terminación de vigencia de los certificados.
  - b) Proporcionar los servicios de acceso al registro de certificados. A dicho registro podrá accederse por medios electrónicos.

Las facultades mencionadas podrán ser ejercidas directamente en cualquier tiempo por el Servicio de Administración Tributaria, pudiendo hacerlo en forma separada o conjunta con las personas autorizadas en los términos de esta fracción.”

El Artículo 17-G nos habla de los requisitos que deberán contener los certificados que emita el Servicio de Administración Tributaria para ser considerados válidos.

El Artículo 17-H nos menciona cuando quedarán sin efectos los certificados que emita el Servicio de Administración Tributaria.

“Artículo 17-I La integridad y autoría de un documento digital con firma electrónica avanzada o sello digital será verificable mediante el método de remisión al documento original con la clave pública del autor.”

Por último, el artículo 17-J nos señala las obligaciones que tendrá el titular de un certificado emitido por el Servicio de Administración Tributaria

Es necesario señalar que los artículos 18 B; 19; 19-A, 20 último párrafo, 22-A, 22-B, 28 con un décimo y décimo primer párrafos; 28, con las fracciones IV y V; 29 párrafos octavo y décimo cuarto; 29-A fracción IX y el último párrafo; y 29-B; también regulan algunos aspectos de los medios electrónicos y la firma electrónica.

Como podemos darnos cuenta, los conceptos que maneja el Código de Comercio fueron tomados de la Ley modelo sobre las firmas electrónicas de la Comisión de las Naciones Unidas para el Derecho Mercantil.

Del presente capítulo se desprende que no existe en México un ley específica que regula a la firma electrónica, sino simplemente un conjunto de ordenamientos jurídicos en diversas leyes, que hacen alusión a la firma electrónica avanzada.



## **CAPÍTULO TERCERO.**

### **VENTAJAS Y DESVENTAJAS DE LA FIRMA ELECTRÓNICA AVANZADA**

Cada día, las personas físicas y morales utilizan Internet para realizar infinidad de transacciones en línea. Cada uno de nosotros compartimos archivos e información confidencial, ya sea por la red o mediante el correo electrónico. Actualmente, los clientes de diversas empresas, como los bancos, ya se encuentran habituados a verificar la información de su cuenta o a realizar pagos en las computadoras, desde la comodidad del hogar utilizando este medio.

El Internet es una herramienta que ha venido a reemplazar al teléfono o al fax en las actividades comerciales u operaciones diarias pero, a la par, se ha convertido en un medio para interceptar mensajes, robar información confidencial, o realizar fraudes.

El avance y auge de las tecnologías de la comunicación y concretamente las relativas a Internet, ha sentado un precedente, en el que surgen herramientas que facilitan el trabajo a través de la red. Por eso se hace necesario, sobre todo en algunas operaciones (transferencias bancarias, consulta de expedientes o aquellas que involucren la circulación de información con datos confidenciales por su naturaleza), garantizar al usuario una seguridad a prueba de cualquier peligro.

La seguridad en los intercambios de información en Internet comprende tres aspectos principales: privacidad, integridad y autenticación. La privacidad hace referencia a que la información enviada no es accesible a un tercero; la integridad asegura que el contenido no sea alterado; y finalmente, la autenticación garantiza la identidad de su remitente.

### **3.1 Firma Autógrafa**

#### **Definición**

El vocablo firma proviene del latín *firmare* que significa afirmar, dar fuerza, y el vocablo *autógrafa* significa grabar o escribir por si mismo. En la práctica no es más que “el conjunto de signos manuscritos por una persona que sabe leer y escribir, con los cuales habitualmente caracteriza los escritos cuyo contenido aprueba”<sup>7</sup>

En Roma, existía la *Manufirmatio*, que consistía en una ceremonia en que leído el documento por su autor, o el funcionario, se colocaba desenrollando y extendido sobre la mesa del escribano y luego de pasar la mano abierta sobre el pergamino en actitud de jurar, pero sin hacerlo, se estampaba el nombre, signo, o una o tres cruces, por el autor o el funcionario en su nombre, haciéndolo seguidamente los testigos. Más que un requisito, la *Manufirmatio* era en sí misma parte del espectáculo solemne en que se realizaba el acto.

---

<sup>7</sup>MANTILLA MOLINA, Roberto; Títulos de Crédito cambiarios; México; Ed. Porrúa; 1977.

En la Edad Media, se inscribía una cruz a la que se le añadían diversas letras y rasgos. Estos signos se utilizaban como firma. Debido a que no sabían leer ni escribir, los nobles remplazaron esta práctica con el uso de sellos.

La diferenciación entre “firmas” y “signos” hizo que se empezase a entender que aquéllas eran, más que simples “signos”, la inscripción manuscrita del nombre o de los apellidos. En ese tiempo, pocas eran las personas que sabían leer y escribir, por lo que generalmente los particulares estampaban en los documentos que suscribían diversos signos o sellos, la extensión de la instrucción y el desenvolvimiento de las transacciones comerciales, hicieron que la firma fuera adquiriendo la importancia y uso que con el transcurso del tiempo se fue consagrando como un símbolo de identificación y de enlace entre el autor de lo escrito o estampado y su persona.

Según la Academia, es “el nombre y apellido, o título, de una persona, que ésta pone con rúbrica al pie de un documento escrito de mano propia o ajena, para darle autenticidad o para obligarse a lo que en él se dice. Por *rúbrica* se entiende “el rasgo o conjunto de rasgos de figura determinada, que como parte de la firma pone cada cual después de su nombre o título”. A veces pónese la rúbrica sola; esto es, sin que vaya precedida de nombre o título de la persona que rubrica.

No se ha escrito hasta la fecha una teoría propia de la firma, su concepto, elementos, consecuencias y efectos; son pocas las referencias que hay sobre la materia y más bien son obras de Derecho Notarial las que se ocupan del tema. Como una primera aproximación debemos entender que “la firma es el conjunto de letras y signos entrelazados, que identifican a la persona que la estampa, en un documento o texto”.<sup>8</sup>

### **Características:**

- a) **Identificativa:** Sirve para identificar quién es el autor del documento.
- b) **Declarativa:** Significa la exaltación del contenido del documento por el autor de la firma. Sobretudo cuando se trata de la conclusión de un contrato, la firma es el signo principal que representa la voluntad de obligarse.
- c) **Probatoria:** Permite identificar si el autor de la firma es efectivamente aquél que ha sido identificado como tal en el acto de la propia firma.<sup>9</sup>

### **Elementos**

Al respecto es necesario distinguir entre dos tipos de elementos:

- a) **Formales.-** Son aquellos elementos materiales de la firma que están en relación con los procedimientos utilizados para firmar y el grafismo mismo de la misma:

---

<sup>8</sup>ACOSTA ROMERO, Miguel; Nuevo Derecho Mercantil, Porrúa, México 2000, p 537.

<sup>9</sup>REYES KRAFFT, Alfredo; La firma electrónica y las entidades de certificación, Porrúa, México 2003, p 159.

- \* *La firma como signo personal.* La firma se presenta como un signo distintivo y personal, ya que debe ser puesta de puño y letra del firmante. Esta característica de la firma manuscrita puede ser eliminada y sustituida por otros medios en la firma electrónica.
- \* *El animus signandi.* Es el elemento intencional o intelectual de la firma. Consiste en la voluntad de asumir el contenido de un documento, que no debe confundirse con la voluntad de contratar, como señala Larrieu.

b) **Funcionales:** Tomando la noción de firma como el signo o conjunto de signos, podemos distinguir una doble función:

- \* *Identificadora:* La firma asegura la relación jurídica entre el acto firmado y la persona que lo ha firmado. La identidad de la persona nos determina su personalidad a efectos de atribución de los derechos y obligaciones. La firma manuscrita expresa la identidad, aceptación y autoría del firmante. No es un método de autenticación totalmente fiable. En el caso de que se reconozca la firma, el documento podría haber sido modificado en cuanto a su contenido -falsificado- y en el caso de que no exista la firma autógrafa puede ser que ya no exista otro modo de autenticación. En caso de duda o negación puede establecerse la correspondiente pericial caligráfica para su esclarecimiento.

- \* *Autenticación*: El autor del acto expresa su consentimiento y hace propio el mensaje: Operación pasiva que no requiere del consentimiento, ni del conocimiento siquiera del sujeto identificado. Proceso activo por el cual alguien se identifica conscientemente en cuanto al contenido suscrito y se adhiere al mismo.

### **3.2 Firma Electrónica**

#### **Definición**

Para Del Pesseo Navarro, la firma electrónica es una señal digital representada por una cadena de bits que se caracteriza por ser secreta, fácil de reproducir y reconocer, difícil de falsificar y cambiante en función del mensaje y tiempo, cuya utilización obliga a lo que se denomina como fedatario electrónico, personaje que será capaz de identificar y verificar la autenticidad de los documentos que circulan a través de las líneas de comunicación, lo que se traduce en tener un respaldo jurídico.<sup>10</sup>

Según el Art. 2 inciso a) de la Ley Modelo de la CNUDMI<sup>11</sup>, por firma electrónica deberá entenderse “los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados, que puedan ser utilizados para identificar

---

<sup>10</sup> Cfr. DEL PESSO NAVARRO, Emilio, Resolución de conflictos en el cambio electrónico de Documentos, Poder Judicial de Madrid, España 1996, p 191.

<sup>11</sup> CNUDMI= Comisión de las Naciones Unidas para el Derecho Mercantil Internacional.

al firmante en relación con el mensaje de datos e indicar que este último aprueba la información recogida en el mensaje de datos”.

De igual forma en la Ley arriba mencionada, en el mismo artículo y en su inciso c) señala lo que habrá de entenderse como mensaje de datos y esto es: “la información generada, enviada, recibida, archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax”.

El documento electrónico está considerado como un medio de expresión de la voluntad con efectos de creación, modificación o extinción de derechos y obligaciones por medio de la electrónica. Siendo la seguridad fundamental en el comercio electrónico para su desarrollo.

La firma electrónica, específicamente, es un conjunto o bloque de caracteres que viaja junto a un documento o mensaje y que puede acreditar cuál es el autor o emisor del mismo (lo que se denomina autenticación) y garantizar la certeza de que nadie ha manipulado o modificado el mensaje en el transcurso de la comunicación (o integridad).

La firma electrónica es una clave única que puede ser: un archivo informático que identifique al firmante a través de un *password* (palabra de acceso) o de forma digitalizada, que se hace con una

pluma digital sobre una pantalla digital (Vgr. Credencial de elector o licencia de conducir).

A partir de un previo acuerdo entre las partes y tomando en cuenta una presunción establecida en la ley, se le adjudica a alguien el uso de una clave. Asimismo se establece si determinada comunicación partió de un sistema programado por el emisor o en su nombre para operar electrónicamente. Esto alude a las operaciones o transacciones que se llevan a cabo a través de e-mail

Sólo funge como medio de relación entre el contenido de un documento con su autor; es insegura debido a que el documento es susceptible de sufrir alteraciones fácilmente y no habrá forma de comprobar la mutilación, de igual forma llanamente puede obtenerse la palabra clave (*password*).

Específicamente definiremos a la Firma Electrónica como el conjunto de datos, en forma electrónica, anexos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge. La debilidad en cuanto al emisor y al receptor radica en la posible suplantación de la identidad de alguno de ellos por parte de elementos ajenos al sistema.<sup>12</sup>

---

<sup>12</sup>. REYES KRAFFT, Alfredo; La firma electrónica y las entidades de certificación, Porrúa; México, 2003, p221.



### **3.3 Firma Electrónica Avanzada**

#### **Definición**

Para efectos de nuestro tema de investigación se entenderá por firma electrónica avanzada: el conjunto de datos que se adjuntan a un mensaje electrónico que permite cifrar información para que sea enviada a través de Internet en forma óptima.

La firma fiable o avanzada es entendida como un proceso que permite al receptor de un mensaje identificar formalmente a su autor, el cual mantiene bajo su exclusivo control los medios para crear la clave privada, de manera que esté vinculada a él a través de un certificado y a los datos que se refiere el mensaje. Esto permite detectar cualquier modificación posterior al contenido del mensaje, el cual es accesible al usuario para consultas siguientes.

Brevemente se explicará que está formada por un par de claves que son diferentes entre si, de las cuales una es pública y por tanto conocida y otra privada que únicamente conoce y conserva su autor.

Para que una firma electrónica sea considerada como fiable debe cumplir con lo siguiente:

- a) Los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante;
- b) Los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante;
- c) Es posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma; y
- d) Cuando uno de los objetivos del requisito legal de firma consista en dar seguridades en cuanto a la integridad de la información a que corresponde; es posible detectar cualquier alteración de esa información hecha después del momento de la firma.

Con lo anterior es factible garantizar:

- a) *Autenticación*, para asegurar la identidad de la persona con la que se está comerciando. Es una característica intrínseca, es decir, el autor del mensaje queda debidamente acreditado al contener sus datos personales, máxime del signo gráfico, plasmado en el documento digital que otorga seguridad y certeza jurídica en la integridad primitiva del mismo y que significa que el autor de la firma electrónica avanzada expresa su voluntad libre de vicios.
- b) *Autorización*, para asegurar que esa persona es la indicada para llevar a cabo una operación concreta.

- c) *Privacidad*, para garantizar que nadie más va a ver los intercambios de datos que se lleven a cabo. Significa que sólo el receptor puede descifrar el contenido del mensaje, debido a que la encriptación transforma el mensaje original en caracteres ininteligibles y el acceso al mensaje original es restringido por medio de claves, por lo que únicamente el contribuyente lo puede descodificar.
  
- d) *Integridad*, para asegurar que la transmisión no sea alterada en ruta o en almacenaje. Al contener la firma el documento, se otorga la seguridad de que la firma está protegida contra alguna modificación, alteración o destrucción de los datos contenidos en el mismo.
  
- e) *No Repudiación*, para garantizar que quien envía el mensaje no puede negar que lo envió el: Ofrece seguridad de que el autor del documento no puede retractarse en el futuro de las opiniones o acciones consignadas en él, ni mucho menos de no haberlo enviado.

### **3.3.1 Contribuyentes que deben utilizar la Firma Electrónica Avanzada**

Aquellas personas físicas y morales que están obligadas a presentar sus solicitudes en materia de RFC, declaraciones, avisos o informes, en documentos digitales con Firma Electrónica Avanzada, son las siguientes:

1. Los contribuyentes personas físicas que realicen actividades empresariales y que en el ejercicio inmediato anterior hubiesen obtenido ingresos superiores a \$1´750,000.00.
2. Las personas físicas que no realicen actividades empresariales y que hubiesen obtenido en el ejercicio inmediato anterior ingresos superiores a \$300,000.00.

### **3.3.2 Características de la Firma Electrónica Avanzada**

Las características de la Firma Electrónica Avanzada ofrecen seguridad y confiabilidad, a continuación se explicarán a detalle cada una:

- a) **Soporte Jurídico y Reconocimiento ante Autoridades Fiscales:** Se refiere a que el uso de la firma electrónica tendrá todas las cualidades de la firma autógrafa y de igual forma poseerá el mismo valor probatorio.
- b) **Infraestructura técnica confiable:** Es decir, la fiabilidad de la creación de la Firma Electrónica Avanzada basada en una infraestructura de clave pública en que se utilizan los logaritmos asimétricos, que son programas y sistemas técnicos, tecnología de punta que permite otorgar seguridad jurídica a las partes...
- c) **Accesibilidad:** Significa que el contenido del mensaje de datos en el que se consignan derechos y obligaciones,

pueda ser disponible al usuario para su posterior consulta siempre y cuando reúna las anteriores características.

### **3.3.3 Requisitos de la Firma Electrónica Avanzada.**

De acuerdo con lo establecido en el artículo 17-D del Código Fiscal de la Federación, la creación de las firmas electrónicas avanzadas podrá ser tramitado por los contribuyentes ante el Servicio de Administración Tributaria o cualquier prestador de servicios autorizados el Banco de México

El caso de que los datos de creación de firmas electrónicas avanzadas que se tramiten ante un prestador de servicios de certificación diversos al Servicio de Administración Tributaria, se requerirá que el interesado previamente comparezca personalmente ante el Servicio de Administración Tributaria para acreditar su identidad.

Las personas físicas no podrán comparecer mediante apoderado o representante legal. Únicamente para la tramitación de los datos de creación del Firma Electrónica Avanzada de una persona moral, solo la podrá efectuar un representante de dicha persona, a quien le haya sido otorgado ante fedatario público, un poder general para actos de dominio o de administración, en este caso el representante deberá contar previamente con un certificado vigente de Firma Electrónica Avanzada.

### ***Procedimiento para obtener la Firma Electrónica Avanzada***

El procedimiento para obtener la Firma Electrónica Avanzada es el siguiente:

1. Los contribuyentes deberán concertar vía telefónica una cita para acudir a la Administración Local de Asistencia al Contribuyente del Servicio de Administración Tributaria
2. Ingresar al portal del Servicio de Administración Tributaria ([www.sat.gob.mx](http://www.sat.gob.mx)), entrar en la sección de “tu firma” y descargar del *software* el programa Solicitud de Certificado Digital “SOLCEDI” en cual se genera el requerimiento de certificado de firma electrónica avanzada (archivo con terminación. *req*) y la clave privada (archivo con terminación. *key*).
3. Una vez obteniendo este programa deberán otorgar sus datos personales, conforme el mismo programa se lo va indicando.
4. El archivo con terminación *.req* deberá presentarse en un disco magnético de 3.5. El archivo con terminación. *key* deberá ser grabado con mucho cuidado por el que contiene los datos de la firma electrónica.
5. Realizando este procedimiento acudirán a su cita ante la autoridad hacendaría donde se presentarán los documentos que se le requirió y entregaran su disco magnético así como el llenado

de solicitud de Firma Electrónica Avanzada que bajaron de la página del Servicio de Administración Tributaria.

6. Durante su comparecencia se proporcionarán los datos de identidad del contribuyente o de la empresa a través de su representante legal según sea el caso; consultarán su situación fiscal y revisarán su documentación, digitalizarán los mismos, su fotografía, su firma autógrafa, así como las huellas dactilares excepto los dedos pulgares; información que forma parte de la base de datos de la autoridad fiscal.

7. Por último para obtener el certificado digital deberá acceder a la sección “tu firma”, en la pestaña de entrega de certificados, utilizando la clave del registro federal de contribuyentes y seguir las instrucciones.

En lo que respecta a los servidores públicos también deberán llevar a cabo este procedimiento y presentarse personalmente para acreditar su personalidad como funcionario público de la Administración Local de Asistencia al Contribuyente otorgando sus datos.

### **3.3.4 Entidades Certificadoras**

Para brindar confianza a la clave pública surgen las entidades de certificación, cuya misión en términos generales es la de emitir certificados que contienen información sobre algún hecho o circunstancia del sujeto del certificado.

Las entidades de certificación nacen debido a la creciente interconexión de los sistemas de información y a las cada vez mayores prestaciones de las actuales redes de telecomunicación, obtenidas plenamente en la digitalización.

Reyes Kraff la define de la siguiente manera “Es la unidad que genera y revoca los certificados para un conjunto de usuarios y es responsable de su autenticidad.”<sup>13</sup>

### ***Funciones de las autoridades de certificación***

Las entidades de certificación tienen diversas funciones y entre las principales están las siguientes:

1. Generación de certificados al garantizar su identidad por medio de una firma digital.
2. Agendar fechas de expiración de los certificados y revocar de los certificados.
3. Revocar los certificados.

Una característica fundamental de la autoridad certificadora es que sea un ente de alta confianza para la comunidad.

---

<sup>13</sup> Ibidem, p.271.



### ***Tipos de certificación.***

Existen diferentes tipos de certificación que las autoridades pueden emitir:

*Los certificados de identidad:* son los más utilizados dentro de los criptosistemas de clave pública y ligan una identidad personal o digital a una clave pública.

*Los certificados de autorización o potestad:* certifican otro tipo de tributo del usuario distinto a la identidad.

*Los certificados transnacionales:* atestiguan que un hecho acontecido o que fue presenciada por un tercero.

*Los certificados de tiempo o de estampilla digital* permiten dar fe de que un documento existía en un tiempo determinado.

Después de ver las funciones y los tipos de certificados que existen es necesario mencionar que el Código Fiscal de la Federación respecto de la certificación de la firma electrónica; se encuentra establecido en el artículo 17 D en el cual nos menciona que: “Cuando las disposiciones fiscales obliguen a presentar documentos, éstos deberán ser digitales y contener una firma electrónica avanzada del autor, salvo los casos que establezcan una regla diferente. Las autoridades fiscales, mediante reglas de

carácter general, podrán autorizar el uso de otras firmas electrónicas.

Para los efectos mencionados en el párrafo anterior, se deberá contar con un certificado que confirme el vínculo entre un firmante y los datos de creación de una firma electrónica avanzada, expedido por el Servicio de Administración Tributaria cuando se trate de personas morales y de los sellos digitales previstos en el artículo 29 de este Código, y por un prestador de servicios de certificación autorizado por el Banco de México cuando se trate de personas físicas. El Banco de México publicará en el Diario Oficial de la Federación la denominación de los prestadores de los servicios mencionados que autorice y, en su caso, la revocación correspondiente

En los documentos digitales, una Firma Electrónica Avanzada amparada por un certificado vigente sustituirá a la firma autógrafa del firmante, garantizará la Integridad del documento y producirá los mismos efectos que las leyes otorgan a los documentos con firma autógrafa, teniendo el mismo valor probatorio.”

Este artículo señala que la Firma Electrónica Avanzada puede ser tramitada en el Servicio de Administración Tributaria o con prestadores de servicio de certificación autorizados por el Banco de México.

También menciona las reglas que deben seguir estos certificados y sus obligaciones de información ante el Servicio de Administración Tributaria.

### ***Vigencia de los Certificados.***

Por último, hablaremos de la vigencia que tienen los certificados, la cual se encuentra establecida también en el artículo 17-D y marca que: “Para los efectos fiscales, los certificados tendrán una vigencia máxima de dos años, contados a partir de la fecha en que se hayan expedido. Antes de que concluya el período de vigencia de un certificado su titular podrá solicitar uno nuevo. En el supuesto mencionado el Servicio de Administración Tributaria podrá, mediante reglas de carácter general, relevar a los titulares del certificado de la comparecencia personal ante dicho órgano para acreditar su identidad y, en el caso de las personas morales, la representación legal correspondiente, cuando los contribuyentes cumplan con los requisitos que se establezcan en las propias reglas. Si dicho órgano no emite las reglas de carácter general, se estará a lo dispuesto en los párrafos sexto y séptimo de este artículo.”

El Servicio de Administración Tributaria, mediante su página de internet señala que en el caso de que se obtenga certificado y se promueva que se quede sin efectos, si aún no vencen los dos años de vigencia, se solicitará la revocación del certificado fiscal

digital y posteriormente se podrá solicitar un nuevo certificado fiscal digital haciendo el trámite de nueva cuenta.

De lo anterior se desprende que la firma electrónica es un instrumento novedoso por medio del cual el firmante expresa su voluntad para realizar diversos trámites fiscales, sin necesidad de ir a las oficinas del Servicio de Administración Tributaria; y sin dejar atrás el hecho de que esta firma cuenta con valor probatorio.

Por lo que respecta a los requisitos para la creación de la Firma Electrónica Avanzada, cabe mencionar que a simple vista parecen sencillos los pasos a seguir; sin embargo, debemos observar que si no se cuenta con los conocimientos esenciales en el uso de la computadora, este trámite se vuelve complicado.

### **3.3.5 Métodos criptográficos (LLAVE PÚBLICA Y PRIVADA)**

El método más básico es el denominado criptosistema o algoritmo de encriptación.

Un sistema que habremos de conocer y que se utiliza en medios profesionales es el de “Criptosistemas”: Se trata de funciones matemáticas en las que los datos de entrada no se pueden obtener a partir de los de salida salvo en plazos tan largos que cualquier información obtenida ya no tiene valor. La seguridad se

basa ahora, no en mantener secreto el algoritmo, que generalmente es pues sino los parámetros (claves) del mismo<sup>14</sup>.

Existen dos tipos fundamentales de criptosistemas:

*1.-Criptosistemas Simétricos o de clave privada.-* Aquí se emplea la misma clave ( $k$ ) tanto para cifrar como para descifrar. El principal inconveniente que se observa en estos sistemas es que para ser empleado en comunicaciones, la clave ( $k$ ) debe ser compartida (dada a conocer) con el receptor. Por lo que surgen dos problemas: 1. El cómo transmitir la clave de forma segura y 2. El cómo asegurarse de que esta clave no será indebidamente filtrada y dada a conocer a terceros, con lo que se pierde certidumbre en estas comunicaciones.

*2.- Criptosistemas Asimétricos o de Llave Pública.-* Estos sistemas emplean una doble clave ( $k_p, k_P$ );  $k_p$  se conoce como clave privada y  $k_P$  se conoce como clave pública. Una de estas claves sirve para la transformación del cifrado (cifrar) y la otra para descifrar. En muchos casos son intercambiables, esto es, si empleamos una para cifrar, la otra servirá para descifrar y viceversa. Para que estos sistemas sean fiables y seguros, deberán cumplir con una condición básica: que el conocimiento de la clave pública ( $k_P$ ) no permita calcular o deducir la clave.

---

<sup>14</sup> ibidem. p.183.

## Cuadro Comparativo de las Diferencias existentes entre la Firma Electrónica y la Firma Electrónica Avanzada

El objetivo de este apartado es enumerar las diferencias más sobresalientes entre la Firma Electrónica Avanzada y la Firma Electrónica, resultando ser la primera, en cuanto a seguridad jurídica, más viable y confidencial.

Firma Electrónica	Firma Electrónica Avanzada
Es una clave única que puede ser: Un password o una Firma digital (es la que se realiza con una pluma digital sobre una pantalla digital).	Está compuesta por un par de claves, que son diferentes entre si, de las cuales una es <b>pública</b> por las personas encargadas de conocer la información y la otra es <b>privada</b> , es decir, que sólo la conocerá el autor.
Es Auténtica en tanto que relaciona el contenido de un documento con su autor.	Además de ser Auténtica, Identifica plenamente al autor del contenido.
El documento es susceptible de sufrir alteraciones con nula forma de comprobación.	El documento que contiene la información difícilmente podrá sufrir algún tipo de alteración, pues deben de conocerse ambas claves y deja huella de alteración.
Resulta fácil la obtención del password por los hackers o bien falsificarse (a través de escáner) la firma digital e insertarla en otro documento.	Las claves funcionan de forma independiente, de manera que al obtenerse una no se estará del conocimiento de la segunda.

	Encripta la información, de modo que los hace inteligibles para cualquier persona ajena al destinatario.
	No se puede desconocer la firma, en razón de que el documento cuenta con un sistema de acuses registrados.

### **3.4 Ventajas y Desventajas de la Firma Electrónica Avanzada**

Al representar la Firma Electrónica Avanzada un tema novedoso y actual, trae consigo cambios difíciles de asimilar, requerirá de práctica y de una nueva cultura de innovación informática; que por su misma naturaleza trae consigo ciertas ventajas y desventajas, que impiden la total satisfacción del servicio para el contribuyente.

#### **3.4.1 Ventajas**

Este apartado se deberá iniciar con las ventajas que el Servicio de Administración Tributaria refiere en su página de Internet, respecto de la Firma Electrónica Avanzada:

1. Elaborar declaraciones de impuestos por medios electrónicos de una manera más segura y sencilla;
2. Los documentos firmados electrónicamente tendrán las mismas funcionalidades y garantías de un documento físico;

3. Reducir el uso del papel en los sectores públicos y privados;
4. Servirá para expedir facturas electrónicas;
5. Gracias a sus características de no repudio y de autenticidad, se brindará mayor certeza jurídica a los contribuyentes en sus transacciones.
6. Mayor seguridad en las transacciones de comercio electrónico.

A la lista anterior agregará otros aspectos relevantes, que a nuestro parecer, de llevarse correctamente a la práctica, representarían un mayor número de ventajas.

1. Debo destacar que este tipo de procedimiento reducirá enormemente el tiempo que debía dedicársele con anterioridad, es decir, las visitas al Servicio de Administración Tributaria o a cualquier oficina recaudadora serán mínimas en comparación con la cantidad de vueltas que se realizaban personalmente o por terceras personas.
2. De aprenderse a utilizar este nuevo sistema de forma adecuada representaría un ahorro pecuniario (opcional), porque podrá prescindirse (no en todos los casos) del personal especializado en el tema, como lo son los contadores (aunque a la fecha la cantidad de trabajo para



estas personas aumento, debido a la gran confusión que impera).

3. Los errores en la documentación se reducirán considerablemente, debido a que la captura o descriptación de datos es exacta.
4. Otras ventajas que se presentan, aunque no directamente para el contribuyente, pero sí para la Secretaría de Hacienda y Crédito Público es que se reducirá considerablemente la carga del servicio; agilizar los intercambios comerciales; reducir la evasión fiscal;
5. En el momento que se expiden los certificados con las claves públicas o privadas, es decir, la Firma Electrónica Avanzada, se establece un periodo de vigencia, es decir, que a determinado tiempo habrá que solicitar una nueva Firma; lo que implica una seguridad constante por el cambio periódico de claves.

### **3.4.2 Desventajas**

Como ya mencione, al ser este tema o este método de solicitud y rendición de informes a Hacienda, de reciente aparición en la sociedad, trae consigo múltiples desventajas, que resultan ser superiores a las ventajas.

1. En primer lugar resaltaría que es muy poco el tiempo el señalado o permitido para que este método sea opcional, debido a que no puede desecharse en uno o dos años el sistema que ha prevalecido por décadas. Los Contribuyentes requieren de un mayor plazo para adaptarse a esta nueva modalidad.
2. Siguiendo con la responsabilidad de las autoridades hacendarías, se debe de poner énfasis en la difusión apropiada de este nuevo sistema, debido a que su publicidad no ha sido la suficiente, se atienden a que los contadores serán los encargados de hacer del conocimiento de sus clientes (personas físicas y morales) esta nueva modalidad.
3. No proporciona una seguridad jurídica para el contribuyente, esto en razón de que los datos de éstos pueden ser conocidos por personas ajenas a la relación emisor – receptor, pues estamos ante la presencia de delitos informáticos.

Tomando en consideración que la informática posee ciertas características que le convierten en un método idóneo para la comisión de diferentes modalidades delictivas y en especial las de carácter patrimonial.

4. Se está de igual manera ante la suplantación de identidad por medios electrónicos, es decir, se puede apropiar de forma no autorizada la identidad de un tercero, con el fin de causar un daño u obtener un beneficio.
5. Creemos que no se ha considerado ampliamente (mucho menos legislado) la responsabilidad de los servidores públicos encargados de recibir la información confidencial del contribuyente

Las autoridades tributarias señalan que esta nueva forma de presentar documentos es inviolable, pero omiten mencionar que sus trabajadores bien podrían revelar a terceros dicha información, porque finalmente existirá un banco de datos, al que tendrán acceso determinadas personas, mismas que pueden revelarlos

6. Enunciación especial debe hacerse al “pirata informático o hacker”, entendiéndose por éstos a aquellos que interceptan dolosamente un sistema informático, para dañar, apropiarse, desviar o difundir y/o destruir información que se encuentra almacenada en ordenadores pertenecientes a instituciones públicas o privadas. Ante esto Hacienda no ha difundido que sus sistemas se encuentren 100% protegidos y libres de cualquier sabotaje.
7. Continuando bajo los mismos parámetros, notamos que no existen herramientas legales apropiadas para defender al

contribuyente ante las autoridades hacendarías, sólo se está ante la cancelación del certificado o comprobante, cuando exista el riesgo de no haberse recibido íntegramente; quedando las personas físicas o morales en estado de indefensión, por no poseer documentos que acrediten su dicho.

8. Finalmente encuentro otra desventaja, respecto a que los certificados en los que se encuentran implícitos las claves públicas y privadas, es decir, la Firma Electrónica Avanzada, tienen un periodo de vigencia, es como si cada dos meses debiera de inventarse una nueva firma autógrafa el contribuyente; ésta, que a determinado tiempo deba solicitar una nueva firma.

## CONCLUSIONES

**PRIMERA:** La evolución tecnológica en la actualidad se encuentra inmersa en todos los ámbitos de la sociedad, es decir, está presente en cada una de las actividades que realizamos en nuestra vida diaria.

**SEGUNDA:** El ámbito jurídico y comercial no han permanecido inmunes a esta tecnología, debido a las nacientes modalidades de celebración de actos jurídicos por estos medios; revelando la necesidad de la ciencia del Derecho de encontrar las formas y condiciones que optimicen el objetivo de dicha tecnología.

**TERCERA:** Por lo que se refiere a la materia fiscal, desde hace un par de años se aprobó la utilización de medios electrónicos para cumplir con obligaciones determinadas, señaladas en el título primero, capítulo segundo de Código Fiscal de la Federación

**CUARTA:** Específicamente el Servicio de Administración Tributaria ha creado la Firma Electrónica Avanzada para que las personas físicas y morales que se encuadren en el supuesto establecido, presenten solicitudes en relación al RFC, declaraciones, avisos o informes, en documentos digitales con Firma Electrónica Avanzada

**QUINTA:** El objetivo fundamental de la Firma Electrónica Avanzada es integrar datos en forma electrónica, asociados a un mensaje de datos, los cuales son utilizados para acreditar la identidad del firmante en relación con el mensaje, e indican que éste asume como propia la información contenida en él, lo que produce los mismos efectos jurídicos que la firma autógrafa.

Aunque cuando se tratara de someter a la Firma Electrónica Avanzada a una prueba para verificar la autenticidad del emisor, no podría comprobarse con plena seguridad o valor probatorio, porque sólo estaríamos ante el elemento de *no repudio* impuesto por el Servicio de Administración Tributaria, para conocer si proviene del propietario; sin embargo, la firma autógrafa sí puede ser sometida a un peritaje y probar quien la emitió, por el hecho de plasmarse rasgos característicos difíciles de imitar a la perfección.

**SÉPTIMA:** Desde mi punto de vista, para que en México se puedan aplicar estos mismos avances tecnológicos e informáticos en materia fiscal falta demasiado conocimiento del tema, pues a pesar de la existencia de la policía cibernética, se carece de los elementos necesarios y presupuesto para capacitación, incluyendo al Servicio de Administración Tributaria.

**OCTAVA:** Sin duda la Firma Electrónica Avanzada posee múltiples ventajas, tanto para el contribuyente como para las autoridades hacendarías; sin embargo, eso no quita el que

todavía haya innumerables circunstancias que el legislador deberá de tomar en cuenta para desarrollar y fortalecer el marco jurídico de la Firma Electrónica Avanzada.

No es el objeto de este trabajo desmeritar esta nueva opción en materia tributaria, sin embargo, es lógico que el gobierno no señalaría de ninguna forma las posibles desventajas que traería aparejada esta modalidad.

**NOVENA:** cabe mencionar que la contratación y el comercio electrónico representan una nueva forma de manifestar la voluntad, derivada de los avances tecnológicos.

Con esta nueva forma de contratar se plantean problemas, como la ausencia del soporte en papel y de la firma autógrafa que acredita la autenticidad y le otorga validez al documento; ante esta situación se cuestiona la validez del documento emitido y contenido en un soporte electrónico.

**DÉCIMA:** Finalmente, destacaría que la Firma Electrónica Avanzada no puede reemplazar y gozar del mismo valor probatorio que la firma autógrafa, en razón de que los medios (la FEA) que sustituyen a la firma autógrafa, están dispuestos en unas Reglas de Miscelánea Fiscal y no en una Ley como lo dispone la Constitución, quedando al arbitrio de la autoridad hacendaría otorgar los mismos efectos de la Firma Electrónica Avanzada a la de la firma autógrafa.

## ANEXO

A continuación se anexan dos jurisprudencias que servirán para ilustrar el presente trabajo.

	<b>Novena época</b>	<b>No. de Registro: 186,038</b>
<b>Instancia</b>	<b>Tribunales Colegiados de Circuito</b>	
<b>Aislada</b>		
<b>Fuente</b>	<b>Semanario Judicial de la Federación y su Gaceta</b>	
	<b>Materia(s): Administrativa</b>	
<b>Tomo;</b>	<b>XV Septiembre de 2002</b>	
<b>Tesis:</b>	<b>I.7o.A.183 A</b>	
<b>Página:</b>	<b>1351</b>	

**DECLARACIONES FISCALES PRESENTADAS POR MEDIOS ELECTRÓNICOS (VÍA INTERNET). EL PRIMER ACTO DE APLICACIÓN SE ACREDITA CON ACUSE DE RECEPCIÓN QUE CONTENGA LOS DATOS REFERENTES A LA HORA, FECHA, FOLIO Y TIPO DE OPERACIÓN, TRANSMITIDO POR LA AUTORIDAD CORRESPONDIENTE.**

Para acreditar el primer acto de aplicación y, por ende, el interés jurídico del gobernado para acudir al juicio de amparo a reclamar una Ley, basta con la exhibición de la constancia de recepción de la declaración y pago correspondiente, presentada a través de los medios electrónicos, específicamente en la página del Servicio de Administración Tributaria de la red respectiva que contenga los datos relativos a 1. hora, fecha, folio y tipo de operación, para considerarse acreditado el acto de aplicación de las normas reclamadas en el juicio de garantías, toda vez que las constancias de referencia son el único documento que se puede obtener para demostrar el cumplimiento de las obligaciones fiscales por esa vía, de conformidad con lo dispuesto en el artículo 31, párrafo segundo, del Código Fiscal de la Federación y la regla número 2.10.7. de la miscelánea fiscal vigente para el año dos mil uno.

**SÉPTIMO TRIBUNAL COLEGIADO EN MATERIA ADMINISTRATIVA DEL PRIMER CIRCUITO.**

Amparo en revisión 1067/2002. Servicios Monte Blanco, SA de C.V y. 22 de mayo de 2002. Unanimidad de votos. Ponente: David Delgadillo Guerrero. Secretaria: Maria del Recio Sánchez Ramírez.



No. de Registro:  
922,766

**Instancia**

**Aislada**

**Fuente**

**Materia(s): Electoral**

**Tomo: Tomo VIII, P.R. Electoral**

**Tesis 147**

**Página: 177**

**Genealogía: Compilacion Oficial de Jurisprudencia y Tesis Relevantes 1997-2002, páginas 484-465, Sala Superior, tesis S3EL 07612002.**

**FIRMA. ES INVÁLIDA LA QUE NO PROVIENE DEL PUÑO Y LETRA DE SU APARENTE AUTOR (LEGISLACIÓN DEL ESTADO DE SAN LUIS POTOSÍ)-**

La interpretación sistemática y funcional de los artículos 27. 66, 122, 130. 132. 192, 201 y 204, de la Ley Electoral del Estado de San Luis Potosí. permite establecer que el requisito de la firma que debe constar en los diversos documentos que establece la propia legislación electoral, debe satisfacerse, ya sea usando una rúbrica o simplemente escribiendo el nombre y apellido, o en casos especiales que la persona no sepa leer o escribir, imprimiendo su huella dactilar, en razón de que, de los artículos 27, fracción III, inciso b), párrafo 2; 122, 132 y 192. fracción Y de la Ley Electoral del Estado do San Luis Potosí, se desprende que ciertos documentos no sólo deben ser firmados, sino que debe manifestarse el nombre completo (nombre y apellidos) de las personas a que dichos documentos les incumben, en virtud de lo cual, debe considerarse que poner el nombre y apellidos es un requisito diferente al de suscribir el documento de propia mano y no por conducto de un medio mecánico o electrónico; además, debe precisarse, que el motivo de que todas estas normas establezcan la necesidad de firmarlas & propia mano, estriba en que, a través de esta suscripción, el legislador pretende asegurar que se exprese la voluntad de obligare con los actos jurídicos que se están realizando; que, en fin, se acredite la autenticidad del documento que suscribe y se logre la eficacia provista en la ley, ya que de estimarse que se ponga en otra forma distinta (mecánica o electrónica), las autoridades electorales tanto administrativas como jurisdiccionales, no tendrían la certeza de que realmente la persona facultada tuviese el propósito de ejecutar el acto o acción que están realizando o poniendo en movimiento a través del ocurso respectivo, en razón de que, cualquier otra persona sin el consentimiento concerniente, podría escribir el nombre de la persona facultada, y con esto, cumplir con el requisito mencionado; de modo que no puede considerarse firmado un escrito por el simple hecho de que en el conste el nombre y apellidos impresos por un medio diferente al puño y letra.

Juicio de revisión constitucional electoral. SUP-JRC-143/2000.-Coalicción Frente Cívico Potosino.-7 de agosto de 2(XXL-Unanimidad de votos-ponente: Alfonsina Berta Navarro Hidalgo-Secretario: Genaro Escobar Ambriz.

Compilación Oficial de Jurisprudencia y Tesis Relevantes 1997-2002. páginas 464-465, Sala Superior, tesis SSEL 076/2002.

## **BIBLIOGRAFIA.**

ACOSTA ROMERO, Miguel, Nuevo derecho mercantil, Porrúa, México, 2000, p.537.

DEL PESO NAVARRO Emilio, Resolución de conflictos en el intercambio electrónico de documentos, Consejo General del Poder Judicial Madrid, 1996, p.191.

MANTILLA MOLINA, Roberto, Títulos de Crédito cambiarios; México, Porrúa, 1977.

PEREZ CHAVEZ Capero Fol, Firma electrónica avanzada, documentos, digitales y comprobantes electrónicos, Tax, México, 2005, p. 20.

RATIA MENDOZA, Alberto; Declaración por medios electrónicos, calidad e información, México, 2000, p.18.

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

RODRÍGUEZ LOBATO Raúl, Derecho Fiscal, segunda edición, Harla, México, 1999, p. 231.

PINO CABALLERO Gil, Introducción a la criptografía, segunda edición, Alfaomega Ra Ma, México, 2003, p.7.

Universidad Pedagógica Nacional, Metodología de la investigación, Limusa, México, 2000.

WITKER VELAZQUEZ Jorge, Metodología jurídica, segunda edición, Mc Graw Hill, México, 2002.

## LEGISLACIÓN.

Constitución Política de los Estados Unidos Mexicanos  
Código Civil Federal  
Código Federal de Procedimientos Civiles  
Código de Comercio  
Código Fiscal de la Federación

## OTRAS FUENTES:

El contrato por medios electrónicos, departamento de derecho de los negocios, Línea de investigación sobre la contratación de medios electrónicos, Universidad Externado de Colombia, 2003, p.135, 136.

CNUDMI= Comisión de las Naciones Unidas para el Derecho Mercantil Internacional

Diccionario de la real Academia de la Lengua Española, Tomo II  
Décimo novena edición, pag, 381.

Enciclopedia Jurídica Ameba, tomo XII, editorial bibliográfica Argentina.

Proyecto de ley española de firma electrónica Madrid, España 1999.

## SITIOS EN INTERNET:

<http://camara.de.diputados.Gob.mx>

<http://sat.gob.mx>

<http://juridicas.unam.mx>

<http://scjn.gob.mx>

<http://www.cervantesvirtual.com>