



Universidad  
Latina

**UNIVERSIDAD LATINA S.C.**

---

---

**INCORPORADA A LA UNAM**

**FACULTAD DE DERECHO**

**“HOMOLOGACIÓN DE LOS CERTIFICADOS  
DIGITALES PARA LA FIRMA ELECTRÓNICA  
AVANZADA”**

**T E S I S**

**QUE PARA OBTENER EL TÍTULO DE:  
LICENCIADO EN DERECHO**

**PRESENTA:**

**VÍCTOR HUGO VALDEZ ROJAS**

**ASESOR:**

**LIC. MARÍA DEL ROSARIO RAMÍREZ CASTRO**

**MÉXICO, D.F**

**2010**



Universidad Nacional  
Autónoma de México



**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

**Gracias...**

**...a Dios**

*“Por permitirme llegar hasta este momento tan importante en mi vida y lograr otra meta más en mi carrera, por estar conmigo en cada paso que doy, por fortalecer mi corazón e iluminar mi mente y por haber puesto en mi camino a aquellas personas que han sido mi soporte y compañía.”*

**...a mis padres Yolanda y Víctor**

*“Por su amor, comprensión y apoyo sin condición ni medida en momentos buenos y no tan buenos. Gracias por guiarme sobre el camino de la educación. Creo ahora entender porque me obligaban a terminar mi tarea antes de salir a jugar, y muchas cosas más que no terminaría de mencionar. Me han enseñado a encarar las adversidades con determinación. Me han dado todo lo que soy como persona, mis valores, mis principios, mi perseverancia y mi empeño, y todo ello con una gran dosis de amor y sin pedir nunca nada a cambio.*

*A aquella incansable mujer que desde que era pequeño me ha cuidado, guiado y acompañado en los momentos en que más la he necesitado. Por su apoyo, por su incondicionalidad de madre y principalmente por su amor.”*

**...a esa persona especial**

*“Por el cariño, apoyo, comprensión y amor que me das y me permite sentir poder lograr lo que me proponga. Gracias por escucharme y darme tus consejos (eso es algo que haces muy bien). Gracias por ser parte de mi vida; y permitirme ser parte de tu vida; eres lo mejor que me ha pasado. Por ser tal y como eres.”*

**...a mi hermano Diego**

*“Por tu ayuda, tus comentarios, sugerencias, opiniones y regaños. Además de ser un buen amigo eres la mejor compañía para compartir el mismo techo. Espero ser un buen ejemplo. No olvides nunca que estoy orgulloso de ti y que siempre vas a contar conmigo.”*

**...a mi hermano Víctor**

*“Por los momentos agradables que convivimos junto con toda tu familia, por que siempre abriste las puertas de tu casa para tus hermanos menores. Por que la vida no ha sido fácil y sin embargo estamos juntos y somos una familia.”*

**...a mis amigos**

*“Que estuvieron conmigo y compartimos aventuras, experiencias, desveladas y buenos reves. Gracias a cada uno por hacer que mi paso por la Universidad haya sido agradable. No voy a olvidar sus consejos y ayuda durante el lapso de la carrera.”*

**...a Mí, por supuesto**

*“Por que me considero un hombre decidido, ambicioso, determinado, perseverante, buena onda, buen amigo, buen hijo, buen hermano y buen novio. Por que siempre encuentro la forma de salir adelante y aun en los momentos difíciles me levanto, miro al frente y sigo caminando.”*

*“El destino no existe; es nuestro futuro vuelto presente el cual vamos creando con nuestras decisiones y del cual somos dueños; podemos modificarlo en cualquier momento”*

**Hugo The Kid**

# **“HOMOLOGACIÓN DE LOS CERTIFICADOS DIGITALES PARA LA FIRMA ELECTRÓNICA AVANZADA”**

## **ÍNDICE**

### **INTRODUCCIÓN**

#### **CAPÍTULO I**

##### **EL COMERCIO ELECTRÓNICO 1**

- 1.1 Comercio 1
- 1.2 Actos jurídicos 8

#### **CAPÍTULO II**

##### **SEGURIDAD EN EL COMERCIO ELECTRÓNICO 25**

- 2.1 Importancia de la seguridad en el Comercio Electrónico 25
- 2.2 Figuras que participan en la emisión de Certificados Digitales 32
  - 2.2.1 Agencia Registradora Central 35
  - 2.2.2 Agencia Registradora y Certificadora 36
  - 2.2.3 Agente Certificador 37
  - 2.2.4 Titular de Certificado Digital 38
- 2.3 Certificado Digital 39
- 2.4 Firma 54
  - 2.4.1 Firma autógrafa 55
  - 2.4.2 Firma electrónica avanzada (FEA) 56
- 2.5 Diferencias y Ventajas de la FEA 57
- 2.6 Diferencias entre el certificado digital y la firma electrónica avanzada 58
- 2.7 Efectos jurídicos de la Firma Electrónica Avanzada 59

#### **CAPÍTULO III**

##### **REGULACIÓN DEL COMERCIO ELECTRÓNICO 70**

- 3.1 Reformas en el Código Civil Federal 71

3.2	Reformas en el Código de Procedimientos Civiles	74
3.3	Reformas en el Código de Comercio	76
3.4	Reformas en otras legislaciones	78

## **CAPÍTULO IV**

	<b>HOMOLOGACIÓN DE LOS DISTINTOS CERTIFICADOS DIGITALES</b>	<b>85</b>
4.1	El uso del certificado digital y firma electrónica avanzada	88
4.2	Beneficios de la homologación de los diversos certificados digitales	97

## **CONCLUSIÓN**

## **BIBLIOGRAFÍA**

## INTRODUCCIÓN

Hablar de Comercio Electrónico aun no es común entre los comerciantes o personas que, por la celebración de actos jurídicos, forman parte del comercio; sin embargo, es una modalidad que conforme pasa el tiempo, va cobrando fuerza y reclama un lugar dentro de los negocios mercantiles.

Para la existencia del comercio electrónico, no sólo es necesario contar con equipo tecnológico y programas computacionales que faciliten este fin, ya que además es necesario garantizar a las partes que intervienen, la seguridad de que la información que envían y reciben se transfiere de modo seguro; de tal forma que nadie pueda interceptar los datos que en ocasiones son de carácter confidencial y hacer mal uso de esa información. Además, no basta con tener la certeza de que la información no es interceptada, sino que esa información está íntegra, es decir, que no fue modificada durante el envío y recepción, y en consecuencia que no está inalterada, ni por el emisor, ni el receptor o por una tercera persona que maliciosamente quisiera modificar la información. En el comercio tradicional, ambas partes comparecen a determinado lugar personalmente, por lo que se conocen físicamente, a diferencia del comercio electrónico, en donde una persona puede estar en sus oficinas en algún lugar de la Ciudad de México y la otra parte en sus oficinas en otro lugar de cualquier ciudad, siendo que se proponen firmar un contrato de compraventa; en este sentido, en donde las partes no se conocen físicamente o no tienen la certeza de que las partes son quien dicen ser, de algún modo deben tener la seguridad de que quien envía y recibe la información es quien dice ser, así como quien firma el contrato es con la persona que se está contratando; aunado a las características antes señaladas, también sabemos que la información que se envió, se recibió, se firmó y se regresó, está íntegra y ninguna de las partes alteró el contenido. Finalmente, adicionando la confidencialidad a las características antes mencionadas, es decir, garantizando que la información enviada sólo puede ser vista por la persona a la que fue enviada, mediante el uso de claves, tenemos que el comercio electrónico, es más seguro que el comercio tradicional.

A diferencia del comercio tradicional, que se presta a la falsificación de documentos, falsificación de firmas, alteración en el contenido de los contratos, robo

de información confidencial o privilegiada y que en un juicio el medio de prueba idóneo es mediante peritos especializados en grafoscopía y documentoscopia, y que el estudio de dichos casos puede llevarse un lapso de tiempo considerable, si tomamos en cuenta que en general se recurre al perito tercero en discordia y que está latente el error humano, tenemos como consecuencia un proceso largo y con un riesgo de error.

Para el comercio electrónico, en cambio, existe una herramienta que lo hace seguro; además, para el caso de prueba en juicio, es un medio totalmente seguro y rápido. Esto se debe al uso de un archivo llamado certificado digital y otro llamado llave privada, lo que en conjunto garantizan que una información enviada y recibida goza de las características de integridad, confidencialidad, no repudiación y auténtico. El funcionamiento de estos archivos en los documentos, dota de seguridad para el intercambio y transferencia de información sin ningún riesgo. Aunado a ello, tenemos que con estos archivos se crea la Firma Electrónica Avanzada, la cual se inserta en los documentos que requieren ser firmados, para manifestar la voluntad de obligarse a lo que está establecido en el contenido del documento, siendo que la firma le da el valor legal probatorio en un juicio.

Esto es posible toda vez que la legislación le otorga por equivalencia funcional, los mismos efectos jurídicos a la firma autógrafa y a la firma electrónica avanzada o digital, siempre y cuando se reúnan los requisitos que la misma ley establece para garantizar que dicha firma proviene de una persona determinada y, en consecuencia, puede ser vinculado el documento firmado con la identidad del firmante.

La Firma Electrónica Avanzada, generada a partir del Certificado Digital, tiene ventajas sobre la firma autógrafa, como los que se mencionaron en el párrafo que antecede. Con estas características tenemos varios factores que contribuyen a garantizar un comercio electrónico seguro para el intercambio de información, documentos y transferencias electrónicas, entre personas tanto físicas como morales, sin importar el lugar en donde se ubican físicamente las partes que intervienen.

Otra ventaja del comercio electrónico, es la reducción de costos y la contribución a una cultura ecológica al reducir el uso de papel. Esto es, si consideramos que en general se elabora un documento en una computadora, se imprimen, por lo menos dos juegos del mismo documento, la empresa de mensajería debe documentar lo que recibe y lo que envía, lo cual representa también un costo, que hay que capturar la información en una base de datos, luego se debe enviar el documento vía terrestre o vía aérea, según el destino que tenga, para finalmente llegar al destinatario, quien firma el acuse y realiza el mismo procedimiento para devolver dicho documento que avala que recibió los documentos. Como se puede observar, el gasto es significativo, sobre todo si se trata de un documento que pudo enviarse electrónicamente, ya que las empresas destinan recursos económicos y humanos para realizar estos procesos que pueden simplificarse y reducir tiempos, ya que en el ejemplo anterior, por lo menos la entrega de un documento puede tardar dos días en el mejor de los casos.

Lo mismo puede suceder con cualquier información. Sabemos que se trata de información sensible o personal, que aun y cuando se envía por mensajería con la consigna de carácter confidencial, esa información puede ser robada, extraviada o incluso alterada, lo que pone en riesgo al dueño de esos datos, y pudiendo generar problemas graves tanto a las personas, empresas, instituciones, etcétera. Ahora, si tomamos en cuenta que mediante el uso de certificados digitales, con los que las personas físicas o morales pueden firmar electrónicamente cualquier mensaje de datos e información y que tiene los mismos efectos que la firma autógrafa, y que con esos mismos certificados digitales se puede cifrar esa información firmada con el objeto de que sólo el destinatario pueda conocer el contenido de el mensaje firmado, se logra eliminar cualquier riesgo en el envío, la recepción y autenticación de la información. Esto es, un hospital, un banco o una empresa, integra la información de manera electrónica y también firma electrónicamente, de tal forma que le da validez a la información que se envía, cifra dicha información, descomponiéndola con la ayuda de la tecnología computacional, en datos que sólo se pueden volver a formar la información inicial por la persona designada por el emisor como único receptor de la información; así aun y cuando el archivo electrónico caiga en manos de otra persona, ésta no podrá conocer el contenido, lo que es igual a no tener nada de información. Además, tenemos que en

el envío de información y recepción de la misma por el destinatario, el tiempo estimado que transcurre es el mismo que tarda un correo electrónico en llegar a la dirección de correo que se envía, es decir, en funcionamiento normal del Internet, no más de 5 minutos.

Podemos ver que se puede enviar cualquier información, ya sea confidencial o no, de manera segura y rápida, pero la finalidad real de los certificados digitales es dotar con validez esa información enviada. Para esto mencionaremos brevemente que es un certificado digital, pues es materia de estudio del presente trabajo.

El certificado digital es un archivo generado por una persona, contiene información propia como nombre, domicilio, número de certificado entre otros datos. Este archivo se genera por medio de una autoridad certificadora, autorizada por una autoridad Central, que en México puede ser: la Secretaría de Economía, Banco de México o la Secretaría de la Función Pública. Junto con el certificado digital se crea otro archivo que tiene un vínculo con el certificado y se denomina llave privada, por lo que existen dos archivos electrónicos por persona. Para firmar un documento sólo debe aplicarse el certificado digital y la llave pública, lo que da como resultado una firma electrónica avanzada, que combina un resumen de la información contenida en el documento, datos de la llave pública y datos del certificado, con lo que sabemos quién creó el documento, cuándo lo firmó y que manifiesta su consentimiento en lo ahí estipulado, es decir, los mismos efectos que la firma autógrafa, pues la ley le confiere a la firma autógrafa y a la firma electrónica la misma validez jurídica.

Con respecto al archivo, denominado llave privada, sirve además para cifrar la información firmada electrónicamente; así, el certificado es una llave pública, es decir, es del conocimiento de toda la gente no así con la llave privada, pues como su nombre lo indica, es de conocimiento exclusivo del poseedor del certificado. Una vez integrada la información firmada, el emisor, aplica la llave pública o certificado del destinatario, lo que descompone el contenido de la información en datos indescifrables para cualquier persona, excepto para quien posee la llave privada del certificado con que se cifró la información, por ejemplo: Víctor firma un contrato con su certificado y su llave privada, lo que le da validez jurídica y manifiesta el

consentimiento de Víctor para obligarse en los términos indicados en el contrato; posteriormente aplica el certificado digital de Alicia, que es la destinataria de dicho contrato, cifrando la información en datos que no podrán ser vistos por ninguna persona a excepción de Alicia, que una vez aplicada su llave privada, la cual se vincula con el certificado aplicado por el emisor, la información se descifra y puede ser leída, con la seguridad de que nadie más tuvo acceso al contenido del documento.

El objeto principal de este estudio es la homologación de los mencionados certificados digitales, pues los tres certificados digitales generados por las tres autoridades centrales en México, tienen las mismas características de seguridad y finalidad, que es sustituir a la firma autógrafa, es decir, tienen las mismas características técnicas; sin embargo, legalmente no tienen el mismo reconocimiento, ya que el código de comercio reconoce el certificado digital generado por la Secretaría de Economía, a través de una autoridad autorizada por esta dependencia, a su vez, el Banco de México reconoce el Certificado Digital emitido por el SAT o una autoridad certificadora autorizada por esta institución y, la Función Pública reconoce los certificados generados por la misma secretaría de la Función Pública.

México, Distrito Federal, 2010.

## **CAPÍTULO I**

### **EL COMERCIO ELECTRÓNICO**

#### **1.1. Comercio**

En términos generales, el comercio implica la investigación de mercado con el fin de interpretar los deseos del consumidor; sin embargo, con el transcurso del tiempo han surgido diferentes formas o tipos de comercio. Alrededor del año 1970, aparecieron las primeras relaciones comerciales que utilizaban una computadora para transmitir datos. Este tipo de intercambio de información, provocó mejoras en los procesos de fabricación en el ámbito privado, entre empresas de un mismo sector. Es por eso que se trataron de fijar estándares para realizar este intercambio, el cual era distinto con relación a cada industria.

La implementación de este intercambio de información produjo importantes beneficios, ya que se eliminaron gran parte de errores de entregas de productos por parte de las empresas o fábricas y se redujeron los tiempos de procesamiento de dichas órdenes. Por otra parte, en el sector público, el uso de estas tecnologías para el intercambio de datos tuvo su origen en las actividades militares.

A través de este proyecto se logró estandarizar las comunicaciones entre computadoras y alrededor de el año 1980 aparece un nuevo servicio, la www (World Wide Web, Telaraña Global), cuando un grupo de investigadores en Ginebra, Suiza, ideó un método a través de la tecnología denominada Internet, enlazando documentos científicos provenientes de diferentes computadoras, a los que podían integrarse recursos multimedia (texto, gráficos, música, entre otros).

Lo sobresaliente de la “www” es su alto nivel de accesibilidad, que se traduce en los escasos conocimientos de informática que exige de sus usuarios. El desarrollo de esta tecnología, junto con las telecomunicaciones, ha producido que los intercambios de información avancen, simplificándose cada vez más y creando nuevas formas de comercio; y es en este marco que se desarrolla el Comercio Electrónico. Así, el comercio electrónico primero vino del desarrollo del intercambio electrónico de datos.<sup>1</sup>

En el año 1995, los dos nombres más grandes en el comercio electrónico fueron lanzados: Amazon.com y eBay.com.there. Son varios objetivos en la historia del comercio electrónico y se han convertido en una industria de miles de millones de dólares.

Hoy el comercio electrónico más grande es el b2b, realizando ventas de sus bienes a otro negocio, entre colegas, es otra forma del comercio electrónico que permite que los usuarios compartan recursos y archivos directamente.<sup>2</sup>

Podemos determinar como definiciones apropiadas para el comercio electrónico las siguientes, en virtud de que dicho término es susceptible a ser interpretado de distintas formas; sin embargo, todas las definiciones se centran en una idea común: el uso de la tecnología o medios electrónicos con el propósito de comerciar:

1. “Es la aplicación de la avanzada tecnología de información para incrementar la eficacia de las relaciones empresariales entre socios comerciales”. (Automotive Action Group in North America)<sup>3</sup>

---

<sup>1</sup> <http://promkusok07.wordpress.com/2007/11/19/origen-e-historia/>

<sup>2</sup> <http://www.ligaturesoft.com/spanish/e-commerce-development/Historia-de-Comercio-electronico.html>

<sup>3</sup> <http://opas.espacioblog.com/categoria/comercio-electronico>

2. “La disponibilidad de una visión empresarial apoyada por la avanzada tecnología de información para mejorar la eficiencia y eficacia dentro del proceso comercial”. (EC Innovation Centre)<sup>4</sup>
3. “Es el uso de las tecnologías computacional y de telecomunicaciones que se realiza entre empresas o bien entre vendedores y compradores, para apoyar el comercio de bienes y servicios”.<sup>5</sup>

El comercio electrónico puede clasificarse en cuatro categorías dependiendo de las partes que intervienen, en donde dicha clasificación se realiza no por el número de participantes, sino por llamarlo de alguna manera el carácter de la persona, pudiendo ser persona física, persona moral o la administración pública.

- a) **Compañía – Compañía.** Se refiere a una compañía que hace uso de una red para hacer órdenes de compra a sus proveedores, recibir facturas y realizar los pagos correspondientes.
- b) **Compañía – Cliente.** Se puede comparar con la venta al detalle de manera electrónica.
- c) **Compañía – Administración.** Se refiere a todas las transacciones llevadas a cabo entre la compañía y las diferentes organizaciones de gobierno.
- d) **Cliente – Administración.** Aún no ha nacido, sin embargo después del nacimiento de las categorías compañía – cliente y compañía – administración, el gobierno hará una extensión para efectuar interacciones electrónicas como pagos de asistencia social y regreso de pagos de impuestos.

---

<sup>4</sup> <http://opas.espacioblog.com/categoria/comercio-electronico>

<sup>5</sup> <http://opas.espacioblog.com/categoria/comercio-electronico>

Además, el comercio electrónico utiliza un amplio rango de tecnologías como son:

- Intercambio electrónico de datos (EDI-Electronic Data Interchange).
- Correo Electrónico (E-mail o Electronic mail).
- Transferencia electrónica de fondos (EFT- Electronic Funds Transfer).
- Aplicaciones Internet: Web, News, Gopher, Archie.
- Aplicaciones de voz: Buzones, servidores.
- Transferencia de archivos.
- Diseño y fabricación por computadora (CAD/CAM).
- Multimedia.
- Tableros electrónicos de publicidad.
- Videoconferencia.

Algunas de las consecuencias, a causa del desarrollo del comercio electrónico; son las siguientes:

- a) Empresas virtuales.** Es la oportunidad para utilizar socios comerciales externos sin una ubicación física, pues se establece una relación basada en transacciones electrónicas.
- b) Los vendedores pequeños acceden al mercado global.** Tradicionalmente estos mercados que sólo han estado abiertos para las multinacionales, se vuelven accesibles a las compañías más pequeñas,

debido a la escasa cantidad de recursos necesarios para funcionar en el extranjero.

**c) Transformación de tiendas de venta al menudeo.** El crecimiento de las compras desde el hogar y de la venta directa por parte de los fabricantes, provocará una disminución de los precios y, en consecuencia, una reducción de las comisiones.

**d) Presión sobre el servicio al cliente, el ciclo de desarrollo y los costos.** Aumentará la necesidad de la entrega rápida y directa. La cadena de valor será cada vez menos tolerante con la necesidad de inventarios y almacenamiento. Será inevitable el crecimiento de la competencia, así como de la necesidad de dinero electrónico.<sup>6</sup>

El comercio electrónico, al igual que el comercio tradicional está sujeto a riesgos, pues como bien sabemos, el comercio gira alrededor de la confianza y la buena fe, que, aun y cuando se tomen las medidas necesarias para hacer seguros los actos de comercio, siempre está latente el incumplimiento de alguna de las partes o el intento de fraude de alguno de los participantes, sin embargo; el comercio electrónico es mas seguro que el comercio tradicional, ya de que aporta candados que hacen posible incrementar la seguridad.

- Entorno empresarial y tecnológico cambiante.
- Privacidad y seguridad.
- Cuestiones legales, políticas y sociales.

El comercio electrónico es básicamente el uso de redes (Internet) para realizar la totalidad de actividades involucradas en la gestión de negocios: ofrecer y demandar productos y servicios, buscar socios y tecnologías, hacer negociaciones con su contraparte, seleccionar el transporte y los seguros que

---

<sup>6</sup> <http://www.monografias.com/trabajos12/monogrr/monogrr.shtml> 2009

más convengan, realizar los trámites bancarios, pagar, cobrar, comunicarse con los vendedores de su empresa, recoger los pedidos, es decir, todas aquellas operaciones que requiere comercio.

Hacer comercio, electrónico significa la posibilidad de establecer una línea de comercio establecer y realizar a través de medios electrónicos toda una conducta mercantil que incluye ofertas, pedidos, negociaciones; en general, todo lo que es usual en el comportamiento de la vida mercantil, incluyendo todos los problemas legales que conllevan en el entorno ajeno a lo electrónico las transacciones de negocios.

En México no existen leyes que protejan a clientes y usuarios para efectuar operaciones mediante comercio electrónico.

Hasta el momento varias organizaciones privadas se han dado a la tarea de trabajar en materia legal, a fin de presentar iniciativas de leyes claras y específicas sobre este tema. Existe consenso por parte de estos grupos, quienes afirman que la falta de leyes inhibe el desarrollo y evolución de la red en materia de negocios. La regulación del comercio por Internet no es fácil de hacer. Hay muchos intereses en juego, sobre todo porque implica formas nuevas de hacer negocios.

Sin embargo, la regulación del comercio por Internet no es fácil de hacer, en parte porque hay muchos intereses de por medio. Lo más cercano a una ley, que puede encontrarse para legislar dentro de los dominios del comercio electrónico, es la ley de Derechos de Autor y dentro de sus parámetros considera al Internet únicamente como una base de datos, esto de acuerdo con especialistas como abogados en Derecho, licenciados en administración de empresas, ingenieros en informática y ejecutivos; tal denominación no refleja los avances que en la red o supercarretera de la información ha alcanzado en los últimos años, razón por la cual en nuestro país la utilización de Internet, mediante comercio electrónico, no ha madurado en los negocios como se esperaba.

Diversas asociaciones como la Asociación Nacional de Abogados de Empresa (ANADE), la Asociación Mexicana de la Industria de Tecnologías de Información (AMITI) y la Cámara Nacional de la Industria Electrónica e Informática (Canieti), que representan al sector público, de telecomunicaciones e informática, coinciden en que el avance en materia legal es prioritario para establecer la adecuación de normas legales, que regulen y garanticen la seguridad en las transacciones comerciales.

Hasta el momento varias organizaciones privadas se han dado a la tarea de trabajar en materia legal a fin de presentar iniciativas de ley claras y específicas sobre este tema.

Entre las principales adecuaciones al Código de Comercio, se encuentran el reconocimiento de uso de medios electrónicos para la realización de transacciones involucrando cuestiones de ejecución y regulación de actos mercantiles, validez de los datos transmitidos así como los medios utilizados para tal efecto. Asimismo, la aprobación también implica alteraciones directas al Código Civil del Distrito Federal y al Código de Procedimientos Civiles, en relación con aspectos nacionales e internacionales. Cabe mencionar que para el desarrollo y presentación de la iniciativa, participaron el grupo Impulsor de la Legislación del Comercio Electrónico (GILCE), la Asociación de Banqueros de México (ABM), la Asociación Mexicana de la Industria de Tecnologías de la Información (AMITI), la Asociación Nacional del Notariado Mexicano y la Cámara Nacional de la Industria Electrónica e Informática (CANIETI).

Hay muchas cosas sobre las cuales tendremos que reflexionar para cambiar procesos y normas legales, pero sobre todo, para los abogados, éste estallido de tecnología representa un cambio de normalidad; siendo que aceptar la electrónica nos hace sentir inseguros ante la novedad.

Tanto los abogados como todos los involucrados en estos asuntos deben empezar a trabajar con registros electrónicos, documentos electrónicos, cibernotarios, firmas digitales, facturas electrónicas, así como con obligaciones

electrónicas y empezar a sustituir los títulos de créditos y los expedientes cosidos pues son cosas del pasado.

Habrán enfrentamientos hacia nuevas reglas administrativas, nuevos tipos delictivos y nuevos modos de incumplimiento de obligaciones.

## **1.2. ACTOS JURÍDICOS**

El comercio electrónico es el resultado de la realización de actos jurídicos que emana de personas físicas o personas morales, pues se producen con la finalidad de crear derechos y obligaciones; por ello, en principio determinaremos qué es un acto jurídico.<sup>7</sup>

El acto jurídico es la manifestación de la voluntad para ser sujeto de obligaciones y derechos, en donde una persona se obliga a dar, hacer o no hacer y, en consecuencia, la otra parte se obliga de igual forma a dar, hacer o no hacer.<sup>8</sup>

Es importante diferenciar al acto jurídico del hecho jurídico, pues si bien es cierto que ambos producen consecuencias de derecho, es decir, derechos y obligaciones, también lo es que en el acto jurídico existe esa voluntad de hacerse acreedor de dichas consecuencias y obligarse con la otra parte, mientras que en los hechos jurídicos no existe la voluntad, por lo que ninguna de las partes tuvo la intención de crear ese vínculo jurídico, en otras palabras, el acto jurídico se caracteriza por la voluntad de la persona para obligarse, mientras que el hecho jurídico es involuntario, producto de un acontecimiento no esperado, en donde a pesar de que se conocen las consecuencias, no es intención producirlas. Como ejemplo del acto jurídico tenemos la compraventa, en donde una persona manifiesta su voluntad de vender un bien o un servicio y otra persona manifiesta

---

<sup>7</sup> Gutiérrez y González Ernesto. Derecho de las obligaciones. Ed. Porrúa Edición séptima. México DF pág. 102-175

<sup>8</sup> <http://www.monografias.com/trabajos34/teoria-de-obligaciones/teoria-de-obligaciones.shtml> 2009

su voluntad de adquirir dicho bien o servicio. A diferencia, el hecho jurídico lo podemos ejemplificar como: dañar una propiedad ajena de manera accidental, al estacionar un donde vehículo, se golpea accidentalmente al vehiculo de enfrente; en ese momento se produce un hecho jurídico, pues se crea un vínculo jurídico entre ambos propietarios, en donde una persona tiene que pagar a la otra la afectación causada a un vehículo; en este ejemplo podemos observar que aun y cuando se conoce que al impactar un vehículo con otro se produce un daño, no se tiene la intención de producir ese daño; desencadenándose una obligación de reparar el daño.

El acto jurídico y el hecho jurídico son similares respecto a que producen consecuencias de derecho; no obstante la diferencia entre ambos, radica en la voluntad de producir dichas consecuencias de derecho, en virtud de que este último es generado de manera accidental, por caso fortuito o fuerza mayor.

El acto jurídico es el acto humano voluntario o consciente, que tiene por fin inmediato establecer entre las personas relaciones jurídicas, crear, modificar o extinguir derechos. El acto jurídico produce una modificación en las cosas o en el mundo exterior porque así lo ha dispuesto el ordenamiento jurídico<sup>9</sup>.

El acto jurídico es considerado como la manifestación de la voluntad humana susceptible de producir efectos jurídicos. Para que esta manifestación de la voluntad produzca efectos jurídicos, es preciso que se realice de acuerdo con los requisitos legales, previamente establecidos para cada caso.

El acto jurídico se compone de diversos elementos que se relacionan intrínsecamente de tal forma, que para la existencia del acto se deben reunir ciertos requisitos determinados por la ley, de modo que a falta de uno de ellos, cabe la posibilidad que se produzca una inexistencia o una nulidad,

---

<sup>9</sup> Enciclopedia Wikipedia, ([http://es.wikipedia.org/wiki/Acto\\_jur%C3%ADdico](http://es.wikipedia.org/wiki/Acto_jur%C3%ADdico) Fecha de consulta, enero de 2009)

extinguendo el vínculo jurídico y, en consecuencia, los efectos jurídicos o en ciertos casos modificando dichos efectos.

Para tener una idea más clara, el acto jurídico se compone de elementos necesarios para su existencia, en el sentido de que si uno de estos elementos no se reúne puede generar una afectación, misma que puede producir desde la nulidad del acto en sus dos aspectos: relativa o absoluta, hasta la inexistencia, y por consiguiente modificando los efectos jurídicos o extinguendo dichos efectos en su totalidad.

Los elementos que componen el acto jurídico son los siguientes:

<b>ACTO JURÍDICO</b>	<b>ELEMENTOS ESENCIALES, EXISTENCIA.</b>
	<ul style="list-style-type: none"><li>• Consentimiento.</li><li>• Objeto.</li><li>• Solemnidad</li></ul>
	<b>ELEMENTOS DE VALIDEZ.</b>
	<ul style="list-style-type: none"><li>• Capacidad.</li><li>• Ausencia de vicios.</li><li>• Objeto y causas lícitos.</li><li>• Forma.</li></ul>

**Cuadro 1. Elementos de que se compone el Acto Jurídico<sup>10</sup>**

Antes de revisar los elementos que conforman al acto jurídico, es relevante distinguir entre la inexistencia del acto jurídico y la nulidad ya sea absoluta o relativa del acto jurídico.

Cabe señalar que la inexistencia se produce por la falta de un elemento esencial en el acto jurídico, lo que provoca que los efectos jurídicos no se produzcan y, en consecuencia, las cosas vuelven al estado en que se encontraban. El artículo 2224 del Código Civil para el Distrito Federal, determina que un acto inexistente no produce efectos legales. En un contrato que no se firma y, en consecuencia, no se expresa el consentimiento, no se producen consecuencias jurídicas.

---

<sup>10</sup> Víctor Hugo Valdez Rojas

La nulidad es absoluta cuando no se reúnen los elementos de validez y aunado a esto no es posible subsanar la deficiencia. Esta nulidad genera efectos legales provisionalmente, hasta en tanto no exista una declaración judicial que la declare para anular los efectos legales producidos; tal es el caso de la existencia de un vicio en el consentimiento, donde en la celebración de una compraventa existe violencia, siendo que el acto jurídico y sus consecuencias prevalecen, hasta en tanto la parte afectada lo denuncie y la autoridad lo determine. Por consiguiente, la nulidad relativa surge cuando falta un elemento de validez; sin embargo, es susceptible de ser subsanado y, en consecuencia, producir efectos jurídicos, como sucedería en un contrato que se realiza verbal entre las partes pero la ley establece su formalidad escrita; así el acto existe y las consecuencias jurídicas subsisten y puede ser subsanado en cualquier momento cumpliendo con dicha formalidad, firmando un contrato sin que implique una afectación en el acto en sí.

Los elementos de que se compone el acto jurídico podemos dividirlos en dos grandes rubros: elementos esenciales y elementos de validez, en donde los primeros, tal y como su nombre lo indica, son fundamentales para que el acto jurídico se considere legalmente existente y debe reunir los tres elementos que lo conforman sin excepción alguna; en cuanto a los segundos, es decir, los elementos de validez son fundamentales para que el acto jurídico produzca efectos legales plenos, aunque a diferencia de los elementos esenciales, el acto jurídico subsiste hasta en tanto no se subsane el elemento de validez afectado, ya que de lo contrario se genera una nulidad en sus dos rubros: relativa o absoluta.

Así para que el acto jurídico exista debe contener el consentimiento de las partes, el cual es la manifestación de la voluntad para ser sujeto de derechos y obligaciones por cada una de las partes, en la creación de un vínculo jurídico, con lo cual se pretenden crear y aceptar las consecuencias que de ahí se deriven.

Respecto a este elemento fundamental en los actos jurídicos, la ley dentro del Código Civil para el Distrito Federal, en su artículo 1803, refiere que puede ser expreso o tácito:

**“Artículo 1803.** El consentimiento puede ser expreso o tácito. Es expreso cuando se manifiesta verbalmente, por escrito o por signos inequívocos. El tácito resultará de hechos o de actos que lo presupongan o que autoricen a presumirlos, excepto en los casos en que por ley o por convenio la voluntad deba manifestarse expresamente.”<sup>11</sup>

El consentimiento es expreso cuando la persona lo exterioriza de manera verbal, por escrito o con la realización de una acción que da por hecho que acepta las consecuencias de derecho, como por ejemplo: la manera verbal se da frecuentemente en la compraventa, donde una persona le oferta a otra un bien y ésta, de manera verbal, le indica que acepta comprar dicho objeto. En cuanto a la aceptación por escrito, es muy común a través del correo electrónico, donde una parte puede ofertar un bien o un servicio, enviando su cotización o presupuesto a la otra parte vía correo electrónico y la parte interesada responde por el mismo medio su aceptación o rechazo, es decir, es claro este consentimiento, pues la aceptación consta en documento por escrito, mismo que no forzosamente debe ser de puño y letra produciendo efectos jurídicos para las partes. Cuando la ley menciona signos inequívocos, se refiere a actos realizados por una persona, que sin necesidad de manifestar textualmente su aceptación se entiende que acepta la relación jurídica creada; un ejemplo de este tipo de consentimiento, el cual cabe señalar que es relevante para lo que será el objeto de este trabajo es la firma de un contrato, en el entendido de que no es necesario que las partes expresen verbalmente su aceptación, pues resulta obvio señalar que al momento en que se firma el contrato, se están contrayendo y aceptando derechos y obligaciones; el mismo tipo de consentimiento podemos ejemplificarlo en una compraventa, en donde el comprador no necesita expresar su aceptación de manera verbal y de igual forma no requiere firmar ningún contrato, pues basta con efectuar el pago de la cosa, para dar a entender que, aun y cuando no exteriorizó su consentimiento verbalmente o por escrito, al momento de dar la contraprestación expresó su aceptación,<sup>12</sup>

---

<sup>11</sup> <http://www.ordenjuridico.gob.mx/Estatal/DISTRITO%20FEDERAL/Codigos/DFCOD01.pdf>, 2009

<sup>12</sup> Gutiérrez y González Ernesto. Derecho de las obligaciones. Ed. Porrúa Edición séptima. México DF pág. 195-304

En el último ejemplo del párrafo anterior, respecto a la manifestación del consentimiento por medio de signos inequívocos, se realizó un énfasis, pues la parte medular de este estudio es el comercio electrónico, donde las partes no se encuentran presentes físicamente, donde no se ven ni se escuchan y muy probablemente, en numerosos casos, no llegan a conocerse directamente; sin embargo, en la actualidad esto no es ningún impedimento para realizar cualquier tipo de negocios, mismos que llevan intrínsecos actos jurídicos. De esta manera, para la realización de un acto jurídico se puede manifestar el consentimiento por medio de signos o actos que no dan lugar a duda esa aceptación, siendo entonces que en el comercio electrónico en donde la partes que intervienen en el acto jurídico no se encuentran presentes físicamente y en por consiguiente no existe una comunicación verbal, la aceptación de los efectos legales y la expresión de la voluntad se exterioriza por medio de la firma electrónica, la cual tiene la característica de vincular a la firma con el firmante, aun y cuando no se conocen directamente, y para el caso del consentimiento, al momento en que se firma electrónicamente, se entiende que se aceptan las consecuencias de derecho emanadas del acto celebrado.

El consentimiento tácito, se refiere a la realización de hechos o actos, incluso la omisión de hacer algo para dar a entender que se aceptan las consecuencias generadas por el acto jurídico. Es común establecer en los contratos una cláusula que se refiere a la renovación del mismo, en el cual se establece que para la renovación del contrato será renovado tácita y automáticamente por determinados periodos de tiempo, lo cual se traduce en que si las partes no manifiestan su deseo de terminar la relación jurídica que los une, se entiende por renovado automáticamente sin necesidad de firmar otro contrato, como por ejemplo, el arrendamiento de una propiedad por un año, al término de la vigencia del contrato. Es decir, a diferencia del consentimiento expreso en donde la peculiaridad es la manifestación verbal, escrita o por medio de acciones inequívocas, ésta si da lugar a duda, sin embargo se entiende que al no oponerse a las consecuencias de derecho se tienen por aceptadas, a excepción de las que la ley indica que no procede el consentimiento tácito.<sup>13</sup>

---

<sup>13</sup> Gutiérrez y González Ernesto. Derecho de las obligaciones. Ed. Porrúa Edición séptima. México DF pág. 195-304

Otro elemento de el acto jurídico es el objeto, el cual implica el vínculo entre las partes, es decir, es el nexo entre las personas que intervienen y consiste en un dar, hacer o no hacer. En este sentido, no debemos confundir el objeto como elemento esencial o de existencia que se refiere a la acción, al dar, hacer o no hacer y no al objeto como un elemento de validez

La solemnidad en los actos jurídicos es la forma, es decir, requisitos que establece la ley para llevar a cabo un acto jurídico, en el entendido que, si la ley establece que debe ser por escrito, las partes deben cubrir ese requisito, plasmando en un documento la voluntad de las partes de someterse recíprocamente al cumplimiento de una obligación. Esta característica de los actos jurídicos se cumple dentro del comercio electrónico, con el resguardo de los documentos firmados electrónicamente, ya sea físicamente, en un disco (CD) una memoria extraíble, un disco duro, pues la ley establece como formalidad su forma escrita, sin que esto se traduzca en puño y letra de los que intervienen, siempre y cuando se reúna con elementos como la firma, el modo de exteriorizar la voluntad, misma que por medio de un certificado digital es insertada en dicho documento, de tal forma que forma parte del mismo y la cual puede ser vinculada con el firmante. Es importante mencionar de manera informativa que actualmente, de acuerdo a la Norma Oficial Mexicana 151 emitida por la Secretaría de Economía, cualquier documento puede ser migrada a una imagen digital y almacenada de tal forma que pueda ser consultada posteriormente, imagen que no implica la pérdida de efectos jurídicos, siempre y cuando esta migración se realice de acuerdo a lo establecido en el Código de Comercio.<sup>14</sup>

Por otra parte, respecto a los elementos de validez, estos son necesarios en el acto jurídico para que se generen los efectos legales plenamente, sin que la falta de alguno o algunos implique la inexistencia del acto en sí, es decir, el acto existe pero por llamarlo de alguna manera tiene un defecto, el cual puede y debe ser subsanado para que sea jurídicamente eficaz.

---

<sup>14</sup> Gutiérrez y González Ernesto. Derecho de las obligaciones. Ed. Porrúa Edición séptima. México DF pág. 260-261

Así, tenemos que la capacidad es la facultad de la o las personas para ser sujetos de derecho. El Código Civil para el Distrito Federal, nos refiere dos tipos de capacidad, la jurídica y la de ejercicio:

**“Artículo 22.** La capacidad jurídica de las personas físicas se adquiere por el nacimiento y se pierde por la muerte; pero desde el momento en que un individuo es concebido, entra bajo la protección de la ley y se le tiene por nacido para los efectos declarados en el presente Código.

**Artículo 23.-** La minoría de edad, el estado de interdicción y demás incapacidades establecidas por la ley, son restricciones a la capacidad de ejercicio que no significan menoscabo a la dignidad de la persona ni a la integridad de la familia; los incapaces pueden ejercitar sus derechos o contraer obligaciones por medio de sus representantes.

**Artículo 24.** El mayor de edad tiene la facultad de disponer libremente de su persona y de sus bienes, salvo las limitaciones que establece la ley.”<sup>15</sup>

Así, la capacidad jurídica, con fundamento en el artículo 22 de dicho ordenamiento, establece que la capacidad jurídica se adquiere con el nacimiento y se extingue con la muerte y consiste en la facultad de ser sujeto de derechos y obligaciones, tal es el caso de un menor de edad que tiene el derecho a recibir alimentos, derecho que es protegido por la ley.

Con respecto a la capacidad de ejercicio, tenemos que se adquiere con la mayoría de edad y consiste en la facultad de disponer libremente de su persona y de sus bienes, salvo las limitaciones que establece la ley.

En la capacidad de ejercicio, tenemos como restricción que los incapaces, aun y cuando son mayores de edad, no pueden disponer de sus bienes o de ellos mismos, limitando esta disposición a ser ejercida por un tutor quien será el responsable de salvaguardar los derechos de su representado.

---

<sup>15</sup> <http://www.ordenjuridico.gob.mx/Estatal/DISTRITO%20FEDERAL/Codigos/DFCOD01.pdf>. 2009

Como ejemplo de dicha capacidad, tenemos una compraventa, en donde una persona con la capacidad legal de ejercicio requerida dispone libremente de un inmueble y trasfiere la propiedad a otra persona; sin embargo, en el caso de que el vendedor fuese menor de edad, la compraventa existe, pues ambos manifiestan su consentimiento, el objeto es jurídica y físicamente posible y cumplen con la formalidad escrita, pero en este caso no se cumple con el elemento de validez de la capacidad jurídica, lo que provoca una nulidad relativa, pues puede subsanarse, ya sin que el menor espere a cumplir la mayoría de edad o que la firma del contrato la realice su representante para cumplir con dicho requerimiento y producir las consecuencias de derecho.

La capacidad que en este tratado nos ocupa es la de ejercicio, pues nos encontramos en el entendido de que los actos de comercio consisten en la disposición de bienes o la prestación de servicios.

La ausencia de vicios es otro elemento de validez, el cual implica la ausencia de dolo, mala fe, error o violencia en la realización de un acto jurídico ya que al existir alguno de estos supuestos, el consentimiento se ve afectado de manera que se genera una nulidad relativa o absoluta del acto.<sup>16</sup>

De acuerdo al Código Civil para el Distrito Federal, el error consiste en una falsa apreciación de la realidad, es decir, tener una perspectiva equivocada del acto en sí o del objeto materia del acto, como puede ser el contratar con una persona cuando en realidad es otra, o el arrendamiento de un inmueble cuando en realidad se trata de otro o la compraventa de un objeto que se presume cierta calidad, siendo inferior.<sup>17</sup> Se entiende como mala fe la disimulación del error, con la finalidad de que la otra parte no identifique el estado real del objeto, como por ejemplo: disimular la calidad de un objeto, presumiendo

---

<sup>16</sup> Gutiérrez y González Ernesto. Derecho de las obligaciones. Ed. Porrúa Edición séptima. México DF pág. 305

<sup>17</sup> Acosta Romero Miguel: Teoría general del acto jurídico y obligaciones, México, ed. Porrúa, año 2002

que se entrega en buenas condiciones, cuando en realidad esta en mal estado.<sup>18</sup> Por otra parte, el dolo consiste en acciones o artificios por parte de una parte para llevar o mantener en el error a la otra; por ejemplo: exagerar las cualidades de un objeto cuando en este no cumple con dichas características, acción que tiene como finalidad la realización del acto jurídico haciendo creer algo que en realidad no es.<sup>19</sup> Por último tenemos la violencia, que se traduce en emplear la fuerza externa física o psicológica como amenazar a una persona para donar parte de su patrimonio utilizando la fuerza física o psicológica.<sup>20</sup>

De los vicios antes mencionados, tenemos que si alguno de estos se presenta durante la celebración de un acto jurídico, dicho supuesto se traduce en una nulidad absoluta o relativa, pues de acuerdo al caso en concreto, ésta puede ser susceptible de ser subsanada y generar los efectos jurídicos, o bien, si no opera ese perfeccionamiento, una vez que la autoridad declare su nulidad absoluta, las cosas vuelven al estado en que se encontraban.

El objeto y las causas lícitas, se refieren a la cosa en sí, en donde el objeto materia del acto jurídico debe ser físicamente posible, es decir, estar dentro de la naturaleza, aunado a la licitud de las causas, lo cual quiere decir que sea jurídicamente posible; en otras palabras, estar dentro del comercio. Ahora bien, de estas dos características, se desprende que para que un acto jurídico sea válido, el objeto debe reunir dos requisitos: que sea jurídicamente y físicamente posible, en el entendido de que al determinar jurídicamente nos referimos a que sea lícito, por lo cual un delito no puede ser parte de un acto jurídico y un objeto que no esté dentro del comercio como una propiedad federal o un órgano parte de un cuerpo humano, tampoco forman parte de un acto de comercio. Por otra parte, al establecer que debe ser físicamente posible, debe existir materialmente y ser

---

<sup>18</sup> Acosta Romero Miguel: Teoría general del acto jurídico y obligaciones, México, ed. Porrúa, año 2002

<sup>19</sup> Gutiérrez y González Ernesto. Derecho de las obligaciones. Ed. Porrúa Edición séptima. México DF pág. 305

<sup>20</sup> Acosta Romero Miguel: Teoría general del acto jurídico y obligaciones, México, ed. Porrúa, año 2002

determinado o determinable, pues no sería posible rentar un inmueble que no existe.<sup>21</sup>

Con respecto a la forma como elemento de validez, se refiere a los requisitos que la ley establece y que el acto jurídico debe cumplir para tener una existencia perfecta. La ley puede determinar que cierto acto jurídico debe cumplir con la forma escrita, en donde las partes deben plasmar la relación jurídica estableciendo su voluntad de obligarse. La falta de este elemento no genera su inexistencia pero si su nulidad relativa, pues es susceptible de ser subsanada al cumplir con la formalidad que la ley establece. Así, si dos personas celebran un contrato de arrendamiento, se producen los efectos jurídicos y ambos contraen obligaciones recíprocas; sin embargo, esta falta de formalidad produce una nulidad relativa, misma que puede ser subsanada en cualquier momento con la firma del contrato de arrendamiento y así, cumplir con lo establecido en la Ley.

Como el acto jurídico no es un fenómeno como el hecho jurídico, sino toda una expresión de la voluntad o de un acuerdo de voluntades de su Autor o autores, para que este acto exista y tenga el reconocimiento y genere efectos jurídicos, será necesario que en su integración se reúnan los elementos, requisitos o condiciones que la Ley exige. Los autores han denominado elementos esenciales o de existencia y elementos de validez<sup>22</sup>.

De lo anteriormente mencionado, podemos resumir al acto jurídico como una acción humana cuya característica principal es la voluntad que tiene como finalidad inmediata establecer entre las personas relaciones jurídicas para crear, modificar o extinguir derechos y obligaciones. Para que dicho acto jurídico exista, no sólo basta que existan personas con capacidad jurídica par ser sujeto de derecho, sino que es necesario que exista ese vínculo que las relaciona.

---

<sup>21</sup> Acosta Romero Miguel: “Nuevo Derecho Mercantil”, Editorial Porrúa, Primera Edición; 15 de agosto del 2000.

<sup>22</sup> TEORÍA GENERAL DEL ACTO JURÍDICO (<http://www.monografias.com/trabajos22/acto-juridico/acto-juridico.shtml>) Fecha de consulta, enero de 2009), Salazar Macías, Ismael, Obra Particular, Pagina 4.

De las definiciones antes citadas, podemos determinar y confirmar que el acto jurídico es la manifestación de la voluntad, cuya finalidad en las partes es ser sujetos de derecho creando un vínculo jurídico entre ellas, del cual emanan derechos y obligaciones recíprocas, en donde la característica esencial es precisamente la intención de producir efectos jurídicos.

Una vez realizada la distinción entre acto jurídico y hecho jurídico, podemos clasificar al acto jurídico de acuerdo a sus características, pudiendo agruparse de la siguiente manera:

De acuerdo a la conducta que implica el acto jurídico, lo podemos dividir en: actos jurídicos positivos y actos jurídicos negativos.<sup>23</sup>

Los actos jurídicos positivos se caracterizan por un dar o un hacer, debido a que implica una acción de una de las partes que intervienen, como ejemplo podemos mencionar de manera enunciativa, la firma de un pagaré, en donde el deudor realiza una acción por la cual se obliga de manera voluntaria frente a otra; de igual forma podemos ejemplificar un acto jurídico positivo, en la entrega de una suma de dinero, en donde podemos apreciar que una de las partes da a otra un objeto para cumplir una obligación contraída o para crear un vínculo jurídico.

Por otra parte, un acto jurídico negativo, a diferencia de los positivos en los que se requiere de una acción, nos encontramos ante una omisión, es decir, un no hacer o no dar, de alguna de las partes, lo cual no implica que no genere consecuencias de derecho, pues si bien nos encontramos ante el supuesto de que es una abstención, es ahí en donde radica el cumplimiento del acto jurídico, en el entendido de que si se obligó a un no hacer. Como ejemplo de este tipo de actos jurídicos, en donde una persona se obliga a no realizar determinada acción, tenemos como ejemplo el arrendamiento de un inmueble, en donde el propietario se obliga a no perturbar el libre uso y goce del objeto materia del contrato de arrendamiento, siendo que el arrendador no debe impedir al

---

<sup>23</sup> <http://www.monografias.com/trabajos12/actjur/actjur.shtml>. 2009

arrendatario el libre uso del inmueble, sin perder de vista las obligaciones derivadas del contrato, siendo que no por el hecho de que se obligue a un no hacer, la parte que renta tenga la libertad de alterar el uso o sobrepasar los límites existentes. Los derechos del arrendador salvaguardan la posibilidad de hacer valer acción alguna, si considera que su patrimonio, el bien arrendado, sufre un desperfecto ocasionado por la parte arrendataria.

Otra clasificación del acto jurídico, se relaciona con la cantidad de voluntades que intervienen. Cabe señalar que no tiene que ver la cantidad de personas que intervienen, sino las voluntades de las personas que interactúan.

En este orden de ideas, de acuerdo a las voluntades de las personas, los actos jurídicos pueden dividirse en unilaterales o bilaterales, en donde tal y como su nombre lo indica, los actos jurídicos unilaterales son los que se perfeccionan con la voluntad de una sola parte, en donde una persona se manifiesta intencional conscientemente para crear un vínculo jurídico entre él y otra u otras personas, sin que se requiera de la voluntad de las demás partes que intervienen, como por ejemplo el testamento, es el acto por el cual se expresa de manera unilateral la voluntad única de una persona, para disponer de sus bienes después de su muerte, aun y cuando si bien es cierto que estos actos requieren de la aceptación de la otra parte, no debe perderse de vista que no se puede equiparar a la voluntad, pues la primera es quien crea el acto jurídico al obligarse voluntariamente ante otra persona.<sup>24</sup>

Para el caso de los actos jurídicos bilaterales o plurilaterales, las voluntades que intervienen son dos o más respectivamente, es decir, por lo menos dos personas se obligan recíprocamente porque es su voluntad hacerlo expresando su consentimiento para ser sujetos de derecho en un vínculo jurídico, como por ejemplo un contrato de compraventa, en donde una o más personas propietarias de un bien, deciden vender y otra u otras personas compran dicho bien; de este ejemplo se desprende que una parte voluntariamente transfiera la propiedad del bien que posee y del cual es propietario, a otra parte que en iguales

---

<sup>24</sup> <http://www.monografias.com/trabajos12/actjur/actjur.shtml>. 2009

circunstancias de forma voluntaria compra el bien adquiriendo derechos y obligaciones sobre el objeto comprado, con las consecuencias de derechos que se derivan de la compraventa.<sup>25</sup>

Esta clasificación de actos jurídicos unilaterales y bilaterales, no se debe confundir con la clasificación de los contratos, los cuales también pueden dividirse en unilaterales y bilaterales: La distinción radica en que para los actos jurídicos la voluntad es una y los contratos jurídicos son siempre bilaterales, esto es, como se mencionó en párrafos anteriores, aun y cuando un contrato se clasifica como unilateral por la razón de que crea obligaciones sólo para una de las partes que intervienen, se requiere de la manifestación de la siendo que voluntad de aceptar de la otra parte, los contratos son unilaterales o bilaterales no por las voluntades que intervienen, sino por las obligaciones que crean, las cuales pueden ser para una sola de las partes o para ambas.

Continuando con la clasificación de los actos jurídicos, tenemos actos entre vivos y actos de última voluntad; los primeros surten sus efectos justo en el momento de la celebración, es decir, al momento de expresar el consentimiento o en una fecha específica determinada por las partes, tal y como se puede apreciar en la celebración de un contrato, en donde el acto jurídico surte efectos al momento de la firma o en la fecha especificada en el mismo instrumento; por el contrario, los actos de última voluntad, están condicionados a un acontecimiento futuro como el fallecimiento de la persona de cuya voluntad emana, este tipo de actos jurídicos son llamados comúnmente mortis causa, en donde el ejemplo claro es un testamento, el cual produce sus consecuencias al momento de la muerte del autor del testamento.<sup>26</sup>

Otra clasificación del acto jurídico corresponde al lucro o la existencia de una ganancia o la obtención de un beneficio, ya sea en dinero o especie, para una o ambas partes, de tal forma que dichos actos jurídicos pueden ser gratuitos u onerosos.

---

<sup>25</sup> <http://derecho.laguia2000.com/parte-general/clasificacion-de-los-actos-juridicos>. 2009

<sup>26</sup> <http://derecho.laguia2000.com/parte-general/clasificacion-de-los-actos-juridicos>. 2009

Los actos jurídicos gratuitos, son aquellos en donde la obligación de dar, hacer o no hacer, está a cargo de una sola parte, sin que exista una obligación recíproca que se vincule de tal forma que dicha obligación esté condicionada a un dar, hacer o no hacer de la otra parte. En este tipo de actos jurídicos, una parte se obliga a título gratuito y responde a un propósito libre, como por ejemplo: una donación, siendo que una persona dispone de un bien del cual posee la propiedad y transfiere dicha propiedad a otra, sin que la parte que recibe el bien, el beneficiario, adquiera la obligación de dar una contraprestación.<sup>27</sup>

En los actos jurídicos onerosos, es totalmente lo opuesto, pues las partes que participan adquieren derechos y obligaciones recíprocas, en donde ambos obtienen un beneficio y al menos una de las partes efectúa el acto con el ánimo de lucro; tal es el caso de un arrendamiento de un inmueble, en donde el arrendador transfiere el uso y goce del inmueble a cambio de una renta mensual. De este ejemplo se aprecia que el propietario del objeto materia del arrendamiento, permite el uso del inmueble a cambio de una contraprestación; ambas partes adquieren derechos y obligaciones y el arrendatario se obliga a dar un pago mensual al arrendador, constituyendo un lucro para el propietario del inmueble.

La siguiente clasificación destaca por la relevancia que con motivo de este trabajo de investigación se relaciona, siendo el objeto principal el certificado digital y la firma electrónica, ligándose con la formalidad de los actos jurídicos en su forma escrita y la firma, la cual puede ser electrónica y no necesariamente un documento físico con firma autógrafa, sin poner en riesgo los efectos jurídicos que emanen y ser admitidos como prueba en un juicio. De tal forma, tenemos que los actos jurídicos pueden ser: formales y no formales, de acuerdo a lo establecido en la ley. Esto es, la legislación vigente y aplicable al caso en concreto, va a determinar si el acto jurídico debe cumplir con esta característica, en donde los formales, también llamados solemnes, para que sean

---

<sup>27</sup> <http://derecho.laguia2000.com/parte-general/clasificacion-de-los-actos-juridicos>. 2009

considerados como existentes y produzcan sus efectos, deben reunir las características que la ley indica, como puede ser la comparecencia física de las partes que intervienen en el matrimonio o la forma escrita en el caso de algunos contratos; por otro lado, los actos no formales, no dependen de solemnidad alguna para producir efectos jurídicos, es decir, no requieren de otro elemento adicional a la voluntad de las partes para existir, tal es el caso de una compraventa simple, en donde se perfecciona al momento de la entrega de la cosa y el recibo de la contraprestación pactada, esto es, no se requiere la firma de un contrato entre comprador y vendedor para producir efectos, lo cual no implica que no exista o que no tenga consecuencias de derecho; por ejemplo, si hubiera un vicio en el consentimiento, es susceptible de ser demandado por el afectado, aun y cuando no a documento por escrito que avale la compraventa, aceptándose en un litigio otras pruebas que acrediten dicha compraventa.

Respecto a una compraventa simple, aun y cuando no existe documento por escrito no causa inexistencia o nulidad; sin embargo, en algunos casos, cuando así lo determina la ley, requiere de documento por escrito que ampare la celebración de dicho acto, en donde la firma de las partes prueba la voluntad y consentimiento de las partes para celebrarlo. Se hace énfasis en lo que se refiere a la firma, pues lo que nos ocupa en este documento es la expresión de la voluntad y el consentimiento en los actos jurídicos, el cual es plasmado en algunos documentos mas no limitativa a los contratos con la firma autógrafa, en donde las partes acreditan su personalidad con una identificación oficial y vigente cabe mencionar que en el comercio electrónico se celebran innumerables compraventas, en donde las partes al estar en lugares distintos deben tener la certeza de que están contratando con la persona con quien pactaron, que el documento firmado electrónicamente es el mismo que firma la otra parte y que no fue alterado por las partes ni por un tercero en el envío de la información por medio de la red y, finalmente, que la firma electrónica insertada en el documento por ambos, manifestando con ello su consentimiento y su voluntad de ser acreedores de derechos y obligaciones generados, le es atribuible al firmante, negando la posibilidad de repudiar en un futuro el documento, pues la firma electrónica vincula al acto jurídico con la persona que firma.

Los actos jurídicos pueden ser patrimoniales o de familia. Los patrimoniales son aquellos en los que existe un fin preponderantemente pecuniario, en donde lo que mueve a las partes es la obtención de una ganancia. Los actos de familia o extrapatrimoniales, se refieren a derechos y deberes relativos a la familia, como por ejemplo un préstamo con interés, en donde lo que mueve a estos actos es una finalidad económica y la obtención de una ganancia para una de las partes. Como el deber de dar alimentos y el derecho a recibirlos, siendo el vínculo creado entre los progenitores y los descendientes, donde los padres se obligan a proporcionar el sustento a los hijos y a su vez, el derecho de los hijos para recibirlos.<sup>28</sup>

Por último, los actos jurídicos, pueden dividirse en: actos de administración o actos de enajenación. Los de administración, consisten en la transmisión de la tenencia, es decir, el propietario de la cosa transfiere el uso, tal es el caso de un comodato o un arrendamiento, en donde una de las partes concede el uso mas no la propiedad. Los actos de enajenación, consisten en la transmisión de la propiedad del objeto, como una compraventa, pues el vendedor transfiere el dominio total de la cosa al comprador.<sup>29</sup>

---

<sup>28</sup> <http://derecho.laguia2000.com/parte-general/clasificacion-de-los-actos-juridicos>. 2009

<sup>29</sup> <http://derecho.laguia2000.com/parte-general/clasificacion-de-los-actos-juridicos>. 2009

## **CAPÍTULO II**

### **SEGURIDAD EN EL COMERCIO ELECTRÓNICO**

#### **2.1. IMPORTANCIA DE LA SEGURIDAD EN EL COMERCIO ELECTRÓNICO**

La seguridad dentro del comercio electrónico es fundamental, debido a que es clave en la confianza ante empresas y particulares, como partes en los actos jurídicos que celebran entre si.

La seguridad en el comercio electrónico, y más específico en las transacciones comerciales, es fundamental para mantener una certeza jurídica entre las partes que interactúan, ya que al ser actos jurídicos y producir efectos legales, los involucrados deben confiar plenamente en que la información tanto enviada como recibida, así como las obligaciones señaladas, no serán modificadas en su contenido, posteriormente. Por la importancia que tiene la seguridad en el comercio electrónico, es necesario contar con una infraestructura segura, por medio de la cual la información relevante sea encriptada y viaje de forma segura.

Del mismo modo que en el comercio tradicional, en el comercio electrónico se encuentra presente un riesgo al realizar una transacción por Internet, generándose en el comprador la desconfianza y el temor a que la información concerniente a su persona como lo son el nombre, dirección, información financiera, por mencionar algunas, sean interceptadas por otra persona y se realice un mal uso de dicha información, como suplantar la identidad del comprador; del mismo modo, el vendedor debe cerciorarse, de que la información recibida pertenece a la persona que dice enviarlos.

Por ello, se ha desarrollado un sistema de seguridad para realizar diversos tipos de transacciones, envío y recepción de información por medio de la red, en donde dicha información viaja encriptada y firmada digitalmente, garantizando tanto al emisor como al receptor, que existe confidencialidad e integridad en la información enviada, así como la autenticidad respectivamente de quien envía y quien recibe dicha información.

Así, tenemos que las transacciones realizadas por Internet son seguras, pues al cifrar la información, se tiene certeza de que la información que se transfiere será confidencial, siendo accesible única y exclusivamente por las partes a quienes va dirigida. Con respecto a la firma digital que es asociada al documento, otorga la certeza al documento de que la información enviada no ha sido alterada por las partes que intervienen o por una tercera persona sin conocer dicha modificación; al mismo tiempo que la firma digital junto con el certificado digital, garantizan la identidad del firmante, evitando de este modo cualquier tipo de falsificación, suplantación de identidad o en un futuro la repudiación del documento, ya que al relacionar el documento y la firma digital con el certificado del firmante que acredita la identidad de la persona, sería incluso absurdo negar la autoría o la aceptación del documento, pues igual que la firma autógrafa, produce efectos legales y vinculan la firma con el firmante, con la distinción de que la firma digital es más fiable que la autógrafa en el sentido de que además de ser vinculante o asociada con el firmante, garantiza la integridad del documento, es decir, que no está alterado ni tiene modificación alguna posterior a la firma, así como que la persona que firma es quien dice ser y no como en la firma autógrafa que es susceptible a ser falsificada.

*“La seguridad es un aspecto clave para generar en las empresas y en los consumidores, la confianza necesaria para que el comercio electrónico se desarrolle. La necesidad de generar confianza es especialmente importante, debido a que Internet es una red abierta y transmite la sensación de inseguridad (quizá a veces excesiva) en los usuarios.*

*Sin embargo, la seguridad de la red, en este caso Internet, es sólo uno de los factores que intervienen en la seguridad del comercio electrónico en conjunto. Más que de la seguridad del pago, los usuarios empiezan a preocuparse sobre todo de problemas como ¿es el vendedor fiable? ¿Podré devolver el producto si no me gusta? ¿Utilizará mis datos personales para enviarme publicidad que no deseo? ¿Cederá esos datos a otras empresas?; en el caso de empresas ¿cuál es la validez de un pedido, factura, etc. hechos electrónicamente?*

*De esta manera, aunque las características de seguridad de las redes y sistemas de comercio electrónico son, obviamente, muy importantes, el hecho de que los usuarios consideren el comercio electrónico como suficientemente seguro, probablemente depende menos de los detalles técnicos, y más de otras cuestiones como la confianza que inspiren las empresas vendedoras, financieras, etcétera.; la existencia y difusión de normas que, por ejemplo, limiten la responsabilidad del usuario en caso de uso indebido de una tarjeta de crédito y que garanticen su derecho a devolver un producto comprado electrónicamente; la creación de códigos éticos de comportamiento de las empresas y de procedimientos efectivos de solución de conflictos; etcétera.*

### *Componentes de Seguridad*

*Las condiciones que debe reunir una comunicación segura a través de Internet (o de otras redes) son en general las siguientes:*

#### *Confidencialidad*

*Evita que un tercero pueda acceder a la información enviada.*

### *Integridad*

*Evita que un tercero pueda modificar la información enviada sin que lo advierta el destinatario.*

### *Autenticación*

*Permite a cada lado de la comunicación asegurarse de que cada uno es realmente quien dice ser.*

### *No repudio o irrefutabilidad*

*Permite a cada lado de la comunicación probar fehacientemente que cada uno ha participado en la comunicación. En el caso de no repudio de origen, el remitente del mensaje no puede negar haberlo enviado. En el caso de no repudio de destino, el destinatario del mensaje no puede negar haberlo recibido.*

*La herramienta básica para cumplir las condiciones anteriores son las técnicas criptográficas, en particular los métodos de cifrado simétrico (usan una misma clave secreta para cifrar y descifrar) o asimétrico (cada usuario tiene una pareja de claves, una pública y otra privada, con la propiedad de que lo que se cifra con una de las claves sólo se puede descifrar con la otra). Para evitar posibles suplantaciones de identidad, es necesario contar con una tercera parte fiable, que acredite de forma fehaciente cuál es la clave pública de cada persona o entidad. Esta es la función básica de las autoridades de certificación.*

*Un certificado digital emitido por una de estas autoridades contiene la identidad de un usuario, su clave pública y otros datos adicionales (por ejemplo, el periodo de validez del certificado; todo ello firmado digitalmente con la clave privada de la autoridad de certificación, con el fin de que el certificado no se pueda falsificar. Pueden existir varios tipos de certificados, válidos para diferentes usos, según la información y garantías que la autoridad de certificación (directamente o a través de una autoridad de registro) pide al usuario antes de emitir el certificado.”<sup>30</sup>*

En primer lugar, antes de hablar de las entidades encargadas de la seguridad en el comercio electrónico, es preciso conocer algunas de las definiciones que el Código de Comercio establece en su artículo 89, con la finalidad de ir comprendiendo más a fondo las partes que intervienen y la función que desempeñan cada una de ellas, así como las definiciones que se utilizan comúnmente dentro de este rubro del comercio.

Al respecto, el Código de Comercio en el artículo 89, señala las definiciones siguientes:

**“Artículo 89.-** Las disposiciones de este Título regirán 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.

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

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

---

<sup>30</sup> Foro – Consumo sobre Comercio Electrónico en Generalitat Valenciana (Generalidad Valenciana) <http://foroconsumo.cepymev.es/ce/seguridad.htm>. 2009

**“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.

**(“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
- 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.”)

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.”

Para identificar a las autoridades encargadas de la seguridad dentro del comercio electrónico, es necesario conocer como se integra la infraestructura, bajo la cual opera la emisión y registro de certificados digitales.<sup>31</sup>

1 Autoridad Registradora Central o Raíz: Secretaría de Economía

2. Prestadores de Servicios de Certificación: Personas físicas o morales que, autorizados por la Secretaría de Economía están facultados para emitir certificados digitales.

---

<sup>31</sup> <http://www.firmadigital.gob.mx/>. 2009

## **2.2. FIGURAS QUE PARTICIPAN EN LA EMISIÓN DE CERTIFICADOS DIGITALES**

Para la emisión de Certificados digitales, interactúan diversas figuras, las cuales tienen un orden jerárquico de acuerdo a la función que desempeña cada una de ellas. Es importante señalar, que actualmente en México existen cuatro tipos de certificados digitales que se emiten por diversas autoridades. Los Certificados digitales son distintos en función a la autoridad que los emite y a la tecnología empleada para generarlos, sin que esto implique en ningún momento que se afecte el objetivo principal o su razón de ser, la cual consiste en brindar seguridad al envío y recepción de información por medio de Internet, generando confianza tanto en el emisor como en el receptor, en virtud de que, aun y cuando no tiene las mismas características técnicas, si cumplen con los requisitos establecidos por la ley que garanticen los elementos fundamentales como la confidencialidad, autenticidad, integridad y la no repudiación futura por parte del emisor, mismos que describimos párrafos anteriores.

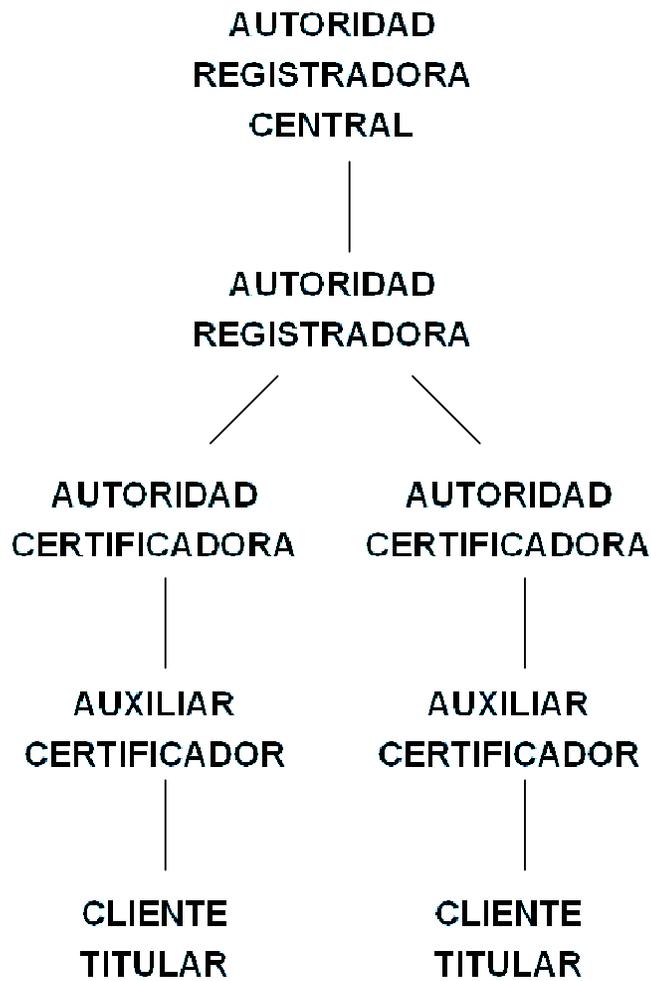
La infraestructura de seguridad se da de la siguiente manera:<sup>32</sup>

1. Autoridad Registradora Central (o raíz) ARC.
2. Agencia Registradora (o Autoridad Registradora) AR.
3. Agencia Certificadora (o Autoridad Certificadora o Prestador de Servicios de Certificación) AC o PSC.
4. Agente Certificador AgC.
5. Titular del Certificado Digital (o Cliente Usuario).

Conforme a esta estructura, las partes que intervienen tienen una función específica en la emisión y registro de los certificados digitales, con la finalidad de contar con seguridad absoluta.

---

<sup>32</sup> <http://www.banxico.org.mx/sistemasdepago/ies/iespub/PDF/IES-DOCTOBANXICO.PDF>. 2009

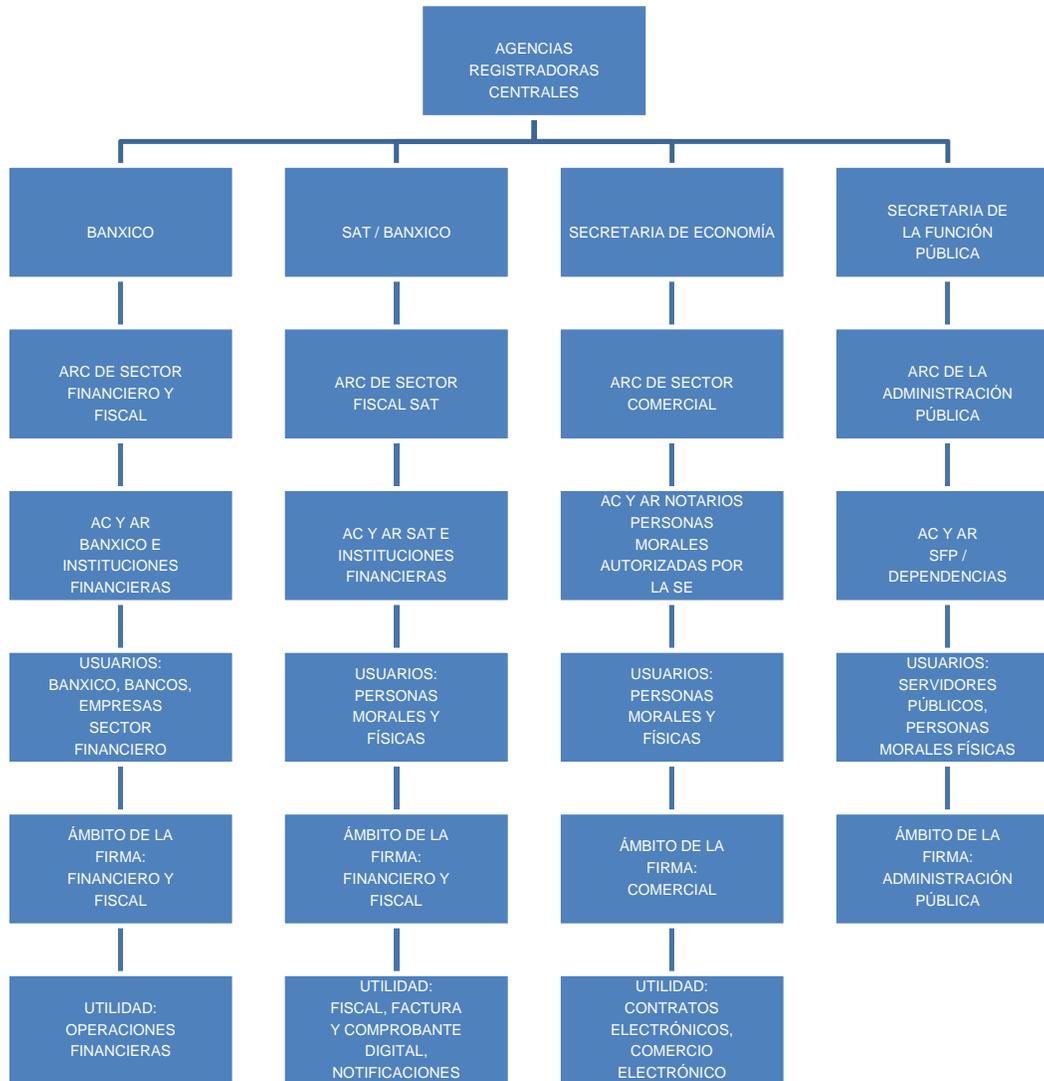


**Cuadro 2. Figuras que participan en la emisión de Certificados Digitales<sup>33</sup>**

Es importante resaltar que de acuerdo al ámbito de aplicación del certificado digital, la autoridad encargada de su vigilancia será un organismo del gobierno, de tal forma que las Agencias Registradoras Centrales dependen de una autoridad de este, las cuales se mencionan a continuación:

---

<sup>33</sup> Víctor Hugo Valdez Rojas



**Cuadro 3. Autoridades Registradoras Centrales y su ámbito de aplicación<sup>34</sup>**

<sup>34</sup> Víctor Hugo Valdez Rojas

Secretaría de Economía – Ámbito comercial.

1. Banco de México – Ámbito financiero y Fiscal.
2. Secretaría de la Función Pública – Ámbito de la Administración Pública.

### **2.2.1. Agencia Registradora Central**

La Autoridad Registradora Central ARC, es una autoridad registradora que depende de un organismo de gobierno y, de acuerdo al ámbito de aplicación del certificado, vigila, regula y mantiene la seguridad en el sistema de seguridad de la emisión y el registro de certificados digitales. Las funciones de la Agencia Registradora Central son las siguientes.<sup>35</sup>

1. Establecer normas y administrar la estructura jerárquica de certificación, conforme a las políticas que establezca la autoridad que las regula y que establece según el ámbito de aplicación del certificado digital.
2. Crear su propio Certificado Digital.
3. Emitir los Certificados Digitales a las personas físicas o morales de carácter público o privado, que hayan sido acreditadas como Agencias Registradoras.
4. Emitir los Certificados Digitales a las personas físicas o morales de carácter público o privado, que hayan sido acreditados como Prestadores de Servicios de Certificación.
5. Garantizar la unicidad de las Claves Públicas del Sistema.

---

<sup>35</sup> <http://www.banxico.org.mx/sistemasdepago/ies/iespub/PDF/IES-DOCTOBANXICO.PDF>. 2009

6. Administrar la base de datos de las Claves Públicas correspondientes a los Certificados Digitales, que las agencias Certificadoras hayan emitido.
7. Publicar la Clave Pública de las Agencias Registradoras y Agencias Certificadoras en Internet.
8. Mantener y establecer medidas que garanticen la seguridad del sistema.

### **2.2.2. Agencia Registradora y Certificadora**

La Agencia Registradora es la persona física o moral, de carácter público o privado, que autorizado por la Agencia Registradora Central, mantiene un registro electrónico de los certificados digitales emitidos por la Agencia Certificadora. La Agencia Registradora tiene a su cargo las siguientes funciones:<sup>36</sup>

1. Registra los Certificados Digitales emitidos por la Agencia Certificadora, siempre y cuando la Agencia Registradora Central confirme la unicidad de claves públicas.
2. Administrar las bases de datos en donde se registren los certificados digitales vigentes y revocados.
3. Mantener una base de datos pública de los certificados digitales emitidos.
4. Revocar certificados digitales cuando así proceda y mantener una base de datos pública de los certificados digitales revocados.

La Agencia Certificadora es la persona física o moral de carácter público o privado, autorizado por la Agencia Registradora Central para operar como prestador de servicios de certificación, es decir, emitir certificados digitales

---

<sup>36</sup> <http://www.banxico.org.mx/sistemasdepago/ies/iespub/PDF/IES-DOCTOBANXICO.PDF>. 2009

a los solicitantes, siempre y cuando reúnan los requisitos establecidos por la Agencia Registradora Central y se confirme la unicidad de sus claves. Las funciones de la Agencia Certificadora son las siguientes:<sup>37</sup>

1. Emitir el certificado digital del Agente Certificador que va a auxiliar a la Agencia Certificadora en sus funciones y acreditarlo como tal.
2. Emitir certificados digitales a los solicitantes, siempre y cuando reúnan los requisitos establecidos por la Agencia Registradora Central.
3. Solicitar a la Agencia Registradora el registro de los certificados digitales emitidos a los solicitantes.
4. Solicitar a la Agencia Registradora la revocación de los certificados digitales emitidos, cuando sea solicitado por el titular del certificado o cuando así proceda, por ubicarse dentro de los supuestos previstos para la revocación del certificado digital.
5. Auxiliarse de personas físicas que actuarán como Agentes Certificadores para la realización de sus funciones.

### **2.2.3. Agente Certificador**

El Agente Certificador es la persona física que previamente fue acreditado como tal por la Agencia Certificadora, para llevar a cabo sus funciones. Las funciones del Agente Certificador son las siguientes:<sup>38</sup>

1. Auxiliar a la Agencia Certificadora en sus funciones.

---

<sup>37</sup> <http://www.banxico.org.mx/sistemasdepago/ies/iespub/PDF/IES-DOCTOBANXICO.PDF>. 2009

<sup>38</sup> <http://www.banxico.org.mx/sistemasdepago/ies/iespub/PDF/IES-DOCTOBANXICO.PDF>. 2009

2. Verificar la identidad de los solicitantes que desean obtener un certificado digital, con base en los documentos oficiales y a las disposiciones establecidas por la Agencia Registradora Central.
3. Notificar al titular de un certificado digital sus derechos y obligaciones.
4. Recibir y verificar el requerimiento de certificado digital elaborado por el solicitante.
5. Obtener la declaración con firma autógrafa del solicitante en la que manifieste su conformidad con las reglas sobre el uso del certificado digital.
6. Proporcionar al solicitante de un certificado digital los medios necesarios para la generación de datos de creación y verificación de la firma electrónica.
7. Solicitar a la Agencia Certificadora la emisión del Certificado digital.
8. Solicitar a la Agencia Registradora la revocación de un certificado digital, cuando así proceda.
9. Entregar al Titular su certificado digital y obtener la carta de aceptación del certificado digital, en donde conste la firma autógrafa del titular.

#### **2.2.4. Titular de certificado digital**

El Titular es la persona física a la que se le emite un certificado digital y está en condición de firmar electrónicamente. Esta figura no tiene funciones asignadas por la Agencia Registradora Central, en virtud de que, al ser un usuario del servicio, no está subordinado a alguna autoridad; sin embargo debe cumplir con los requisitos establecidos para la obtención de su certificado digital y mantener resguardada su llave privada, debido a que será responsable

del uso que se le dé a su certificado y asumirá las consecuencias emanadas de cualquier documento que contenga una firma digital, que resulte vinculante con su certificado digital.<sup>39</sup>

### **2.3. CERTIFICADO DIGITAL**

Un Certificado Digital, es un mensaje de datos firmado por una Autoridad Certificadora que confirma un vínculo existente, entre la identidad de una persona y una firma electrónica, y a su vez, crea un vínculo entre el titular del certificado digital y el mensaje firmado electrónicamente por el titular del certificado digital.<sup>40</sup>

Esto es así, un Certificado Digital es un mensaje de Datos digital que contiene información de la persona titular de dicho Certificado que lo hace identificable. Este mismo objeto opera en las identificaciones físicas, es decir, cuando una persona acredita su identidad lo hace mediante una identificación, en virtud de que contiene datos como lo son el nombre, edad, sexo, nacionalidad, vigencia y autoridad que emitió la identificación. Siendo mas seguro un Certificado Digital que un documento físico en virtud de que el primero es infalsificable e inalterable, no así el documento físico que puede ser copiado, clonado o alterado.

Este Certificado Digital, además esta firmado electrónicamente por la autoridad Certificadora que generó dicho Certificado, lo que le da presunción de ser cierto. Al igual que en una identificación en donde está implícita la autoridad que emitió el documento y le da validez, el Certificado esta Firmado por la Autoridad Certificadora que emitió el Certificado. Es importante resaltar que el Certificado está firmado por una Autoridad Certificadora para verificar su autenticidad, es decir, que es integro, no se modificó y en consecuencia, le da reconocimiento y validez.

---

<sup>39</sup> <http://www.banxico.org.mx/sistemasdepago/ies/iespub/PDF/IES-DOCTOBANXICO.PDF>. 2009

<sup>40</sup> <http://www.banxico.org.mx/tipo/disposiciones/bancos/cir6-2005.htm>. 2009

Cabe señalar que al ser un Certificado Digital un mensaje de Datos, este puede contener cualquier información además de las datos de identificación del Titular, por mencionar algunos de forma enunciativa y no limitativa, tipo de sangre, alergias, discapacidades físicas, enfermedades para el caso de un historial clínico de una persona, o bien, limitaciones o permisos o restricciones a lugares restringidos para el caso de una identificación, entre otros.

Para comprender que es un certificado digital, es necesario conocer el proceso de emisión del mismo, así como su utilidad.<sup>41</sup>

Para generar un Certificado Digital, primero hay que generar un archivo de requerimiento (archivo.req) y otro archivo que será la llave privada (archivo.key). Estos archivos se generan a partir de un programa generador de requerimientos, en donde se captura información personal de quien será el titular del Certificado, siendo indispensable el nombre, dirección, correo electrónico, teléfono, entre otros datos; posteriormente se genera una contraseña que permitirá el acceso al certificado digital.

De esta manera, en un inicio tenemos dos archivos, un requerimiento (archivo.req) y una llave privada (archivo.key) además de una contraseña, los cuales son creados bajo el absoluto control y secreto del solicitante del certificado digital.

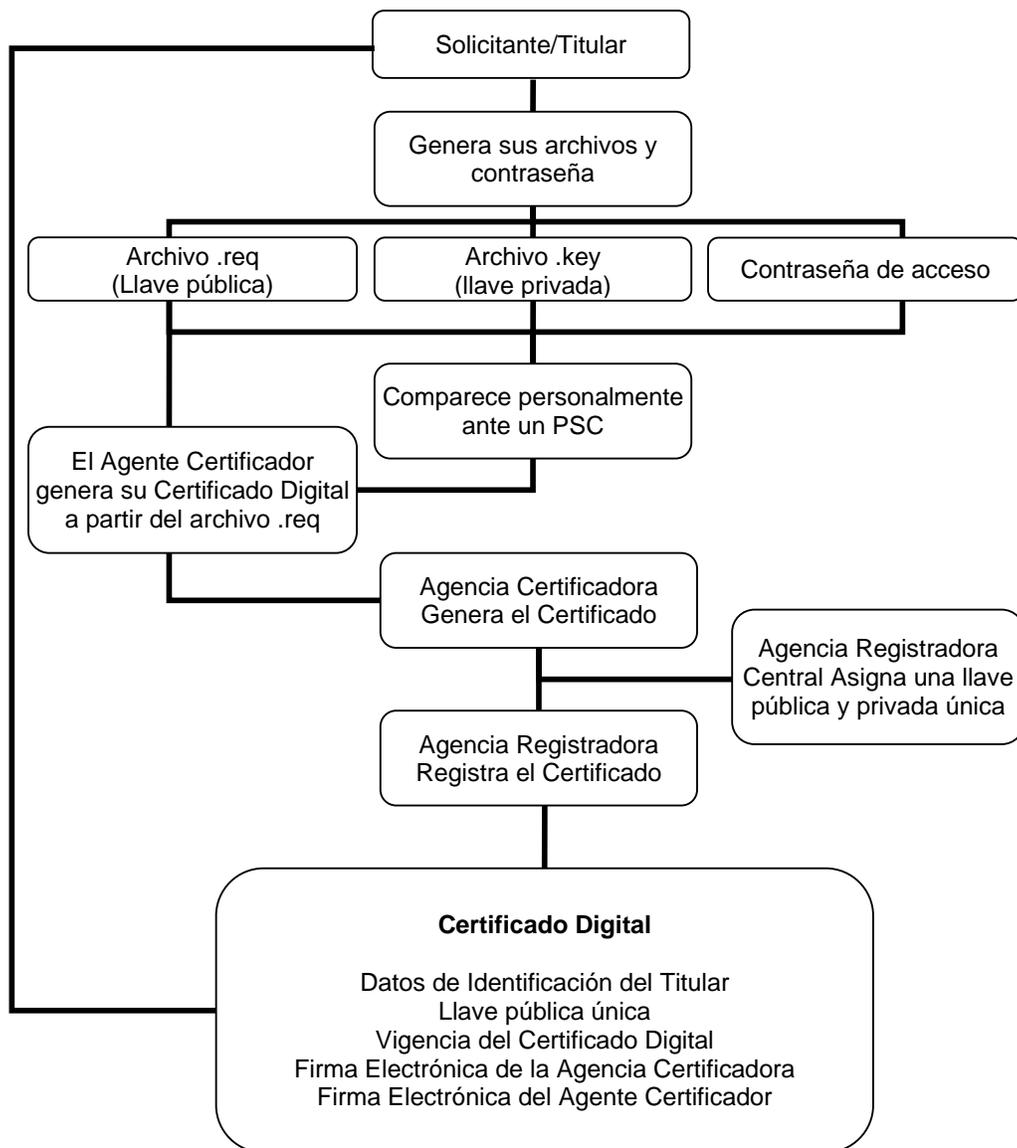
El solicitante deberá comparecer personalmente ante el prestador de servicios de certificación o Agencia Certificadora, con su requerimiento (archivo.req), que previamente fue elaborado por el solicitante y el cual se guarda en una memoria extraíble para que, por medio del funcionario facultado por la Agencia Certificadora se genere el Certificado Digital.

La forma de obtener el Certificado Digital, es a través del funcionario facultado por la Autoridad Certificadora siguiendo el procedimiento establecido para tal efecto, en donde en primer lugar se deberá acreditar la identidad del

---

<sup>41</sup><https://www.cecoban.org.mx/agencias/Soporte/Guia%20para%20requerimiento%20de%20certificado%20digital.pdf>. 2009

solicitante con documentos oficiales y vigentes como identificación con fotografía, constancias de nacimiento, nacionalidad, documentos comprobatorios de domicilio y de los cuales deberá obtener copia simple y cotejarlos con la información que se capturó en el archivo de requerimiento (archivo.req) y a partir del requerimiento, generar otro archivo que será el certificado digital (archivo.cer). Así tenemos que el Titular tendrá dos archivos, de los cuales uno es la llave privada (archivo.key) y otro es el certificado digital (archivo.req) y una contraseña de acceso.



**Cuadro 4. Proceso de emisión de un Certificado Digital<sup>42</sup>**

<sup>42</sup> Víctor Hugo Valdez Rojas

La forma de obtener el Certificado Digital, es a través del funcionario facultado por la Autoridad Certificadora siguiendo el procedimiento establecido para tal efecto, en donde en primer lugar se deberá acreditar la identidad del solicitante con documentos oficiales y vigentes como identificación con fotografía, constancias de nacimiento, nacionalidad, documentos comprobatorios de domicilio y de los cuales deberá obtener copia simple y cotejarlos con la información que se capturó en el archivo de requerimiento (archivo.req) y a partir del requerimiento, generar otro archivo que será el certificado digital (archivo.cer). Así tenemos que el Titular tendrá dos archivos, de los cuales uno es la llave privada (archivo.key) y otro es el certificado digital (archivo.req) y una contraseña de acceso.

El Certificado Digital deberá contener los Datos de identificación del titular de éste como son nombre, dirección, teléfono, correo electrónico, entre otros; así mismo, debe contener una llave pública única que asigna la Agencia Registradora Central, la vigencia del Certificado Digital, que no será mayor a dos años y la firma digital de la Agencia Certificadora que emitió el Certificado Digital.

<b>CERTIFICADO DIGITAL</b>	
<b>NOMBRE:</b>	Víctor Hugo Valdez Rojas
<b>RFC:</b>	VARV112233X1X
<b>DIRECCIÓN:</b>	Insurgentes 11, Extremadura, Benito Juárez, México, D.F. CP. 1234
<b>E-MAIL:</b>	victor@servidor.com
<b>TELEFONO:</b>	1122 3344
<b>CLAVE PÚBLICA:</b> 123456789	
<b>VIGENCIA DEL CERTIFICADO DIGITAL</b> De: 01/01/2009                      A: 01/01/2011	
<b>AGENCIA CERTIFICADORA:</b> <b>ELEKTROFIRMA, S.A. DE C.V.</b>	
<b>FIRMA ELECTRÓNICA:</b> UIO/(6g749(6u55fUT/89i9/()/B/u8fr5uiji	

**Cuadro 5. Contenido de un Certificado Digital <sup>43</sup>**

<sup>43</sup> Víctor Hugo Valdez Rojas

## **Certificado Digital**

(Archivo con extensión .cer)



## **Llave Privada**

(Archivo con extensión .key)



## **Apariencia de certificado digital**

*Titulo de la ventana*

*Pestañas de opciones*

*Información de  
uso del  
certificado*

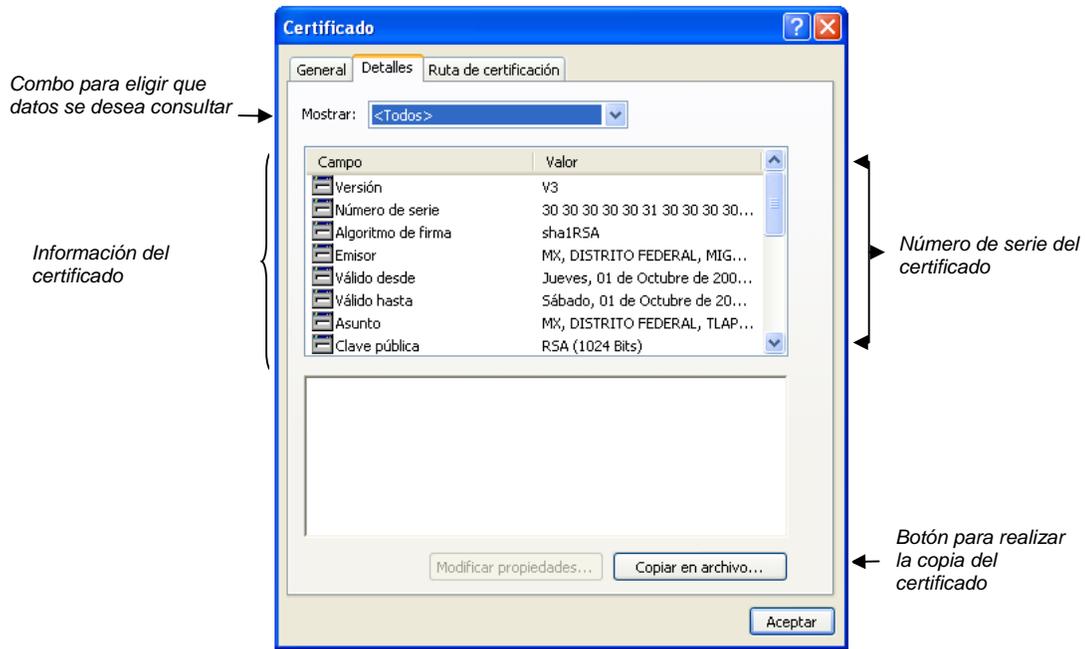
*Nombre del titular  
del Certificado*

*Botón para instalar el  
certificado en el  
almacén de  
certificados del  
Internet Explorer*

*Nombre de la Agencia  
Certificadora que emitió  
el certificado*

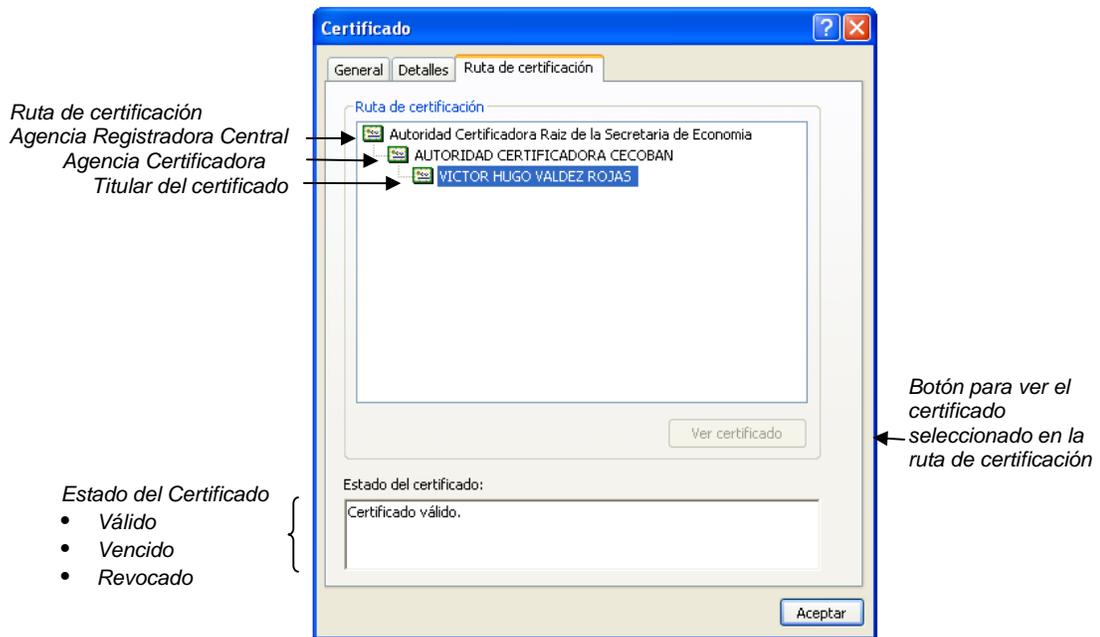
*Fecha de inicio y fin de  
vigencia del certificado*

*Botón de aceptar para  
cerrar la ventana*



**3030303030313030303039393030303030343435**

Serie del Certificado en formato Hexadecimal



**Apariencia de certificado digital**

**Cuadro 6. Certificado Digital<sup>44</sup>**

<sup>44</sup> Víctor Hugo Valdez Rojas

Cabe señalar que el certificado digital es un archivo electrónico, un mensaje de datos que contiene información del titular del certificado digital y una llave pública, la cual es conocida y utilizada para identificar al certificado digital. Este mensaje, además de los datos de identificación del titular del certificado digital, está firmado electrónicamente por un Prestador de Servicios de Certificación, lo cual le da certeza jurídica, en virtud de que un tercero ajeno es quien acredita que el titular del Certificado Digital es quien dice ser, y que fue previamente identificado por un Agente Certificador en auxilio de las funciones de la Agencia Certificadora. Se debe tomar en cuenta que no se utilizó el término fe pública, ya que el tercero que emite el Certificado Digital, que es una Autoridad Certificadora, no tiene fe pública, pues su responsabilidad se limita a identificar a la persona titular del certificado digital y contar con toda la infraestructura tecnológica y de seguridad para que, en un momento dado, se pueda vincular al Titular con el Certificado emitido a su nombre.

Para dejar mas claro este punto, podemos realizar una analogía del certificado digital con la credencial para votar, de la siguiente manera:

El Certificado Digital se puede equipar a la credencial para votar, la cual contiene datos de identificación de la persona titular. Al igual que el Certificado Digital, la credencial para votar contiene información personal que vincula a la persona física con la firma estampada, de puño y letra, en el anverso de la identificación. De igual forma, dicha identificación es emitida por una autoridad, el Instituto Federal Electora, la cual no da fe pública, sino que se limita a vincular a la persona con la identificación.

Ahora bien, si queremos celebrar un contrato en forma física, nos podemos identificar con la credencial para votar, con el objeto de asegurarnos que las partes que comparecemos somos quien decimos ser y por consiguiente se determina que la persona que comparece (titular del certificado digital) se identifica con la credencial para votar (Certificado Digital) con número de Folio (llave pública) expedida por el Instituto Federal Electoral (Prestador de Servicios de Certificación) y al momento de firmar autógrafamente, podemos comparar las firmas para asegurarnos que dicha firma corresponde a la persona física que se

está identificando. Sin embargo, es en esta parte en donde la firma electrónica avanzada, generada a partir de un certificado digital, cobra mayor importancia por sus ventajas.

Sobre las ventajas tenemos que, un comerciante no es perito para determinar si la identificación con que acredita su identidad es falsa o verdadera; en cambio, si es posible conocer a quien pertenece determinado certificado digital, el cual no puede ser falsificado por su complejidad y sólo puede ser emitido por un prestador de servicios de certificación, aunado a que los certificados digitales son únicos.

De igual forma, un comerciante no puede saber si la firma efectivamente corresponde al firmante, dado que en caso de no identificarse al momento de la firma de un contrato, no sabemos si efectivamente es la firma de quien dice ser, es decir, para el caso de un contrato en donde no se identifican las partes con identificación oficial, no tenemos la certeza de que efectivamente es quien dice ser y si la firma que estampó en el contrato corresponde y le puede ser atribuible en un futuro; en cambio, con una firma digital tenemos la seguridad de que la firma corresponde o no a determinado certificado digital, el cual es vinculable al titular de dicho certificado digital, por lo que la firma no puede ser falsificada, pues no sería vinculable al certificado digital con que se firmó el documento, aunado a que la firma digital es infalsificable, lo cual es posible debido a que a diferencia de la firma autógrafa, que siempre es el mismo signo, la firma digital no. Esto se debe a que para la creación de una firma digital, se utiliza tanto información del certificado digital como información del documento que se está firmando, por lo que nunca es exactamente igual, sin que esto implique que no sea atribuible a determinado certificado digital. Para mayor claridad veamos el siguiente ejemplo:

En el texto que a continuación está escrito de manera muy simple, se va a mostrar cómo se crea una firma digital, tomando en consideración que en la realidad para la creación de dicha firma, se utilizan formulas matemáticas complejas que la determinan.

<b>Documento:</b>
El acto jurídico es el acto humano voluntario o consciente, que tiene por fin inmediato establecer entre las personas relaciones jurídicas, crear, modificar o extinguir derechos.

Ahora bien, dicho texto es firmado digitalmente con un certificado digital, mismo que cumple con todos y cada uno de los requisitos establecidos por la ley, en conjunto con la llave privada y en consecuencia producen una firma digital que contiene información, tanto del certificado como del contenido del texto:

<b>CERTIFICADO DIGITAL</b>	
<b>NOMBRE:</b>	Víctor Hugo Valdez Rojas
<b>RFC:</b>	VARV112233X1X
<b>DIREC:</b>	Insurgentes 11, Extremadura, Benito Juárez, México, D.F. CP. 1234
<b>E-MAIL:</b>	victor@servidor.com
<b>TEL.</b>	1122 3344
<div style="border: 1px solid red; border-radius: 50%; width: fit-content; margin: 0 auto; padding: 5px;"> <b>CLAVE PÚBLICA:</b> V1H2V3R4         </div>	
<b>VIGENCIA DEL CERTIFICADO DIGITAL</b> De: 01/01/2009      A: 01/01/2011	
<b>AGENCIA CERTIFICADORA:</b> ELEKTROFIRMA, S.A. DE C.V.	
<b>FIRMA ELECTRÓNICA:</b> UIO/(6g749(6u55fUT/89i9/()/)B/u8fr5uiji	
<div style="border: 1px solid red; border-radius: 50%; width: fit-content; margin: 0 auto; padding: 5px;"> <b>Clave Privada:</b> VHVR         </div>	

**Cuadro 7. Ejemplo de Certificado Digital/Llave Pública y Llave Privada<sup>45</sup>**

<sup>45</sup> Víctor Hugo Valdez Rojas. Los ejemplos que se muestran son con fines explicativos, dado que, en la realidad, ambas claves se componen de algoritmos matemáticos que solo por medio del uso de computadoras es posible revisar, los cuales están vinculados entre si, de tal forma que, aun y cuando son archivos independientes, tiene una conexión que los relaciona. Por cada Certificado Digital, solo hay una llave privada.

Se debe identificar que en este ejemplo, la Clave Pública y la Clave Privada están relacionadas; la Clave Pública contiene las letras VHVR en el mismo orden que la Clave Privada. En la realidad es exactamente la misma función, se relacionan ambas claves pero de forma más compleja al estar determinada por algoritmos matemáticos y requiere de un conocimiento técnico en informática e ingeniería computacional específico.

En el siguiente ejemplo se utilizará un certificado digital, con la finalidad de verificar la autenticidad de la firma, el contenido del texto y el vínculo entre el documento firmado, el certificado digital y el titular de dicho certificado.

<b>Documento:</b>
El acto jurídico es el acto humano voluntario o consciente, que tiene por fin inmediato establecer entre las personas relaciones jurídicas, crear, modificar o extinguir derechos.
<b>Certificado</b>
VHVR
<b>Firma Electrónica Avanzada:</b>
VEHaVjReVeHaVhRvVoHcVqRtVp HfViReVeHIVpRrVjHcVmRoVeHd
La firma si corresponde

Para ilustrar el funcionamiento de la firma digital, en este ejemplo utilizamos la llave privada, la cual está relacionada con el certificado digital y en su conjunto nos permite firmar digitalmente; no hay que perder de vista que, tal y como se explicó anteriormente, dicha firma se determina con la aplicación de fórmulas matemáticas, aplicadas de tal forma que la computadora puede determinar la firma y puede ser verificada y atribuible al certificado digital,

vinculando la firma con el titular del certificado digital, produciendo los mismos efectos jurídicos que la firma autógrafa.

Por otra parte, al mismo texto se le aplica un certificado digital distinto con su respectiva llave privada de este otro certificado (de lo contrario no se podría aplicar la firma, pues el certificado digital y la llave privada están ligadas) y que no corresponde a la persona con quien estamos contratando, lo cual, al momento de verificar la autenticidad del certificado y el vínculo que existe entre dicho certificado digital y la firma podemos observar que no corresponde, ya a que la firma es distinta y no es vinculable al certificado digital; en consecuencia, tampoco lo es con la persona que deseamos celebrar el acto jurídico, lo cual se puede equiparar a una firma falsa en documento impreso.

<b>Documento:</b>
El acto jurídico es el acto humano voluntario o consciente, que tiene por fin inmediato establecer entre las personas relaciones jurídicas, crear, modificar o extinguir derechos.
El documento es idéntico
<b>Certificado</b>
VHVC
Es distinta
<b>Firma Electrónica Avanzada:</b>
VEHaVj <u>Ce</u> VeHaVh <u>Cv</u> VoHcVq <u>Ct</u> Vp HfVi <u>Ce</u> VeHIVp <u>Cr</u> VjHcVm <u>Co</u> VeHd
La firma digital es distinta

En otro supuesto, tenemos que el certificado digital si corresponde con la persona que deseamos contratar; sin embargo, en este caso en particular, el contenido del documento fue alterado, modificando los términos pactados, lo que implica una modificación en las consecuencias de derecho, pero al momento

de verificar la firma digital, esta no corresponde, debido a que, aun y cuando el certificado digital si es vinculable con la persona titular del mismo, el contenido del documento fue alterado y al no ser atribuible la firma digital con los firmantes, se extingue cualquier efecto jurídico.

<b>Documento:</b>
El <b>hecho</b> jurídico es el acto humano voluntario o consciente, que tiene por fin inmediato establecer entre las personas relaciones jurídicas, crear, modificar o extinguir <b>obligaciones</b> .
El documento es distinto
<b>Certificado</b>
VHVR
Es idéntico
<b>Firma Electrónica Avanzada:</b>
VE <u>Hh</u> VjReVeHaVhRvVoHcVqRtVp HfViReVeHIVpRrVjHcVmRoVe <u>Ho</u>
La firma digital es distinta

Así, tenemos que el certificado digital, no sólo es útil para identificar a las partes que intervienen en un acto jurídico, sino que además brinda mayor seguridad en las transacciones comerciales, pudiendo extenderse su utilidad a un mayor ámbito de aplicación más allá del comercio electrónico, al tener la peculiaridad de ser infalsificable, lo cual se tratará en capítulos posteriores.

A igual que la credencial para votar, el certificado digital sirve para identificar a una persona, y de la misma manera en que se verifica que la firma en dicha identificación sea similar a la que se suscribe en un contrato, el certificado

digital verifica que la firma digital de un documento electrónico, sea vinculable con el contenido del documento y el titular del certificado digital.

De tal forma, se cumple con la finalidad esencial de la firma autógrafa, es decir, la exteriorización de la voluntad al manifestar el consentimiento, con la inserción de la firma digital, la cual legalmente tiene los mismos efectos legales que la firma autógrafa.

La autenticidad del certificado digital en el comercio electrónico es fundamental en virtud de que, para la celebración de un acto jurídico en forma escrita, las partes que intervienen e incluso testigos deben firmar, teniéndose por satisfecho dicho requisito de ley, si se cuenta con un documento electrónico firmado digitalmente.

Es importante mencionar que de los ejemplos señalados anteriormente, respecto a cómo es que el certificado digital funciona para generar una firma digital, se debe comprender a partir del contenido del documento se genera la firma electrónica o firma digital, de tal forma que siempre que el mismo certificado digital se aplique a el mismo documento, se generará la firma exactamente igual, es decir, siempre y cuando el mismo certificado y el mismo documento se conjuguen, pero cuando al mismo contenido se le aplique un certificado distinto, la firma digital será distinta, o en su defecto, en el supuesto de que el certificado digital no varíe sino que el contenido del documento se modifique, aun y cuando sólo sea un espacio o un punto mas o menos, la firma digital será distinta. Aclarado esta, regresamos un poco al inicio de este documento, en donde determinamos las características del certificado y la firma digital. Tenemos que se goza de autenticidad, siendo que el receptor y el emisor es quien dice ser, pues es identificable por medio de su certificado digital y al estar debidamente firmado un documento con su certificado digital, podemos atribuir la autoría del documento y el consentimiento al estar plasmada la firma digital, así como también gozamos de integridad en el documento, pues al momento de verificar la firma digital, podemos conocer si el documento fue alterado o está intacto, lo cual crea una certeza jurídica absoluta.

Este beneficio es relevante, pues como bien sabemos, en un juicio en donde una parte puede demandar el cumplimiento forzoso de una obligación por el incumplimiento a lo pactado de un contrato, el cual se exhibe como prueba en la litis como documento “físico” y en donde el demandado opone sus excepciones y defensas, alegando que el documento fue alterado o incluso que se falsificó su firma, puede ser un proceso largo, aunado a que no es garantía que al final se dicte una sentencia justa, pues durante la secuela procesal, el documento base de la acción es sujeto a revisión por peritos en la materia, quienes van a determinar la autenticidad de el documento, su integridad y la autenticidad de las firmas, pudiendo prolongarse un juicio por varios años, estando latente el error humano que por negligencia o alguna otra causa provoque que el dictamen de los peritos sea erróneo, dejando en un estado e indefensión a una de las partes. En cambio, cuando un documento electrónico firmado digitalmente es sujeto de un juicio, la forma de saber si el contenido de un documento fue alterado o si la firma corresponde o no a determinada persona, es instantáneo, con un margen de error nulo, debido a que al momento de verificar la firma digital con el certificado digital, debe existir un vinculo, de tal forma que si es vinculable, es atribuible el contenido y, por obvias razones, produce sus consecuencias legales el acto jurídico y, por el contrario, si no es vinculable el certificado digital con la firma digital o con el contenido del documento, no pueden ser atribuidas las obligaciones emanadas de dicho acto jurídico.

Una vez aclarado el funcionamiento del certificado digital, en la creación de la firma electrónica y que sin lugar a duda puede determinarse que el autor definitivamente es el emisor del documento y, en consecuencia, está expresando su consentimiento en dicho documento, así como que el receptor al añadir su firma digital con su certificado digital, acepta lo estipulado en dicho documento electrónico, nos queda una característica más: la confidencialidad.

Como se mencionó al principio de este trabajo, en el comercio electrónico, el certificado digital que la información enviada y recibida cuente con las siguientes características:

### Integridad

Autenticación

No repudio o irrefutabilidad

Confidencialidad

Cabe recordar de manera breve, que la integridad consiste en que la firma digital generada a partir del certificado digital, nos ayuda a saber si el documento es íntegro o fue alterado, siendo que la firma digital se genera a partir de el certificado digital y del contenido del texto firmado, de tal forma que si cambia una sola letra del texto, se modifica la firma digital. Así mismo, la información es auténtica, pues el certificado digital con que se firmó el documento, nos garantiza que la persona que es firma, es la misma que es titular del certificado digital, y la cual es identificable por medio de dicho certificado, ya que el certificado digital contiene información que ayuda a identificar al autor del documento, es decir, ambas partes tienen la garantía de estar completamente seguros si quien firmó el documento es el mismo titular del certificado, de lo contrario, no correspondería la firma digital con el certificado digital con que se firmó. De esta característica se desprende la irrefutabilidad o la no repudiación del documento, toda vez que como el certificado digital garantiza la identidad del emisor, es ilógico que en un futuro el emisor niegue la autoría, en otras palabras, si un documento lo firma una persona con su certificado digital, que lo vincula por medio de los datos de identificación del certificado, no puede negar su autoría.

En este orden de ideas, la última característica se refiere a la confidencialidad; se basa en el segundo archivo generado al momento de crear el requerimiento (archivo .req) a partir del cual se genera el certificado digital.

Así, al momento de generar el requerimiento, se crean dos archivos: el .req que es utilizado para crear el certificado por un Agente Certificador, mientras que el otro archivo denominado .key, es la llave privada que contiene información única y que es vinculante con el certificado digital.

Para garantizar la confidencialidad de un documento, es decir, tener la certeza de que sólo el receptor podrá ver la información firmada el emisor, crea un candado que sólo podrá ser abierto por el receptor.

El certificado digital contiene una llave pública, que como su nombre lo indica, es del conocimiento de cualquier persona, por lo que el emisor del documento conoce dicha llave. El emisor, como se vio el proceso de firmado de documentos, genera un documento digital, lo firma con su certificado digital y le inserta la llave pública del receptor, con lo que la información se cifra y solo podrá ser abierta con la llave privada del receptor.

## 2.4. FIRMA

La palabra firma proviene del vocablo latino *firmare*, que significa afirmar, dar fuerza. Para la Academia de la Lengua, firmar se define como: 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, para expresar que se aprueba su contenido o para obligarse lo que en el se dice.<sup>46</sup>

En el vocablo jurídico de Couture, se define como Trazado gráfico, conteniendo habitualmente el nombre, los apellidos y la rúbrica de una persona, con el cual se suscriben los documentos para darles autoría y virtualidad y obligarse en lo que en ellos se dice.<sup>47</sup>

La firma, la podemos definir como una serie de signos, símbolos o palabras que una persona adjunta a un documento y que sirven para identificar al autor de dicho documento o de una obra y que además expresa el consentimiento con el contenido del documento.

La firma tiene como objetivo principal, vincular al titular de la misma con el contenido de una obra o un escrito, expresando su entero consentimiento y obligándose a lo establecido en el documento.

---

<sup>46</sup> Enciclopedia Jurídica Omeba, Tomo XII, Editorial Bibliográfica Argentina, pp. 290 293

<sup>47</sup> [http://descargas.cervantesvirtual.com/servlet/SirveObras/01159852653479324108813/008469\\_5.pdf](http://descargas.cervantesvirtual.com/servlet/SirveObras/01159852653479324108813/008469_5.pdf). 2009

Existen dos tipos de firmas: autógrafa y la electrónica avanzada, las dos son reconocidas por la ley en su totalidad, produciendo los mismos efectos jurídicos, siendo aceptadas como medios de prueba, aun y cuando se obtienen de forma distinta, pues una proviene del puño y letra de una persona y la otra proviene de archivos que fueron generados previamente; ambas tienen la misma finalidad y por consecuencia los mismos efectos, pues en el entendido de que el titular tiene el control absoluto al momento de su creación, se entiende que la firma exterioriza la voluntad para obligarse a un dar, hacer o no hacer.<sup>48</sup>

El *Animus Signandi* es un elemento intencional o intelectual de la firma, que consiste en la voluntad de asumir el contenido de un documento.

#### **2.4.1. Firma autógrafa**

La firma autógrafa es la que suscribe la persona física con su propia mano y consiste en un conjunto de letras, su nombre y a veces, el nombre y apellido, aunado a trazos que pueden abarcar toda gama de evoluciones del instrumento de escritura, que señalan e identifican al sujeto y lo separan de otros en los documentos que suscribe; es un elemento que refleja permanentemente su voluntad de expresar lo que firma o de obligarse al tenor del texto que suscribe<sup>49</sup>

Para ¿quién es? José Mustapich<sup>50</sup>, la firma es el nombre escrito por propia mano en caracteres alfabéticos y de una manera particular, al pie del documento, a efecto de autenticar su contenido.<sup>51</sup>

---

<sup>48</sup> [http://descargas.cervantesvirtual.com/servlet/SirveObras/01159852653479324108813/008469\\_5.pdf](http://descargas.cervantesvirtual.com/servlet/SirveObras/01159852653479324108813/008469_5.pdf). 2009

<sup>49</sup> ACOSTA ROMERO, Miguel, "Nuevo Derecho Mercantil", capítulo XVIII. La firma en el derecho mercantil mexicano. Pp 537 a 562, Editorial Porrúa, primera edición.

<sup>50</sup> José Mustapich, Escribió la siguiente obra: *Tratado teórico-práctico de Derecho Notarial*. Editorial Bibliográfica Argentina, Buenos Aires, 1960, voz "Firma", Tomo XII, página 290

<sup>51</sup> MUSTAPICH, J.M. Tratado de Derecho Notarial, Tomo I

## 2.4.2. Firma electrónica avanzada (FEA)

La firma electrónica avanzada es definida por el Código de Comercio, en el artículo 89 en relación con el artículo 97, que determina las características que se deben reunir para que la firma electrónica se considere como avanzada o fiable.

“Artículo 89...

...

**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.

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

**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 demuestre de cualquier otra manera la fiabilidad de una Firma Electrónica; o presente pruebas de que una Firma Electrónica no es fiable.”

## 2.5. DIFERENCIAS Y VENTAJAS DE LA FEA

Las ventajas de la Firma Electrónica sobre la firma autógrafa, son las siguientes:<sup>52</sup>

1. Produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio.
2. Los Datos de Creación de la Firma, en el contexto en que son utilizados, corresponden exclusivamente al Firmante.
3. Los Datos de Creación de la Firma estaban, en el momento de la firma, bajo el control exclusivo del Firmante.
4. Es posible detectar cualquier alteración de la Firma Electrónica hecha después del momento de la misma.
5. 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.

Algunas utilidades que se le puede dar al certificado digital y uso de la firma electrónica avanzada, son las siguientes:<sup>53</sup>

Contratación electrónica: en cualquier tipo de servicio como banca, seguros, telefonía, etcétera.

---

<sup>52</sup> [www.slideshare.net/.../firma-electronica-1410248](http://www.slideshare.net/.../firma-electronica-1410248). 2009

<sup>53</sup> Martínez Nadal Apollonia: La ley de firma electrónica, Madrid, España, segunda edición, año 2001, p. 342.

Cualquier clase de relación con la Administración: pago impuestos, consultas, dictámenes, recursos, reclamaciones, denuncias, etcétera.

Historia clínica única electrónica, recetas electrónicas, etcétera.

Relaciones entre particulares por medios electrónicos: compra venta, pagos, etcétera.

Voto electrónico: en el Estado y en las organizaciones, cualquier tipo de participación que implique identificación previa.

Todo tipo de actividad electrónica que requiera identificación y certificación de cualquier tipo de documento (CVs con calificaciones de una institución, dictámenes profesionales, documentos públicos...)

## **2.6. DIFERENCIAS ENTRE EL CERTIFICADO DIGITAL Y LA FIRMA ELECTRÓNICA AVANZADA**

Actualmente es común que la mayoría de las personas identifiquen como sinónimo al certificado digital y la firma electrónica avanzada; sin embargo, estos dos términos no se refieren a lo mismo, pues uno depende del otro, es decir, para que exista una firma electrónica avanzada se requiere de la existencia de un certificado digital.

Ocasionalmente, la gente que desconoce este tema o que no ha tenido ningún contacto al respecto, puede confundir entre un certificado digital y una firma electrónica avanzada, pues al no tener el conocimiento preciso de qué es cada una, cómo se obtiene y para qué sirve, puede ser sujeto de que ambos términos se asimilen como sinónimos.

La diferencia entre ambos es simple. El Certificado Digital es un archivo que emite una Agencia Certificadora y sirve para acreditar la identidad del

firmante, vinculando al titular del certificado digital con el documento firmado electrónicamente. Por otro lado, la firma electrónica avanzada es una serie de datos adheridos a un documento, que se obtienen de la combinación del contenido del documento electrónico y el certificado digital, por lo que la firma electrónica contiene información del titular del certificado digital y del contenido del documento, pudiendo autenticar que el contenido del documento no está alterado y que fue consentido por el firmante que es titular del certificado digital y es identificable por medio de la información insertada en la firma electrónica avanzada.<sup>54</sup>

En otras palabras, el certificado digital es un archivo electrónico que contiene información de una persona, quien previamente acreditó su identidad ante una agencia certificadora, y la firma electrónica avanzada es una serie de datos adjuntados electrónicamente a un documento, que surge de la combinación del certificado digital y el contenido del documento, por lo que, al contener información del titular del certificado, le es atribuible la autoría del documento o su consentimiento de lo ahí establecido, y al mismo tiempo, se puede corroborar la autenticidad de la información, de tal forma que si el contenido es modificado posteriormente, la firma electrónica avanzada no coincidiría y por lo tanto pierde su fuerza legal.

## **2.7. EFECTOS JURÍDICOS DE LA FIRMA ELECTRÓNICA AVANZADA**

Los Certificados Digitales son mensajes de datos firmados digitalmente, donde la seguridad se basa en el uso de firmas electrónicas, mediante la aplicación de algoritmos criptográficos que garantizan la confidencialidad e integridad de la información que se transmite y a su vez acreditar la identidad del remitente.

---

<sup>54</sup> Martínez Nadal Apollonia: La ley de firma electrónica, Madrid, España, segunda edición, año 2001, p. 342.

Los algoritmos criptográficos tienen como función primordial transformar un mensaje en un texto no inteligible, excepto para el destinatario, ya que éste es el único que puede efectuar la transformación inversa y por lo tanto conocer el mensaje original. Al texto ininteligible se le conoce como documento cifrado o criptograma.

La firma electrónica se puede definir como el conjunto de datos que se agrega o adjunta a un documento electrónico y está asociado en forma lógica al propio documento y al signatario.

La firma electrónica tiene las mismas funciones que la firma autógrafa, siendo más confiable la primera. La firma electrónica difiere de la firma autógrafa, en que la primera está vinculada al documento y al signatario, mientras que la segunda sólo depende del signatario y es invariable.

Dado que la firma electrónica de un documento es una función de la clave privada del signatario y a su vez del contenido del propio documento, las principales propiedades de una firma electrónica son:

- ⇒ Es única por documento y signatario.
- ⇒ Es atribuible al signatario.
- ⇒ Es infalsificable.
- ⇒ No puede transferirse a otro documento.

El Certificado Digital que emite una Agencia Certificadora, se genera de acuerdo con lo establecido en la IES y al Sistema Internacional de Criptografía de clave pública (PKI) de RSA, bajo el formato ITU-TX.509 v3.

Con un tamaño en sus claves públicas y privadas de 1024 bits, dicho Certificado proporciona los elementos para agregar a los mensajes de datos, las siguientes características de seguridad:

- ⇒ Confidencialidad.- El destinatario es el único que puede leer el mensaje cifrado.
- ⇒ Autenticidad.- Se puede verificar que el mensaje proviene de la persona que lo emitió.
- ⇒ Integridad.- Se asegura que la información contenida en el mensaje no está alterada.
- ⇒ Aceptación de Autoría.- El emisor no puede negar válidamente, ser el autor del mensaje.

De conformidad con la legislación vigente y aplicable al caso en concreto, tenemos que la información enviada de manera electrónica, así como la firma electrónica generada a partir de el certificado Digital emitido por la Autoridad Certificadora, tiene validez jurídica, en virtud de que satisface todos los requisitos de confidencialidad, autenticidad, integridad y no repudiación de la información, que establece la ley.

## LEY DEL BANCO DE MÉXICO

**“ARTÍCULO 24.- El Banco de México podrá expedir disposiciones sólo cuando tengan por propósito la regulación monetaria o cambiaria, el sano desarrollo del sistema financiero, el buen funcionamiento del sistema de pagos, o bien, la protección de los intereses del público.** Al expedir sus disposiciones el Banco deberá expresar las razones que las motivan.

**Las citadas disposiciones deberán ser de aplicación general,** pudiendo referirse a uno o varios tipos de intermediarios, a determinadas operaciones o a ciertas zonas o plazas.

Las sanciones que el Banco imponga conforme a lo previsto en los artículos 27, 29 y 33, deberán tener como objetivo preservar la efectividad de las normas de orden público establecidas en la presente Ley y, de esta manera,

proveer a los propósitos mencionados en el primer párrafo de este precepto.”

**“ARTÍCULO 68.- La Ley de Instituciones de Crédito, la legislación mercantil, los usos bancarios y mercantiles y el Código Civil para el Distrito Federal, en Materia Común, y para toda la República en Materia Federal, se aplicarán a las operaciones del Banco, supletoriamente a la presente Ley y en el orden en que están mencionados.”**

La supletoriedad de la Ley, implica que la ley suplida regula deficientemente una determinada institución jurídica que sí se encuentra prevista en la ley suplente, por lo que no puede existir supletoriedad cuando el ordenamiento legal suplido sí contempla la figura jurídica de que se trate.

La supletoriedad de la ley surte efecto cuando en determinada institución jurídica prevista por la ley a suplir, existen lagunas u omisiones, las cuales podrían ser subsanadas con las disposiciones que la ley supletoria contenga en relación a dicha institución jurídica.

Así, para que exista supletoriedad de normas respecto de otras, deben existir requisitos, como son los siguientes:<sup>55</sup>

a) Que el ordenamiento que se pretenda suplir lo admita expresamente, y señale el estatuto supletorio;

b) Que el ordenamiento objeto de supletoriedad prevea la institución jurídica de que se trate;

c) Que no obstante esa previsión, las normas existentes en tal cuerpo jurídico sean insuficientes para su aplicación a la situación concreta presentada, por carencia total o parcial de la reglamentación necesaria y,

---

<sup>55</sup> Díaz Bravo Arturo: Derecho mercantil, México, segunda edición, año 2006.

d) Que las disposiciones o principios con los que se vaya a llenar la deficiencia no contraríen, de algún modo, las bases esenciales del sistema legal de sustentación de la institución suplida.

Conforme a lo establecido por el precepto legal que antecede, tenemos que, supletoriamente, para lo no contemplado en la Ley del Banco de México son aplicables la Legislación Mercantil, es decir, el Código Federal de Comercio y el Código Civil Federal, entre otros.

En este orden de ideas, tenemos que si bien es cierto que la Ley del Banco de México es omisa, al manifestarse expresamente sobre los efectos jurídicos del Certificado Digital y la Firma Electrónica, son aplicables de manera supletoria para subsanar estas deficiencias lo establecido por el Código Federal de Comercio y el Código Civil Federal.

CÓDIGO DE COMERCIO  
TÍTULO SEGUNDO DE COMERCIO ELECTRÓNICO  
CAPÍTULO 1  
DE LOS MENSAJES DE DATOS

**“Artículo 89 bis.-** 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.”

El código de comercio, legislación supletoria aplicable de acuerdo al artículo 68 de la Ley del Banco de México, le concede efectos jurídicos a cualquier tipo de información contenida en un mensaje de datos, de tal forma que el certificado digital IES tiene validez jurídica.

De las Firmas

**“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

**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 demuestre de cualquier otra manera la fiabilidad de una Firma Electrónica; o presente pruebas de que una Firma Electrónica no es fiable.”

De los artículos antes citados, tenemos que la firma electrónica generada por medio del Certificado Digital IES, cuenta con la validez jurídica que le otorga la legislación Mexicana, toda vez que reúne los requisitos que establece el artículo 97 del Código de Comercio, actuando de manera supletoria. De tal forma, la Ley no distingue entre Certificados Digitales diversos, pues si reúne las características de seguridad, confidencialidad y es atribuible al emisor, tiene la fuerza legal de la firma autógrafa, pues nos encontramos ante el supuesto de la expresión de la voluntad para crear un vínculo jurídico y ser sujeto de derechos y obligaciones.

CÓDIGO CIVIL FEDERAL.

LIBRO CUARTO. DE LAS OBLIGACIONES.

PRIMERA PARTE. DE LAS OBLIGACIONES EN GENERAL.

TÍTULO PRIMERO. FUENTES DE LAS OBLIGACIONES.

CAPÍTULO I. CONTRATOS.

## DEL CONSENTIMIENTO.

**“Artículo 3.- Las leyes, reglamentos, circulares o cualesquiera otras disposiciones de observancia general, obligan y surten sus efectos tres días después de su publicación en el Periódico Oficial.**

En los lugares distintos del en que se publique el Periódico Oficial, para que las leyes, reglamentos, etc., se reputen publicados y sean obligatorios, se necesita que además del plazo que fija el párrafo anterior, transcurra un día más por cada cuarenta kilómetros de distancia o fracción que exceda de la mitad.”

Del artículo 3 del Código Civil Federal, en relación al artículo 24 de la Ley del Banco de México, tenemos que las disposiciones y reglamentos emitidos por el Banco de México, son de carácter general, es decir, de observancia para todo el Territorio nacional.

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

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

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

Del artículo antes citado, se desprende que el consentimiento para aceptar derechos y obligaciones puede ser manifestado por medios electrónicos, ópticos o cualquier otra tecnología.

**“Artículo 1832.- En los contratos civiles cada uno se obliga en la manera y términos que aparezca que quiso obligarse, sin que para la validez del contrato se requieran**

formalidades determinadas, fuera de los casos expresamente designados por la ley.”

Conforme a la “pacta sun servanda”, podemos determinar que las personas se obligan en los términos y condiciones que quisieron obligarse; por lo tanto, conforme a una de las fuentes del derecho como lo es la doctrina, si las partes en un contrato manifiestan su voluntad por un medio electrónico como la firma digital y están conformes, dicho acto jurídico produce sus efectos jurídicos.

**“Artículo 1834.-** 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 no sabe firmar, lo hará otra a su ruego y en el documento se imprimirá la huella digital del interesado que no firmó.”

**“Artículo 1834 Bis.-** 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.”

De conformidad a lo establecido en los artículos que anteceden, se desprende que para los actos jurídicos en que se requiera la firma de las partes que intervienen, se tendrá por cumplido con este requisito, siempre y cuando se

utilicen medios electrónicos, ópticos o cualquier otra tecnología, con la condición de que la información generada y comunicada sea atribuible a las personas obligadas y de igual forma sea accesible para consultas posteriores, requisitos que satisface la firma digital generada a partir del certificado digital emitido por una Agencia Certificadora, pues una de sus características es verificar la integridad del documento y la atribución de la información firmada al emisor de dicho documento.

CÓDIGO FEDERAL DE PROCEDIMIENTOS CIVILES  
LIBRO PRIMERO DISPOSICIONES GENERALES  
TÍTULO CUARTO PRUEBA  
CAPÍTULO IX VALUACIÓN DE LA PRUEBA

**“Artículo 210-a.- Se reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología.”**

Para valorar la fuerza probatoria de la información a que se refiere el párrafo anterior, se estimara 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 presentado en su forma original, ese requisito quedara 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 genero por primera vez en su forma definitiva y esta pueda ser accesible para su ulterior consulta.”

De lo anterior se desprende que, además de contar con una certificado digital, con las medidas de seguridad suficientes de conformidad a lo establecido en el artículo 97 del Código de Comercio, es fundamental conservar la información para futuras eventualidades como podría ser un juicio judicial, en el que para acreditar las pretensiones del actor o desvirtuar los hechos por parte del demandado, es indispensable presentar como medio de prueba el certificado digital con el cual se firmó el documento materia del juicio, así como la

información o el mensaje de datos que se firmó, para que al realizar el peritaje correspondiente se determine si la información fue o no alterada y la firma digital estampada en dicho documento corresponde o no al certificado digital y su titular.

Podemos concluir que el certificado digital produce efectos jurídicos, siempre y cuando se reúnan los requisitos de seguridad y tecnológicos, y cuentan con validez legal y fuerza probatoria, en virtud de que un documento que contiene la firma electrónica es susceptible de poder ser consultado y verificar la información con el certificado digital con que se firmó, para poder comprobar si la firma digital generada corresponde al vínculo entre el certificado y el mensaje de datos o documento firmado.

CÓDIGO FEDERAL DE PROCEDIMIENTOS CIVILES  
LIBRO PRIMERO DISPOSICIONES GENERALES  
TÍTULO CUARTO PRUEBA  
CAPÍTULO IX VALUACIÓN DE LA PRUEBA

**“Artículo 210-a.- Se reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología.”**

Para valorar la fuerza probatoria de la información a que se refiere el párrafo anterior, se estimara 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 presentado en su forma original, ese requisito quedara 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 genero por primera vez en su forma definitiva y esta pueda ser accesible para su ulterior consulta.”

Del artículo 210-A del Código Federal de Procedimientos Civiles, tenemos que se reconoce el efecto legal que produce la información transmitida y

firmada por medios electrónicos, ópticos o cualquier otra tecnología, en consecuencia, la información transmitida y firmada a través de un Certificado Digital, como los que emite una Autoridad Certificadora, tiene validez jurídica.

## **CAPÍTULO III**

### **REGULACIÓN DEL COMERCIO ELECTRÓNICO**

La legislación Mexicana se encontraba rezagada en el tema de comercio electrónico, creando un conflicto para reconocer los efectos legales y hacerlos cumplir en las formas modernas de concretar negocios, esto es, por medio del uso de la tecnología como el correo electrónico y documentos digitales, estando México dependiente solo de la forma escrita para llevar a cabo actos jurídicos.

Actualmente en México se está en un proceso hacia una nueva etapa en el comercio, lo cual puede extenderse hacia otros ámbitos de aplicación y modernizar diferentes rubros en la vida cotidiana que conlleve derechos y obligaciones, actos que impliquen el reconocimiento legal dada su naturaleza, que ahora puede ser realizado de un modo electrónico utilizando la tecnología; sin embargo, es un proceso que se está dando y que trae aparejado una modernización en la legislación, a efecto de que no se deje a la interpretación sino que se contemple la figura de realizar cualquier acto de forma electrónica.

Para llevar a cabo la modernización antes referida, México ha comenzado a reformar la legislación, lo que lleva un gran e importante esfuerzo para asegurar y garantizar las transacciones comerciales.

Uno de los grandes pasos en esta materia, se dio con las reformas realizadas a nuestro Código Civil Federal, Código de Procedimientos Civiles y Código de Comercio en el año 2000, con lo cual se provee de reconocimiento a los medios ópticos y electrónicos, así como cualquier tecnología, por virtud de la cual una persona puede manifestar su consentimiento en un acto jurídico, además

de las formas escrita, oral o signos inequívocos que ya eran regulados por la legislación.

En las reformas a la legislaciones encargadas de regular los actos jurídicos para poder dotar de valor legal a los que se realicen utilizando los medios electrónicos, fue necesario primero dotar de seguridad en el uso de la tecnología, protegiendo no sólo los datos personales, confidenciales o información privilegiada para evitar algún peligro si fuera interceptada por otra persona que no fuera el destinatario, lo que se logró utilizando los certificados digitales, mismos que ya se describieron en capítulos anteriores y que dada su complejidad algorítmica de seguridad, proveen de confianza a los usuarios al enviar y recibir información, que aunado a la seguridad, confirman el vínculo existente entre el emisor de determinada información y el firmante, lo que da fuerza legal tanto por equivalencia funcional como por el reconocimiento legal; la firma electrónica avanzada es aceptada como expresión de la voluntad y como medio de prueba ante los tribunales judiciales.

### **3.1. REFORMAS EN EL CÓDIGO CIVIL FEDERAL**

El Código Civil ha tenido reformas en materia del uso de la tecnología en la celebración de actos jurídicos, regulando de esta forma los aspectos que pudieran surgir a partir de esta práctica. De tal modo que, actualmente en el Código Civil existe la figura de uso de medios electrónicos o alguna otra tecnología como un mecanismo para manifestar la voluntad con reconocimiento plena por parte de la legislación, produciendo todos los efectos legales que como si se tratara de un documento físico o de una firma autógrafa.

El artículo 1834 del Código Civil Federal, establece que en los casos en que la ley determine como requisito, que un acto jurídico deba otorgarse por escrito y además deba contener las firmas de los interesados o las partes involucradas, se tendrá por cumplido si para tal efecto se utilizaron medios electrónicos, ópticos o alguna otra tecnología, siempre que la información

generada o comunicada en forma íntegra a través de dichos medios, pueda atribuirse a las partes que intervinieron, siendo que dicha información sea accesible para consultas posteriores:

El Código Civil Federal ha sido reformado en su contenido, en lo que se refiere a distintos aspectos relativos a la Firma Electrónica Avanzada y sus efectos jurídicos. Estas reformas tienen impacto no solo en cuanto a que la Firma Electrónica Avanzada es reconocida por la ley y se le confieren los mismos efectos legales que a la Firma Autógrafa, en virtud de que, por equivalencia funcional, es utilizada la primera en sustitución por la segunda con la ventaja de ser más segura.

El artículo 1803 del ordenamiento mencionado en el párrafo anterior, regula lo referente al consentimiento, manifestando la: posibilidad de que el consentimiento puede ser expreso o tácito. Expreso: “cuando la voluntad se manifiesta verbalmente, por escrito, por medios electrónicos, ópticos o cualquier otra tecnología, o por signos inequívocos”

A su vez el artículo 1805 del Código Civil Federal, señala que cuando la oferta se hace entre presentes, sin plazo de aceptación, el oferente queda desligado si la aceptación no es inmediata, y esta regla se aplicará a la oferta hecha por teléfono o por cualquier otro medio electrónico, óptico o de cualquier otra tecnología que permita la expresión de la oferta y la aceptación de ésta de forma inmediata.

## CÓDIGO CIVIL FEDERAL.

### **Forma**

**“Artículo 1832.-** En los contratos civiles cada uno se obliga en la manera y términos que aparezca que quiso obligarse, sin que para la validez del contrato se requieran

formalidades determinadas, fuera de los casos expresamente designados por la ley.”

“**Artículo 1833.-** Cuando la ley exija determinada forma para un contrato, mientras que éste no revista esa forma no será válido, salvo disposición en contrario; pero si la voluntad de las partes para celebrarlo consta de manera fehaciente, cualquiera de ellas puede exigir que se dé al contrato la forma legal.”

“**Artículo 1834.-** 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 no sabe firmar, lo hará otra a su ruego y en el documento se imprimirá la huella digital del interesado que no firmó.”

“**Artículo 1834 Bis.-** 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.”

Tal y como se aprecia en los artículos anteriores, del Código Civil Federal, tenemos que con fundamento en el artículo 1832, también conocida como pacta Sun Servanda, las partes se obligan en los términos y en la forma en que quisieron obligarse, incluyendo si acordaron el uso de la tecnología para celebrar algún acto jurídico. Adicionalmente, se determina que cuando la ley exija la forma escrita, esta formalidad se entenderá por satisfecha si se utilizan los medios electrónicos, ópticos o cualquier otra tecnología.

Tiene gran trascendencia en materia Civil, el artículo 1834 del Código Civil Federal, en el cual se establece que cuando la Ley exige como formalidad en un acto jurídico que éste debe ser por escrito y contener las firmas de las partes involucradas, estos requisitos se tendrán por cumplidos mediante el uso de medios electrónicos, ópticos o cualquier otra tecnología, siempre que la información que se generó y que es transmitida por estos medios, debe estar íntegra, ser atribuible a las partes que se están obligando y ser posible realizar su ulterior consulta. Estos requisitos se cumplen con la utilización de los certificados digitales, que como ya se señaló en el Capítulo anterior, garantiza la seguridad en el envío y recepción de información.

Las reformas y adiciones al Código Civil Federal se centraron en el reconocimiento a la celebración de actos jurídicos a través de medios electrónicos, ópticos o de cualquier otra tecnología, añadiéndose los “medios tecnológicos” como medio idóneo para expresar el consentimiento. Es importante resaltar que se estableció una equivalencia funcional entre el consentimiento expresado por medios tecnológicos y la firma autógrafa “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”.

### **3.2. REFORMAS EN EL CÓDIGO DE PROCEDIMIENTOS CIVILES**

El Código de Procedimientos Civiles Federal, fue modificado por los legisladores, con el objeto de regular los aspectos que pudieran surgir de un litigio, en donde las pruebas en las que el Juzgador se basará para condenar o absolver al demandado se relacionen con los Certificados Digitales y la Firma Electrónica Avanzada, es decir, la legislación Civil procesal contempla en la parte probatoria de los procedimientos judiciales, a los mensajes de datos como elemento importante que en el desahogo de pruebas el Juez deberá analizar para determinar su resolución, dado que tiene validez jurídica.

Para esto, la legislación procesal prevé la forma en que el Juez, que conoce de determinado asunto, debe valorar diversos aspectos, como la fiabilidad del Certificado Digital, es decir, que se haya emitido por una Autoridad Certificadora autorizada para fungir como tal, así como los mecanismos utilizados en la generación de el Certificado, la forma en que el documento electrónico se generó, se archivo o almacenó, o en su defecto, se insertó en otro documento.

***“Artículo 210-A***

**Se reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología.**

Para valorar 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.”

De las reformas realizadas en el Código Procesal en Materia Civil, lo más importante es que se facultará a los Tribunales encargados de dirimir alguna controversia para dar el debido valor probatorio a los mensajes de datos, la firma electrónica y al certificado digital, cuidando siempre que se cumplan los requisitos necesarios establecidos, por la ley para garantizar la seguridad en la información que se envía, se transmite y se almacena.

Mientras que anteriormente los Tribunales encargados de solucionar un litigio, consideraban dentro de la clasificación de prueba documental a los documentos físicos públicos o privados como medio de prueba, en adelante

deberá cambiar esa perspectiva en el sistema de impartición de Justicia, aceptando también documentos electrónicos.

Se reconoce en el Código Federal de Procedimientos Civiles como prueba, la información contenida en los medios electrónicos, ópticos o en cualquier otra tecnología, dando una serie de reglas para su valoración por parte del juzgador: La fiabilidad del método para generar, comunicar, recibir o archivar la información (que pueda conservarse sin cambio), su atribución a las personas obligadas y la posibilidad de acceder a ella en ulteriores consultas. Asimismo y para que la información generada, comunicada, recibida o archivada por medios electrónicos se considere como original (para su conservación o presentación) deberá acreditarse que dicha información 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

### **3.3. REFORMAS EN EL CÓDIGO DE COMERCIO**

Las reformas hechas al Código de Comercio dieron lugar a un nuevo capítulo en su contenido denominado “Del Comercio Electrónico”. La introducción de este capítulo presentado por los legisladores, tiene como finalidad reconocer el significado del mensaje de datos y la forma en que se relaciona con los medios de prueba de la tecnología. Se establece en el artículo 89 que a la información generada, enviada, recibida, archivada o comunicada a través de dichos medios, se denominará mensaje de datos.

**“Artículo 89.**

...

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

...”

**“Artículo 89 bis**

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.”

En este sentido, el artículo 90 reformado considerará que un mensaje de datos se presume proviene del emisor, cuando ha sido enviado usando medios de identificación como claves o contraseñas, o cuando ha sido enviado por un sistema de información programado por el emisor o en su nombre para que opere automáticamente.

**“Artículo 90**

Se presumirá que un Mensaje de Datos proviene del Emisor si ha sido enviado:

- I. Por el propio Emisor;
- II. 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
- III. Por un Sistema de Información programado por el Emisor o en su nombre para que opere automáticamente.”

La primera hipótesis bien podría atender problemas de tarjetas de crédito y el cumplimiento forzoso de los contratos relativos, bastante común en México, hasta hace poco. El segundo caso podría ayudar a compradores mediante la sanción de ventas hechas automáticamente, por medio de un sitio Web a través del Internet, y no respetadas.

De las reformas en el ámbito comercial más relevantes, podemos mencionar las siguientes:

## REFORMAS AL CÓDIGO DE COMERCIO

- Reformas al Código de Comercio en materia de firma electrónica publicadas el 29 de agosto del 2003 en el D.O.F.
- Reformas al Código de Comercio en materia de firma electrónica publicadas el 29 de mayo del 2000 en el D.O.F.

## REGLAMENTOS Y REGLAS

- Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación (Publicado el 19 de julio del 2004 en el D.O.F.)
- Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación (Publicadas el 10 de agosto del 2004 en el D.O.F.)
- ACUERDO que modifica las Reglas Generales a las que deberán sujetarse los prestadores de servicios de certificación (Publicado el 5 de marzo del 2007 en el D.O.F.)

### **3.4. REFORMAS EN OTRAS LEGISLACIONES**

De conformidad con la legislación mexicana, vigente y aplicable, tenemos que la información enviada de manera electrónica, así como la firma electrónica generada a partir de el Certificado Digital, emitido por una Autoridad Certificadora, tiene validez jurídica, esto en virtud de que satisface todos los requisitos de confidencialidad, autenticidad, integridad y no repudiación de la información, que establece la ley.

El Banco de México, conforme al artículo 24 de la Ley de dicha Institución, tiene la facultad de expedir disposiciones de carácter general, es decir, de aplicación para todo el territorio nacional mexicano, con base en esta facultad;

el Banco de México por medio de la Circular TELEFAX 6/2005, con el propósito de otorgar mayor seguridad a las operaciones financieras, implementó la Infraestructura Extendida de Seguridad, cuya función principal es verificar las firmas electrónicas mediante la expedición de certificados digitales y administración.<sup>56</sup>

## LEY DEL BANCO DE MÉXICO

“**ARTICULO 3o.-** El Banco desempeñará las funciones siguientes:

**I. Regular la emisión y circulación de la moneda, los cambios, la intermediación y los servicios financieros, así como los sistemas de pagos;**

II. Operar con las instituciones de crédito como banco de reserva y acreditante de última instancia;

III. Prestar servicios de tesorería al Gobierno Federal y actuar como agente financiero del mismo;

IV. Fungir como asesor del Gobierno Federal en materia económica y, particularmente, financiera;

V. Participar en el Fondo Monetario Internacional y en otros organismos de cooperación financiera internacional o que agrupen a bancos centrales, y

VI. Operar con los organismos a que se refiere la fracción V anterior, con bancos centrales y con otras personas morales extranjeras que ejerzan funciones de autoridad en materia financiera.”

“**ARTÍCULO 24.- El Banco de México podrá expedir disposiciones sólo cuando tengan por propósito la regulación monetaria o cambiaria, el sano desarrollo del sistema financiero, el buen funcionamiento del sistema de pagos, o bien, la protección de los intereses del público.** Al expedir sus disposiciones el Banco deberá expresar las razones que las motivan.

**Las citadas disposiciones deberán ser de aplicación general,** pudiendo referirse a uno o varios tipos de intermediarios, a determinadas operaciones o a ciertas zonas o plazas.

---

<sup>56</sup> <http://www.banxico.org.mx/tipo/disposiciones/marconormativo/LeyBM/TextoVigente.html>. 2009

Las sanciones que el Banco imponga conforme a lo previsto en los artículos 27, 29 y 33, deberán tener como objetivo preservar la efectividad de las normas de orden público establecidas en la presente Ley y, de esta manera, proveer a los propósitos mencionados en el primer párrafo de este precepto. “

De esta forma, El Banco de México en ejercicio de las facultades que la ley le confiere, diseñó y administra un sistema denominado Infraestructura Extendida de Seguridad (IES) con el objetivo de brindar de una mayor fortaleza e incrementar la seguridad en la transmisión de de la información enviada y recibida tanto en los sistemas de pago como entre el sistema financiero y la Banca Central.

Esta Infraestructura Extendida de Seguridad del Banco de México se basa en el uso de Certificados Digitales para poder firmar digitalmente la información enviada y recibida, mediante la aplicación de algoritmos criptográficos para garantizar la confidencialidad e integridad de la información transmitida a de esta al mismo tiempo que se acredita la identidad del emisor y el receptor de dicha información.

**“ARTICULO 68.- La Ley de Instituciones de Crédito, la legislación mercantil, los usos bancarios y mercantiles y el Código Civil para el Distrito Federal, en Materia Común, y para toda la República en Materia Federal, se aplicarán a las operaciones del Banco, supletoriamente a la presente Ley y en el orden en que están mencionados.”**

Así mismo se reformó la Ley Federal de Protección al Consumidor para reconocer la utilización de medios electrónicos, ópticos o cualquier otra tecnología en la instrumentación de las operaciones que celebren los proveedores con los consumidores, dando las bases sobre las cuales habrán de realizarse dichas operaciones (confidencialidad, certeza, seguridad en la información proporcionada al consumidor, etc.), previendo sanciones administrativas (acaso

las mas altas) para el caso de que los proveedores no cumplan con dichas disposiciones.

La Ley Federal de Procedimiento Administrativo regula las actuaciones y procedimientos del Poder Ejecutivo Federal (dependencias y organismos descentralizados de la Administración Pública Federal). Reformada el 30 de mayo del 2000, habilita el empleo de medios electrónicos para llevar a cabo algunos procedimientos administrativos de gestión:

- Notificaciones, citatorios, emplazamientos, requerimientos, solicitud de informes, documentos y resoluciones administrativas, entre otros, cuando así lo haya aceptado expresamente el promovente y siempre que pueda comprobarse fehacientemente la recepción de los mismos
- Las promociones o solicitudes que los particulares presenten, en las etapas que las propias dependencias y organismos así lo determinen mediante reglas de carácter general, empleando medios de identificación electrónica tendrán el mismo valor probatorio que los firmados en forma autógrafa

El uso de dichos medios de comunicación electrónica será optativo para cualquier interesado, incluidos los particulares que se encuentren inscritos en el Registro de Personas Acreditadas

La certificación de los medios de identificación electrónica del promovente, así como la verificación de la fecha y hora de recepción de las promociones o solicitudes y de la autenticidad de las manifestaciones vertidas en las mismas, deberán hacerse por las dependencias u organismos descentralizados, bajo su responsabilidad y de conformidad con las disposiciones generales.

El Acuerdo "Tramitanet" publicado en el DOF el 17 de enero del 2002 por la Secretaría de Contraloría y Desarrollo Administrativo, tiene por objeto

la certificación del medio de identificación electrónica que utilicen los particulares en los trámites electrónicos que realicen; La verificación de la fecha y hora de recepción de las promociones y solicitudes formuladas a través de medios de comunicación electrónica (marca de tiempo o sello digital); La comprobación de la autenticidad de las manifestaciones vertidas en dichas promociones o solicitudes, y las notificaciones, citatorios, emplazamientos, requerimientos, solicitudes de informes o documentos y las resoluciones administrativas que emitan por medios electrónicos, relacionados con el trámite electrónico promovido por el particular.

En el acuerdo se establece también que se utilizará un sistema de encriptación de clave pública para generar el certificado digital y dos tipos de certificación; básica y de alta seguridad, dependiendo de la necesidad o no de la presencia física del particular o su representante para acreditar identidad, existencia legal y facultades de su representante, en su caso, los cuales podrán ser emitidos por las dependencias u organismos descentralizados de la Administración Pública Federal (Entidad Certificadora), que estuvieren autorizadas para ello por la Secretaría de la Contraloría y Desarrollo Administrativo (Autoridad Certificadora Central) , previa solicitud de los interesados.

Cada dependencia interesada en fungir como Entidad Certificadora, debe declarar en un documento a disposición de los interesados las prácticas de certificación adoptadas (Tipos de certificación que emitan, trámites en los que podrán ser utilizados los certificados expedidos, métodos para identificar al titular del certificado, mecanismos que permitan al titular verificar su propio certificado, procedimientos para emitir y consultar la lista de certificados revocados, procedimientos de auditoría establecidos, mecanismos de custodia de identificación electrónica e impresa).

El acuerdo presidencial de la comisión intersecretarial para el desarrollo del gobierno electrónico publicado en el DOF el 9 de Diciembre del 2005 por la Secretaría de la Función Pública, tiene por objeto promover y consolidar el uso y aprovechamiento de las tecnologías de la información y comunicaciones, mediante la adecuada coordinación de las acciones propuestas

por la Secretaría de la Función Pública con las dependencias de la Administración Pública Federal y a través de éstas con las entidades paraestatales.

De igual forma el 9 de diciembre del 2005 se publicó en el Diario Oficial de la Federación el Acuerdo Presidencial para la creación de la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico, mismo que constituyó a la Subcomisión de Firma Electrónica Avanzada (FEA) con la finalidad de que exista una adecuada coordinación y homologación de los procesos de emisión y operación de Certificados Digitales de FEA.

Esta Subcomisión está integrará por el Servicio de Administración Tributaria (SAT), la Secretaría de Economía (SE) y por la Secretaría de la Función Pública (SFP). Actualmente la presidencia de esta Subcomisión es presidida por la Secretaría de la Función Pública y su objetivo principal es establecer los Lineamientos para la homologación, implantación y uso de la FEA en la Administración Pública Federal.

Los principales objetivos de esta Subcomisión son los siguientes:

- El reconocimiento de los certificados digitales de FEA por todas las Dependencias y Entidades de la Administración Pública Federal, independientemente de la Autoridad Certificadora que los haya emitido.
- Alineación de las estrategias de emisión y uso de certificados digitales de FEA del Gobierno Federal y aprovechamiento de la infraestructura tecnológica que actualmente está operando en la SFP, SE y el SAT.
- Simplificación del uso y aplicación de la FEA en los procesos del Gobierno Federal.

En este sentido, tenemos que la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico tiene las siguientes principales responsabilidades a su cargo:

- Coordinar con la Secretaría de Gobernación, por medio de la Dirección General del Registro Nacional de Población e Identificación Personal RENAPO, los mecanismos de registro e identificación de las personas, así como los procedimientos de certificación electrónica de identidad.
- Emitir el dictamen de acreditación para la integración de una AC a la ITFEA para el reconocimiento de sus certificados digitales.
- Promover la instrumentación y aplicación de los lineamientos en la Administración Pública Federal.
- Establecer las condiciones técnicas que permitan el reconocimiento de los certificados digitales de FEA y la interoperabilidad entre las Dependencias que conforman la Subcomisión.
- Emitir los lineamientos para la homologación, implantación y operación de la FEA en la Administración Pública Federal.
- Promover la celebración de acuerdos de colaboración con otras Instituciones Públicas y/o Privadas para el desarrollo de la ITFEA.

## **CAPÍTULO IV**

### **HOMOLOGACIÓN DE LOS DISTINTOS CERTIFICADOS DIGITALES**

Las transacciones electrónicas en México han encontrado el desarrollo de una regulación jurídica, la cual les otorga la seguridad necesaria para el impulso y perfeccionamiento de los negocios electrónicos en nuestro país.

Aunque de manera tardía, pero finalmente nuestro país se ha sumado al proceso de legalizar y darle viabilidad a la firma electrónica; sin embargo, ahora queda pendiente el desarrollo de la factura electrónica y su vinculación a la contabilidad. El pasado 29 de agosto de 2003, se estableció el antecedente más importante en esta materia al marcar una actualización en la legislación mexicana en relación con la forma como las nuevas tecnologías han modificado el derecho mercantil y la interacción en la sociedad.

A pesar de las reformas que reconocen la validez jurídica de la firma electrónica, las empresas de nuestro país requerían de la motivación para cambiar la forma de hacer negocios y poner en práctica las nuevas tecnologías en su “portafolio” de estrategias de negocio; además, hacía falta un impulso en materia fiscal que permitiera llevar a la práctica conceptos plasmados en la ley mercantil, tales como: firma electrónica, certificado digital, contratos electrónicos, etc.

En este sentido, el Sistema de Administración Tributaria (SAT) desarrolla la estructura y la función de la firma electrónica a través de Internet con el proyecto e-firm, mismo que se pondrá en operación en el año 2005; éste proporcionará un certificado digital, con el cual los contribuyentes tendrán la posibilidad de usar la tecnología electrónica para cumplir con sus obligaciones fiscales. Se prevé que la puesta en marcha del uso de los medios electrónicos

facilite la realización del pago de impuestos; por ejemplo, al enviar las declaraciones fiscales o realizar consultas al SAT por parte de las personas morales.

Es claro que la política fiscal planteada por la Secretaría de Hacienda y Crédito Público (SHCP), está apostando a las nuevas tecnologías para reducir el índice de evasión fiscal, aumentar la recaudación y agilizar el intercambio de información; muestra de ello es que para el próximo año, el SAT se prepara para el funcionamiento de la factura electrónica y la posibilidad de llevar la contabilidad a través de los sistemas digitales, utilizando en estos procesos la firma electrónica basada en criptografía asimétrica y el uso de la llave pública y privada.

En un estudio de Gartner, se muestra que los costos de operación descienden a 50%, pues la utilización de la factura tradicional conlleva un gasto de 80 centavos de dólar estadounidense, frente a 35 centavos que implica el uso de comprobantes fiscales electrónicos.

A pesar de las reformas en los códigos civiles, procesales, de comercio, fiscal y la realización de los diferentes proyectos por parte del gobierno, prevalece una incertidumbre al omitir de las regulaciones una figura como la firma electrónica avanzada única para todas las operaciones, no sólo las tributarias. Hasta ahora, la firma electrónica avanzada es empleada por: la SHCP; la Secretaría de la Función Pública la esgrime para efectuar las declaraciones patrimoniales de los funcionarios de la Administración Pública Federal; por su parte los Registros Públicos de la Propiedad y del Comercio la operan con el propósito de que sus empleados capturen información en el programa de cómputo de gestión de registros públicos (SIGER); además, las dependencias de la Administración Pública y los notarios públicos y corredores públicos pueden emitir certificados de firmas electrónicas, principalmente de aquéllas empleadas en el extranjero.

En cuanto al proceso de certificación que se llevará a cabo ante el SAT, es importante resaltar la participación y responsabilidad de los altos mandos

de las empresas en los trámites fiscales a través de medios electrónicos, pues el proceso de certificación requiere de la comparecencia de los representantes legales que cuenten con facultades para realizar actos de administración o de dominio de las empresas a las cuales representan, mismas que no deben ser tomadas a la ligera, ya que este tipo de apoderados será el único que podrá presentar declaraciones o promociones; también en el proceso de emisión de facturas electrónicas serán ellos quienes podrán obtener los sellos digitales que hace las veces de firma electrónica para su empleo en las facturas.

Una de las ventajas del uso de la firma electrónica en las facturas es que impide la violación o alteración de los datos, en particular del sello digital, puesto que se encuentra protegido por mecanismos criptográficos, es decir, una serie de procesos matemáticos que garantizan la fiabilidad y la seguridad de los datos. Al recibir una factura electrónica, el cliente podrá reconocer su validez mediante un proceso de autenticación que deberá tener desarrollado; así, sabrá si el documento es auténtico o tuvo alteraciones, o si la firma corresponde o no al emisor.

Se prevé que en el lapso de cinco años aproximadamente, el sector empresarial emitirá facturas electrónicas, debido a que será una obligación fiscal; sin embargo, es necesario considerar que se trata de una modificación sustancial de los procesos de negocio, dada la incidencia de la relación costo-beneficio.

Por ello, las empresas deberán cumplir con los requisitos y procedimientos establecidos por el Banco de México, el SAT, la Secretaría de Economía y cuidar su perfecta operación desde el punto de vista fiscal, legal y tecnológico; de no hacerlo, se estarían incumpliendo las obligaciones fiscales, con la consecuente responsabilidad legal, contractual, entre otras.

Por último, cabe destacar que la responsabilidad de expedir facturas fiscales electrónicas por la inclusión del sello digital, es idéntica a la de la firma electrónica avanzada, esto es, tendrá las mismas consecuencias jurídicas por el uso de la firma electrónica, incluso penales, del titular del certificado que ampara la firma electrónica.

#### 4.1. EL USO DEL CERTIFICADO DIGITAL Y FIRMA ELECTRÓNICA AVANZADA

Internet ha transformado al mundo. Gracias al desarrollo de las **Tecnologías de la Información y Comunicación (TICs)**, el tiempo y la distancia dejan de ser obstáculos. Las redes mundiales de información, como Internet, no conocen fronteras y ello supone la expansión y diversificación de los mercados mundiales.

Al nacer el comercio electrónico nace también una alternativa de reducción de costos y una herramienta fundamental en el crecimiento de las líneas de venta. Sin embargo adquiere mayor relevancia la seguridad informática y la imputabilidad de actos a través de medios electrónicos.

Actualmente, se ha comenzado a adoptar la firma electrónica avanzada (FEA) por los grandes beneficios que proporciona, sobre todo por garantizar la integridad y autenticidad de la información.

La legislación establece que para que un mensaje de datos pueda considerarse legalmente válido, es necesario asegurar que la información en él contenida reúna las siguientes características: Integridad, Autenticidad y No Repudio, cualidades otorgadas por la FEA lo que le permite tener una equivalencia funcional a la firma autógrafa.

Estos tres elementos, en adición a la confidencialidad, son proporcionados por una tecnología denominada Infraestructura de Llave Pública (PKI) la cual utiliza procesos matemáticos complejos que hasta este momento se considera mundialmente como una opción de alta seguridad.

Los factores que hacen posible la Firma Electrónica Avanzada son, entre otros, la oportunidad en la información, tanto en la recepción como en el envío, el ahorro en el consumo de papel, una importante reducción de la probabilidad de falsificación, el tener procesos administrativos más rápidos y

eficientes, y la posibilidad de encontrar la información requerida de manera ágil y efectiva.

Las empresas ya no necesitarán de costosas bodegas para almacenar documentos históricos, y podrán dar usos más productivos a esos espacios, al tiempo que se obtiene mayor seguridad en el resguardo de los documentos y se facilitan los procesos de auditoría.

Esto es sólo el principio, porque, una vez que las empresas comiencen a operar con documentos electrónicos, se verán incentivadas a digitalizar otros documentos, logrando eficiencia y ahorro en otras áreas de la empresa, lo que a la larga, la hará más productiva pues, en el proceso de sustituir el papel por los datos electrónicos, tendrá que hacer una revisión de sus procesos de negocios.

El gobierno también se ve beneficiado con la proliferación del uso de la factura electrónica, pues el control tributario se incrementa. Para el gobierno, la factura electrónica representa beneficios significativos, pues permite un mayor control del cumplimiento tributario y simplificación de la fiscalización, lo cual se traduce en una mayor eficiencia recaudatoria.

Por mencionar un ejemplo en donde es utilizada la Firma Electrónica Avanzada, la factura electrónica coloca a México en una mejor posición para enfrentar la competencia global. Nos permite, como país, estar mejor preparados para tratar con las empresas de los países con los que hemos firmado tratados comerciales y en los que ya se usa de manera extensa la factura electrónica, impulsando así el comercio electrónico. Cabe mencionar que, en América Latina, Chile ha sido el pionero en la introducción de los comprobantes fiscales electrónicos, a partir del 2002.

En fin, que ya es una realidad. Ahora podemos “firmar” documentos de manera segura y confiable desde una computadora. Gracias a la Firma Electrónica Avanzada (FEA) es posible realizar diversos trámites ante el SAT sin

tener que asistir a sus oficinas, con un considerable ahorro de tiempo, utilizando cualquier computadora que tenga acceso a Internet.

Para que una firma electrónica avanzada sea válida ante el SAT, es necesario identificar debidamente al usuario y establecer cuál será su firma electrónica avanzada. El usuario la crea, utilizando una aplicación (SOLCEDI) localizada dentro del portal del SAT, y después debe presentarse, ante esa dependencia, para obtener un certificado digital que compruebe que ese usuario es el dueño de la Firma.

Para el organismo recolector de recursos para financiar al gobierno, entre los beneficios de la firma electrónica se cuenta que ahora es posible elaborar las declaraciones de impuestos por medios electrónicos de una forma más sencilla y segura. Para el SAT, los documentos firmados electrónicamente tienen las mismas funcionalidades y garantías de un documento físico, mayor seguridad en las transacciones de comercio electrónico y con la ventaja de reducir el uso de papel en los sectores público y privado. Gracias a sus características de no repudio y de autenticidad, el organismo puede brindar mayor certeza jurídica a los contribuyentes en sus transacciones.

El Certificado Digital puede ser utilizado para diversas aplicaciones, si bien es cierto en el Comercio Electrónico tiene por ahora una mayor utilidad, no es el único ámbito de aplicación.

Como ya se revisó anteriormente, el Certificado Digital vincula al Titular del Certificado con la Firma Electrónica y al Documento Firmado; sin embargo, existen un sin número de aplicaciones como enviar información de forma confidencial, y autenticar la identidad de una persona que envía un mensaje de datos que contiene cualquier información.

Si una persona requiere un medicamento controlado y por alguna razón el médico o el paciente no están en el mismo lugar, el paciente no tendría otra opción más que se realice otra receta médica debidamente firmada por el médico, lo que podría repercutir en la salud y ocasionar un problema más grave al

no suministrarse el medicamento en tiempo. Mediante el uso del Certificado Digital, el médico podría enviar una receta digital firmada electrónicamente con el uso de su certificado; de esta forma, independientemente del lugar en el que se encuentren, se puede contar con la receta médica para comprar el medicamento.

Otro ejemplo es el envío de Estados de Cuenta Bancarios, u otro servicio como telefónico, televisión de paga y demás servicios que requieran el envío de dichos documentos que actualmente se envían en documentos de papel y de los cuales sólo algunos son enviados digitalmente a correos electrónicos pero no cuentan con validez jurídica, y que de ser firmados digitalmente, contarían con validez jurídica representando un ahorro en papel, además de contribuir a una cultura ecológica de cero papel.

Para las empresas representaría un ahorro económico considerable en la emisión y entrega de facturas por los servicios prestados, dado que en la actualidad se debe imprimir al menos tres facturas y utilizar un servicio de mensajería; en caso de que el envío deba realizarse al interior de la República, los costos y tiempos de entrega podrían ser muy altos, los cuales pueden ser suplidos con la facturación digital. Esto se debe a que se pueden generar facturas digitales firmadas electrónicamente y ser enviadas por medio del uso de tecnología como el correo electrónico, o implementando terminales específicas para la impresión de documentos con validez jurídica, con la garantía que el Certificado proporciona como es la integridad en el documento, no repudiación y confidencialidad.

Dependiendo del volumen de las empresas, el ahorro por concepto de administración de facturas (recepción, almacenaje, búsqueda, firma, devolución, pago, envío, etc.) puede fluctuar entre el 40% y el 80%. Entre los motivos que hacen esto posible este ahorro se encuentran:

- Oportunidad en la información, tanto en la recepción como en el envío.
- Ahorro en el gasto de papelería.

- Facilidad en los procesos de auditoría.
- Mayor seguridad en el resguardo de los documentos.
- Menor probabilidad de falsificación.
- Agilidad en la localización de información.
- Eliminación de bodegas para almacenar documentos históricos.
- Procesos administrativos más rápidos y eficientes.

Una vez que las empresas empiecen a operar con esta tecnología, se verán incentivadas a digitalizar otros documentos, logrando eficiencia y ahorro en otras áreas de la empresa.

Con la factura electrónica, el control tributario se incrementa, pues la factura electrónica representa beneficios significativos, pues permite un mayor control del cumplimiento tributario y simplificación de la fiscalización, lo cual se traduce en una mayor eficiencia recaudatoria. Como referencia, en América Latina, sólo Chile ha introducido los Documentos Tributarios Electrónicos, a partir del 2002.

Otro aspecto en que las empresas pueden ser beneficiadas es en el pago de la nómina, donde sobre todo para las empresas medianas y grandes, o aquellas que tienen sucursales en distintos puntos de la República Mexicana, y que ocupan parte de su capital en el envío y devolución de recibos de nómina, para contar con un documento que ampare el cumplimiento de la obligación patronal. Si consideramos a las grandes empresas que tienen un número de personal elevado, en consecuencia resultará más costoso la elaboración de recibos de nómina físicos, la entrega y la devolución, además del personal que tendrían ocupado en dicha actividad, siendo que adicionalmente deben gastar en almacenar grandes cantidades de documentos, lo que debe realizarse cada mes, posiblemente recurran a la omisión de este documento, teniendo constantemente

el riesgo de que sean demandados por falta de pago y no contar con un documento que acredite el pago, y en juicio probar que si se realizó el pago correspondiente.

Se puede tener un certificado digital que nos identifique y autentique para ingresar de manera remota a computadoras, correos electrónicos y diversas aplicaciones que requieran de una contraseña, la cual puede ser reemplazada por un certificado digital para identificarse y acceder a dichas aplicaciones, haciendo más seguro el contenido de la información almacenada.

Como podemos apreciar, el uso del Certificado Digital no es limitativo, pues al ser un medio de identificación y autenticación, es un medio de manifestación de voluntad y aceptación del contenido del documento firmado, el cual es reconocido jurídicamente, atribuyéndole efectos legales; es posible utilizarlo en un sin número de aplicaciones y en un futuro con el desarrollo de la tecnología utilizarlo para realizar elecciones, las cuales podrían ser más seguras con el uso de el Certificado Digital, siendo que las personas puedan identificarse y seleccionar al candidato de su elección, obteniendo un resultado instantáneo, con la certeza del número de votantes exacto e identificables, eliminando cualquier posible fraude o falsificación, descartando el uso de papel y optimizar tiempos. Así mismo, sería posible insertar Certificados Digitales mediante el uso de chips en credenciales de identificación y licencia de manejo, con el objetivo de identificar a una persona.

En una tarjeta de crédito se podría insertar el certificado digital para asegurar la identidad de quien la utiliza, eliminando así los fraudes o uso de tarjetas robadas y clonadas. Gracias al Certificado Digital, el cajero automático puede verificar la autenticidad de la tarjeta, pues una tarjeta clonada o alterada no sería reconocida, validada y autenticada sin la presencia del Certificado Digital, lo que representa mayor seguridad tanto para las personas como para las Instituciones Bancarias, donde ambas partes pierden cantidades de dinero por la delincuencia.

Este mecanismo de seguridad permite evitar distintos riesgos asociados a las transacciones con tarjetas crédito en Internet. El más importante es, sin dudas, el de la falsificación o clonado de sitios, mediante el cual la persona ingresa los datos de su *tarjeta crédito* en una Web que simula ser la de una empresa conocida en el mercado, pero que en realidad es un sitio montado en la red por piratas informáticos. La existencia del certificado digital posibilita evitar este tipo de engaños.

El otro gran inconveniente son los denominados datos abiertos. Cuando se efectiviza una transacción con tarjetas crédito, el cliente debe aportar en algún momento los datos de su cuenta, e incluso facilitar su clave personal. En sistemas de datos abiertos, no existe ninguna protección que garantice que la información que viaja por la red no pueda ser interceptada en algún momento. En cambio, con los certificados digitales y los mecanismos de seguridad anexos esto no puede suceder.

Incluso suelen habilitarse claves de sesión únicas, que sirven con exclusividad para realizar una operación determinada. Esto permite garantizar la privacidad del tráfico de información en el momento de la compra, con un password que conoce únicamente el cliente.

Respecto a los celulares, podría almacenarse certificados digitales que identifiquen y autenticuen al propietario del teléfono móvil, asegurando que en caso de hacer un mal uso de dicho dispositivo, se conocerá la identidad del propietario, o incluso, por medio del uso de tecnología como el bluetooth, transmitir el certificado digital para identificarse en cualquier lugar con receptor; así, al ingresar a un área que requiera identificación como edificios, empresas, dependencias de gobierno, no sería necesario llenar formularios y dejar identificaciones, sino que con el envío del certificado digital, en segundos se podría verificar en una computadora la identidad de la persona permitiendo o negando el acceso.

En trámites judiciales, por ejemplo en los Juzgados, se puede implementar la revisión de expedientes por medios tecnológicos mediante el uso de el Internet, obteniendo la certeza de que cualquier resolución que un Juzgador emita es firmada digitalmente por el Juez y su Secretario, lo que le atribuye la validez jurídica requerida y que además es enviada por correo electrónico encriptado para que sólo el receptor pueda abrir el documento, sin tener que utilizar papel ni asistir físicamente al juzgado para revisar el expediente, esto podría ser enviado a una cuenta de correo electrónico previamente autorizado por las partes. De la misma forma, se podrían presentar todo tipo de promociones y escritos, electrónicamente firmados digitalmente, por la parte interesada o el abogado autorizado sin que resulte necesario asistir físicamente a la oficialía de partes para presentarla. Así se optimizan tiempos, se contribuye con la conciencia ecológica y es más seguro el sistema judicial. Esto representa un cambio radical, incluso en la cultura; en los escritos presentados además debería adicionarse en la parte de las autorizaciones, la facultad de enviar y recibir todo tipo de notificaciones electrónicas, señalando no solo un domicilio sino un correo electrónico para tales efectos.

El Certificado Digital como medio de identificación, además de ser un medio para crear la firma electrónica en documentos digitales, representa un cambio importante en la forma de realizar cualquier acto jurídico. En el entendido de que la firma electrónica avanzada tiene los mismos efectos jurídicos que la firma autógrafa, todos aquellos trámites y actos que requieran de la firma para manifestar el consentimiento, pueden ser realizados desde cualquier lugar en donde las partes que intervienen tengan acceso a una computadora con conexión a la red, para enviar y recibir información de manera inmediata, segura y más confiable que la firma autógrafa.

Gracias a la firma digital, los ciudadanos podrán realizar transacciones de comercio electrónico seguras y relacionarse con la Administración con la máxima eficacia jurídica, abriéndose por fin las puertas a la posibilidad de obtener documentos como la cédula de identidad, carnet de conducir, pasaporte,

certificados de nacimiento, o votar en los próximos comicios cómodamente desde su casa.

En la vida cotidiana se presentan muchas situaciones en las que los ciudadanos deben acreditar fehacientemente su identidad, por ejemplo, a la hora de pagar las compras con una tarjeta de crédito en un establecimiento comercial, para votar en los colegios electorales, con el fin de identificarse en el mostrador de una empresa, al firmar documentos notariales, etc.

En estos casos, la identificación se realiza fundamentalmente mediante la presentación de documentos acreditativos como el DNI, el pasaporte o el carnet de conducir, que contienen una serie de datos significativos vinculados al individuo que los presenta, como:

- Nombre del titular del documento
- Número de serie que identifica el documento
- Período de validez: fecha de expedición y de caducidad del documento, más allá de cuyos límites éste pierde validez
- Fotografía del titular
- Firma manuscrita del titular.
- Otros datos demográficos, como sexo, dirección, etc.

En algunos casos en los que la autenticación de la persona resulta importante, como en el pago con tarjeta de crédito, se puede exigir incluso que estampe una firma, que será comparada con la que aparece en la tarjeta y sobre su documento de identificación. En el mundo físico se produce la verificación de la identidad de la persona comparando la fotografía del documento con su propia

fisonomía y en casos especialmente delicados incluso comparando su firma manuscrita con la estampada en el documento acreditativo que porta. En otras situaciones, no se requiere el DNI o pasaporte, pero sí la firma, para que el documento goce de la validez legal (cheques, cartas, etc.), ya que ésta vincula al signatario con el documento por él firmado.

Ahora bien, en un contexto electrónico, en el que no existe contacto directo entre las partes, ¿resulta posible que los usuarios de un servicio puedan presentar un documento digital que ofrezca las mismas funcionalidades que los documentos físicos, pero sin perder la seguridad y confianza de que estos últimos están dotados? La respuesta, por fortuna, es afirmativa, ya que el uso de la firma digital va a satisfacer los siguientes aspectos de seguridad:

#### **4.2. BENEFICIOS DE LA HOMOLOGACIÓN DE LOS DIVERSOS CERTIFICADOS DIGITALES**

La Firma Electrónica Avanzada permite cifrar información e identificar al emisor como autor legítimo del documento, tal y como si se tratara de una firma autógrafa. Asegura la identidad y confidencialidad del firmante y garantiza, además, que el mensaje enviado no sea modificado.

Los principales beneficios de esta modalidad de facturación son, para las empresas que facturan, el ahorro en costos operativos, administrativos y de oficina. Un estudio realizado entre empresas del sector comercial demostró que una compañía ahorra el 80% del costo al generar una factura de manera electrónica. Esto sin contar una notoria aceleración en la entrega de la información, lo que representa también un ahorro de tiempo en administración y trámites, y el ahorro de cargar con un archivo físico. Si para las grandes empresas la contabilidad fiscal representa entre el uno y el dos por ciento de sus ventas totales, para una pequeña empresa los ahorros pueden ser sustancialmente mayores.

En la actualidad las autoridades registradoras centrales reconocidas en México y como el SAT (aún y cuando depende de Banco de México), Banco de México, la Secretaría de Economía y La Función Pública, emiten sus propios Certificados Digitales, los cuales deben utilizarse para sus propios procesos.

Por otra parte, los Certificados digitales, que como propuesta en esta tesis se considera deberían homologarse, son los Certificados digitales que emite el SAT para el pago de impuestos, los que emite la Secretaría de Economía a través de las Autoridades Certificadoras autorizadas para el sector comercial y los que emite el Banco de México para las operaciones del sector financiero.

Esto es importante, debido a que por equivalencia funcional se sustituye la firma autógrafa por la Firma Electrónica Avanzada; sin embargo, tanto una persona física como una persona moral necesitan de dichos certificados digitales para realizar actos jurídicos, creando derechos y obligaciones; desde un punto de vista objetivo, equivale a que una persona tenga tres distintas firmas autógrafas, utilizando una para declaraciones de impuestos, otra para operaciones financieras y otra para actos de comercio.

El deber ser, es que una persona que tiene una sola identidad tenga una sola firma autógrafa y electrónica, que sirva para identificar y vincular a una persona, aun y cuando haya celebrado un acto de comercio, firmando un contrato de arrendamiento de manera electrónica, o bien, haya declarado sus impuestos ante la dependencia competente y realizado una transferencia electrónica bancaria utilizando su firma electrónica. En este orden de ideas, se debe homologar el certificado digital, el cual cumple con las mismas características, ya sea del SAT de Banxico o bien de la Secretaría de Economía, reformando las legislaciones aplicables para cada dependencia, o bien, creando un solo reglamento o legislación que regule la firma electrónica avanzada y de pleno reconocimiento al Certificado que emite el SAT para ser utilizado en operaciones financieras, al certificado digital que emite el Banco Central para firmar un contrato de compraventa y al Certificado digital que genera la Secretaría de Economía para declaraciones de impuestos y que además en dichas reformas o en la legislación que sugiere para regular a los Certificados Digitales, se

determinen las características técnicas que deba contener el Certificado Digital para que exista una compatibilidad entre dichos Certificados digitales; de tal forma que como se mencionó en el capítulo anterior, se extienda el uso de esta herramienta tecnológica y que el mismo Certificado nos resulte útil, incluso para realizar cualquier trámite ante cualquier dependencia de gobierno.

De manera muy precisa, la propuesta se refiere a la reforma de las legislaciones aplicables tanto para el SAT, Banco de México y Secretaría de Economía, reconociendo los Certificados Digitales emitidos por cualquier otra Autoridad Registradora Central, a través de sus Autoridades Certificadoras autorizadas para su aplicación en cualquier acto Fiscal, Financiero o Comercial, o bien, la creación de una sola legislación encargada de regular los Certificados Digitales, tanto en su generación, aplicación y reconocimiento para que cualquier persona física o moral pueda firmar contratos, operaciones financieras y declarar impuestos con una sola firma electrónica.

Esta propuesta no sólo conlleva un beneficio para las personas al facilitar la administración de un solo Certificado, sino que a su vez facilita a la autoridad la identificación y administración de un padrón de Certificados Digitales, trayendo consigo ventajas como facilitar trámites oficiales que a la fecha son burocráticos y tardados.

De la propuesta de la homologación de los Certificados Digitales emitidos por las Autoridades Registradoras Centrales que existen en México, el SAT, Banxico y la Secretaría de Economía, se pueden concluir varios beneficios: primeramente la existencia de una sola firma electrónica por persona física o moral para la realización de cualquier acto jurídico, y no tres como se realiza en la actualidad, tomando en cuenta que el contar con tres firmas electrónicas equivale a que una persona firme autógrafamente de manera diferente para presentar sus impuestos, realizar una operación bancaria o bien un acto de comercio. En segundo lugar, se facilitaría a las dependencias de gobierno, la administración centralizada de un padrón de certificados digitales para la realización de trámites oficiales, manteniendo un control evitando posibles delitos y en caso de que se configurara un delito identificar de manera más sencilla al presunto responsable.

En tercer lugar, considerando que el Certificado Digital emitido por cualquiera de estas tres Autoridades Registradora Centrales, garantizan la misma seguridad y tiene los mismos efectos jurídicos, se estaría en posibilidad de ampliar el uso de la firma electrónica en la realización de trámites de carácter oficial, ante cualquier dependencia de gobierno, así se evitaría la afluencia de un número abrumador de gente en delegaciones, registro civil, juzgados, etc., eliminando problemas como aglomeraciones de gente innecesaria, agilizando trámites y más importante, aún eliminar la corrupción al poder solicitar, por mencionar un ejemplo, un acta de nacimiento desde el trabajo o la casa, e incluso desde un negocio de renta de Internet, utilizando el certificado digital para identificarse y la autoridad utilizando a su vez su certificado digital para enviar dicha acta de nacimiento, firmada digitalmente dotándola de fuerza legal. Como cuarto beneficio tenemos también la homologación en los requisitos para tramitar un Certificado Digital, estandarizando la documentación que se solicita para integrar el expediente, con que el solicitante de Certificado Digital acredita su identidad y no solicitando información distinta o documentación de más o de menos por cada dependencia.

Como se puede apreciar, la homologación de los Certificados Digitales, trae aparejadas ventajas de las cuales se puede obtener un beneficio sustancial por parte de las dependencias de gobierno y a su vez facilita a los titulares de dichos Certificados la administración, de uno solo y no, como sucede en la actualidad la administración de tres Certificados. De esto no hay que perder de vista que, si evaluamos la posibilidad de que en un futuro se amplíe el uso del Certificado Digital a un mayor número de trámites y servicios, sería absurdo pensar que cada dependencia de gobierno emita su propio Certificado, o bien, de otra forma sería aun más complicado homologar los certificados existentes actualmente, considerando un incremento importante en el número de usuarios, que llegado el momento podría haber en el uso de esta herramienta tecnológica.

Los certificados ayudan a evitar que alguien utilice una clave falsa haciéndose pasar por otra persona, por lo cual los beneficios que se obtienen al usarlos son:

- Disminuir riesgos de negocio, al contar con documentos electrónicos firmados que mantienen el mismo valor legal que un documento en papel
- Disminuir riesgos de fraudes, debido a que los documentos que originan una transacción comercial no pueden ser alterados
- Establecer claramente y en forma rápida las obligaciones de una persona, al conocer inequívocamente la identidad de la persona que firma un documento electrónico
- Disminuir el riesgo de robo de información por medios electrónicos, al permitir que un documento electrónico sólo pueda ser visto por la persona que deba conocerlo

Las transacciones electrónicas de uso cotidiano, integrados a distintas aplicaciones se realizan de una forma segura y práctica, manteniendo su valor

## CONCLUSIÓN

**Primera.** Si tomamos en consideración que los certificados digitales tienen las mismas características, se le da la misma función, y tiene un objetivo común cualquiera de los certificados citados en este trabajo, por equivalencia funcional deberían estar reconocidos sin importar el ámbito de la materia que se trate y no limitados a una sola materia como el de la Secretaría de Economía para el ámbito comercial, el de Banxico para el sector financiero y la Función Pública para el gobierno. Esto es, que para una mejor administración de los certificados debería existir un solo padrón, sin importar la autoridad que lo genera, pudiendo utilizar el mismo certificado en cualquier ámbito y no que una persona deba tener por lo menos tres certificados digitales.

**Segunda.** La homologación de los mismos trae ventajas como es una base de datos única, donde las autoridades puedan identificar al titular de un certificado digital para el caso de la comisión de un delito; que las personas puedan contar con un solo archivo de identificación, que además no sólo puede limitarse a su uso en el comercio y actos jurídicos que deriven de esta actividad, sino que se utilice como medio de identificación para acreditar la identidad en una licencia para conducir, en la credencial para votar, al ingresar a un edificio gubernamental sin dejar identificación, realizar trámites seguros y confidenciales ante cualquier autoridad, desde el trabajo o el hogar, teniendo la dependencia de gobierno la certeza de con quién está tratando.

Una ventaja más, es la creación de una legislación federal o general para la República, que regule la emisión, almacenamiento, resguardo de los certificados digitales, las reglas generales de su uso, alcances y efectos legales, el almacenamiento de los datos y documentos personales, con los que las personas acreditan su identidad ante una autoridad certificadora para solicitar la emisión de un Certificado Digital y las sanciones respectivas por transgredir alguna norma.

**Tercera.** La homologación de los certificados Digitales es un adelanto en la forma de realizar cualquier acto jurídico, ya sea en el comercio o

pudiendo extenderse su aplicación a cualquier acto que requiera la identificación de una persona y su firma, para manifestar su consentimiento o aceptación y ser sujeto de derechos y obligaciones. Por esta razón, el presente trabajo tiene como objeto principal, explicar el funcionamiento del certificado digital y la llave privada como medio de identificación de las partes, como medio para crear y firmar digitalmente cualquier mensaje de datos, entendido este como documento digital que contenga cualquier tipo de información que, dada su naturaleza, requiera de la firma del emisor y del receptor para manifestar su consentimiento con el contenido del mensaje, o como forma de aceptar las obligaciones que de dicho documento emanen. Así mismo, se estudia al certificado digital como mecanismo para firmar digitalmente sustituyendo a la firma autógrafa, dado que la legislación le concede los mismos efectos jurídicos y que por equivalencia funcional es más eficiente y segura que la firma autógrafa. En este sentido, la homologación del Certificado Digital es más en un aspecto legal que técnico, pues como vimos en los capítulos que integran este documento, la existencia de distintos Certificados no radica en que contengan características técnicas distintas o no resulten compatibles entre sí. Lo que en realidad sucede, es la existencia de una laguna legal o falta de regulación, lo que deja a la interpretación total el ámbito en el cual opera cada uno de estos Certificados y que en consecuencia los criterios son divididos.

**Cuarta.** Es por esta razón que durante la secuencia del presente trabajo, el enfoque principal es la forma de operación de el Certificado Digital, para posteriormente revisar la equivalencia funcional y la sustitución de la firma autógrafa por la firma electrónica avanzada, las diferencias entre si, y las razones por las cuales es más segura la firma electrónica o digital que la firma autógrafa. De igual forma se estudia como enviar información cifrada para que de manera confidencial sea sólo el receptor quien tenga acceso y conozca el contenido de la información. También, es importante estudiar el reconocimiento que la legislación hace de la firma electrónica y que se le da valor legal e igual de importante, valor probatorio en la substanciación de un juicio.

**Quinta.** Asimismo, se estudian algunas de las legislaciones mexicanas que abordan la firma electrónica y reconocen sus efectos legales,

consecuencias de derecho y aceptación en la solución de un proceso judicial. Finalmente, se estudian los beneficios de contar con un solo certificado digital, o en el mejor de los casos, la homologación de los certificados digitales, donde una persona no necesita obtener uno por cada autoridad, sino que el mismo le sería útil para realizar cualquier acto jurídico, sin importar la materia de la que se trate. Se hace mención de los múltiples actos que, a partir de un certificado como medio de identificación, se podrían realizar y facilitarían cualquier trámite ante la autoridad judicial o incluso permitirían el inserción de dichos certificados en chips adheridos a una identificación o la licencia para conducir, eliminando definitivamente la falsificación de cualquier documento oficial, pues si consideramos que el mejor falsificador de documentos falsifica o altera un documento, es totalmente inútil, pues al comprobar el certificado en una computadora o algún dispositivo portátil, se verificaría la autenticidad del documento, y de no coincidir la identidad, la vigencia o datos adicionales agregados al certificado, o incluso, la falta del certificado, sería irrefutablemente falso.

**Sexta.** El tema de los Certificados Digitales es amplio y permite un desarrollo importante en la forma de realizar actos jurídicos. Por esta razón es fundamental homologar los certificados digitales, lo que representaría una ventaja a corto, mediano y largo plazo, en el sentido de que es conveniente contar con un solo certificado de identificación por cada persona y es mas fácil para las autoridades administrar un solo certificado y no tres, siendo que a falta de esta homologación en un futuro pudieran llegar a ser más los certificados.

## **BIBLIOGRAFÍA**

- Acosta Romero Miguel: “Nuevo Derecho Mercantil”, Editorial Porrúa, Primera Edición; 15 de agosto del 2000.
- Acosta Romero Miguel: Teoría general del acto jurídico y obligaciones, México, ed. Porrúa, año 2002,
- Ángeles Hernández Xavier: PYMES: (pequeñas y medianas empresas): Modernización tecnológica o quiebra, México, ed. Fiscales ISEF, año 2007,
- Award. Elías M.: Manual fundamental de comercio electrónico, Madrid, ed. Anaya Multimedia, año 2007,
- Charlesworth, Alan: Key concepts in e-commerce, New York, ed. Palgrave Macmillan, año 2007,
- Díaz Bravo Arturo: Derecho mercantil, México, segunda edición, año 2006,
- Díaz González Luis Raúl: Los medios electrónicos en el derecho mexicano: Aspectos civiles, mercantiles, tributarios, administrativos y penas, México, ed. Gasca-SICCO, año 2006,
- Gallego Higuera Gonzalo F.: Código de derecho informático y de las nuevas tecnologías, Madrid, España, año 2002,
- Illescas Ortiz Rafael: Derecho de la Contratación Electrónica. Civitas, año 2002.
- Martínez Nadal Apollonia: La ley de firma electrónica, Madrid, España, segunda edición, año 2001,
- Reyes Krafft Alfredo Alejandro: La firma electrónica y las entidades de certificación, México, ed. Porrúa, año 2003,
- Solís García José Julio: Factura y firma electrónica avanzada, México, ed. Gasca-SICCO, año 2005,
- Téllez Valdez Julio: Derecho Informático. McGraw Hill. 2003.
- Vial del Río Víctor: Actos jurídicos y personas, Santiago, Chile, ed. Universidad Católica de Chile, tercera edición, año 1998.

## **LEYES**

- Código de Comercio
- Código Civil para el Distrito Federal

- Código de Procedimientos Civiles para el Distrito Federal
- Ley del Banco de México

### **Otras leyes, decretos, reglamentos y normas**

- BANCO DE MÉXICO (SECTOR BANCARIO)
  - Transitorio Cuarto Reformas Código Comercio 2003 faculta a Banxico para regular y coordinar a la autoridad registradora central, registradora y certificadora de las instituciones financieras y de las empresas que les prestan servicios auxiliares o complementarios relacionados con TEF o valores que presten servicios de certificación.
  - Circular Telefax 1/2002.
  - Circular Telefax 6/2005, de 15 de marzo de 2005 de Infraestructura Extendida de Seguridad (sustituyendo a las anteriores Circulares 19/2002 bis, de 5 de julio de 2002 y de 11 de julio de 2003) y la Circular Telefax 6/2005 bis, de 23 de diciembre de 2005.
- SAT (FISCAL)
  - Anexo 20 de la Resolución Miscelánea Fiscal para 2004.
  - Decreto por el que se reforman, adicionan y derogan diversas disposiciones del Código Fiscal de la Federación. (5/01/04).
  - Primera Resolución de Modificaciones a la Resolución Miscelánea Fiscal para 2004.
- SECRETARÍA DE ECONOMÍA (COMERCIO)
  - Decreto por el que se reforman y adicionan diversas disposiciones del Código Civil para el Distrito Federal en Materia Común y para toda la República en Materia Federal, del Código Federal de Procedimientos Civiles, del Código de Comercio y de la Ley Federal de Protección al Consumidor. (23/05/00).
  - Decreto por el que se reforman y adicional diversas disposiciones del Código de Comercio en Materia de Firma Electrónica. (29/08/03).
  - Norma Oficial Mexicana NOM-151-SCFI-2002, Prácticas comerciales-Requisitos que deben observarse para la conservación de mensajes de datos. (19/12/05, vacatio legis 17/2/06).

- Reglamento del Código de Comercio en materia de Prestadores de servicios de Certificación. (19/07/04).
- Reglas generales a las que deberán sujetarse los prestadores de servicios de certificación. (10/08/04).
- SECRETARÍA DE FUNCIÓN PÚBLICA (GOBIERNO)
  - Acuerdos Tramitanet. (17/02/02).
  - Comisión Intersecretarial para el desarrollo del Gobierno Electrónico (9/12/05).
  - Ley Federal de Procedimiento Administrativo (LFPA), habilitando el empleo de medios electrónicos para algunos procedimientos administrativos de gestión. (30/05/00).

### **Manuales y revistas**

- Manual de la Agencia Certificadora. Autor Cecoban, S.A. de C.V.
- Manual del Agente Certificador. Autor Cecoban, S.A. de C.V.
- Manual Generador de requerimiento. Autor Cecoban, S.A. de C.V.

### **En Línea (Internet)**

- [ADVANTAGE SECURITY, S. DE R.L. DE C.V.](http://www.advantage-security.com/)  
<http://www.advantage-security.com/>
- [Banco de México](http://www.banxico.org.mx/)  
<http://www.banxico.org.mx/>
- [CECOBAN](http://www.cecoban.org.mx/)  
<http://www.cecoban.org.mx/>
- [EDICOMUNICACIONES MEXICO S.A DE C.V.](http://www.edicomgroup.com/mx/)  
<http://www.edicomgroup.com/mx/>
- Firma Digital – Secretaria de Economía  
<http://www.firmadigital.gob.mx/tabla.html>
- Perspectivas de la Factura Electrónica en Chile.  
<http://www.ccs.cl/html/destacados/estudioFacturaElectronica.PDF>
- Portal del SAT  
<http://www.sat.gob.mx>

- PSC WORLD, S.A. DE C.V.  
<http://www.pscworld.com/>
- Secretaría de Economía  
<http://www.economia.gob.mx/>
- Otras páginas Web  
[http://es.wikipedia.org/wiki/Certificado\\_digital](http://es.wikipedia.org/wiki/Certificado_digital)  
<http://www.monografias.com/trabajos908/firma-digital/firma-digital.shtml?monosearch>  
<http://www.monografias.com/trabajos42/firmas-digitales/firmas-digitales.shtml?monosearch>  
<http://www.monografias.com/trabajos908/firma-digital/firma-digital.shtml>  
<http://www.monografias.com/trabajos44/firma-digital/firma-digital2.shtml?monosearch>  
<http://www.monografias.com/trabajos12/actjur/actjur.shtml>  
<http://derecho.laguia2000.com/parte-general/clasificacion-de-los-actos-juridicos.2009>  
<http://www.banxico.org.mx/sistemasdepago/ies/iespub/PDF/IES-DOCTOBANXICO.PDF>  
<https://www.cecoban.org.mx/agencias/Soporte/Guia%20para%20requerimiento%20de%20certificado%20digital.pdf>  
[www.slideshare.net/.../firma-electronica-1410248](http://www.slideshare.net/.../firma-electronica-1410248). 2009  
[http://www.amedip.com/pdf/26\\_seminario/GalindoSifuentesErnesto.PDF](http://www.amedip.com/pdf/26_seminario/GalindoSifuentesErnesto.PDF)