

**FIRMA ELECTRÓNICA: UN ENFOQUE DIFERENTE**  
**ADVANCED ELECTRONIC SIGNATURE: A DIFFERENT APPROACH**

**Mariana Michelle Reyes Hernández<sup>1</sup>**

**RESUMEN:** El problema no se sitúa en las tecnologías de la información y la comunicación en materia jurídica, sino en la poca información sobre los medios alternativos, el problema era la formación y adecuación de las personas, la gente estaba acostumbrada al uso de la firma autógrafa, lo cual implicaba la presencia física, pero lo que fue de vital importancia para el presente estudio es el hecho de que las tecnologías han ido avanzando con el paso de los tiempos y es posible poder hacer toda clase de transacciones que proporcionan una mayor credibilidad al derecho y a la propia administración de justicia.

**ABSTRACT:** The problem is not in information and communication technologies in legal matters, but in the little information about alternative means, the problem was the training and adaptation of people, people were accustomed to the use of the autograph signature, which implied the physical presence, but what was of vital importance for the present study is the fact that technologies have been advancing with the passage of time and it is possible to be able to make all kinds of transactions that provide greater credibility to the right and the administration of justice itself.

**PALABRAS CLAVE:** Comercio, firma electrónica, contratación, certificación digital.

**KEYWORDS:** Commerce, electronic signature, contracting, digital certification.

**SUMARIO:** Introducción I.-Antecedentes de la firma electrónica, II.- Concepto de la firma electrónica, III.- Comercio electrónico IV. - Regulación Jurídica, V.- Uso y validez de la firma electrónica avanzada, VI. - Certificación digital, VII.-Función de los prestadores de servicio de certificación, VIII.-Comercio Digital, IX.- La firma electrónica a nivel internacional, Conclusiones, Bibliografía.

---

<sup>1</sup> Licenciada en Derecho por la Universidad Juárez Autónoma de Tabasco. *marianamichellereyes@hotmail.com* adscrita al CANACINTRA Tabasco.

## **INTRODUCCIÓN**

El enfoque de este estudio, es apreciar la firma electrónica desde dos perspectivas. En primer lugar, hacer un acercamiento a un concepto lo más profundo posible, para admitir su justa relevancia. En segundo término, analizar la regulación jurídica que existe en nuestro país y en el extranjero, aplicando un análisis jurídico y un comparativo de la legislación mexicana e internacional, de igual forma tomando en cuenta ciertos puntos fundamentales como lo son uso y validez de la firma electrónica, la función de los prestadores de servicio de certificación, al igual que los procedimientos para la certificación digital y el valor de la firma electrónica en un proceso.

Para enfocar el tema de una mejor manera, se debe considerar que la firma electrónica debe tener el mismo valor que una firma manuscrita, es por ello que el legislador le debe dar la importancia sucinta a tal tema.

Un aspecto que es apreciable y que impacta a la sociedad, es que, la firma electrónica se trata de una nueva modalidad en la que manifiesta la voluntad de las partes acompañada de los avances tecnológicos, con el uso de las nuevas tecnologías de información y la comunicación (TIC`S), lo que hoy en día facilita la vida humana, especialmente ahora que se pueden utilizar en las transacciones jurídicas comerciales, dado el alcance que tiene y ha adquirido el internet a lo largo de los tiempos.

Es por ello, que en este nuevo enfoque que se le pretende dar a la firma electrónica es para desarrollar un comercio electrónico que esté al alcance y conocimiento de las personas, para que exista el reemplazo de las firmas autógrafas por su equivalente (firma electrónica), los cuales posean la misma confianza y la misma seguridad jurídica.

La definición y las características esenciales de la firma electrónica se verán analizadas a lo largo del presente estudio, al igual que la importancia y la necesidad que existe entre la población para la admisión de la firma electrónica y que por diversas cuestiones, muy pocas personas la aplican.

### **I. ANTECEDENTES DE LA FIRMA ELECTRÓNICA**

Para analizar la firma electrónica avanzada es necesario, conocer en primer lugar un poco de su historia, que versa sobre la firma autógrafa, ya que esta es la base de la firma actual y ambas son sustentadas bajo el principio de "*animus signandi*" Es la intención de firmar, como un acto automático relacionado con la grafomotricidad, pero muchas

veces, esta intención de firmar, se le relaciona con la voluntad de asumir el contenido de un documento, que no debe confundirse con la voluntad a contratar.<sup>2</sup>

El origen histórico de la firma, se encuentra en el ordenamiento jurídico romano y para ser más en específico en la figura de *manufirmitio* que consistía en “una ceremonia formal en la que, tras la lectura del documento por su autor, o el *notarius*, era desplegado sobre una mesa y se le pasaba la mano por encima en señal de aceptación. Tras ello se hacía figurar el nombre del autor, el signo o tres cruces en referencia a la Santísima Trinidad, haciéndolo a continuación los testigos. En época medieval, las firmas eran signos, normalmente cruces en torno a las cuales se añadían letras y símbolos. Dado que eran muy pocos los que sabían firmar, se generalizó también el uso del sello como “grabación o impresión de una imagen, cargada de significado, que se obtiene sobre un soporte, y sirve para identificar a una persona física o jurídica. La firma comenzó a recogerse en los textos normativos de la época, como el Fuero real, las Partidas o la Pragmática de Alcalá”.<sup>3</sup>

En México la Suprema Corte de Justicia de la Unión también se ha pronunciado respecto a la importancia que tenía la firma autógrafa en la época, en la cual era necesario que la firma fuera 100% autógrafa, desprendiendo que dicha firma debía ser realizada del puño y letra del autor. Firma. es inválida la que no proviene del puño y letra de su aparente autor (legislación del estado de san luis potosí).

La interpretación sistemática y funcional de los artículos 27, 66, 122, 130, 132, 192, 201 y 204, de la Ley Electoral del Estado de San Luis Potosí, permite establecer que el requisito de la firma que debe constar en los diversos documentos que establece la propia legislación electoral, debe satisfacerse, ya sea usando una rúbrica o simplemente escribiendo el nombre y apellido, o en casos especiales que la persona no sepa leer o escribir, imprimiendo su huella dactilar, en razón de que, de los artículos 27, fracción III, inciso b), párrafo 2; 122, 132 y 192, fracción V de la Ley Electoral del Estado de San Luis Potosí, se desprende que ciertos documentos no sólo deben ser firmados, sino que debe manifestarse el nombre completo (nombre y apellidos) de las personas a que dichos documentos les incumben, en virtud de lo cual, debe considerarse que poner el nombre y

---

<sup>2</sup> MACEDO MAYO, Roberto, “Elementos y características de la firma autógrafa” (<http://estudiojuridicocriminalisticomacedom.blogspot.com/2011/09/elementos-y-caracteristicas-de-l-firma.html>), (última consulta 30 de septiembre de 2011).

<sup>3</sup> RODRÍGUEZ GARCÍA, Enrique A., “Las recogidas de firmas desde el punto de vista del Derecho”, Revista Dialnet (1), 2009, 124 pp.

apellidos es un requisito diferente al de suscribir el documento de propia mano y no por conducto de un medio mecánico o electrónico;

Además, debe precisarse, que el motivo de que todas estas normas establezcan la necesidad de firmarlas de propia mano, estriba en que, a través de esta suscripción, el legislador pretende asegurar que se exprese la voluntad de obligarse con los actos jurídicos que se están realizando; que, en fin, se acredite la autenticidad del documento que suscribe y se logre la eficacia prevista en la ley, ya que de estimarse que se ponga en otra forma distinta (mecánica o electrónica), las autoridades electorales tanto administrativas como jurisdiccionales, no tendrían la certeza de que realmente la persona facultada tuviese el propósito de ejecutar el acto o acción que están realizando o poniendo en movimiento a través del recurso respectivo, en razón de que, cualquier otra persona sin el consentimiento concerniente, podría escribir el nombre de la persona facultada, y con esto, cumplir con el requisito mencionado; de modo que no puede considerarse firmado un escrito por el simple hecho de que en él conste el nombre y apellidos impresos por un medio diferente al puño y letra.<sup>4</sup>

A lo largo de la historia y siendo parte del ciclo del tiempo y del desarrollo es normal la transformación de ciertos mecanismos, la firma autógrafa es y será la idea más concreta que la humanidad tiene respecto para la validación de un documento, ya que en esta se expresa íntegramente la voluntad de las personas.

## **II. CONCEPTO DE LA FIRMA ELECTRÓNICA**

Ahora bien, entendiéndose la relevancia que ha tenido la firma autógrafa, entraremos al estudio del concepto de la firma electrónica la cual se entiende como cualquier método tecnológico a través del cual se puede firmar un documento informático,

Nuestro código de comercio es el único ordenamiento jurídico federal que define a la firma electrónica, por lo tanto, a lo largo de esta redacción se harán algunos comentarios acerca de tal definición. En este mismo orden de ideas se puede definir a la firma electrónica, según nuestro Código de comercio en su artículo 89 como:

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

---

<sup>4</sup> Tesis CXLIII, C.J/Semanario Judicial de la Federación y su Gaceta, Tercera época, t. VIII PR, agosto 2002, 177 p.

firmante aprueba la información contenida con el mensaje de datos, y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicios.

De esta enunciación podemos obtener las siguientes peculiaridades, en primer lugar el código nos habla de que la firma electrónica es un conjunto de datos, códigos o claves criptográficas las cuales deben ser privadas, la cual ha nuestra manera de ver nos parece preciso aclarar que la firma electrónica, sea de uso personalísimo, por diversas cuestiones de las políticas legislativas y también porque muchos de los efectos jurídicos no han sido regulados de forma correcta por nuestras legislaciones.

Esta clase de firmas digitales utilizan un sistema criptográfico que poseen una clave pública y una clave privada, la clave que aparece en el certificado electrónico es solo la clave pública. La clave privada no aparece en el certificado. Aunque dicha clave privada haya podido ser generada por la misma autoridad de certificación que expidió el certificado, y se corresponde solo con la clave pública que aparece en el certificado.

En segundo punto, marca que estos datos pueden ser utilizados como un medio para la identificación del firmante, lo cual garantiza la entidad del emisor y evitar el rechazo en origen y el autor no pueda negarse.

En tercer lugar, la firma electrónica no solo es para la identificación del firmante, sino que también manifiesta el consentimiento de las partes sobre la obligación que ha efectuado a la firma el acto, dado que la función que tiene la firma electrónica es la misma que tiene una firma caligráfica.

Se pueden hacer múltiples analogías respecto al dicho concepto señalado, ya que en ocasiones utilizamos medios electrónicos con los cuales se puede hacer la comparación, ejemplo de ello es al utilizar el correo electrónico, este posee una base de datos con claves criptográficas, la clave pública del usuario sería ejemplo@hotmail.com y la clave privado es la contraseña del usuario, este entre tantos ejemplos que se pueden mencionar.

### **III.DIFERENCIA ENTRE FIRMA ELECTRÓNICA SIMPLE Y AVANZADA**

De igual forma nuestra legislación mexicana en el artículo 89 del Código de Comercio hace referencia a la firma electrónica avanzada o fiable.

Firma electrónica avanzada o fiable: Aquella firma que cumpla con los requisitos contemplados en las fracciones I a V del artículo 97. En aquellas disposiciones que se refieran a firma digital, se considerará a éstas como una especie de 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.

Esto nos lleva en la misma secuencia a la Ley de Firma electrónica avanza que a su vez, también aporta su propia definición en el artículo 2.

Artículo 2 fracción XIII.- Firma Electrónica Avanzada: el conjunto de datos y caracteres que permite la identificación del firmante, que ha sido creada por medios electrónicos bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos, la cual produce los mismos efectos jurídicos que la firma autógrafa.

Igualmente, para poder definir y enunciar la diferencia entre la firma electrónica simple y avanzada es necesario que invoquemos el nuevo marco regulatorio para los servicios de identificación y confianza de las transacciones electrónicas en el mercado interior, conocido como el Reglamento (UE) número 910/2014, esto con el fin de que este proyecto tenga contenido de derecho internacional.

Este reglamento ya mencionado con anterioridad hace una distinción de tres tipos de firmas electrónicas, las cuales son: firma electrónica avanzada, simple y cualificada, todas estas firmas son legalmente vinculantes y también son admisibles ante cualquier tribunal.

Firma electrónica simple son “los datos den formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar.”

Firma electrónica avanzada “es aquella firma que cumple con los requisitos contemplados en el artículo 26 del Reglamento (UE) N° 910/2014”

Los requisitos para la firma electrónica avanzada son los siguientes:

- a) Estar vinculada al firmante de manera única;
- b) Permitir la identificación del firmante;
- c) Haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo; y
- d) Estar vinculada con los datos del firmante por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable.

Firma electrónica cualificada “una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica.<sup>5</sup> Para dar una mejor referencia y que se pueda entender la diferencia que existe entre la firma electrónica simple, avanzada, daremos los siguientes ejemplos:

La firma electrónica simple por ejemplo si nos piden enviar un documento, este es enviado firmado y escaneado por correo, es claro que existe una asociación entre la cuenta de correo electrónico y la firma, pero no existe una ninguna certeza de que realmente la firma fue realizada por el firmante, es por ello que la firma electrónica simple tiene un nivel muy mínimo de seguridad.

Por otro lado, la firma electrónica avanzada o fiable posee un mayor número de seguridad que la firma electrónica simple, se asegura la asociación de que el firmante

---

<sup>5</sup> SORO MUÑOZ, José Félix, “Firma Electrónica”, Diputación provincial de Huasteca (1), 2017, 16-17 pp.

realmente haya realizado la firma. Esta clase de firma otorga seguridad, certeza, confidencialidad y validez ante diversas áreas judiciales y otorga múltiples beneficios para las personas que se encuentran fuera y dentro del país.

	<b>Firma electrónica simple</b>	<b>Firma electrónica avanzada</b>	<b>Firma electrónica cualificada</b>
Facilidad de uso	✓	✓	
Seguridad		✓	✓
Garantías legales		✓	✓
Token de seguridad			✓

**Fuente:**

<http://www.inegi.gob.mx/inegi/contenidos/espanol/ciberhabitat/comercio/firma/index.html> (Última consulta 14 de agosto de 2016).

#### **IV. REGULACIÓN JURÍDICA**

Como bien hemos expresado la firma electrónica, tiene sus umbrales en lo que es el comercio, es por ellos que encontramos su base constitucional en el artículo 73 fracción X, donde se establece la facultad del Congreso General para legislar en materia de comercio:

Artículo 73 fracción X Para legislar en toda la República sobre hidrocarburos, minería, sustancias químicas, explosivos, pirotecnia, industria cinematográfica, comercio, juegos con apuestas y sorteos, intermediación y servicios financieros, energía eléctrica y nuclear y para expedir las leyes del trabajo reglamentarias del artículo 123.

Código de comercio

El 28 de marzo de 2018 fue publicada la más reciente reforma publicada en el DOF6 y las adhesiones al código de comercio en materia de firma electrónica, en las cuales se enmarca la autonomía de la firma electrónica y en la que se reconoce que posee la misma calidad que la firma autógrafa.



Por otro lado, estas reformas se acoplan a las sugerencias dadas por la CNUDMI<sup>7</sup>. De esta forma, el código de comercio señala:

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.

En el Código Civil, Artículo 1803. "El consentimiento puede ser expreso o tácito, para ellos se estará dispuesto a lo siguiente".

1. Será expreso cuando la voluntad se manifiesta verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología. O por signos inequívocos”.

Artículo 1814 bis, párrafo segundo...”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 los rige”.

El Código Federal de Procedimientos Civiles que en su Artículo 210, señala: “Se reconoce como prueba la información generada o comunicada que consiste en medios electrónicos, ópticos o en cualquier otra tecnología”.

En el código civil para el Estado de Tabasco en su artículo 1925 manifestación del consentimiento establece: “el consentimiento de quienes contratan debe manifestarse claramente tal que no deje lugar a dudas.”

Y en el artículo 1926 expresa que “el consentimiento puede ser expreso o tácito. Es expreso cuando se manifiesta verbalmente, por escrito o por signos inequívocos. El tácito resulta de hechos o de actos que lo presupongan o que autoricen presumirlo, excepto en los casos en que por ley o por convenio de voluntad deba manifestarse expresamente.”

El artículo 1955 en su párrafo segundo...” Serán válidos los contratos celebrados por cualquier medio electrónico, si así lo pactaron las partes su perfeccionamiento.” La firma electrónica no se contempla expresamente en materia civil, pero se reconoce con la expresión de voluntad, la cual es emitida por medios electrónicos.

Y en la ley federal de protección al consumidor en sus disposiciones generales del artículo primero fracción VIII “La real y efectiva protección al consumidor en las transacciones efectuadas a través del uso de medios convencionales, electrónicos, ópticos o de cualquier otra tecnología y la adecuada utilización de los datos aportados;”

Y para concluir esta sección la ley de firma electrónica avanzada pronuncia en su artículo segundo párrafo XIII. Firma Electrónica Avanzada: “el conjunto de datos y

caracteres que permite la identificación del firmante, que ha sido creada por medios electrónicos bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos, la cual produce los mismos efectos jurídicos que la firma autógrafa".

#### Instrumentos Internacionales

La comisión de las naciones unidas para el derecho mercantil internacional (por sus siglas en inglés UNCITRAL) fue creada en el año de 1966 con el fin de realizar ilustraciones sobre el comercio internacional para promover la conjunción e innovación de las normas en materia de comercio.

Para cumplir con este fin, la comisión funciona a través de grupos de trabajo, los cuales preparan documentos que contienen lineamientos generales sobre la regulación de un área determinada del comercio internacional para proponer a los Estados miembros su incorporación al derecho interno, ya sea a través de convenios o leyes modelo.

También existen otros instrumentos como la convención de las naciones Unidas sobre la utilización de las comunicaciones electrónicas en contratos internacionales, la cual ha observado que las comunicaciones electrónicas han ayudado a la eficiencia de las actividades comerciales, ya que brinda circunstancias y facilidades a las partes. Lo cual eliminaría los problemas y los obstáculos que se han dado en el comercio internacional, con esto se aumentaría la certidumbre jurídica y la previsibilidad comercial en los contratos internacionales.

### **V. USO Y VALIDEZ DE LA FIRMA ELECTRÓNICA AVANZADA**

Como ya hemos expresado con anterioridad a lo largo de este trabajo la firma electrónica tiene la misma validez que una firma autógrafa y esta puede ser utilizada a través de los medios electrónicos y también por medio de mensaje de datos, es por ellos que tienen el mismo valor probatorio a cualquier disposición legal aplicable.

En disposición de lo emitido con anterioridad es necesario que la firma electrónica cuente con ciertos principios rectores, los cuales están contemplados en el artículo 8 de la Ley de firma electrónica avanzada.

Artículo 8. Para efectos del artículo 7 de esta Ley, la firma electrónica avanzada deberá cumplir con los principios rectores siguientes:

- I. Equivalencia Funcional: Consiste en que la firma electrónica avanzada en un documento electrónico o en su caso, en un mensaje de datos, satisface el requisito de firma del mismo modo que la firma autógrafa en los documentos impresos.
- II. Autenticidad: Consiste en que la firma electrónica avanzada en un documento electrónico o, en su caso, en un mensaje de datos, permite dar certeza de que el mismo ha sido emitido por el firmante de manera tal que su contenido le es atribuible al igual que las consecuencias jurídicas que de él deriven.
- III. Integridad: Consiste en que la firma electrónica avanzada en un documento electrónico o, en su caso, en un mensaje de datos, permite dar certeza de que éste ha permanecido completo e inalterado desde su firma, con independencia de los cambios que hubiere podido sufrir el medio que lo contiene como resultado del proceso de comunicación, archivo o presentación.
- IV. Neutralidad Tecnológica: Consiste en que la tecnología utilizada para la emisión de certificados digitales y para la prestación de los servicios relacionados con la firma electrónica avanzada será aplicada de modo tal que no excluya, restrinja o favorezca alguna tecnología en particular.
- V. No Repudio: Consiste en que la firma electrónica avanzada contenida en documentos electrónicos garantiza la autoría e integridad del documento y que dicha firma corresponde exclusivamente al firmante, y
- VI. Confidencialidad: Consiste en que la firma electrónica avanzada en un documento electrónico o, en su caso, en un mensaje de datos, garantiza que sólo pueda ser cifrado por el firmante y el receptor.

## **VI. CERTIFICACIÓN DIGITAL**

- VII. Para explicar lo que es la certificación digital es necesario en primera instancia dar una pequeña descripción de esta, en nuestra ley de firma electrónica avanzada en el artículo segundo fracción V a letra dice "el mensaje de datos o registro que confirme el vínculo entre un firmante y la clave privada" esta certificación digital es un medio por el cual se permite garantizar legalmente la identidad del firmante y su clave particular.
- VIII. En implementaciones reales de la firma digital, es necesaria la utilización de certificados digitales a fin de proveer confianza en el proceso, ya que al igual

que en el mundo real, es necesario contar con algo o alguien que le de validez a la identidad de alguien. De forma análoga a un documento oficial que garantiza la identidad de una persona, los certificados digitales funcionan como identificaciones para un usuario en una transacción que involucre una firma digital, ya que es el certificado digital de un firmante el que se usa para verificar las firmas que él genera. El estándar X.509 especifica, entre otras cosas, formatos para certificados digitales y un algoritmo de validación de la ruta de certificación. Los formatos de codificación más comunes son *DER (Distinguish Encoding Rules)* o *PEM (Privacy Enhanced Mail)*. X.509 es la pieza central de la infraestructura de clave pública y es la estructura de datos que enlaza la clave pública con los datos que permiten identificar al titular. <sup>8</sup>

- IX. Con esta certificación digital es necesario que exista a través de una página de internet, un servicio por medio del cual exista tal vínculo. Cuenta con una vigencia de cuatro años como máximo.
- X. Las únicas secretarías que pueden dar legalidad a tal certificación son la secretaría, la Secretaría de Economía y el Servicio de Administración Tributaria, estas de manera conjunta establecen los procedimientos, los términos de las disposiciones aplicables y la verificación de elementos de identificación, emisión, renovación y revocación de los certificados digitales.
- XI. En nuestra legislación mexicana aplicable a la firma electrónica avanzada hay un apartado en el cual explica el procedimiento y la estructura que debe contener un certificado digital.
- XII. Artículo 17. El certificado digital deberá contener lo siguiente:
- XIII. I. Número de serie;
- XIV. II. Autoridad certificadora que lo emitió;
- XV. III. Algoritmo de firma;
- XVI. IV. Vigencia;
- XVII. V. Nombre del titular del certificado digital;
- XVIII. VI. Dirección de correo electrónico del titular del certificado digital;
- XIX. VII. Clave Única del Registro de Población (CURP) del titular del certificado digital;
- XX. VIII. Clave pública, y

---

<sup>8</sup> MORALES SANDOVAL Miguel, DÍAZ PÉREZ Arturo y DOMÍNGUEZ PÉREZ Luis Julián, "Firma electrónica: concepto y requerimientos para su puesta en práctica", <https://www.tamps.cinvestav.mx/~mmorales/documents/dsMexico.pdf>, (última consulta junio 2013)

- XXI. IX. Los demás requisitos que, en su caso, se establezcan en las disposiciones generales que se emitan en términos de esta Ley.

## **VII.FUNCIÓN DE LOS PRESTADORES DE SERVICIO DE CERTIFICACIÓN**

Quienes pueden ejercer la función de prestador de servicio de digitalización, con previa certificación por parte de la secretaria, en nuestro Código de comercio, en el artículo 101 que a la letra dice:

- I. Los notarios públicos y corredores públicos;
- II. Las personas morales de carácter privado, y
- III. Las instituciones públicas, conforme a las leyes que les son aplicables.

En el artículo 25 de la LFEA nos expresa cuales son la atribución y las obligaciones que tienen los prestadores de servicio de certificación.

Artículo 25: I. Emitir, administrar y registrar certificados digitales, así como prestar servicios relacionados con la firma electrónica avanzada;

II. Llevar un registro de los certificados digitales que emitan y de los que revoquen, así como proveer los servicios de consulta a los interesados;

III. Adoptar las medidas necesarias para evitar la falsificación, alteración o uso indebido de certificados digitales, así como de los servicios relacionados con la firma electrónica avanzada;

IV. Revocar los certificados de firma electrónica avanzada, cuando se actualice alguno de los supuestos previstos en el artículo 19 de esta Ley conforme a los procedimientos a que se refiere el artículo 18 de la misma;

V. Garantizar la autenticidad, integridad, conservación, confidencialidad y confiabilidad de la firma electrónica avanzada, así como de los servicios relacionados con la misma;

VI. Preservar la confidencialidad, integridad y seguridad de los datos personales de los titulares de los certificados digitales en términos de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, su Reglamento y demás disposiciones aplicables, y

VII. Las demás que les confieran las disposiciones jurídicas aplicables.

Lo anterior, sin perjuicio de las atribuciones que, en su carácter de autoridad certificadora, corresponden al Servicio de Administración Tributaria en términos de la legislación fiscal y aduanera.

## VIII. COMERCIO DIGITAL

El comercio electrónico es entendido como la venta y compra directa o indirecta de cualquier tipo de información, que pueden ser productos y servicios por medio de redes de computadora, así como también, el apoyo brindado a cualquier tipo de transacción de negocios sobre una infraestructura digital. Es tal la dimensión del comercio electrónico que no puede ser visto como un simple canal usado para mercadear los productos; y tampoco puede ser visto como uno nuevo que sustituye o se agrega a los ya existentes minoristas, mayoristas e intermediarios.

La audiencia que logra reunir el comercio electrónico supera cualquier otra forma de comercio hasta ahora conocido. Aunque el internet pareciera ser la infraestructura adecuada para generar comercio electrónico, no es un requisito para su existencia, dado que en el futuro pareciera que todo comercio electrónico será fusionado con nuevas tecnologías de tipo inteligente, multimedia y TV interactiva.<sup>9</sup>

Otra definición de comercio electrónico es la que ofrece Jay Tenenbaum quien fue durante 1998 presidente y director ejecutivo de commersNET: Un modelo que permite a las empresas intercambiar, de forma electrónica, información y servicios esenciales para sus negocios y que no involucra necesariamente transacciones monetarias.<sup>10</sup>

De la misma forma Osio define lo que se ha llamado en inglés e-bussines o en español comercio electrónico, "la actividad de adquirir o enajenar a través de medios electrónicos bienes corporales o incorporales".<sup>11</sup>

En la actualidad, los avances tecnológicos han llegado a tal grado que en el existe la capacidad de adquirir bienes, servicios, asistencia, información, entretenimiento que generan relaciones que crean obligaciones y derechos para las partes que han decidido interactuar vía internet.

---

<sup>9</sup> RODRÍGUEZ, Gladys Stella, "El comercio electrónico, algunas nociones de seguridad" *Revista de derecho, Universidad del Norte* (1), 2001, 144-145 pp.

<sup>10</sup> CASTELLS ARTAL, Manuela, *Dirección de ventas: Organización del departamento de ventas y gestión de vendedores*, Madrid, Editorial HESIC, 2009, 481 pp.

<sup>11</sup> RODRIGUEZ, Gladys, "El comercio electrónico: Necesidad de una infraestructura de seguridad" *Vlex OMDI*, 2001. 2 p. (<https://studylib.es/doc/545387/el-comercio-electr%C3%B3nico-necesidad-de-una>)

## **IX. LA FIRMA ELECTRÓNICA A NIVEL INTERNACIONAL**

Actualmente hay múltiples países que cuentan con una legislación en materia de Firma electrónica podemos enumerar a los siguientes, con el fin de hacer un comparativo entre la legislación mexicana y el ámbito internacional:

ALEMANIA (El 13 de junio de 1997 fue promulgada la Ley sobre Firmas Digitales y el 7 de junio del mismo año, fue publicado su Reglamento. *Law Governing Framework Conditions for Electronic Signatures and Amending Other Regulations (Bundesgesetzblatt - BGBl. Teil I S. 876 vom 21. Mai 2001). Published 16 May 2001. Official Journal N° 22, 22 May 2001. In Force 22 May 2001).*

ARGENTINA (El 17 de marzo de 1997, el Sub-Comité de Criptografía y Firma Digital, dependiente de la Secretaría de la Función Pública, emitió la Resolución 45/97 -firma digital en la Administración Pública- el 14/12/2001 Ley de Firma Digital para la República Argentina 25/506.

BELGICA: *Loi fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification (Moniteur belge du 29 septembre 2001). Loi introduisant l'utilisation de mohines de télécommunication et de la signature électronique dans la procédure judiciaire et extrajudiciaire, 20 octobre 2000. Belgisch Staatsblad, 22/12/200. Moniteur Belge. C.E.E. (Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre, por la que se establece un marco comunitario para la firma electrónica.- Decisión de la Comisión, de 6 de noviembre de 2000, relativa a los criterios mínimos que deben tener en cuenta los Estados miembros para designar organismos de conformidad con el apartado 4 del artículo 3 de la Directiva 1999/93/CE del Parlamento Europeo y del Consejo por la que se establece un marco comunitario para la firma electrónica (2000/709/CE).*

CANADÁ (British Columbia Bill 13-2001, The Electronic Transactions Act).

COLOMBIA: (Ley 527 de 1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación)

CHILE: (2002 Ley sobre documentos electrónicos, firma electrónica y servicios de certificación).

DINAMARCA: *Act 417 of 31 May 2000 on Electronic Signatures. Bill L 229. Executive Order on Security Requirements etc. for Certification Authorities. Executive Order N° 923 of 5*



*October 2000. Executive Order on Reporting of Information to the National Telecom Agency by Certification Authorities and System Auditors. Executive Order N° 922 of 5 October 2000.*

ESPAÑA: (Real Decreto Ley 14/1999 sobre Firmas Electrónicas. Septiembre de 1999, Instrucción sobre el Uso de la Firma Electrónica de los Fedatarios Públicos Orden de 21 de febrero de 2000 por la que se aprueba el Reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de firma electrónica. -Ley de Servicios de la Sociedad de Información-).

El Proyecto de Ley de firma electrónica, de 20 de junio de 2003, ha introducido diversas modificaciones respecto del vigente Real Decreto ley 14/1999 de firma electrónica. Tras su ratificación por el Congreso de los Diputados, se acordó someterlo a una más amplia consulta pública y al posterior debate parlamentario para perfeccionar su texto, entre los puntos más importantes que considera están: Promoción de Autorregulación de la Industria, Concepto de Firma Electrónica Reconocida, *Time stamping*, Declaración de prácticas de certificación, Documento Nacional de Identidad Electrónico y el más debatido, Certificados para Personas Morales, un caso distinto a la firma electrónica de los representantes de las personas morales, pues se persigue dar firma a las empresas, no a sus representantes, si bien, evidentemente, con el objeto de que así se pueda distribuir entre sus empleados.

FRANCIA: *Décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique. Loi 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.*

IRLANDA: *Electronic Commerce Act, 2000 (Number 27 of 2000)* ITALIA (El 15 de marzo de 1997, fue publicado el "Reglamento sobre: Acto, Documento y Contrato en Forma Electrónica" aplicable a las diversas entidades de la Administración Pública, el 15 de abril de 1999 las reglas técnicas sobre firmas digitales y el 23 de enero del 2002 la ley sobre firma electrónica).

JAPÓN: (1/04/2001 Ley sobre firma electrónica y Servicios de Certificación).

REINO UNIDO: *Electronic Communications Act, 2000.*

SUECIA: *Qualified Electronic Signatures Act* (FSF 2000:832) En este trabajo analizaremos la legislación de algunos de los países que consideramos representativos.

ESTADOS UNIDOS La primera ley en materia de Firma Digital en el Mundo fue la denominada "*Utah Digital Signature Act*", publicada en mayo de 1995 en el Estado de UTAH, en Estados Unidos. Su objetivo es facilitar mediante mensajes electrónicos y firmas digitales las transacciones. Procurar las transacciones seguras y la eliminación de fraudes.

Establecer normas uniformes relativas a la autenticación y confiabilidad de los mensajes de datos, en coordinación con otros Estados. Su ámbito de aplicación son las transacciones mediante mensajes electrónicos, su confiabilidad, así como las firmas digitales.

Esta ley, define a la Firma Digital como la "transformación de un mensaje empleando un criptosistema asimétrico tal, que una persona posea el mensaje inicial y la clave pública del firmante pueda determinar con certeza si la transformación se creó usando la clave privada que corresponde a la clave pública del firmante, y si el mensaje ha sido modificado desde que se efectuó la transformación."

Al Criptosistema Asimétrico, como aquel "algoritmo o serie de algoritmos que brindan un par de claves confiable."

Al Certificado, como aquel registro basado en la computadora que identifica a la autoridad certificante que lo emite; nombra o identifica a quien lo suscribe; contiene la clave pública de quien lo suscribe, y está firmado digitalmente por la autoridad certificante que lo emite. En cuanto a la Supervisión y al control, estos recaen sobre la División, quien actúa como autoridad certificadora. También formula políticas para la adopción de las tecnologías de firma digital y realiza una labor de supervisión regulatoria.

La emisión de los certificados corre a cargo de la autoridad certificadora que ha sido acreditada se equipara el valor probatorio de un mensaje de datos que uno en papel siempre y cuando contenga una firma digital confirmada mediante la clave pública contenida en un certificado que haya sido emitida por una autoridad certificadora autorizada. No se contempla el reconocimiento de certificados extranjeros, solo se menciona que la División puede reconocer la autorización emitida por Autoridades Certificadoras de otros Estados. No contempla sanciones. ABA: El Comité de Seguridad de la Información, de la División de Comercio Electrónico, de la *American Bar Association*, emitió, en agosto de 1996, la "Guía de Firmas Digitales". NCCSL: El 15 de agosto de 1997, la Conferencia Nacional de Comisionados sobre Derecho Estatal Uniforme, elaboró la

“*Uniform Electronic Transactions Act*” (UETA), la cual se aprobó el 30 de julio de 1999. El 4 de agosto del 2000 se aprobó la “*Uniform Computer Information Transactions Act*” (UCITA), la cual se encuentra en proceso de adopción por los diversos Estados de la Unión Americana. PRESIDENCIA: El 30 de junio del 2000 se emite la “*Electronic Signatures in Global and National Commerce Act*” (*E-Sign Act.*) vigente a partir del 1 de octubre del 2000 (otorgando a la firma y documento electrónico un estatus legal equivalente a la firma autógrafa y al documento en papel).

COLOMBIA: En Colombia existe la Ley de Comercio Electrónico en Colombia (Ley 527 de 1999) Su objetivo es la reglamentación y la definición del acceso y el uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, además del establecimiento de las Entidades de Certificación.

Su ámbito de aplicación es el uso de firmas digitales en mensajes de datos Define como Firma Digital, al valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje, permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación. Como Mensaje de Datos a la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax.

Como Entidad de Certificación a aquella persona que, autorizada conforme a la presente Ley, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales.

En cuanto a la Supervisión y al control, estas recaen sobre las Entidades de Certificación autorizadas por la Superintendencia de Industria y Comercio. Se equipará el valor probatorio de un mensaje de datos que uno en papel siempre y cuando contenga lo siguiente:

1. Es única a la persona que la usa.
2. Es susceptible de ser verificada.

3. Está bajo el control exclusivo de la persona que la usa.
4. Está ligada a la información o mensaje, de tal manera que, si éstos son cambiados, la firma digital es invalidada.
5. Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional.

Si da Reconocimiento a Certificados Extranjeros. Las sanciones serán impuestas por la Superintendencia de Industria y Comercio de acuerdo con el debido proceso y el derecho de defensa, podrá imponer según la naturaleza y la gravedad de la falta, estas van de la Amonestación a la Revocación de la Autorización.

PERU: En Perú existe la Ley No. 27269 Ley de Firmas y Certificados Digitales (2000).

Su Objetivo es utilizar la firma electrónica otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad.

Su Ámbito de Aplicación son aquellas Firmas electrónicas que, puestas sobre un mensaje de datos puedan vincular e identificar al firmante, y garantizar su integridad y autenticación.

Define como Firma Digital aquella que utiliza una técnica de criptografía asimétrica, basada en el uso de un par de claves único; asociadas una clave privada y una clave pública relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave privada.

Como Certificado Digital a aquel documento electrónico generado y firmado digitalmente por una entidad de certificación, la cual vincula un par de claves con una persona determinada confirmando su identidad. Por su parte la Entidad de Certificación es aquella que cumple con la función de emitir o cancelar certificados digitales.

Existe una Entidad de Registro o Verificación que es la encargada de recolectar y comprobar la información del solicitante del Certificado, además identifica y autentica al suscriptor de firma digital y acepta y autoriza las solicitudes de emisión y cancelación de certificados digitales.

La Supervisión y el Control, corren a cargo de la autoridad administrativa designada por el Poder Ejecutivo. Las Entidades de certificación intervienen en la emisión de certificados y pueden asumir las funciones de entidades de registro o verificación. Las Entidad de Certificación deberán de contar con un Registro.

Esta ley no establece el Valor probatorio de la Firma Electrónica. Para que un Certificado Extranjero sea reconocido, este debe contar con el aval de una Entidad nacional No existen Sanciones.

VENEZUELA: Ley sobre Mensajes de Datos y Firmas Electrónicas (2001).

Su Objetivo es otorgar y reconocer eficacia y valor jurídico al mensaje de datos, a la firma electrónica y a toda información inteligible en formato electrónico.

Su Ámbito de Aplicación son los mensajes de datos y firmas electrónicas. Define a la Firma Electrónica como aquella información creada o utilizada por el signatario, asociada al mensaje de datos, que permite atribuirle su autoría bajo el contexto en el cual ha sido empleado. Como Mensajes de Datos a toda información inteligible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio.

Como órgano de control, existe la Superintendencia de Servicios de Certificación Electrónica, como un servicio autónomo con autonomía presupuestaria, administrativa, financiera y de gestión, en las materias de su competencia, dependiente del Ministerio de Ciencia y Tecnología.

Los Proveedores de Servicios de Certificación, son los que emiten los certificados La firma tendrá valor probatorio cuando vincule al signatario con el mensaje de datos y se pueda atribuir su autoría.

Cuando los certificados extranjeros estén garantizados por un proveedor de servicios de certificación acreditado, tendrán la misma validez y eficacia jurídica Las Sanciones para los proveedores de servicios de certificación van de entre 500 a 2,000 Unidades Tributarias.

ESPAÑA: Real Decreto Ley 14/1999, de 17 de septiembre, sobre Firma Electrónica (1999).

Su objetivo es establecer una regulación sobre el uso de firma electrónica, atribuyéndole eficacia jurídica, además de establecer lineamientos para los prestadores de servicios de certificación.

Su Ámbito de Aplicación son las firmas electrónicas, su eficacia jurídica y la prestación al público de servicios de certificación.

Define a la Firma electrónica como un conjunto de datos, en forma electrónica, ajenos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge.

Define también a la Firma Electrónica Avanzada como aquella que permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos. Como certificado aquella certificación electrónica que vincula unos datos de verificación de firma a un signatario y confirma su identidad.

Como Prestador de Servicios de Certificación a aquella persona física o jurídica que expide certificados, pudiendo prestar, además, otros servicios en relación con la firma electrónica. La supervisión corre a cargo del Ministerio de Fomento a través de la Secretaría General de Comunicaciones. Existe un Registro de Prestadores de Servicios de Certificación en el Ministerio de Justicia, en el que se solicita su inscripción antes de iniciar actividades. Cuando la firma electrónica avanzada esté basada en un certificado reconocido y que haya sido producida por un dispositivo seguro de creación de firma, tendrá Valor probatorio.

Para otorgarle Reconocimiento de certificados extranjeros, estos deben cumplir los siguientes requisitos:

- a) Que el prestador de servicios reúna los requisitos establecidos en la normativa comunitaria sobre firma electrónica y haya sido acreditado, conforme a un sistema voluntario establecido en un Estado miembro de la Unión Europea.
- b) Que el certificado esté garantizado por un prestador de servicios de la Unión Europea que cumpla los requisitos establecidos en la normativa comunitaria sobre firma electrónica. c) Que el certificado o el prestador de servicios estén reconocidos en virtud de un acuerdo bilateral o multilateral entre la Comunidad Europea y terceros países u organizaciones internacionales.

Las Sanciones son impuestas conforme a los siguientes parámetros:

- a) Por la comisión de infracciones muy graves, se impondrá multa por importe no inferior al tanto, ni superior al quíntuplo, del beneficio bruto obtenido como consecuencia de los actos u omisiones en que consista la infracción o, en caso de que no resulte posible aplicar este criterio lo constituirá el límite del importe de la sanción pecuniaria.

b) La reiteración de dos o más infracciones muy graves, en el plazo de cinco años, podrá dar lugar, en función de sus circunstancias, a la sanción de prohibición de actuación en España durante un plazo máximo de dos años.

c) Por la comisión de infracciones graves, se impondrá multa por importe de hasta el duplo del beneficio bruto obtenido como consecuencia de los actos u omisiones que constituyan aquéllas o, en caso de que no resulte aplicable este criterio o de su aplicación resultare una cantidad inferior a la mayor de las que a continuación se indican, esta última constituirá el límite del importe de la sanción pecuniaria.

d) Por la comisión de infracciones leves, se impondrá al infractor una multa por importe de hasta 2.000.000 de pesetas (12.020,23 euros). Instrucción sobre el Uso de la Firma Electrónica de los Fedatarios Públicos Orden de 21 de febrero de 2000 por la que se aprueba el Reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de firma electrónica. -Ley de Servicios de la Sociedad de Información-) Proyecto de Ley de Firma Electrónica: Promoción de Autorregulación de la Industria, Concepto de Firma Electrónica Reconocida, Time stamping, Declaración de prácticas de certificación, Documento Nacional de Identidad Electrónico y Certificados para Personas Morales.

La directiva de la unión europea

La Directiva del Parlamento Europeo y del Consejo por la que se establece un marco común para la firma electrónica (1999).

Su Objetivo es garantizar el buen funcionamiento del mercado interior en el área de la firma electrónica, instituyendo un marco jurídico homogéneo y adecuado para la Comunidad Europea, y definiendo criterios que fundamenten su reconocimiento legal.

Su Ámbito de aplicación se limita al reconocimiento legal de la firma electrónica y establece un marco jurídico para determinados servicios de certificación accesibles al público. Define a la Firma electrónica a la realizada en forma digital integrada en unos datos, ajena a los mismos o asociada con ellos, que utiliza un signatario para expresar conformidad con su contenido y que cumple los siguientes requisitos:

1. Estar vinculada al signatario de manera única;
2. Permitir la identificación del signatario;

3. Haber sido creada por medios que el signatario pueda mantener bajo su exclusivo control
4. Estar vinculada a los datos relacionados de modo que se detecte cualquier modificación ulterior de los mismos.

Como Dispositivo de creación de firma a los datos únicos, como códigos o claves criptográficas privadas, o un dispositivo físico de configuración única, que el signatario utiliza para crear la firma electrónica. El Dispositivo de verificación de firma son los datos únicos, tales como códigos o claves criptográficas públicas, o un dispositivo físico de configuración única, utilizado para verificar la firma electrónica.

El Certificado reconocido es el certificado digital que vincula un dispositivo de verificación de firma a una persona y confirma su identidad, y que cumple con los requisitos establecidos en el Anexo Y de la ley. El Proveedor de Servicios de Certificación es la persona o entidad que expide certificados o presta otros servicios al público en relación con la firma electrónica. La Comisión ejerce la supervisión con ayuda del Comité de Firma Electrónica, de carácter consultivo, compuesto por representantes de los Estados miembros y presidido por el representante de la Comisión. Los Estados miembros velarán porque la firma electrónica sea considerada como firma que cumple los requisitos legales de una firma manuscrita y produce los mismos efectos que la manuscrita cuando cumpla con los requisitos establecidos en ley.

Los Estados miembros velarán porque los certificados expedidos por un proveedor de servicios de certificación establecido en un tercer país tengan la misma validez que un local cuando cumplan con los siguientes requisitos:

1. El proveedor de servicios de certificación cumple los requisitos establecidos en la presente Directiva y ha sido acreditado en el marco de un sistema voluntario de acreditación establecido por un Estado miembro;
2. Un proveedor de servicios de certificación establecido en la Comunidad, que cumpla las prescripciones del Anexo II, avala el certificado en la misma medida que los suyos propios;
3. El certificado o el proveedor de servicios de certificación están reconocidos en virtud de un acuerdo bilateral o multilateral entre la Comunidad y terceros países u organizaciones internacionales. No establece Sanciones.



Es apreciable el hecho de que en otros países la regulación de la firma electrónica data a los años 90's, lo cual se puede atribuir en el sentido del avance legal, el uso de diversas tecnologías aplicadas para el sistema jurídico y comercial.

En nuestro país el primer indicio de alguna reglamentación jurídica se sitúa el 03 de febrero de 2006 en cual se hacen modificaciones a la resolución de misceláneas ficales, dando oportunidad a que las empresas tengan acceso a los certificados de firmas electrónicas, este siendo un pequeño pero significativo paso para México, nos hace darnos cuenta de que realmente como país es difícil estar a la vanguardia de las reglamentaciones jurídicas que existen en nuestros días. Y he aquí por qué la mayor parte las leyes que contemplan nuestra constitución son tomadas del ámbito internacional.

## **CONCLUSIONES**

Con el paso del tiempo un gran el internet es una red que está a disponibilidad de la mayoría, aunque a pesar de que puede facilitarnos la vida, nos puede acarrear problemas respecto a la confidencialidad y la seguridad de los usuarios, es por ello que en el Estado de Derecho crea el comercio electrónico, para solventar y regular tales actividades que contemplan cualquier servicio o producto que se pueda ofrecer.

Un claro ejemplo de que el comercio electrónico ha ido avanzando, es la firma electrónica, que, aunque pocos entiendan que es está inmersa en nuestra sociedad, por lo cual es necesario que los usuarios tengan un conocimiento exacto respecto de cómo se utiliza para que de igual forma tenga la certeza y la seguridad jurídica de que sus derechos comerciales se están protegiendo por diversos organismos, y que tiene contienen la misma validez jurídica que una firma caligráfica.

En nuestro parecer muchas veces, tenemos dudas e inquietudes respecto a la forma en como las nuevas tecnologías se apoderan de las transacciones, lo cual nos hace dudar y tener discernimiento respecto de los nuevos modelos del comercio electrónico, sin saber que estos nos facilitan las relaciones comerciales y utilizándolos podemos llegar a tener una mayor credibilidad al derecho y con ello a la propia administración de justicia.

## **BIBLIOGRAFÍA**

**Libros:**

CASTELLS ARTAL, Manuela, Dirección de ventas: Organización del departamento de ventas y gestión de vendedores, Madrid, Editorial HESIC, 2009, 481pp.

**Revistas:**

GARCÍA, E. A. (2009). Las recogidas de firmas desde el punto de vista del Derecho. Salamanca, España.

RODRÍGUEZ GARCÍA, Enrique A., "Las recogidas de firmas desde el punto de vista del Derecho", Revista Dialnet (1), 2009, pp. 124.

RODRÍGUEZ, Gladys Stella, "El comercio electrónico, algunas nociones de seguridad" Revista de derecho, Universidad del Norte (1), 2001, pp144-145.

SORO MUÑOZ, José Félix, "Firma Electrónica", Diputación provincial de Huasteca (1), 2017, pp. 16-17.

**Jurisprudencias:**

Tesis CXLIII, C.J/Semanario Judicial de la Federación y su Gaceta, Tercera época, t. VIII PR, agosto 2002, p. 177

**Artículos publicados en internet:**

MACEDO MAYO, Roberto, "Elementos y características de la firma autógrafa" (<http://estudiojuridicocriminalisticormacedom.blogspot.com/2011/09/elementos-y-caracteristicas-de-l-firma.html>), (última consulta 30 de septiembre de 2011).

MORALES SANDOVAL Miguel, DÍAZ PÉREZ Arturo y DOMÍNGUEZ PÉREZ Luis Julián, "Firma electrónica: concepto y requerimientos para su puesta en práctica", <https://www.tamps.cinvestav.mx/~mmorales/documents/dsMexico.pdf>, (última consulta junio 2013).

RODRIGUEZ, Gladys, "El comercio electrónico: Necesidad de una infraestructura de seguridad" vlex OMDI, 2001. P. 2. (<https://studylib.es/doc/545387/el-comercio-electr%C3%B3nico--necesidad-de-una.>)