UNIVERSIDAD NUEVO MUNDO

ESCUELA DE DERECHO

CON ESTUDIOS INCORPORADOS

A LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MEXICO

“Propuesta para la creación de ley de la Firma Electrónica”

T E S I S

QUE PARA OBTENER EL TITUTLO DE:

LICENCIADO EN DERECHO

P R E S E N T A:

GUILLERMO GONZÁLEZ HOLGUIN

Directora de tesis Lic. Mª. de Lourdes Jiménez Ricardez

Estado de México **2006**

“LA NECESIDAD JURÍDICA-CIVIL DE REGULAR LA FIRMA ELECTRÓNICA”

ÍNDICE

INTRODUCCIÓN

En la década de los setenta, cuando dos matemáticos de la Universidad de Standford y otros estudiosos del Instituto Tecnológico de Massachussets, descubrieron que aplicando conceptos matemáticos era posible autentificar la información digital. A este conjunto de fórmulas se le denominó “Criptografía de Llave Pública” y con ello cobraban especial importancia términos como la confidencialidad, referente a la capacidad de mantener accesible un documento electrónico a determinadas personas; y la autenticidad, que determina el compromiso de un individuo sobre el contenido del documento electrónico.

Ambos conceptos, por tanto, se solucionaban mediante una firma autógrafa en un documento tradicional. Sin embargo, con la aparición del documento electrónico, se hacía necesario garantizar la confidencialidad y la autenticidad mediante técnicas de “firma digital”.

La tecnología de la firma digital surge en el contexto de un esfuerzo más general que persigue sustituir al tradicional documento impreso con el documento electrónico, especialmente en las transacciones no presenciales (o sea, entre ausentes). Aún cuando ha sido desarrollada pensando muy particularmente en el comercio electrónico, lo cierto es que, sus aplicaciones potenciales van mucho más allá. Específicamente en el campo jurídico, esta tecnología resulta vital para una adecuada implementación de avances tales como el procedimiento administrativo y judicial electrónico, el notariado electrónico o el registro telemático de gestiones ante las dependencias públicas.

Firmar digitalmente un documento electrónico tiene dos propósitos centrales:

- Garantizar su autenticidad, informando de manera cierta acerca de su autoría (no sólo en cuanto a la identidad del autor sino eventualmente incluso en cuanto a la hora y fecha precisas de su redacción) y, por esta vía, contribuyendo a evitar una posible repudiación de sus consecuencias legales o de otra índole; y,

- Garantizar su integridad, en la medida en que permite asegurar que el contenido del documento no ha cambiado desde el momento de su firma.

En este sentido, la firma digital pretende cumplir con las mismas tres funciones primordiales que históricamente ha llenado la firma manuscrita o autógrafa que son la función indicativa, en virtud de la cual una firma revela la identidad del autor de un documento; así también, la función declarativa, por medio de la cual se entiende que una firma implica la aceptación del autor del contenido del documento y por último, la función probatoria, que permite vincular jurídicamente a un documento con su autor, para efectos demostrativos.

¿Cómo funciona el sistema? La firma digital es una aplicación concreta de la tecnología de criptografía asimétrica, que descansa a su vez sobre el empleo de dos claves matemáticamente relacionadas entre sí; una privada y otra de conocimiento público. A diferencia de la encriptación de mensajes, en que se emplea la clave pública del destinatario para codificar y enviarle un documento electrónico que sólo él o ella podrá descodificar con su clave privada; en la firma digital empleamos nuestra propia clave privada para encriptar y remitir al destinatario tanto el texto legible como su versión codificada por una llamada función hash. La computadora del receptor descodifica el texto con nuestra clave pública y lo compara con el original legible. Si esta comparación es exacta, el mensaje es validado.

El sistema de firma digital debe estar respaldado por una amplia infraestructura no sólo técnica sino también jurídica, para lo cual diversos países alrededor del mundo han venido legislando sobre el tema. Los organismos internacionales especializados también han venido dedicando esfuerzos a procurar que las regulaciones nacionales y supranacionales guarden la mayor armonía posible, destacando en particular el trabajo de la Comisión de las Naciones Unidades para el Derecho Mercantil Internacional (CNUDMI), con su proyecto de Ley Modelo sobre Firmas Digitales; y del "World Wide Web Consortium" (W3C).

Por razones de confiabilidad y seguridad jurídica, es necesario que el funcionamiento global de esta tecnología esté supervisado y garantizado, por lo que en doctrina se llama una tercera parte confiable; una persona o entidad que por su carácter oficial -o por la aceptación general de su seriedad y prestigio- dé pleno respaldo a la firma digital. Las funciones cruciales de esta instancia incluyen las de asignar las claves públicas y privadas sobre las que descansa la firma digital, certificar las primeras ante terceros (por lo cual también se les conoce como "autoridades certificantes") y velar por su empleo correcto.

Esta tercera parte confiable no es necesariamente una entidad única. Por el contrario, lo usual respecto de la firma digital es la existencia de toda una jerarquía de autoridades certificantes especializadas, con el propósito de que aquélla que finalmente se encargue de asignar a una persona física o jurídica las claves necesarias para el uso de la firma, sea idealmente alguien que pueda responder de la identidad del solicitante, ya sea porque lo conozca personalmente o porque cuente con los medios idóneos para verificar sus calidades.

Y tampoco es exigido que una autoridad certificante sea una entidad oficial (es decir, estatal). Como se indicó arriba, la práctica de la firma digital alrededor del mundo ha reconocido la posibilidad de que existan personas privadas que presten este servicio, incluso lucrativamente, caso en el cual la validez y veracidad de las claves que emitan descansará en el prestigio y seriedad acreditada de la respectiva empresa u organización, tanto como en la supervisión general que de su funcionamiento puedan hacer las entidades oficiales competentes (en particular, una superintendencia o dependencia similar que fiscalice la operación general del sistema).

¿De qué sirve la firma digital a las y los abogados y notarios?; por medio de esta tecnología, sería posible litigar electrónicamente, enviando escritos a los despachos judiciales y recibiendo resoluciones de éstos, sin sujeción a un horario de oficina ni a las restricciones de un perímetro judicial. En el plano notarial, sería factible remitir

escrituras electrónicamente al Registro Público, de nuevo sin consideración de horarios ni distancias geográficas. La firma digital es además un paso adelante a favor del concepto del gobierno electrónico, en virtud del cual el Estado es capaz de recibir peticiones y reclamos de los administrados y resolver sobre éstos por medios automatizados.

Desde luego, todo lo anterior se une a las evidentes ventajas que el sistema provee, en términos de celeridad, minimización de errores, reducción de costos por consumo de papel y los consiguientes pluses ambientales.

Pues bien, este trabajo pretende plantear de manera conceptual el escenario dónde se ve involucrado la *firma digital* y de manera inseparable el propio documento digital, donde observando los conceptos tradicionales del sujeto y su personalidad jurídica sustentados en el Derecho Civil. Así también, resulta necesario definir la naturaleza de la firma como la expresión de la voluntad y elemento esencial del acto jurídico.

Al contar con todos estos elementos, se verá que realmente se requiere y existe la necesidad real y concreta de crear la" **ley especial sobre la firma electrónica."**

CAPÍTULO 1

LOS SUJETOS EN EL DERECHO CIVIL.

El avance de la ciencia en las últimas décadas, y la gran injerencia que en la vida moderna tienen la informática y las telecomunicaciones han planteado ciertas situaciones que parece menester estudiar

Este fenómeno, que medido a la luz de los tiempos del derecho es absolutamente nuevo, viene de la mano de un gran cambio para la ciencia del derecho.
En este primer capítulo, es necesario cristalizar lo que es el sujeto de derecho civil; esto en virtud de que el presente tema se refiere a la expresión de ese sujeto de derecho civil como es su consentimiento revelado en su firma.

Así, para empezar a detallar nuestro estudio, es necesario hacer un análisis de los sujetos como persona, pero después en el capítulo segundo, observar cómo sobreviene la firma, su naturaleza y la trascendencia en la manifestación de la voluntad del sujeto civil que veremos en este primer capítulo.

1.1.- BREVE RESEÑA HISTÓRICA DE LA FORMACIÓN DEL DERECHO CIVIL EN MÉXICO.

En términos generales, la ruta de confección que ha seguido nuestro derecho civil, parte de las instituciones romanas, la organización francesa, la situación política española hasta llegar a nuestro país e imponer las normas vigentes en la época colonial.

Sin lugar a dudas, los diversos cuerpos de leyes que se han ido formando a través del desarrollo histórico de nuestro derecho civil, han permitido que la organización social pueda seguir teniendo reglas de conducta que aseguren su permanencia.

Las instituciones de Justiniano, las diversas codificaciones romanas, el Corpus Juris Canonici, el Corpus Juris Civili, el Código Napoleónico, y todo lo que es la legislación española, va a sobrevenir en nuestro país puesto que fue una región sometida a la corona española.

El autor e historiador Agustín Cue Cánovas nos dice sobre la legislación colonial lo siguiente: "las leyes dictadas durante tres siglos coloniales para América y la Nueva España, se singularizan por ciertas características que es necesario mencionar:

En primer término, no obedecieron a un plan previo…
Por otra parte, las leyes desprendidas fueron principalmente de carácter administrativo y reglamentario…

Muchas de las leyes expedidas si obedecían pero no se cumplían."[1]

La legislación española tuvo su aplicación en la Nueva España, e incluso aún después de que nuestro país se convirtiera en independiente, debido a la falta de promulgación legislativa, todavía se tenían que aplicar la legislación establecida como la novísima recopilación.

Así, las Leyes del todo, la Nueva Recopilación y la Novísima Recopilación, Los Ordenamientos de Alcalá, Las Siete Partidas, El Foro Real y El Foro Juzgo fueron orígenes de lo que ahora conocemos como el Derecho Civil.

[1] Cue Cánovas, Agustín: "Historia Social y Económica de México"; México, Editorial Trillas, 8° Ed. 2001 Pág. 168.

Claro está, que es importante observar en la historia que en el momento en que nuestro país empieza a generar su independencia, uno de los puntos principales en los cuales se basa, es la libertad.

De ahí, la necesidad de establecer reglas que permitieran gozar de la libertad, y por supuesto permitieran también el reglamentar las conductas humanas.

Así, se va a generar como ejemplo para el Código Civil el Código Francés de 1804, o el Código Napoleón.

Ahora bien, el autor Ignacio Galindo Grafías, habla de las circunstancias civiles en el México Independiente y menciona lo siguiente: "Consumada la independencia, continúa en vigor la legislación española, hasta la promulgación del primer Código Civil para el distrito y territorio federales, de 13 de diciembre de 1870, aún cuando las leyes de reforma promulgadas por el presidente Juárez en 1856 y 1859, contienen disposiciones sobre materias propias del derecho civil, a saber: el desconocimiento de personalidad a las asociaciones religiosas, el matrimonio como contrato civil y la institución del registro civil.

El Código Civil de 1870 tiene como antecedente un proyecto que por encargo oficial redactó en 1859 el Dr. Justo Sierra. Este proyecto fue concluido en el año de 1861; pero la situación política y el estado de guerra por el que atravesaba entonces el país, impidieron que sus disposiciones se pudieran poner en vigor."[2]

Este proyecto de Don Justo Sierra, se inspiró en gran parte de lo que fue el Código Francés de 1804, llamado el Código de Napoleón.

De tal manera, que se van extrayendo los lineamientos más importantes que pudieran servir en nuestra nación.

[2] Galindo Garfias, Ignacio: "Derecho Civil"; México, Editorial Porrúa S.A., 11° edición 2001. Pág.107.

Otro autor como es Rafael de Pina explica también, algunas circunstancias históricas diciendo: "partiendo de los trabajos de la comisión redactora de el proyecto Sierra, surge una nueva comisión que redacta un nuevo Código Civil que entró en vigor el 1° de junio de 1884 y fue promulgado el 31 de marzo del mismo mes; este código expresa fundamentalmente ideas individualistas en materia económica, la autoridad casi absoluta del marido sobre la mujer y los hijos, consagró la desigualdad de los hijos naturales, estableció la indisolubilidad del matrimonio, instituyó la propiedad como un derecho absoluto, exclusivista e irrestricto y como novedad mas importante introdujo la libertad de testar; este código fue reformado posteriormente, prohibiendo ventas en pacto de retroventa."[3]

Tanto el código de 1870 como el de 1884, va generando para lo que es la población de aquel momento, diversos derechos y obligaciones tanto en relación con la familia como en las relaciones dentro de la sociedad en forma individual.

De tal manera, que se va gestando para nuestro país, este código de conductas que van a darle organización a la sociedad.

Por último, el autor Ignacio Galindo Garfias, vuelve a explicar la forma en que nuestro actual código con las reformas que ha tenido, sigue en vigor; dicho autor menciona: "el 30 de agosto de 1928 se promulgó el Código Civil actualmente en vigor, que entró en vigencia el 1° de octubre de 1932. Sus disposiciones son aplicables en el Distrito Federal en materia común y en toda la República en materia federal. Este código se encuentra influido por la idea de socialización del derecho. Las ideas que lo inspiraron, han sido tomadas en parte del código de 1884, la Ley de Relaciones Familiares y los códigos alemanes, suizos, argentino y chileno, así como el proyecto de Código de Obligaciones y Contratos Italo-Francés, que formuló la comisión de estudios de la Unión Legislativa de estos dos países."[4]

[3] Pina, Rafael, D: "Derecho Civil"; México, Editorial Porrúa S.A.: XVI Ed. 1998. Pág. 98.
[4] Galindo Garfias, Ignacio; ob.cit:. Pág. 108.

Como consecuencia inmediata, hay que considerar en esta breve reseña la historia y formación del Derecho Civil en México; es importante valorar que la legislación va haciéndose positiva, esto es, que continuamente va a tener que ir avanzando en relación directa con el avance tecnológico que la propia sociedad tiene, con el fin de cubrir todas las relaciones de la sociedad, y de esta manera, establecer las reglas para llevar a cabo dichas relaciones ínter sociales.

1.2.- CONCEPTO DE DERECHO CIVIL.

En relación al concepto de Derecho Civil, quisiera citar las palabras del autor Joaquín Escriche quien dice sobre el particular: "Derecho Civil es el que se ha establecido en cada pueblo para el arreglo de los derechos y deberes de los individuos; o sea, el conjunto de las leyes que cada nación tiene establecidas para la administración de los intereses generales del estado y para todo lo relativo a la extensión y ejercicio de las facultades o derechos particulares de cada uno de los individuos. Llámese Derecho Civil el derecho particular de cada pueblo o nación, por contraposición al derecho natural y al de gentes que son comunes a todas las naciones; también se dice que el Derecho Civil es el conjunto de leyes que recaen solamente sobre las materias civiles, a diferencia del derecho criminal o penal que comprenden las leyes relacionadas en materias criminales."[5]

A la luz de lo dicho por el autor antes citado, se encuentra que el Derecho Civil parte de lo que sería la idea de la relación común entre las personas de una región o de un pueblo como menciona dicho autor.

Evidentemente, que el comportamiento que cada uno toma respecto de los intereses que se van formando por la relación social, debe tener un marco jurídico

[5] Escriche, Joaquín: "Diccionario Razonado de Legislación y Jurisprudencia"; México, Cárdenas Editor. 3° Ed. 1995. Tomo I. Pág. 544.

que le ofrezca la seguridad jurídica a la persona y de esta manera pueda considerarse como una entidad dentro del grupo social.

Otro autor que ayuda a explicar este concepto, es Miguel Ángel Ochoa Sánchez quien sobre el particular dice: "el Derecho Civil regula a la persona como sujeto del derecho, definiendo su capacidad y atributos; las relaciones de ella con la familia y con sus semejantes, así como el poder de la propia persona respecto a los bienes, ocupándose por último de la transmisión de dichos bienes por deceso, así, podemos decir que el Derecho Civil comprende seis aspectos:

1.- La Persona;
2.- La Familia;
3.- Los Bienes;
4.- Las Obligaciones;
5.- Los Contratos;
6.- Las Sucesiones." [6]

Como se puede observar, se va clasificando la materia que corresponderá al contenido del Derecho Civil; evidentemente, el interés, será el hecho de observar al individuo como sujeto de Derecho Civil.

Esto es, el interés en la persona en sí, y su estado frente a la manifestación de su voluntad, y todo el entorno que lo rodea.

1.3.- EL INDIVIDUO COMO SUJETO DE DERECHO CIVIL.

Sin lugar a dudas, solamente es el individuo, la persona, el único que puede en un momento determinado ser sujeto de derechos y obligaciones.

[6] Ochoa Sánchez Miguel Ángel:"Derecho Positivo Mexicano";México, Mac.Graw- Hill 9° Ed. 2001 Pág.164.

Así tenemos que las personas sean físicas o morales, van a generar una relación con las demás personas, y se van a comprometer a través de lo que sería el contrato, siempre y cuando, la persona tenga la personalidad necesaria para hacerlo.

Ahora bien, sobre este concepto de personalidad jurídica se hablará en el inciso siguiente; por el momento, quisiera citar las palabras de los autores Fernando Floresgómez González y Gustavo Carvajal Moreno quienes sobre el sujeto del Derecho Civil opinan lo siguiente: "persona es todo ente susceptible de adquirir derechos o contraer obligaciones. Para la ciencia jurídica la noción de persona es puramente de derecho, la palabra significa simplemente sujeto de derechos y obligaciones. Ahora bien, se dice que quien es capaz de tener derechos tiene personalidad o lo que es lo mismo, es persona. Se consideran derechos de personalidad la suma de hechos que la ley reconoce mientras que las obligaciones de la personalidad, se resumen en todas las cargas y deberes que la ley ordena sean a su encargo.

Este vocablo deriva de personare, máscara, careta, que usaban los actores en el mundo antiguo para cubrir su cara con el fin de darle resonancia a su voz; tiempos después la palabra significó el actor enmascarado, es decir, el personaje que representaba. Posteriormente, la palabra pasó a dominar al hombre mismo, siendo éste el calificativo que en la actualidad se le da."[7]

El hombre como entidad de derechos y obligaciones, es sin lugar a dudas, el objetivo mismo del Derecho Civil.

El conjunto de normas reguladoras de las relaciones ordinarias y más generales de la vida del hombre, en donde fija su actividad, generándose derechos y obligaciones, y con esto apropiándose de un cierto patrimonio y riqueza, van a darle a el sujeto como entidad del Derecho Civil, su naturaleza de ser el principio,

[7] Floresgómez González, Fernando y Carvajal Moreno, Gustavo: "Nociones de Derecho Positivo Mexicano"; México, Editorial Porrúa S.A. XXXI Ed. 1999. Pág. 270 y 271.

la persona sobre la cual, todos y cada una de las normas estarán evocadas para guardarle bienes jurídicos tutelados, que son propios de la persona, de sus derechos o de su patrimonio.

Esta circunstancia definitivamente es importante, en virtud de que toda norma, llámese laboral, civil, penal etc., trata de proteger un bien jurídico tutelado que es un bien de la sociedad protegido y reconocido por el derecho.

Las palabras del autor Raúl Goldstein, acerca del bien jurídico tutelado, explica lo siguiente: "es el interés medio o jurídico tenido en cuenta por el orden jurídico y cuya lesión constituye el contenido material del injusto. El bien jurídico así entendido, puede presentarse como objeto de protección de la ley o como objeto de ataque contra el que se dirige el delito, por lo cual no debe confundírsele con el objeto de la acción, que pertenece al mundo sensible. Aclarando el concepto de bien jurídico, que se define como el interés jurídico protegido, se señala que el bien jurídico no es un bien del derecho, sino un bien de los hombres reconocido y protegido por el derecho."[8]

Es importante, considerar lo establecido por el autor citado en relación a la amalgama de normas que están establecidas en los diversos códigos, especialmente en el Código Civil, y que éstas, van a generar para el grupo social, un cierto estatus a través del cual, se otorga la seguridad jurídica.

José Nodarce define el concepto de sociedad de la siguiente manera: "vamos a seguir ahora el concepto de sociedad a una clase de agrupación humana permanente, que tiene la cultura definida y un sentimiento y una conciencia más o menos vivos de los vínculos que unen a sus miembros en la coparticipación de intereses, actitudes, criterios de valores; sociedad es cualquier grupo humano relativamente permanente, capaz de subsistir en un medio físico dado y con cierto grado de realización que asegura su perpetuación biológica y el mantenimiento de

[8] Goldstein, Raúl: "Derecho Penal y Criminología"; Buenos Aires, Argentina, Editorial Astrea 4° Ed. 1998. Pág. 85.

una cultura, y que posee, además, una determinada conciencia de su unidad espiritual e histórica."[9]

El grupo social exige necesariamente que el individuo pueda quedar determinado y además protegido en su persona, sus derechos y su patrimonio. De tal manera, que de esta forma pueda extender su personalidad jurídica hacia lo que es la actividad de negocio. A esto se le llama actos de negocio.

No se puede llevar a cabo ningún acto, si no se tiene personalidad jurídica, que es el punto inicial en donde el individuo como sujeto del Derecho Civil, parte para reglamentar sus actos jurídicos dentro de la sociedad.

1.4.- SU PERSONALIDAD JURÍDICA.

La legislación civil, establece claramente, desde que momento empieza la personalidad y hasta qué momento debe de terminarse en el contenido del artículo 22 del Código Civil para el Distrito Federal, el cual menciona lo siguiente: "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."[10]

La personalidad jurídica del individuo, empieza a surgir desde que dicho individuo, nace; incluso, como lo dice la propia legislación citada, vamos a encontrar que desde que es concebido, puede el individuo llegar a tener una cierta personalidad.

Efraín Moto Salazar cuando habla de un concepto de personalidad y hace los comentarios siguientes: "todo derecho, estudiándolo desde el punto de vista

[9] Nodarce, José: "Elementos de Sociología"; México, Editorial Selecto, XXXV Ed. 1999. Pág. 2 y 3.
[10] Código Civil para el Distrito Federal. México, Editorial Sista. Pág. 6.

subjetivo, es decir, como la facultad reconocida al individuo por la ley para realizar determinados actos en satisfacción de sus propios intereses, presupone, necesariamente, un titular, es decir, un ser que sea capaz de poseerlo. Ahora bien, el hombre es el único ser que puede ser sujeto de derechos, éstos son fundamentalmente humanos, no pueden existir independientemente del hombre, exigen, necesariamente, alguien que los posea, que sea su titular, ese alguien es el hombre mismo.

En el lenguaje jurídico se dice que quien es capaz de tener derechos tiene personalidad o, en otras palabras, es persona. Por tanto, se puede definir a la persona desde el punto de vista jurídico, diciendo que es todo ser capaz de tener obligaciones y derechos; y la personalidad, como la actitud o idoneidad, para ser sujeto de derechos y obligaciones. Este concepto de la personalidad se confunde, con lo que es la capacidad jurídica."[11]

Tal vez esto tendría que ser el primer conflicto que se deba resolver, la distinción entre lo que es la capacidad jurídica de las personas y la personalidad de las mismas.

Un ser, tiene personalidad desde el momento en que es concebido para algunos efectos; de tal manera que, si en un momento determinado el autor de un testamento no deja la pensión alimenticia o bienes suficientes para que puedan garantizar la pensión alimenticia de su hijo póstumo, pues simple y sencillamente el testamento puede declararse inoficioso.

A través del ejemplo anterior, se puede notar cómo el ser concebido, tiene una cierta personalidad jurídica.

[11] Moto Salazar, Efraín: "Elementos de Derecho"; México, Editorial Porrúa S.A. XXXVI Ed. 2001. Pág. 129.

Desde otro ángulo, se aprecia que el que tiene interés o tiene una cierta relación con el acto jurídico, es aquél que tiene la personalidad necesaria para llevarlo a cabo.

Hay una íntima relación o legitimación de la personalidad jurídica con el acto jurídico que se realiza.

1.5.- ATRIBUTOS DE LA PERSONALIDAD.

El hombre no puede vivir como una persona aislada, sino que entra a un grupo social en donde se agolpan los intereses, y es el lugar en donde se tiene que ofrecer la seguridad jurídica para que dichos intereses no entren en conflicto.

La personalidad puede representarse en dos formas; la física y la material. La personalidad moral, por otro lado, es sin lugar a dudas una ficción del derecho, cuando varias personas se asocian o se reúnen, establecen un marco estatutario y generan una personalidad distinta a la de los socios, es en ese momento cuando estaremos frente a una persona moral.

Tanto las personas físicas como las morales tienen capacidad jurídica y por supuesto personalidad.

Por lo que, estos atributos de la personalidad jurídica los he desglosado para estudiarlos por separado:

1.5.1.- LA CAPACIDAD.

Para comenzar, considero importante distinguir el concepto de personalidad con relación a la capacidad.

El autor Rafael Rojina Villegas, en el momento en que nos habla de la capacidad dice lo siguiente: "la capacidad es el atributo mas importante de las personas. Todo sujeto de derecho, por serlo, debe tener capacidad jurídica; ésta puede ser total o parcial. Es la capacidad de goce, el atributo esencial e imprescindible de toda persona, ya que la capacidad de ejercicio que se refiere a las personas físicas, puede faltar en ellas y, sin embargo, existir la personalidad.

La capacidad de goce, es la aptitud para ser titular de derechos o para ser sujeto de obligaciones. Todo sujeto debe de tenerla. Si se suprime desaparece la personalidad por cuanto impide al ente la posibilidad jurídica de actuar…

La capacidad de ejercicio y representación supone la posibilidad jurídica en el sujeto de hacer valer directamente sus derechos, de celebrar en nombre propio actos jurídicos, de contraer y cumplir sus obligaciones y de ejercitar las acciones conducentes ante los tribunales."[12]

El autor antes citado hace una distinción inicial de lo que sería la personalidad y los tipos de capacidades. Se debe recordar que en el artículo 22 del Código Civil citado, habla de capacidad. De tal manera que, la capacidad es un atributo esencial del hombre, no puede faltar puesto que de lo contrario, deja de existir la personalidad.

Esa capacidad de goce, todos y cada uno de nosotros la tenemos, aún a pesar de que sean menores de edad o estén privados de razón; esto es, que existen

[12] Rojina Villegas, Rafael: "Compendio de Derecho Civil, Introducción, Personas y Familia"; México, Editorial Porrúa S.A., XXVIII Ed. 1999. Tomo I. Pág 158 y 164.

mayores de edad que tienen incapacidad legal y natural, puesto que no pueden manifestar correctamente su voluntad, necesitan a otra persona que lo represente.

De tal manera, que “la firma” que como concepto que ocupa en este trabajo de tesis, no se refiere a la capacidad de goce, sino a la capacidad de ejercicio.

Y no como capacidad de sujeto sino más que nada, como una expresión de su voluntad.

Para explicar esto, quisiera citar el artículo 450 del Código Civil que menciona lo siguiente:

“Tienen incapacidad legal y natural:

1. Los menores de edad;
2. Los mayores de edad que por causa de enfermedad reversible o irreversible, o que por su estado particular de discapacidad, ya sea de carácter físico, sensorial, intelectual, emocional, mental o varias de ellas a la vez, no puedan gobernarse, obligarse o manifestar su voluntad, por sí mismos o por medio que las supla.”[13]

El primer atributo de la personalidad como es la capacidad, nos lleva a lo que sería el yo interno del sujeto.

Esto es, que aún a pesar de que una persona caiga en los presupuestos del artículo 450 del Código Civil, tendrá la posibilidad de ser sujeta de derechos y obligaciones, pero contando con un tutor, con un representante, situación distinta a aquellas personas que la ley les reconoce capacidad de ejercicio.

[13] Código Civil. México, Editorial Sista. Obra Citada. Pág. 54.

1.5.2.- EL NOMBRE O DENOMINACIÓN SOCIAL.

Por otro lado, lo que es el concepto del nombre como atributo de la personalidad jurídica, será la forma distintiva y además personalizada a través de la cual, el individuo quedará individualizado y clasificado dentro de lo que es su grupo social.

Incluso, lo que son las personas morales tendrán una denominación social, para lograr los mismos efectos.

Sobre lo que es el nombre, Efraín Moto Salazar considera: "el nombre es la denominación verbal o escrita de la persona, sirve para distinguirla de las demás que forman el grupo social, haciéndola, en cierto modo inconfundible. El nombre de una persona se forma de varios vocablos unidos, que no tienen el mismo origen ni la misma importancia; el nombre propiamente dicho es arbitrario, lo dan los padres al niño según nuestra costumbre; los hijos legítimos toman el apellido de su padre. Esta es una regla que se ha impuesto por costumbre, y los hijos legitimados, es decir, los nacidos de dos personas no unidas en matrimonio, pero que posteriormente lo hacen, llevan el apellido de sus padres, cuando éstos lo reconocen ya sea antes o después de celebrado el matrimonio."[14]

Sin lugar a dudas, el nombre, como distintivo inconfundible de la persona, debe antes y sobretodo, fijarse para que, de alguna manera, se establezca la individualización del sujeto y todos los derechos y obligaciones, que se van generando, sean respondidos por dicho nombre.

1.5.3.- EL DOMICILIO.

Otro elemento, atributo de las personas, es el domicilio.

[14] Moto Salazar, Efraín. Obra Citada. Pág. 130 y 131.

El articulo 29 del Código Civil dice lo siguiente: “el domicilio de las personas físicas es el lugar donde residen habitualmente; y a falta de éste, el lugar del centro principal de sus negocios; en ausencia de éstos el lugar a donde simplemente residan y, en su defecto el lugar donde se encuentren.

Se presume que una persona reside habitualmente en un lugar, cuando permanezca en él por mas de seis meses.”

Y a mayor abundancia el artículo 30 dice: “el domicilio legal de una persona física es el lugar donde la ley le fija su residencia para el ejercicio de sus derechos y el cumplimiento de sus obligaciones, aunque de hecho no esté ahí presente.”

Sin duda, el domicilio es el lugar en donde una persona reside habitualmente o bien con el propósito de establecerse en él. Evidentemente que los artículos señalados, señala, las clases de domicilio, el voluntario y el convencional.

El voluntario evidentemente es donde la persona reside, y el convencional, puede llevarse a cabo dependiendo de las situaciones convenientes para la persona, siendo que una de ellas, es el citar el domicilio de sus representantes legales para cualquier otra circunstancia o situación.

1.5.4.- PATRIMONIO

El patrimonio se refiere a uno de los atributos de la personalidad más trascendental para el hombre.

El contexto de la seguridad jurídica se basa en la defensa de los derechos de la persona y de su patrimonio.

De esta forma, el ángulo protectivo de la norma, se protege a la persona como individuo, a sus derechos como derechos subjetivos y a su patrimonio; es en este último elemento en donde más existen normas jurídicas que hacen que el patrimonio sea uno de los bienes jurídicos tutelados por las normas de más alta prioridad.

Julián Bonecase, cuando se refiere al tema menciona lo siguiente: "el patrimonio en su más alta expresión es, la personalidad misma del hombre considerada en sus relaciones con los objetivos exteriores, sobre los cuales puede o podrá tener derechos que ejercitar; comprende no solamente en acta, los bienes ya adquiridos, sino también en potencia, los bienes por adquirirse; es esto lo que expresa correctamente la palabra "Vermögen" que significa a la vez perder el patrimonio. El patrimonio de una persona es su potencia jurídica, considerada de una manera absoluta y libre de todo límite de tiempo y espacio. El patrimonio declaran los autores, es el conjunto de los bienes de una persona, considerados como una universalidad de derechos."[15]

La riqueza y el acaparamiento de bienes, van a permitir al hombre diferenciarse de otros hombres que de alguna manera, no han tenido mayor fortuna que el otro.

Esta diferenciación económica, marca incluso actualmente las diferencias de estrato social.

De tal manera que, este elemento atributo de la persona, que le permite la apropiación, y con la apropiación el dominio y disposición de la cosa, hacen que todo aquello que es susceptible de apropiarse, pueda pasar a su peculio, y a su disposición, con la necesaria seguridad jurídica que requiere para su disponibilidad.

Ahora bien, he considerado a la seguridad jurídica, pero no se ha mencionado una definición de ella, por lo que se considera de interés, citar las palabras de Rafael

[15] Bonecase, Julián: "Tratado Elemental del Derecho Civil"; México, Editorial Harla 8° Ed. 1998. Pág. 466.

Preciado Hernández: “es la garantía dada al individuo de que su persona, sus bienes y sus derechos, no serán objeto de ataques violentos o que, si estos llegan a producirse, le serán asegurados por la sociedad, protección y reparación. En otros términos, está en seguridad aquel quien tiene la garantía de que su situación no será modificada sino por procedimientos societarios y, por consecuencia, regulares, legítimos y conforme a la ley.”[16]

Todo el contenido de la seguridad jurídica se ofrece al individuo, ya sea con una personalidad física o bien moral; pero aún en lo que es la formación de la persona moral ésta necesariamente está respaldada por personas físicas. Incluso las empresas piramidales o holding, que van formándose de personas morales, nacen en algún momento de personas físicas. De tal manera, que la seguridad jurídica, va a otorgarle al individuo, tanto la posibilidad en el derecho, de proteger a su persona, a sus derechos y por supuesto a su patrimonio. Y esto lo hace a través de las reglas que establecen tanto dentro de la Constitución, como en el Derecho Civil, en el Derecho Mercantil, etc.

Le va dando al hombre, reglas específicas para que en sus actos de negocio exista la efectividad legal.

[16] Preciado Hernández, Rafael: “Lecciones de Filosofía del Derecho”; México, Editorial Jud. XXI Ed. 1998. Pág. 233.

CAPÍTULO 2

LA FIRMA COMO LA EXPRESIÓN DE LA VOLUNTAD DEL INDIVIDUO.

El hecho de referirse a la firma como esa expresión del consentimiento de la persona, hace que el acto jurídico que dicha persona lleva acabo, le genere derechos y obligaciones que en un momento determinado haya consentido.

Evidentemente, que la firma también va a significar una constancia; el hecho de que la suscripción de su puño y letra sea característica distintiva de cada una de las personas y que de alguna manera podrán parecerse las firmas pero no ser iguales, hace que la huella digital especial de la persona frente a su relación de negocios con el mundo que lo rodea, sea diferente y además identificable por lo que, pudiésemos decir que la firma llega a ser también un atributo de la persona.

A continuación se hablará acerca de la firma como aquella expresión de la voluntad en los actos jurídicos que se llevan a cabo.

2.1.- DE LA TEORÍA DEL ACTO JURÍDICO.

Todo lo que es el acto jurídico, puede observarse desde dos ángulos generales desde el punto de vista de la teoría bipartita; El primero basado en que el hombre expresa su voluntad a través de lo que es el acto jurídico y se generan derechos y obligaciones a través de lo que es el hecho jurídico; y por el otro lado, la apertura en relación a la naturaleza de la intervención de la actividad humana para crear o extinguir derechos y obligaciones, como es el negocio jurídico frente al acto jurídico, en donde no interviene la voluntad del hombre para producir consecuencias de derecho. Y segundo lo que es el

hecho jurídico en relación a hechos de la naturaleza y que por supuesto producen consecuencias de derecho.

Para fundamentar estas ideas es necesario citar las palabras de el autor Ángel Caso referente al acto jurídico: "La vida humana es una sucesión de hechos o acontecimientos que se ligan entre sí y cuya existencia depende, bien de la voluntad del hombre, o bien de las circunstancias ajenas de la misma. Los hechos que se producen en la vida del hombre caen, con frecuencia, dentro del campo de derecho; en el primer caso tenemos los llamados hechos simples, en el segundo, los hechos jurídicos propiamente dichos, los cuales podemos definir como los acontecimientos o circunstancias positivos o negativos a los cuales la ley les atribuye consecuencias jurídicas.

Los hechos jurídicos más importantes son los actos humanos. El acto es una acción ejecución o modo de proceder, y en el interviene generalmente la voluntad.
Los fenómenos o circunstancias a los cuales atribuye la ley efectos jurídicos, que se realizan por la intervención de la voluntad del hombre y con intención de crear, modificar o extinguir relaciones jurídicas, o dicho sintéticamente y dado el conocimiento de los anteriores hechos jurídicos voluntarios o intencionales son el acto jurídico con voluntad del hombre."[17]

Desde un punto de vista tripartita, el hecho que produce consecuencias de derecho, en donde interviene la voluntad del hombre, se le denomina negocio jurídico.

De tal manera, que a lo que al hombre le interesa crear o modificar, y en donde va a estampar su firma como la expresión de su consentimiento, será a través de el negocio jurídico o bien el acto jurídico dependiendo la teoría que podamos considerar para este trabajo de tesis.

[17] Caso, Ángel: "principios de derecho"; México, Editorial Cultura, 3ra Ed. 1998 Pág. 22 y 23.

Para un mayor desglose se considerará al acto jurídico como:

1.- Negocio jurídico: al acto del ser humano, al cual esta dirigiéndose la voluntad con un cierto interés, y al cual, la legislación le establece consecuencias de derecho.

2.- Al acto jurídico: en donde la voluntad del hombre no interviene, pero se producen consecuencias de derecho por su obrar imprudente o falto de cuidado.

3.- Hecho jurídico: cuando la naturaleza sufre cataclismos de cualquier índole y hacen que estas circunstancias naturales produzcan consecuencias de derecho.

El negocio jurídico es el que me interesa para este trabajo de tesis, en virtud de que en esta naturaleza del actuar del hombre, va estar dirigida la voluntad de la persona.

2.1.1.-EL NEGOCIO JURÍDICO.

La intencionalidad en lo que es la producción de las consecuencias de derecho, se ha de reflejar a través de lo que es la negociación jurídica, por lo que el planteamiento dependerá de la voluntad y su manifestación.

Julián Bonnecase cuando se refiere al negocio jurídico menciona lo siguiente: “Cuando se considera en general el acto jurídico y el contrato, desde el punto de vista de la voluntad, se plantea un doble problema admitiéndose, naturalmente, que no se discute la necesidad de que existe una voluntad y la manifestación de ésta para que haya un acto jurídico. Pero establecido lo anterior, se trata en primer lugar, de precisar si de acuerdo con una pretendida regla, considerada hasta hoy, como indiscutible, se haya la voluntad totalmente sustraída, en el derecho civil moderno de una manera general, a la

influencia de la forma siendo, por tanto soberana, en cuanto a la formación de el acto jurídico."[18]

Lo que distingue al negocio jurídico como acto, es la manifestación de la voluntad, esa expresión a través de la cual, se van a producir las consecuencias de derecho, y que es aceptada por las partes que han entrado en la negociación.

Para un mayor desglose, se considerará al acto jurídico como: *La expresión soberana de la voluntad del individuo para producir consecuencias de derecho.*

En la negociación jurídica la voluntad del individuo es la que determina hacia dónde se producirán dichas consecuencias de derecho.

2.1.2- EL ACTO JURÍDICO.

Desde el punto de vista causalista, esto es, un obrar del individuo, se producen consecuencias de derecho, en donde hemos de encontrar que se lleva a cabo un acto jurídico según la teoría tripartita o bien un hecho jurídico según la teoría bipartita.

Desde el punto de vista de el derecho penal, se aprecia subjetivamente cual es en si, la naturaleza principal a través de la cual se puede exteriorizar el caso de la causalidad, esto es, que por la causa y el efecto se producen las consecuencias de derecho.

En este caso la voluntad ya no está dirigida, ya no hay una negociación previa, ya no hay una toma y daca, por lo que se produce la consecuencia por una negligencia por parte de la persona; y como resultado de lo anterior, las consecuencias de derecho.

[18] Bonnecase, Julián: "Tratado elemental de derecho civil"; México, Editorial Harla, 8vaEd. 1998 Pag.765.

Esta es una culpabilidad o bien, un actuar imprudente que se denota mejor desde el punto de vista del derecho penal y, por lo tanto, quisiera citar las palabras del autor Cesar Augusto Osorio Nieto que cuando nos habla de la imprudencia nos dice lo siguiente: “La culpa o imprudencia la encontramos cuando el activo no desea realizar una conducta que lleve un resultado delictivo, pero por un actuar imprudente, negligente, carente de atención, cuidados y reflexión verifique una conducta que produce un resultado, previsible delictuoso.” En este caso, la conducta es imprudencial culposa o no intencional.

“Los elementos de la culpa son: una conducta positiva o negativa, ausencia de cuidados o precauciones exigidas por el estado, resultado típico, previsible, evitable y no deseado de una relación causal entre la conducta y el resultado.”[19]

Básicamente el resultado de las consecuencias de derecho se da por causalidad. La causa - efecto y el resultado dañino que produce una responsabilidad para el agente que impulsa dicha causa, produciéndose un efecto dañino. De tal naturaleza, es un hecho jurídico un momento determinado, ya que no va a intervenir la voluntad del hombre, sino la mano del hombre.

2.1.3.- EL HECHO JURÍDICO.

También por acontecimientos naturales o del hombre, se van ha generar consecuencias de derecho, consistentes en crear, trasmitir, modificar o extinguir derechos u obligaciones, donde no intervine la voluntad del hombre. Como por ejemplo en desastres naturales, nacimiento o muerte.

[19] Osorio y Nieto, Cesar Augusto: “Síntesis del derecho penal”; México, Editorial Trillas 3°Ed. 1999. Págs. 66 y 67.

Evidentemente habría que encontrar el nexo de causalidad para establecer la responsabilidad para quien en un momento determinado pueda tener la obligación de resarcir los daños. Esto resulta una situación especial, puesto que tienen que ventilarse los casos concretos para observar los detalles de la causalidad.

Básicamente el hecho jurídico parte de los actos y hechos de la naturaleza, en donde no intervienen la voluntad del hombre ni su actuar, sino que se produce por actos de la naturaleza con consecuencias de derecho.

2.2.- LA FIRMA: SU CONCEPTO.

El autor Raúl Goldstein explica el concepto de la firma: "La firma es un nombre escrito de una manera particular, según el modo habitual observado por la persona en diversos actos sometidos a esta formalidad. No es la simple escritura que se hace del nombre y apellido. Si es frecuente que esta expresión grafica tenga una rubrica, es decir, rasgo o rasgos de determinada figura que se colocan después del nombre o titulo, ello no es absolutamente común ni tampoco indispensable. No es, así mismo, necesario que sea la reproducción textual de los nombres de quien la escribe; ni es exigencia que lo sea, ni es por otra parte usual. Pero es necesario y suficiente que sea el modo habitual, frecuente, empleado por la persona como firma. Tiene la firma una superlativa importancia en el ámbito de las transacciones y de los negocios jurídicos, lo cual explica la protección penal que se le dispensa."[20]

La conceptualización que el autor citado ha ofrecido, revela esa habitualidad en la exposición del nombre y los apellidos de la persona, o bien un símbolo representativo de su identidad.

[20] Goldstein, Raúl :"Derecho Penal y Criminología"; Buenos Aires Argentina, Editorial Astrea, 4°Ed. Pág. 356.

Sin lugar a dudas, con lo expuesto en el capítulo primero, se observó como dentro de los atributos de la personalidad, el nombre o denominación social, se encuentran en la posibilidad de crear una identidad única para cada una de las personas, y como consecuencia de esto, la diferenciación entre una persona y otra.

Los derechos y obligaciones que nacen, no son exactamente los mismos entre el marido y la mujer, ni tampoco son exactamente iguales entre hermanos o hermanas; cada una de las personas, tiene una gran individualidad en cuanto a sus derechos y obligaciones, aunque claro está, existen en algunas circunstancias, que la obligación de reparar los daños o resarcirlos, pasan a otras personas como por ejemplo de los menores de edad, quienes están al cuidado de sus padres, quines tiene la obligación de resarcir los daños que en una momento determinado puedan ocasionar sus hijos.

Otro autor que habla sobre la firma es Rafael de Pina quien menciona: “La firma es el nombre y apellido que una persona pone con rubrica o sin ella, al pie de un escrito como señal de autenticidad.

Puede suceder una firma en blanco que es la que se pone en un papel o pliego destinado a ser cubierto posteriormente por determinada persona autorizad por al autor de la suscripción y en los términos convenidos; firmar es autorizar un escrito o documento con la firma.”[21]
Dentro de lo que es el concepto de la firma, vamos a encontrar la exteriorización de la personalidad.

Sin lugar a dudas, es un símbolo que representa para toda la sociedad o bien para toda la universalidad de personas, el hecho de que la persona esta consintiendo como dice el autor de Pina; puesto que ha estampado su símbolo al calce o al margen de un documento.

[21] Pina, Rafael, de::”Derecho Civil”; México, Editorial Porrúa S.A. XXI Ed. 1995 Pág. 181.

O bien, está aceptando como suya alguna declaración o alguna circunstancia cuando estampa su emblema o su firma en un documento.

Esto quiere decir que autoriza lo que literalmente está escrito en el documento, y que, por supuesto lo acepta por que así consta en el documento.

2.3.- LA FIRMA COMO EXPRESIÓN DE LA VOLUNTAD DEL INDIVIDUO.

La voluntad se expresa a través del consentimiento y ese consentimiento se expresa a través del símbolo o de la firma que se estampe en un documento en donde se esta reconociendo absolutamente la situación que literalmente se expresa en el propio documento.

El autor Efraín Moto Salazar, cuando habla de la voluntad y la firma menciona: "La voluntad de una persona no puede obligarse cuando son menores de edad o los mayores faltos de razón, carece de valor legal; así mismo no tiene valor alguno la voluntad que, a pesar de expresarse, no responde plenamente a la intención que el autor del acto tuvo al realizarlo, como ocurre el los casos de error, dolo, o violencia. Para que la voluntad produzca efectos jurídicos es necesario que se manifieste o se exprese plenamente. Esta puede manifestarse en dos formas: en una forma expresa o en una forma tácita."

"Se dice que la voluntad es expresa, cuando se manifiesta sea verbal o por escrito o bien por signos o por firmas que no dejen lugar a dudas. Se dice que la voluntad es tacita, cuando resulta de actos que la presuponen o autorizan a presumirla."[22]

Nótese como la naturaleza sobre la cuál esta sentada la firma es de alta trascendencia para la existencia y validez de cualquier contrato.

[22] Moto Salazar, Efraín:"Elementos de Derecho"; México. Editorial Porrúa S.A. XXXVI Ed. 2001 Pag. 25.

En este inciso, se verán los elementos esenciales del contrato, en donde se estudiará con mayor profundidad lo que es la voluntad.

Pero, en estos momentos quisiera atraer la atención en el sentido de lo que el autor citado ha comentado, ya que se puede distinguir entre la aceptación expresa a través de los signos escritos como es la firma, y la autorización tácita como es el hecho de que a través de actos o circunstancias, se revela la intención de aceptación.

Ahora bien, debido a que la voluntad es parte esencial de lo que es la formación de los contratos, pasemos al siguiente inciso.

2.4.-ELEMENTOS ESENCIALES EN LOS CONTRATOS.

La actividad del individuo, se va a reflejar con mayor formalidad como negocio jurídico, en lo que son los contratos.

Esa manifestación de voluntades que llegan a un acuerdo para crear, modificar o extinguir derechos y obligaciones, es sin lugar a dudas, la manifestación más formal del negocio jurídico.

Rafael Rojina Villegas, cuando habla sobre lo que son los contratos menciona: “El contrato se define como un acuerdo de voluntades para crear o transmitir derechos y obligaciones; es una especie dentro de el género de los convenios. El convenio es un acuerdo de voluntades para crear, trasmitir, modificar o extinguir obligaciones y derechos reales o personales; por lo tanto, el convenio tiene dos funciones: una positiva, que es crear o transmitir obligaciones y derechos, y otra negativa: modificarlos o extinguirlos. Preferimos decir derechos reales y personales, y no derechos

patrimoniales, en virtud de que pueden existir derechos personales de contenido extra patrimonial."[23]

Independientemente de que se puede denotar algunas diferencias entre lo que son los contratos y lo que son los convenios, se dirá que en el contrato, básicamente lo que interesa para este trabajo de tesis, es el hecho de la manifestación de la voluntad a través del consentimiento quien a su vez se manifiesta por la firma estampada en un documento sea o no electrónico.

De tal manera, que a través de los contratos, se pueden crear o modificar derechos y obligaciones.

Para cada una de las partes que intervienen en los contratos, se genera un derecho y una obligación.

El contrato para que pueda tener existencia, se requiere que existían básicamente dos elementos:

1.-La expresión de la voluntad;
2.-El objeto en los contratos

Desde el punto de vista general, hay autores que consideran a la formalidad como parte de los elementos esenciales, y existe otra corriente de autores que consideran a la formalidad, como parte de los elementos de validez.

Para efectos de este estudio, hay que considerarlo tanto dentro del elemento esencial como también elemento de validez.

De tal naturaleza, que cuando la ley exige una cierta solemnidad para el acto, sino se tiene o se lleva a cabo, pues simplemente el acto podría resultar inexistente, pero en

[23] Rojina Villegas, Rafael: "Compete de derecho civil"; México, Editorial Porrúa S.A., XX111 Ed. Tomo IV, Contratos , 2001 Pág. 7

ocasiones, puede surtir ciertos efectos, con lo que se hace la solemnidad como un requisito de validez.

Para poder desglosar estos términos, es importante analizarlos uno por uno.

Desde el punto de vista de los elementos de validez del contrato:

1. La licitud en el objeto motivo o fin determinante en el contrato, la falta de ésta produce la nulidad absoluta del contrato.

La acción para pedir la nulidad absoluta la puede hacer valer cualquiera que tenga interés jurídico, ya que trata de disposiciones de orden publico.

2. La capacidad de los contratantes es decir que deberán contar con la mayoría de edad y estar en pleno uso de sus facultades mentales.

La capacidad puede ser de goce o de ejercicio cuando únicamente cuenta con la capacidad de goce debe de ser representada para celebrar contratos e inclusive de obtener autorización judicial para efectuarlos.

3. La formalidad o forma que deba revestir para perfeccionarlo.

4. Ausencia de vicios en el consentimiento como el dolo, la mala fe, la violencia, lección y error en los contratos.

A falta de los tres últimos elementos de validez el contrato será nulo relativamente, siempre y cuando alguno de los contratantes haga valer en tiempo su acción para demandar la nulidad del contrato, ya que la misma es prescriptible; la nulidad relativa es susceptible de convalidarse.

2.4.1.- LA VOLUNTAD EXPRESADA A TRAVES DEL CONSENTIMIENTO.

Sin lugar a dudas, la necesidad de expresar la voluntad, es el elemento principal a través del cual, se va a fijar el derecho y obligación que nace del acto jurídico que se realiza.

El autor Francisco Lozano Noriega cuando se refiere a esta circunstancia dice lo siguiente: "El papel que desempeña la voluntad de los contratantes en todo contrato, supone un acuerdo de voluntades, que es condición "sine qua non" para la existencia del contrato papel que puede ser desigual; en ocasiones es una de las partes la que redacta el contrato; hace, incluso, una policitación de carácter general, oficiosa. En otras palabras: ofrece a la colectividad, al público en general la celebración de un contrato ya determinado; la otra parte únicamente acepta las condiciones. Es decir: el contrato viene a hacer la obra de dos voluntades, puesto que se requiere el acuerdo de voluntades como en todo contrato, pero, en realidad, la influencia de una de las voluntades ha sido preponderante en la confección y preparación del contrato. Desde este punto de vista distinguimos los contratos de adhesión y los contratos de igual a igual."[24]

Sin lugar a dudas, la voluntad en los contratos, es la fórmula esencial a través de la cual, se ha de manifestar el consentimiento de la persona.

Esto es, que esa posibilidad de querer y entender lo que se lleva a cabo, y aceptarlo, va a darle la efectividad jurídica a la obligación consignada literalmente en el contrato.

Así, el hecho de llevar a cabo un acto jurídico de tal naturaleza, enviste la necesidad de que sea perfectamente legal, esto es de que no existe una cierta falsificación de firmas.

[24] Lozano Noriega, Francisco: "Contratos"; México, Asociación Nacional de Notariado, 8° Edición, 1999 Pág. 13.

Raúl Goldstein cuando habla sobre el particular dice: “Es condición para la existencia y validez de todo acto bajo forma privada, de todo instrumento privado, es decir, de cualquier documento creado por voluntad de las partes sin intervención oficial pública, el estampar una firma. Falsificar la firma es poner las grafías empleadas habitualmente por otra persona para la suscripción de documentos. La persona que tal acto realiza, crea un instrumento capaz de engendrar consecuencias jurídicas; es preciso determinar si dicha creación debe ser o no imitativa de su original, aspecto en el cual las opiniones son divergentes, desde el punto de vista doctrinario, aunque jurisprudencialmente el criterio ha sido uniformado en el sentido de no exigir que la firma apócrifa haya sido estampada tratando de imitar la original, bastando simplemente que reúna caracteres que le otorguen un aspecto general de autenticidad, en cuya virtud sea capaz de ocasionar perjuicios a terceros. La opinión contraria sustenta el criterio de que es imposible pensar siquiera en otro modo de falsificación que no sea la limitación de los signos que individualizan al supuesto otorgante.”[25]

Las grafías como lo dice el autor citado, van a significar para cada uno de los otros, la manera ideal a través de la cual, personalizamos la expresión de nuestro consentimiento, la expresión de nuestra voluntad.

De tal naturaleza, que sin la existencia de la voluntad, el acto jurídico no puede existir.

2.4.2.- EL OBJETO EN LOS CONTRATOS.

Otro de los elementos esenciales para que el contrato pueda existir, sin lugar a dudas es el objeto.

Evidentemente, que el objeto y fin de los contratos, debe necesariamente ser sobre hechos posibles que de alguna manera estén en el comercio.

[25] Goldstein, Raúl: Obra citada; Pág. 356.

El Código Civil cuando establece algunas ideas sobre el objeto del contrato, menciona que dicho objeto es la cosa que el obligado debe de dar, o el hecho que el obligado debe de hacer o no hacer.

La naturaleza de este objeto, debe de reunir tres características como son:

1.-Existir en la naturaleza;

2.-Ser determinada o determinable en cuanto a su especie.

3.-Estar en el comercio.

Para llevar a cabo contrato sobre cosas futuras, que puedan ser objeto de contrato, deben de quedar debidamente especificados.

De ahí, que el artículo 1827 del Código Civil para el Distrito Federal, básicamente manifiesta lo siguiente:

"Artículo 1827.- El hecho positivo negativo objeto de contrato, debe ser:

Fracción I: posible;

Fracción II: licito."[26]

Ese objeto que sea de naturaleza determinada o determinable, que pueda existir en la naturaleza y estar en el comercio, debe por fuerzas ser licito.

No se puede comerciar sobre cosas ilícitas, puesto que, no existiría un objeto dentro del contrato, y el contrato tendría que declararse inexistente.

[26] Código Civil Para El Distrito Federal" México, Editorial SISTA, Edición 2002, Pág. 148.

2.4.3.-SOLEMNIDAD.

La forma a través de la cual la voluntad se ha de expresar, llega a ser un elemento esencial, en algunos casos jurídicos, se requiere para que dicho acto pueda tener validez.

Por ejemplo, más que nada lo que son los actos registrables públicos.

Los nacimientos, el matrimonio, la defunción, que son actos totalmente registrables, y que si no cumplen con la formalidad de registro no pueden existir. Por lo tanto, representan el antecedente en el articulado de la ley que se propone en materia de excepción de la firma digital.

También, algunos actos como son la traslación en compra-venta de bienes y muebles registrables, en donde tiene que sobrevenir una cancelación de una escritura para poder establecer la nueva, y de esa manera, una vez que esté registrado pueda hacer efectos en contra de terceros.

De tal manera, que la ley en algunos casos, señala la necesidad de que el acto jurídico, deba de celebrase tanto por funcionario publico como también, dicho acto necesariamente tenga que estar debidamente registrado.

2.5.- ELEMENTOS DE VALIDEZ.

A diferencia de los elementos esenciales de existencia, los de validez van a permitir que exista el acto jurídico, pero en una forma relativa.

Dicho de otra manera, que ha pesar de que existe algún vicio en algunos de los elementos, la ley permite las consecuencias de derecho, con una cierta nulidad relativa

en lo que atañe a las formas que de alguna manera no son exactamente las que la ley establece para que el acto jurídico pueda tener la validez que la propia legislación fija.

Los elementos de validez son los siguientes:

1.- Los vicios en el consentimiento;
2.- La falta de capacidad;
3.- La forma.

2.5.1.- VICIOS EN EL CONSENTIMIENTO.

Son varios los vicios que se pueden dar en el consentimiento:
1.- El error;
2.- El dolo;
3.,- La violencia;
4.- La lesión.

Cuando una persona no tiene el estricto conocimiento de la realidad, esto es, que se le pueden falsear los hechos sobre los cuales motivan el otorgamiento de su firma, podemos decir que ésta se ha dado con un cierto error.

Ahora bien, es importante denotar en este momento, como es la intima relación de la persona, con la expresión de su voluntad y su situación frente a los vicios.
Esto en virtud de que la firma, necesariamente tiene una trascendencia jurídica que va a estar opacada por los vicios que de alguna manera hemos enumerado.

De tal manera, que la idea de la firma, debe necesariamente ser todo lo apersonado que se requiere para individualizar ese procedimiento que nace desde la idea del hombre, se expresa con un acto de exteriorización de la voluntad, y que manifiesta su

consentimiento, pero que lo hace, ya sea con error, o bien por efectos de un dolo, una violencia, e incluso, puede incurrir en una lesión en el acto jurídico.

El autor Hans Kelsen explica algunas situaciones filosóficas sobre la persona, y dice: "Queda abierto el camino para reconocer que el concepto sujeto de derecho o persona, no es otra cosa que una construcción artificial, un concepto auxiliar que se ha creado por el conocimiento jurídico con el fin de representarse gráficamente el material que trata de nominar, y bajo la presión de un lenguaje jurídico antropomórfico y personificado. La persona no es mas que una expresión unitaria personificadora de un haz de deberes y facultades jurídicas, es decir, de un complejo normativo: este punto de vista garantiza al derecho contra posibles hipótesis perturbadoras, que no reduplican inútilmente con objeto del conocimiento. Solo de ese modo es posible dar plena satisfacción a la antigua exigencia de la teoría positivista del derecho: comprender la persona jurídica y la persona física como cosa esencialmente idénticas."[27]
Cuando la persona está intuida por un dolo, o por una sugestión artificiosa, que lo induce al error, o bien se disimula un error para que se cree un falso concepto de las circunstancias, entonces está afectando a lo que el autor citado nos ha comentado como el respeto del derecho frente a la persona.

Se crea para la persona, una esfera jurídica de protección tal que le garantiza su existencia decorosa

Lo mismo sucede cuando se le impone una violencia sea física o moral a través de amenazas, que importen el peligro tanto de perder la vida, la honra, la libertad, la salud o parte considerable de sus bienes que hagan un temor dentro de la persona, y a la luz de esta circunstancia, se nulifique la posibilidad de consentir libremente.

Así, dentro de los vicios del consentimiento, estas circunstancias, van a generar su nulidad relativa, puesto que en un momento determinado, sabiéndose la verdad o

[27] Kelsen Hans: " Teoría Pura Del Derecho"; México, Editorial Colofón, 10° Ed. 2001, Pág. 43.

eliminándose la violencia o la lesión en la que se encontraba la persona, puede convalidarse el acto jurídico si así convienen las partes.

Por ejemplo, lo que es la lesión, cuando alguien se aprovecha de la inexperiencia o ignorancia de otra persona, ignorante puede demandar la disminución de su contraprestación o bien lograr una cierta indemnización proporcional que haga que entre lo que se da y lo que se recibe en el contrato, exista una equidad proporcional.(Art. 17 del C.C.D.F..).

2.5.2.- LA FALTA DE CAPACIDAD.

La capacidad es la fórmula idónea, a través de la cual, se genera la posibilidad de querer y entender lo que sucede en el medio ambiente.

El autor Rafael Rojina Villegas genera la siguiente redacción: “La capacidad es el atributo mas importante de las personas. Todo sujeto de derecho, por serlo, tiene que tener capacidad jurídica; esta puede ser total o parcial. Es la capacidad de goce el atributo esencial e imprescindible de toda persona, ya que la capacidad de ejercicio que se refiere a las personas físicas, puede faltar en ellas y, sin embargo, existir la personalidad.

“La capacidad de goce es la actitud de ser titular de derechos y obligaciones…”

“La capacidad de ejercicio o representación, supone la posibilidad jurídica en el sujeto de hacer valer directamente sus derechos, a celebrar el nombre propio sus actos

jurídicos, de contraer y cumplir sus obligaciones y de ejercitar las acciones conducentes ante los tribunales."[28]

La capacidad de ejercicio, es la necesaria para la realización de todo negocio jurídico; Los menores de edad y las personas privadas de razón que sean mayores de edad, necesitan un tutor, necesitan un representante especial a través de el cual van a poder llevar a cabo sus negociaciones jurídicas.

De tal manera que la propia legislación hace una esfera jurídica de protección, para que la persona no quede en un estado de indefensión, en un estado de lesión, y de esta manera, pueda tener un representante suficientemente capacitado, que vele por sus intereses.
Como consecuencia de lo anterior, puede ser que una persona en el momento en que firma un compromiso, no esté en sus capacidades, pero si se le pueda nombrar tutor, y con ello, puede convalidarse ese acto, si así le conviene a la persona que padece de la incapacidad.

La capacidad como un elemento de validez, puede convalidarse en el futuro cuando haya desaparecido la causa de nulidad.

[28] Rojina Villegas, Rafael: "Compendios De Derecho Civil"; México, Editorial Porrua S.A., Vigésimo Octava Edición, Tomo 1, 1999, Pág. 158 Y 164.

CAPÍTULO 3

DE LA FIRMA ELECTRÓNICA.

Proviene del latín "firmare" que significa corroborar o confirmar el contenido de un documento, lo cual se hacía poniendo la mano sobre él y después suscribiéndolo.

Según el Diccionario de la Lengua Española de la Real Academia, la firma es el "Nombre y apellido, o título, que una persona escribe de su propia mano en un documento, para darle autenticidad o para expresar que aprueba su contenido". [29]

A continuación mencionaré a varios autores que definen a la firma electrónica:

Planiol y Ripert la definen: "La firma es una inscripción manuscrita que indica el nombre de una persona que entiende hacer suya las declaraciones del acto". [30]

El Uniform Commercial Code de los EE.UU. establece en su sección 1-201 respecto de la expresión signed (firmado): "Includes any symbol executed or adopted by a party with present intention to authenticate a writing" ("Incluye cualquier símbolo realizado o adoptado por una parte con la actual intención de autentificar un escrito").

Llambias dice que la firma es "El trazo peculiar mediante el cual el sujeto consigna habitualmente su nombre y apellido o sólo su apellido, a fin de hacer constar las manifestaciones de su voluntad".[31]

---

[29] Diccionario de la Lengua Española de la Real Academia, Vigésima segunda edición, Madrid, 2002.

[30] Planiol y Ripert. Traite Pratique de Droit Civil Francais, T.VII, Nº1458. Cit por Siri García de Alonso, Julia y Wonsiak, María en El documento electrónico. Revista de la Facultad de Derecho y Ciencias Sociales, Nº 3 Y 4, Pág.294, julio-diciembre 1988

[31] Llambías, Joaquín, "Tratado de Derecho Civil, Parte General", Tº II, pág. 404).

Como se puede observar, estas definiciones pueden incluir un número muy amplio de "formas" de firmar, no sólo la clásica que todos conocemos.

Se debe hacer notar que las dos últimas definiciones hacen hincapié en la habitualidad de la firma, receptando la corriente doctrinaria tradicional. Sin embargo, la doctrina moderna sostiene que la habitualidad no hace a la esencia de la firma sino la comprobación de su autenticidad a través del cotejo con otras registradas en asientos indubitables. La firma es la prueba de la manifestación de la voluntad que permite imputar la autoría e identificar al firmante de un instrumento.

Ahora bien, la firma es pues, una forma de exteriorización de la voluntad humana y ésta puede manifestarse por diferentes formas, por un gesto, palabras, escritura, fax, etc. La manifestación de la voluntad en relación a un documento electrónico no puede ser la firma manuscrita. Por ello la ley debe reconocer una forma electrónica de consentir como válida y eficaz para la suscripción de documentos electrónicos. Así como lo es un signo grafoscopio salido del puño y letra de una persona, y que significa, la manifestación de consentimiento para estar de acuerdo o no a una circunstancia determinada.

En las transacciones electrónicas este sello o firma digital básicamente va adherido al documento y consta de dígitos alfa-numéricos o de otros símbolos.

Esto le permite tener los elementos necesarios de autenticidad y confidencialidad que requiere cualquier documento electrónico y con esto tener atributos necesarios para darle el mismo valor que una firma autógrafa.

3.1.- SU CONCEPTO.

La incorporación de las nuevas tecnologías de la información hace que, en muchas ocasiones, los conceptos jurídicos tradicionales resulten poco idóneos para interpretar las nuevas realidades, por ello, la firma electrónica es una manera de representación y confirmación de la identidad de un sujeto en los medios electrónicos. La doctrina jurídica conviene en que la firma es el género, la firma electrónica una especie y dentro de ésta encontramos subespecies, tales como las denominadas en algunas legislaciones como firma digital, firma electrónica avanzada, ó firma electrónica certificada.

Conforme a la norma ISO/IEC 7498-2 de la Organización por la Estandardización internacional (OEI), la firma digital es definida como "Datos asociados con, o la transformación criptográfica de una unidad de datos que permite al recipiente probar la fuente y la integridad de la unidad de datos y proteger contra una falsificación, como el recipiente por ejemplo". En otras palabras, la firma digital puede ser realizada con la criptografía asimétrica como con la simétrica asociada a un dispositivo incorruptible de creación de firma y un dispositivo incorruptible de verificación de firma. Sin embargo, la legislación positiva asocia el término "firma digital" con los mecanismos de clave públicas y considera la "firma digital OEI" como una "firma electrónica", definida en general como letras, caracteres, números u otros símbolos en forma digital adjuntos o lógicamente asociados con un mensaje electrónico, y ejecutados o adoptados con la intención de autentificar o aprobar el mensaje electrónico. Sólo la ley italiana así como algunas leyes americanas están utilizando la definición original de la OEI. En consecuencia, estamos utilizando el término genérico de "firma virtual" que incluye por una parte la firma digital designando la infraestructura de clave pública y, por otra parte, la firma electrónica designando de manera general todas las otras formas de firmas en el ambiente electrónico. Haría confusión de decir que la firma electrónica incluye la firma digital en la medida que algunas leyes hacen la distinción entre estos dos tipos de firma.

Para redondear lo dicho con anterioridad, la firma digital, es un bloque de caracteres que acompaña a un documento (o fichero) acreditando quién es su autor (**autenticación**) y que no ha existido ninguna manipulación posterior de los datos (**integridad**). Para firmar un documento digital, su autor utiliza su propia clave secreta (sistema criptográfico asimétrica), a la que sólo el tiene acceso, lo que impide que pueda después negar su autoría (**no revocación o no repudio**). De esta forma, el autor queda vinculado al documento de la firma. Por último la validez de dicha firma podrá ser comprobada por cualquier persona que disponga de la clave pública del autor.

El autor Hugo Daniel Carrión diferencia entre la firma manuscrita y la firma digital: "Actualmente la firma manuscrita permite certificar el reconocimiento, la conformidad o el acuerdo de voluntades sobre un documento por parte de cada firmante, aspecto de gran importancia desde un punto de vista legal. La firma manuscrita tiene un reconocimiento particularmente alto, pese a que puede ser falsificada, ya que tiene peculiaridades que la hacen fácil de realizar, comprobar y de vincular a quien la realiza. Para conseguir los mismos efectos que la firma manuscrita se requiere el uso de criptología que es el empleo de algoritmos matemáticos.

La firma digital consiste en la utilización de un método de encriptación llamado asimétrico o clave pública. Este método consiste en establecer un par de claves asociadas a un sujeto, una pública, conocida por todos los sujetos intervinientes en el sector y otra privada solo conocida por el sujeto en cuestión. De esta forma, cuando se desea establecer una comunicación segura con otra parte, basta con encriptar el mensaje con la clave única del sujeto para que a su recepción sólo el sujeto que posee la clave privada puede leerlo".[32]

Técnicamente la firma digital se define como una secuencia de datos electrónicos (bits) que se obtienen mediante la aplicación a un mensaje determinado de un algoritmo (fórmula matemática) de cifrado asimétricos o de clave pública, y que equivale

[32] Carrión , Hugo Daniel: "Análisis comparativo de la legislación y proyectos a nivel mundial sobre firmas y certificados digitales"; Información Internet, pp.1

funcionalmente a la firma autógrafa en orden a la identificación del autor del que procede el mensaje.

Desde un punto de vista material, la firma digital es una simple cadena o secuencia de caracteres que se adjuntan al final del cuerpo del mensaje firmado digitalmente.

El autor Emilio del Peso Navarro dice lo siguiente al respecto: "Es una señal digital representada por una cadena de BITS que se caracteriza por ser secreta, fácil de reproducir y conocer, difícil de falsificar y cambiante en función del mensaje y en función del tiempo, cuya utilización obliga a la aparición de lo que denomina fedatario electrónico o telemático que será capaz de verificar la autenticidad de los documentos que circulan a través de las líneas de comunicación, al tener no solamente una formación informática, sino también de tipo jurídica."[33]

La expresión a través de la firma digital, debe obligatoriamente de revelar esa exteriorización de la voluntad humana para que la misma quede debidamente expresada.

3.2.- DE LA FIRMA AUTÓGRAFA.

Siguiendo a Carrascosa López, se puede indicar que en Roma, los documentos no eran firmados. Existía una ceremonia llamada *manufirmatio*, por la cual, luego de la lectura del documento por su autor o el *notarius*, era desplegado sobre una mesa y se le pasaba la mano por el pergamino en signo de su aceptación. Solamente después de cumplir esta ceremonia se estampaba el nombre del autor.

[33] Peso Navarro, Emilio: "La Solución de Conflictos en el Intercambio Electrónico de Documentos"; Madrid, España, Cuadernos De Derecho Judicial, Escuela Judicial Consejo General Del Poder Judicial, 1996, Pág. 191.

En el Sistema Jurídico Visigótico existía la confirmación del documento por los testigos que lo tocaban (*chartam tangere),* signaban o suscribían (*firmatio, roboratio, stipulatio).* La firma del que da el documento o librador es corriente, pero no imprescindible. Los documentos privados son, en ocasiones, confirmados por documentos reales. Desde la época euriciana las leyes visigodas prestaron atención a las formalidades documentales, regulando detalladamente las suscripciones, signos y comprobación de escrituras. La "*subscriptio"*, representaba la indicación del nombre del signante y la fecha, y el "*signum"*, un rasgo que la sustituye si no sabe o no puede escribir. La "*subcriptio"* daba pleno valor probatorio al documento y el "*signun"* debía ser completado con el juramento de la veracidad por parte de uno de los testigos. Si falta la firma y el signo del autor del documento, éste es inoperante y debe completarse con el juramento de los testigos sobre la veracidad del contenido.

En la Edad Media, la documentación regia viene garantizada en su autenticidad por la implantación del sello real. Sello que posteriormente pasó a las clases nobles y privilegiadas.

La firma es definida en la doctrina como el signo personal distintivo que, permite informar acerca de la identidad del autor de un documento, y manifestar su acuerdo sobre el contenido del acto.

La Real Academia de la Lengua define la firma 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 a lo que en él se dice".[34]

En el Vocabulario Jurídico de Coutoure 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".[35]

3.3.- CARACTERÍSTICAS DE LA FIRMA.

De las anteriores definiciones se desprenden las siguientes características:

- ≤**Identificatíva:** Sirve para identificar quién es el autor del documento.

- **Declarativa:** Significa la asunción del contenido del documento por el autor de la firma. Sobre todo cuando se trata de la conclusión de un contrato, la firma es el signo principal que representa la voluntad de obligarse.

[34] Diccionario de la Lengua Española de Real Academia Española, Editorial: Espasa-Calpe sa, 22ª ed. 2 vols. 2001.

[35] Couture, Eduardo J. "Vocabulario Jurídico". Editorial:-Julio César Faira, Tercera Ed, actualizada y ampliada por Ángel Landoni Sosa – Empastada. Montevideo, Buenos Aires:2004.

- **Probatoria:** Permite identificar si el autor de la firma es efectivamente aquél que ha sido identificado como tal en el acto de la propia firma.

3.4.- ELEMENTOS DE LA FIRMA.

Se distinguen los siguientes elementos:

- **Elementos formales**

Son aquellos elementos materiales de la firma que están en relación con los procedimientos utilizados para firmar y el grafismo mismo de la firma.

- *La firma como signo personal*

La firma se presenta como un signo distintivo y personal, ya que debe ser puesta de puño y letra del firmante. Esta característica de la firma manuscrita puede ser eliminada y sustituida por otros medios en la firma electrónica.

- *-El animus signandi*

Es el elemento intencional o intelectual de la firma. Consiste en la voluntad de asumir el contenido de un documento, que no debe confundirse con la voluntad de contratar.

- **Elementos funcionales**

Tomando la noción de firma como el signo o conjunto de signos, se distinguie una doble función:

- *Identificadora*

La firma asegura la relación jurídica entre el acto firmado y la persona que lo ha firmado.

La identidad de la persona nos determina su personalidad a efectos de atribución de los derechos y obligaciones.

La firma manuscrita expresa la identidad, aceptación y autoría del firmante. No es un método de autenticación totalmente fiable. En el caso de que se reconozca la firma, el documento podría haber sido modificado en cuanto a su contenido -falsificado- y en el caso de que no exista la firma autógrafa parece que ya no exista otro modo de autenticación. En caso de duda o negación puede establecerse la correspondiente pericial caligráfica para su esclarecimiento.

- *Autenticación*

El acto expresa su consentimiento y hace propio el mensaje. Destacando:

- Operación pasiva que no requiere del consentimiento, ni del conocimiento siquiera del sujeto identificado.

- Proceso activo por el cual alguien se identifica conscientemente en cuanto al contenido suscrito y se adhiere al mismo.

3.5.- FIRMA DIGITAL (ELECTRÓNICA).

Desde el punto de vista técnico, como alternativa a la firma manuscrita sobre papel se ofrecen las firmas electrónicas y/o digitales.

En el comercio electrónico el clásico documento de papel es sustituido por el documento electrónico. Correlativamente, desaparecen las tradicionales firmas manuscritas, que pueden ser remplazadas usando una variedad de métodos que son incluidos en el concepto amplio de firma electrónica, dentro del que tiene cabida, como categoría particular, el de firma digital.

Las firmas digitales basadas sobre la criptografía asimétrica se puede encuadrarlas en un concepto más general de firma electrónica, que no presupone necesariamente la utilización de las tecnologías de cifrado asimétrico. Aunque, generalmente, varios autores hablan indistintamente de firma electrónica o de firma digital.

Tiene los mismos cometidos que la firma manuscrita, pero expresa, además de la identidad y la autoría, la autentificación, la integridad, la fecha, la hora y la recepción, a través de métodos criptográficos asimétricos de clave pública (RSA, GAMAL, PGP, DSA, LUC, etc.), técnicas de sellamiento electrónico y funciones Hash, lo que hace que la firma esté en función del documento que se suscribe (no es constante), pero que la hace absolutamente inimitable como no se tenga la clave privada con la que está encriptada, verdadera atribución de la identidad y autoría.

La firma electrónica supone una serie de características añadidas al final de un documento. Es elaborada según procedimientos criptográficos, y lleva un resumen codificado del mensaje, y de la identidad del emisor y receptor.

Para Del Peso Navarro es una señal digital representada por una cadena de bits que se caracteriza por ser secreta, fácil de reproducir y de reconocer, difícil de falsificar y cambiante en función del mensaje y en función del tiempo, cuya utilización obliga a la aparición de lo que denomina fedatario electrónico o telemático que será capaz de verificar la autenticidad de los documentos que circulan a través de las líneas de comunicación, al tener no solamente una formación informática, sino también jurídica.

Una firma electrónica sería simplemente cualquier método o símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención actual de vincularse o autenticar un documento, cumpliendo todas o algunas de las funciones características de una firma manuscrita. En este concepto amplio y

tecnológicamente indefinido de firma, tendrían cabida técnicas tan simples como un nombre u otro elemento identificativo (p. ej. la firma manual digitalizada) incluido al final de un mensaje electrónico, y de tan escasa seguridad que plantean la cuestión de su valor probatorio a efectos de autenticación, aparte de su nula aportación respecto de la integridad del mensaje.

Las firmas electrónicas o digitales consisten básicamente en la aplicación de algoritmos de encriptación a los datos, de esta forma, sólo serán reconocibles por el destinatario, el cual además podrá comprobar la identidad del remitente, la integridad del documento, la autoría y autentificación, preservando al mismo tiempo la confidencialidad.

La seguridad del algoritmo va en relación directa a su tipo, tamaño, tiempo de cifrado y a la no violación del secreto.

Los criptosistemas de clave pública, son los más idóneos como firma digital, están basados en el uso de un par de claves asociadas: una clave privada, que se mantiene en secreto, y una clave pública, libremente accesible por cualquier persona. Este par de claves esta matemáticamente relacionado de tal forma que sólo con la clave pública correspondiente a la clave privada utilizada para firmar puede verificarse el mensaje firmado; además técnicamente son muy resistentes, se calcula en miles de siglos la duración media que tardaría el ordenador más potente para poder romper la clave. Su mecanismo de seguridad se basa sobre todo en el absoluto secreto de las claves privadas, tanto al generarse como al guardarse y en la certificación de la clave pública por la autoridad certificadora.

Entre los objetivos de la firma electrónica está el conseguir una universalización de un estándar de firma electrónica.

A mayor abundamiento, mas adelante se hablará sobre la criptografía y sus antecedentes, tema reservado para su mayor estudio y comprensión.

3.6.- CARACTERÍSTICAS DE LA FIRMA ELECTRÓNICA.

Es necesario, cualquiera sea el sistema de firma digital que se utiliza, que esta cumpla con determinados requisitos, en función de garantizar ciertas pautas, que son las que nos permiten equiparar la firma digital a la firma ológrafa. Estos tienen que ver esencialmente con las finalidades que persigue la firma de todo documento.

a) Autenticación o Autoría

La firma digital, para ser eficaz, debe poseer un mecanismo tal que permita aseverar con un alto grado de certeza la identidad del autor de un documento firmado digitalmente.

Esta autenticación de autoría es imprescindible para el correcto funcionamiento del sistema, ya que endilga a un sujeto un compromiso por el cual deberá responder a todos sus efectos.

b) Integridad

Igual, o tal vez más significativo que lo anterior, es certificar que la información contenida en el documento electrónico sea la que su autor suscribió. Esto equivale a decir, que en el proceso de firmado de un documento digital, se debe asegurar que luego los datos no puedan ser alterados por terceros sin que esta acción quede posteriormente evidenciada.

c) Ausencia de revocación

Todo sistema de firma digital idóneo para los fines perseguidos, debe además garantizar que el firmante no pueda luego desconocer la firma puesta en un documento, desvirtuando de esta manera su adhesión de voluntad.

Si un sistema de firma digital no asegurara este tópico, la inseguridad jurídica no tendría límites y el sistema se tornaría meridianamente inútil.

d) Adhesión

Firmar digitalmente un documento, indica que el signatario expresa su adhesión de voluntad o conformidad con lo expresado o contenido en el documento digital. Esto nos lleva pensar que sería recomendable que las aplicaciones informáticas que se utilicen para signar digitalmente documentos, deberían de alguna manera recordar esto al usuario al momento de producir la firma.

3.7.- OTROS TIPOS DE FIRMA ELECTRÓNICA.

a) La firma digitalizada mediante dispositivos de captura de imagen.

Se refiere en este punto a las firmas manuscritas “escaneada”. Esta no puede considerarse en forma alguna firma digital pues carece de los requisitos mínimos para asegurar la autoría, la adhesión de voluntad y la integridad de los datos contenidos en un documento electrónico.

Se aclara que algunas nuevas aplicaciones de software de manejo de documentos[36] están utilizando una imagen escaneada de la firma del usuario para “enmascarar” la firma digital verdadera, pero esto no deja de ser un detalle de estética que nada aporta a la seguridad del documento.

b) Sistemas biométricos.

Estos sistemas analizan alguna parte del cuerpo humano, que tiene la característica de ser genérica en todos los seres humanos, y de ser a la vez único para cada persona, como por ejemplo el patrón de voz, las huellas dactilares, el patrón vascular de la retina ocular, la estructura visible del iris.

Estos sistemas en una primera impresión pueden resultar de lo más atractivos, en efecto cada persona se constituye en su propia clave o llave para abrir pasos en sistemas de seguridad o para firmar algún documento. Sin embargo veremos continuación y brevemente que no sólo no son la panacea, sino que además tienen sus bemoles.

[36] En este sentido podemos nombrar Adobe Acrobat 5.0 de Adobe Systems Incorporated. www.adobe.com Tesinas Firma y documento digital. Su desarrollo, teórico, técnico y legislativo 21

Las técnicas de identificación biométricas, decíamos, se basan en comparar alguna característica del cuerpo humano, con la información guardada en una base de datos. Aquí se empiezan a producir los primeros inconvenientes: la información debe ser previamente almacenada, esto importa la definición de un proceso de carga en las mismas, que debe respetar ciertos estándares de seguridad y calidad. Supone además la custodia y el mantenimiento de estas bases actualizadas. Por otra parte, la técnica planteada no difiere en mucho de un sistema de claves simétricas, pues en definitiva, la clave es única, y se heredan todas las debilidades que este supuesto origina.

Estos sistemas tienen un costo relativamente elevado, lo cual no los hace aún aptos para un uso masivo, así resulta interesante su aplicación para usos específicos, como por ejemplo para determinar el acceso a áreas o sistemas restringidos dónde la identidad de la persona resulta un tópico de alta sensibilidad y que normalmente no puede ser cubierta con el uso de tarjetas inteligentes u otro tipo de llaves. Un claro ejemplo de esta aplicación está dada en la Honorable Cámara de Diputados de la Nación, dónde se implementó el sistema de escáner de huella dactilar en las bancas para asegurar que los legisladores puedan emitir su voto para la sanción de las leyes sin que otras personas puedan tomar su lugar y asegurar un sistema de votación de alta transparencia. Cabe destacar que este sistema se implementó, luego de que fracasara el anteriormente implementado, que no tenía la finalidad de determinar la identidad de las personas, sino su asistencia en el recinto a los efectos de la determinación del quórum y que consistía en un sensor de peso que detectaba si el escaño esta ocupado.

c) Sistemas de análisis de escritura.

Este sistema consiste en el análisis del patrón de escritura de una persona. El sujeto, cuando pretende identificarse ante algún sistema de seguridad debe firmar o realizar un cuerpo de escritura normalmente sobre una tableta digitalizadota, que transmitirá los datos a una computadora dónde se realizará la comparación

con un cuerpo de escritura previamente almacenado en una base de datos.

Se utiliza aquí un procedimiento similar al de los sistemas biométricos, y muchos autores de hecho la incluyen entre ellos. Sin embargo, debemos reseñar que esto es en principio conceptualmente incorrecto.

Pues la escritura no constituye un aspecto físico del individuo como lo son su voz, su huella dactilar o su iris, sino un aspecto psicológico en cuanto el modo de escribir, está generalmente aceptado, es un aspecto de la personalidad del sujeto. Esto mismo debilita el sistema, pues la escritura como aspecto de la personalidad, tiende a cambiar de acuerdo al estado de ánimo de la persona lo que podría causar el rechazo de la autenticación pretendida.

Además la escritura, se ve modificada por el paso del tiempo, según el sujeto vaya adquiriendo o perdiendo capacidades motrices, siendo esto algo del todo normal durante la vida de las personas, lo que ocasionaría la necesidad de actualizar las bases de datos en períodos muy cortos.

d) Tarjetas inteligentes

En rigor de verdad, este tampoco es un sistema de firma. Estas tarjetas, si bien se utilizan en un gran número de aplicaciones de seguridad (cajeros automáticos, tarjetas de crédito y débito, control acceso a áreas restringidas, asistencia puestos de trabajo y estudio, cajas de supermercados, etc...) y están ampliamente difundidas, no constituyen un sistema de firma, sino un medio de almacenamiento de datos que luego se utilizan para identificar a la persona ante un sistema de seguridad. Estas varían en capacidad, bastante reducida en las ya antiguas tarjetas de banda magnéticas, algo más importante en las tarjetas “inteligentes” que tienen un chip electrónico incrustado, y en el tope de línea las tarjetas PCMCIA que no sólo pueden contener datos, sino programas enteros.

En su funcionamiento, se las asocia con una clave, que el usuario debe mantener secreta y que le asegura ser la única persona que puede utilizar la misma para identificarse ante cualquier dispositivo apto para leer la tarjeta.
Debemos entonces tener cuidado de no confundir el contenido con el continente, estas tarjetas podrían eventualmente contener una clave de identificación, pero en sí no se constituyen en un sistema de firma o inscripción.

El avance de la tecnología nos muestra cada día nuevas maravillas en este rubro, de hecho la compañía IOMEGA ha publicado el lanzamiento de un dispositivo del tamaño de un llavero, que unido de un puerto USB (Universal Serial Bus), permite el almacenamiento de hasta 2 gigabyte de información[37], sin necesidad de ningún tipo de conexión especial ni alimentación eléctrica, por un lapso de hasta 10 años.

3.8.- LEGALIDAD DE LOS DOCUMENTOS CON FIRMA DIGITAL.

Se plantea el problema de que algunas legislaciones imponen requisitos de escrito y de firma manuscrita como condición de validez o como condición de pruebas de ciertos contratos y actos jurídicos. En consecuencia, para que desde un punto de vista legal estos contratos sean plausibles, o bien la jurisprudencia debe interpretar el término firma y escrito de forma suficientemente amplia para acoger la firma digital, o bien debe modificarse la ley tratando de asimilar la firma digital a la firma manuscrita.

[37] A modo ilustrativo, el mismo volumen de información puede ser almacenado en 711 disquetes de 1.44 Mb (3 ¼) o en dos Discos
Compactos. www.iomega.com
Tesinas Firma y documento digital. Su desarrollo, teórico, técnico y legislativo 22

En entornos criptográficos se considera la firma digital con capacidad superior a la manuscrita, ya que no sólo comporta la autenticidad del documento firmado, sino su integridad; o lo que es lo mismo, la certidumbre de que no ha sido alterado en ninguna de sus partes. Actualmente no existe problema legal para el uso de la firma digital por un grupo de usuarios, siempre que éstos firmen "manualmente" un acuerdo previo acerca de su uso en sus transacciones comerciales, así como el método de firma y los tamaños (y valores) de las claves públicas a emplear.

Resulta necesario, aunque parezca repetitivo, mencionar lo siguiente;

3.8.1.- SEGURIDAD EN LA FIRMA ELECTRÓNICA.

1. La firma digital proporciona un amplio abanico de servicios de seguridad:

- *Autenticación*: permite identificar unívocamente al signatario, al verificar la identidad del firmante, bien como signatario de documentos en transacciones telemáticas, bien para garantizar el acceso a servicios distribuidos en red.

- *Imposibilidad de suplantación*: el hecho de que la firma haya sido creada por el signatario mediante medios que mantiene bajo su propio control (su clave privada protegida, por ejemplo, por una contraseña, una tarjeta inteligente, etc.) asegura, además, la imposibilidad de su suplantación por otro individuo.

- *Integridad*: permite que sea detectada cualquier modificación por pequeña que sea de los datos firmados, proporcionando así una garantía ante alteraciones fortuitas o deliberadas durante el transporte, almacenamiento o manipulación telemática del documento o datos firmados.

- *No repudio*: ofrece seguridad inquebrantable de que el autor del documento no puede retractarse en el futuro de las opiniones o acciones consignadas en él ni de haberlo enviado. La firma digital adjunta a los datos un timestamp, debido a la imposibilidad de ser falsificada, testimonia que él, y solamente él, pudo haberlo firmado.

- *Auditabilidad*: permite identificar y rastrear las operaciones llevadas a cabo por el usuario dentro de un sistema informático cuyo acceso se realiza mediante la presentación de certificados,

- *El acuerdo de claves secretas*: garantiza la confidencialidad de la información intercambiada ente las partes, esté firmada o no, como por ejemplo en las transacciones seguras realizadas a través de SSL.

3.8.2.- APLICACIONES

La firma digital se puede aplicar en las siguientes situaciones:

- E-mail
- Contratos electrónicos
- Procesos de aplicaciones electrónicos
- Formas de procesamiento automatizado
- Transacciones realizadas desde financieras alejadas
- Transferencia en sistemas electrónicos, por ejemplo si se quiere enviar un mensaje para transferir $100,000 de una cuenta a otra. Si el mensaje se quiere pasar sobre una red no protegida, es muy posible que algún adversario quiera alterar el mensaje tratando de cambiar los $100,000 por 1000,000,con esta información adicional no se podrá verificar la firma lo cual indicará que ha sido alterada y por lo tanto se denegará la transacción
- En aplicaciones de negocios, un ejemplo es el Electronic Data Interchange (EDI) intercambio electrónico de datos de computadora a computadora intercambiando mensajes que representan documentos de negocios

En sistemas legislativos, es a menudo necesario poner un grupo fecha / hora a un documento para indicar la fecha y la hora en las cuales el documento fue ejecutado o llegó a ser eficaz. Un grupo fecha / hora electrónico se podría poner a los documentos en forma electrónica y entonces firmado usando al DSA o al RSA. Aplicando cualquiera de los dos algoritmos al documento protegería y verificaría la integridad del documento y de su grupo fecha / hora.

Firma digital y documentos electrónicos utilizados en la Administración del Estado, salvo la Contraloría General de la República, el Banco Central y las Municipalidades.

3.9.- AUTORIDAD O ENTIDADES DE CERTIFICACIÓN DE LAS CLAVES.

La creciente interconexión de los sistemas de información, posibilitada por la general aceptación de los sistemas abiertos, y las cada vez mayores prestaciones de las actuales redes de telecomunicación, obtenidas principalmente de la digitalización, están potenciando formas de intercambio de información impensables hace pocos años. A su vez, ello está conduciendo a una avalancha de nuevos servicios y aplicaciones telemáticas, con un enorme poder de penetración en las emergentes sociedades de la información. Así, el teletrabajo, la teleadministración, el comercio electrónico, etc., están modificando revolucionariamente las relaciones económicas, administrativas, laborales de tal forma que en pocos años serán radicalmente distintas de como son ahora.

Todos estos nuevos servicios y aplicaciones no podrán desarrollarse en plenitud a no ser que se les dote de unos servicios y mecanismos de seguridad fiables.

Dentro del sistema de seguridad que indicamos, para que cualquier usuario pueda confiar en otro usuario se deben establecer ciertos protocolos. Los protocolos sólo especifican las reglas de comportamiento a seguir.

Existen diferentes tipos de protocolos en los que intervienen terceras partes confiables (*Trusted Third Party, TTP,* en la terminología inglesa):

- Los **protocolos arbitrados.** En ellos una TPC o Autoridad de Certificación participa en la transacción para asegurar que ambos lados actúan según las pautas marcadas por el protocolo.

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

- Los **protocolos autoverificables.** En estos protocolos cada una de las partes puede darse cuenta si la otra actúa deshonestamente, durante el transcurso de la operación.

La firma digital en sí, es un elemento básico de los protocolos autoverificables, ya que no precisa de la intervención de una Autoridad de Certificación para determinar la validez de una firma.

La Autoridad o Entidad de Certificación debe reunir los requisitos que determine la ley, conocimientos técnicos y experiencia necesaria, de forma que ofrezca confianza, fiabilidad y seguridad. Se debería prever el caso de desaparición del organismo certificador y crear algún registro general de certificación tanto nacional como internacional, que a su vez auditase a las entidades encargadas, y fuese garante en su funcionamiento. Pues aun se carece de normas que regulen la

autoridad o entidad de certificación. Para una certificación de naturaleza pública, el Notario, en el momento de suscribir los acuerdos de intercambio y de validación de prueba, puede generar y entregar con absoluta confidencialidad la clave privada.

El documento WP.71 de 31 de diciembre de 1.996 de la Secretaría de las Naciones Unidas indica en su párrafo 44 que las entidades certificadoras deben seguir unos criterios:

- independencia
- recursos y capacidad financieros para asumir la responsabilidad por el riesgo de pérdida
- experiencia en tecnologías de clave pública y familiaridad con procedimientos de seguridad apropiados
- longevidad
- aprobación del equipo y los programas
- mantenimiento de un registro de auditoría y realización de auditorías por una entidad independiente
- existencia de un plan para casos de emergencia (programas de recuperación en casos de desastres o depósitos de claves).
- selección y administración del personal
- disposiciones para proteger su propia clave privada
- seguridad interna
- disposiciones para suspender las operaciones, incluida la notificación a los usuarios
- garantías y representaciones (otorgadas o excluidas)
- limitación de la responsabilidad
- seguros

- capacidad para intercambiar datos con otras autoridades certificadoras
- procedimientos de revocación (en caso de que la clave criptográfica se haya perdido o haya quedado expuesta).

Las autoridades de Certificación pueden emitir diferentes tipos de certificados:

- Los certificados de Identidad, que son los más utilizados actualmente dentro de los criptosistemas de clave pública y ligan una identidad personal (usuario) o digital (equipo, software, etc.) a una clave pública.
- Los certificados de Autorización o potestad que son aquellos que certifican otro tipo de atributos del usuario distintos a la identidad.
- Los Certificados Transaccionales son aquellos que atestiguan que algún hecho o formalidad acaeció o fue presenciada por un tercero.
- Los Certificados de Tiempo o estampillado digital de tiempo permiten dar fe de que un documento existía en un instante determinado de tiempo.

El Sector de autoridades de certificación, hasta la fecha, está dominado por entidades privadas americanas, aunque ya existen iniciativas propias de la Unión Europea que se circunscriben a las fronteras de sus países de origen, es decir, sin salir a otros Estados miembros.

El término TTP (Tercera Parte Confiable) indica aquellas asociaciones que suministran un amplio margen de servicios, frecuentemente asociados con el

acceso legal a claves criptográficas. Aunque no se descarta que las TTP actúen como Autoridades de Certificación (AC), las funciones de ambas se van considerando progresivamente diferentes; decantándose la expresión AC para las organizaciones que garantizan la asociación de una clave pública a una cierta entidad, lo que por motivos obvios debería excluir el conocimiento por parte de dicha Autoridad de la clave privada; que es justamente lo que se supone debería conocer una TTP.

La Comisión Europea distingue entre:

- Autoridades de certificación (AC)

El cometido esencial es "autenticar la propiedad y las características de una clave pública, de manera que resulte digna de confianza, y expedir certificados".

- Terceros de confianza (TC)

Ofrecen diversos servicios, pudiendo gozar de acceso legitimo a claves de cifrado. Una TC podría actuar como una AC.

Lo que la Comisión pretende es que las legislaciones sobre firma digital y AC/TC de los distintos países miembros:

- Se basen en criterios comunitarios.

- Delimiten las tareas -certificación o administración de claves- y servicios.
- Puedan establecerse prescripciones técnicas comunes para los productos de firma digital, en caso de que las disposiciones nacionales no se reconozcan mutuamente y ello merme el buen funcionamiento del Mercado Interior.
- Normas claras en materia de responsabilidades (usuarios frente a AC).
- Errores, etc.

3.10.- FUNCIONES DE LAS AUTORIDADES DE CERTIFICACIÓN.

Las funciones de una Autoridad de Certificación deben ser, entre otras, las siguientes:

Verificar la identidad de los usuarios y su vinculación con los medios de identificación electrónica;

II. Comprobar la integridad y suficiencia del Mensaje de Datos del solicitante y verificar la Firma Electrónica de quien realiza la verificación;

III. Llevar a cabo registros de los elementos de identificación de los Firmantes y de aquella información con la que haya verificado el cumplimiento de fiabilidad de las Firmas Electrónicas Avanzadas y emitir el Certificado.

IV. Deberá Almacenar de forma segura las claves privadas de los usuarios.

V. Deberá dar mantenimiento de las claves vigentes y revocadas.

VI. ofrecer servicios de directorio.

3.11.- AUTORIDADES PÚBLICAS DE CERTIFICACIÓN.

En los métodos asimétricos, cada entidad sólo ha de poseer un par de claves (privada y pública) independientemente del número de sistemas con los que se comunique. El único requisito que se ha de cumplir es la integridad de la clave, para así evitar que un posible atacante sustituya una clave pública y suplante a su usuario legítimo. Para evitar esto se recurre a lo que se denominan los certificados de clave pública, que son emitidos por unas entidades de confianza llamadas Autoridades Certificadoras (CAs, Certification Authorities) y que garantizan que una determina clave pública pertenece a su verdadero poseedor.

Estas entidades permiten garantizar los servicios de confidencialidad e integridad de los datos y el no repudio de origen y destino.

Una arquitectura de gestión de certificados, como se podrá ver mas adelante (en las valoraciones tecnicas) (Public Key Infrastructure) ha de proporcionar un conjunto de mecanismos para que la autenticación de emisores y recipientes sea simple, automática y uniforme, independientemente de las políticas de certificación empleadas.

Las CAs tienen como misión la gestión de los denominados certificados (de clave pública). Un certificado está compuesto básicamente por la identidad de un usuario (subject), su clave pública, la identidad y la clave pública de la CA emisora (issuer) del certificado en cuestión, su periodo de validez y la firma digital del propio certificado. Esta firma, realizada por la CA emisora, permite que aquellas entidades que deseen realizar comunicaciones con la persona poseedora del certificado, puedan comprobar que la información que éste contiene es auténtica (suponiendo que confíen en la CA emisora).

Una vez que los certificados han sido firmados, se pueden almacenar en servidores de directorios o transmitidos por cualquier medio (seguro o no) para que estén disponibles públicamente.

Antes de enviar un mensaje encriptado mediante un método asimétrico, el emisor ha de obtener y verificar los certificados de los receptores de dicho mensaje. La validación de un certificado se realiza verificando la firma digital en él incluida mediante el empleo de la clave pública de su signatario, que a su vez ha de ser validada usando el certificado correspondiente, y así sucesivamente hasta llegar a la raíz de la jerarquía de certificación.

Por lo tanto los usuarios pueden chequear la autenticidad de las claves públicas de otros usuarios verificando la firma de la CA en el certificado usando la clave pública del CA.

En el proceso de verificación se ha de comprobar el periodo de validez de cada certificado y que ninguno de los certificados de la cadena haya sido revocado.

VeriSign es una de las empresas que brinda servicios de certificación. Estos servicios han sido diseñados básicamente para brindar seguridad al comercio electrónico y a la utilización de la firma digital. Para el logro de este objetivo, las autoridades de emisión (Issuing Authorities, "IA") autorizadas por VeriSign funcionan como trusted third partie (o “garantes”), emitiendo, administrando, suspendiendo o revocando certificados de acuerdo con la práctica pública de la empresa.

Las IA facilitan la confirmación de la relación existente entre una clave pública y una persona o nombre determinado. Dicha confirmación es representada por un certificado: un mensaje firmado digitalmente y emitido por una IA.

Esta empresa ofrece tres niveles de servicios de certificación. Cada nivel o clase de certificados provee servicios específicos en cuanto a funcionalidad y seguridad. Los interesados eligen entre estos grupos de servicios el que más le conviene según sus necesidades. Cumplidos los requisitos exigidos se emite el certificado.

Los Certificados Clase 1 son emitidos y comunicados electrónicamente a personas físicas, y relacionan en forma indubitable el nombre del usuario o su "alias" y su dirección de E-mail con el registro llevado por VeriSign. No autentican la identidad del usuario. Son utilizados fundamentalmente para Web Browsing e E-mail, afianzando la

seguridad de sus entornos. En general, no son utilizados para uso comercial, donde se exige la prueba de identidad de las partes.
Los Certificados Clase 2 son emitidos a personas físicas, y confirman la veracidad de la información aportada en el acto de presentar la aplicación y que ella no difiere de la que surge de alguna base de datos de usuarios reconocida. Es utilizado para comunicaciones intra-inter organizaciones vía E-mail; transacciones comerciales de bajo riesgo; validación de software y suscripciones online. Debido a las limitaciones de las referidas bases de datos, esta clase de certificados está reservada a residentes en los Estados Unidos y Canadá.

Los Certificados Clase 3 son emitidos a personas físicas y organizaciones públicas y privadas. En el primer caso, asegura la identidad del suscriptor, requiriendo su presencia física ante un notario. En el caso de organizaciones, asegura la existencia y nombre mediante el cotejo de los registros denunciados con los contenidos en bases de datos independientes. Son utilizados para determinadas aplicaciones de comercio electrónico como electronic banking y Electronic Data Interchange (EDI).
Como las IAs. autorizadas por VERISIGN firman digitalmente los certificados que emiten, la empresa asegura a los usuarios que la clave privada utilizada no está comprometida, valiéndose para ello de productos de hardware. Asimismo, recomiendan que las claves privadas de los usuarios sean encriptadas vía software o conservadas en un medio físico (smart cards o PC cards).

3.11.1.- INFRAESTRUCTURA DE FIRMA DIGITAL PARA EL SECTOR PÚBLICO.

Esta clase de Infraestructura es también conocida como de "clave pública" o por su equivalente en inglés (Public Key Infrastructure, PKI). Crea el marco regulatorio para el empleo de la Firma Digital en la instrumentación de los actos internos del Sector Público Nacional que no produzcan efectos jurídicos individuales en forma directa, otorgándole a esta nueva tecnología similares efectos que a la firma ológrafa.

La disposición establece la configuración de la siguiente estructura:

- Organismo Licenciante (OL)
- Organismo Auditante (OA)
- Autoridad Certificada Licenciada (ACL)
- Subscritores

A.- ORGANISMO LICENCIANTE

Es la Autoridad Certificante Raíz que emite certificados de clave pública a favor de aquellos organismos o dependencias del Sector que deseen actuar como Autoridades Certificantes Licenciadas, es decir como emisores de certificados de clave pública para sus funcionarios y agentes.

Dentro del marco creado por dicho decreto, las funciones de Autoridad de Aplicación y de Organismo Licenciante son asumidas por la Subsecretaría de la Gestión Pública, SGP.

En cumplimiento de esa responsabilidad, se ha dispuesto la asignación de los recursos materiales y humanos, incluyendo la adquisición de equipamiento de última generación. Además, se ha elaborado una serie de documentos disponibles en este sitio - que se encuentran en proceso permanente de revisión - y que servirán como base para el funcionamiento de Autoridades Certificantes que se licencien.

La Infraestructura del Organismo Licenciante ha sido instalada en la sede de la Subsecretaría de la Gestión Pública

B.- ORGANISMO AUDITANTE

Es el órgano de control, tanto para el Organismo Licenciante como para las Autoridades Certificantes Licenciadas. Según lo establecido, el rol del Organismo Auditante dentro de la Infraestructura de Firma Digital para el Sector Público es cumplido por el ejecutivo federal a través de la Secretaría de Economía, y se desahogarán en los términos previstos por la Ley Federal de Procedimiento Administrativo para las visitas de

verificación, las cuales se practicarán de oficio o a petición del Titular del Certificado, Firmante o de la Parte que Confía.

1.- AUTORIDADES CERTIFICANTES LICENCIADAS

Son aquellos organismos o dependencias del Sector Público que soliciten y obtengan la autorización, por parte del Organismo Licenciante, para actuar como Autoridades Certificantes de sus propios agentes. Es decir que, cumplidos los recaudos exigidos por el Decreto mencionado, podrán emitir certificados de clave pública a favor de sus dependientes.

PROCEDIMIENTOS:

1.-Licenciamiento.

El licenciamiento es el procedimiento por el cual el Organismo Licenciante emite un certificado de clave pública a favor de un organismo público (quien adquiere la calidad de Autoridad Certificante Licenciada), quedando éste habilitado para emitir certificados a favor de sus dependientes.
Para obtener dicha licencia, el postulante debe completar un formulario de solicitud y adjuntar un requerimiento de certificado.

2.-Revocación.

La revocación es el procedimiento por el cual el Organismo Licenciante cancela la autorización otorgada a la Autoridad Certificante Licenciada para emitir certificados.
Esta cancelación puede efectuarse a solicitud de esta última o bien por decisión del Organismo Licenciante, según las pautas establecidas en la Política de Certificación.
Si una Autoridad Certificante Licenciada desea pedir al Organismo Licenciante la revocación de su certificado, puede utilizar un formulario de solicitud de revocación.

2.- LABORATORIO DE FIRMA DIGITAL

Para optimizar el proceso de difusión de la tecnología de Firma Electrónica, se debe de implementar un Laboratorio, donde el público en general, y particularmente los funcionarios de la Administración Pública, en sus tres niveles de Gobierno, se capaciten, practicando ellos mismos generando un par de claves, la gestión de su propio certificado y el envío de correo electrónico firmado, al tiempo de ofrecerles información diversa sobre esta tecnología.

3.14.- LA CRIPTOGRAFÍA.

ANTECEDENTES

Criptografía es la ciencia de la seguridad de la información aunque muchas veces ha sido descrita como el arte o la ciencia de la escritura secreta. Por medio de ella se puede almacenar o transmitir información en una forma tal que permite ser revelada únicamente a aquellos que deben verla. La palabra viene del griego kryptos, que significa “oculto”. La criptografía está relacionada con el criptoanálisis, que es la práctica de violar los intentos de esconder información y es parte de la criptología, donde se incluye la criptografía y el criptoanálisis.

El origen de la criptografía data de el año 2000 AC., con los egipcios y sus jeroglíficos. Los jeroglíficos estaban compuestos de pictogramas complejos, donde sólo el significado completo podría ser interpretado por algunos. El primer indicio de criptografía moderna fue usado por Julio César (100 AC. a 44 AC.), quien no confiaba en sus mensajeros cuando se comunicaba con los gobernadores y oficiales. Por esta razón, creó un sistema en donde los caracteres eran reemplazados por el tercer carácter siguiente del alfabeto romano. No solo los romanos, sino los árabes y los vikingos hicieron uso de sistemas de cifrado.

Gabriel de Lavinde hizo de la criptografía una ciencia más formal cuando publicó su primer manual sobre Criptología en 1379.

Samuel Morse. El Código Morse, desarrollado en 1832, aunque no es propiamente un código como los otros, es una forma de cifrar las letras del alfabeto dentro de sonidos largos y cortos.

En tiempos modernos, la criptografía se ha convertido en una compleja batalla entre los mejores matemáticos del mundo y de los ingenieros en sistemas computacionales. La habilidad de poder almacenar de manera segura y de transferir la información ha dado un factor de éxito en la guerra yen los negocios.

Dado a que los gobiernos no desean que ciertas entidades entren y salgan de sus países para tener acceso a recibir o enviar información que puede comprometer y ser de interés nacional, la criptografía ha sido restringida en muchos países, desde la limitación en el uso, la exportación o la distribución de software de conceptos matemáticos que pueden ser usados para desarrollar sistemas criptográficos.

De cualquier manera, el Internet ha permitido que todas estas herramientas sean distribuidas, así como las tecnologías y técnicas de criptografía, de tal manera, que al día de hoy, la mayoría de los sistemas criptográficos avanzados están en dominio público.

La criptografía incluye técnicas como esconder texto en imágenes y otras formas de esconder información almacenada o en tránsito llamada estenografía.

Simplificando el concepto, hoy en día la criptografía se asocia más a convertir texto sencillo a texto cifrado y viceversa. La Criptografía se ocupa de dar solución a los problemas de identificación, autenticación y privacidad de la información en los sistemas informáticos. Debido a la naturaleza de un medio no físico, no resultan

útiles los métodos tradicionales de sellar o firmar documentos, con propósitos comerciales o legales.

En lugar de esto, dentro de la información digital que se desea proteger, debe colocarse algún tipo de marca codificada que sirva para identificar el origen, autenticar el contenido y asegurar la privacidad ante posibles intrusos. La protección de la privacidad utilizando un algoritmo simétrico como por ejemplo el contenido en el estándar DES (Data Encryption Standard), es sencillo en redes pequeñas, pero requiere el intercambio de la clave secreta de encriptación entre cada una de las partes. En la medida en que han proliferado las redes, el intercambio seguro de las claves secretas se ha vuelto costoso e inadecuado. Por tanto, el empleo aislado de esta solución, es inadecuado para grandes redes de comunicación. El estándar DES sufre una desventaja adicional: requiere que se comparta el conocimiento de la Clave Privada. Cada persona debe confiar en la otra respecto de la custodia de la clave secreta común y, además, no transmitírsela a nadie más. Teniendo en cuenta que el usuario debe tener diferentes claves para cada una de las personas con las que se quiere comunicar, debe compartir con cada una de ellas una de sus claves secretas. Esto significa que desde el punto de vista de la implantación práctica, solamente se puede establecer una comunicación segura entre personas que tengan alguna relación previa.

Por tanto, los aspectos fundamentales que DES no cubre son la autenticación y el no repudio. El hecho de que la clave secreta sea compartida implica que cada una de las partes no puede estar absolutamente segura de lo que la otra ha hecho con la misma. Incluso, una de las partes puede, maliciosamente, modificar los datos sin que un tercero pueda determinar la verdadera identidad del remitente ni quién es el culpable de la alteración. La misma clave que hace posible comunicaciones seguras puede ser empleada para crear documentos falsificados en nombre del otro usuario.

3.12.1.- VALORACIONES TECNICAS DE LA FIRMA DIGITAL

En las siguientes láminas se tratará de explicar de manera gráfica las valoraciones técnicas de la firma digital, de tal manera que se pueda tener una visión más amplia del tema:

FIRMA DIGITAL

Valoraciones técnicas

Autor: Guillermo González Holguín

Elementos que componen la Firma Digital

- **Motor de Encripción:** elemento utilizado para garantizar la CONFIDENCIALIDAD del Mensaje.
- **Digesto Seguro o HASH:** elemento utilizado para garantizar la INTEGRIDAD e INALTERABILIDAD del Mensaje.
- **Sistema de Claves Confiables:** elemento utilizado para garantizar la AUTORIA y el NO REPUDIO del Mensaje.

Encripción

Criptografía: Qué es?

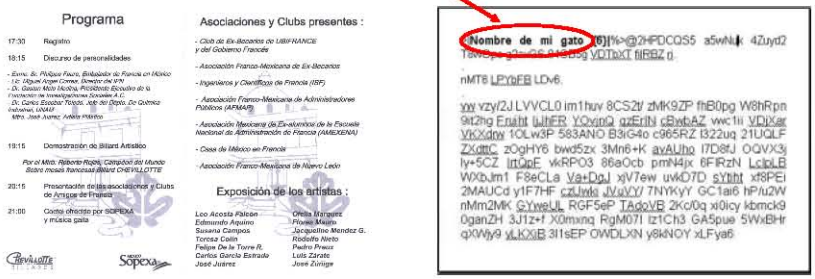
- Es un proceso matemático que convierte información (el texto plano) en algo aparentemente ininteligible (el texto cifrado), en base a una clave secreta (password).
- El proceso es reversible, o sea que se puede volver a obtener el texto plano en base al texto cifrado, pero únicamente si se posee la clave secreta correspondiente.

Encriptar vs. Desencriptar

- **Encriptar:**

Texto plano + Clave de Encriptado = Texto Cifrado

Clave de archivo

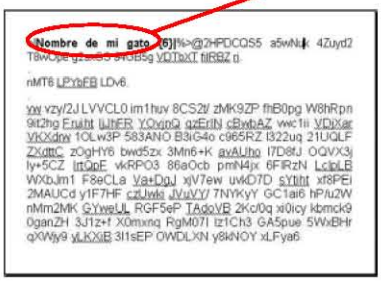


Encriptar vs. Desencriptar

- **Desencriptar:**

Texto Cifrado + Clave de Desencriptado = Texto Plano Recuperado

Clave de archivo



Repaso: Encriptar vs. Desencriptar

- **Encriptar:**
  Texto Plano + Clave de **En**criptado --->
  ---> Texto Cifrado

- **Desencriptar:**
  Texto Cifrado + Clave de **Des**encriptado --->
  ---> Texto Plano Recuperado

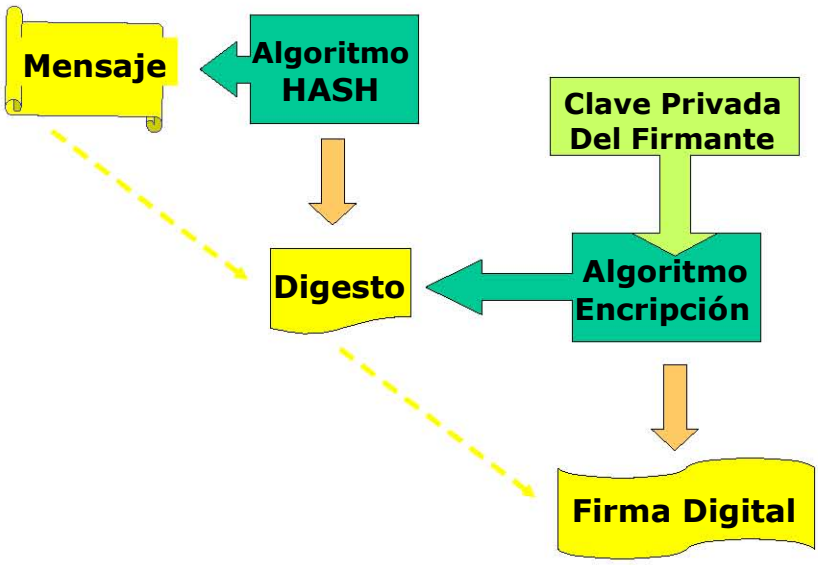
Digesto Seguro

HASH

El Sistema de Digesto seguro se perfecciona mediante la utilización de:

Un **Algoritmo Hash**, que actúa sobre el código binario del documento electrónico, tomando de éste ciertas características distintivas, y creando una sentencia de 160 bits “única” que conforma un resumen (Digesto) del Documento.

A este Digesto se le aplica el Algoritmo de encripción conjuntamente con la clave privada del firmante y de esta manera se crea la firma digital.



La Firma Digital NO es:

- La impresión del dígito pulgar derecho
- La imágen escaneada de una firma quirografaria
- Porqué no? Porque son fácilmente duplicables!

La Firma Digital es:

- Un proceso que permite **asegurar** la
  - **IDENTIDAD** del autor del documento, y la
  - **INALTERABILIDAD** del contenido del documento luego de haber sido firmado.
  - **FECHA y HORA** de la firma.
- Mediante métodos CRIPTOGRAFICOS

Definiciones:

Mensaje: Representación digital de la información.

Criptosistema Asimétrico: Algoritmo o serie de algoritmos que brindan un par de claves Confiables.

Clave Privada: de dos claves, una de ellas se usa para crear una firma digital.

Clave Pública: de dos claves, una de ellas se usa para Verificar una firma digital.

Verificar una firma digital: Determinar fehacientemente que la firma digital fue creada por la clave privada correspondiente a la clave pública, y que el mensaje no ha sufrido modificaciones con posterioridad a la creación del mensaje.

Definiciones:

Suscriptor: Persona que:
- Es el sujeto cuyo nombre figura en un certificado;
- acepta el certificado, y
- tiene una clave privada que corresponde a la clave pública mencionada en dicho certificado.

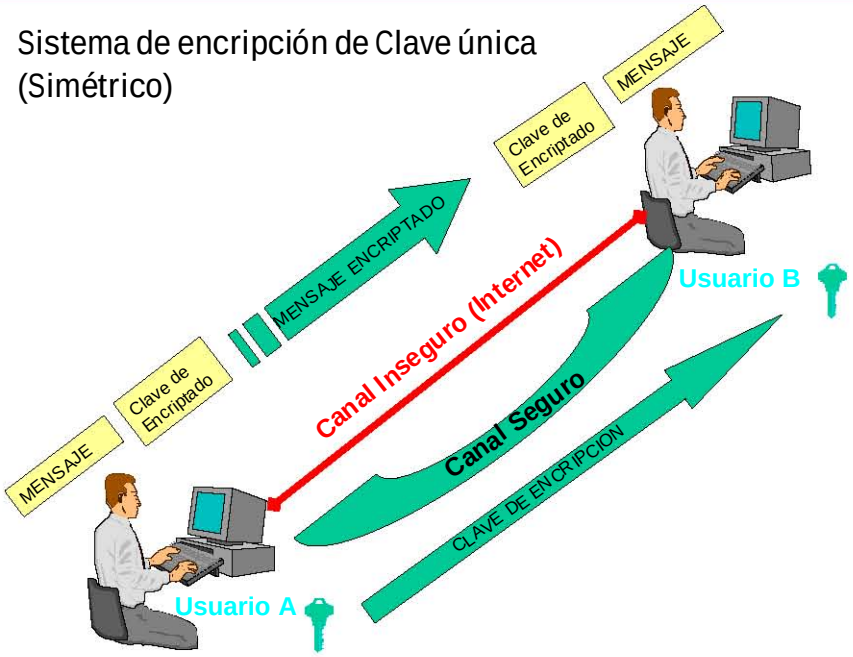
Certificado Válido: Certificado:
- Que ha sido emitido por una autoridad certificante.
- Que ha sido aceptado por el suscriptor allí mencionado.
- Que no ha sido revocado ni suspendido.
- Que no ha vencido.

Suspender un Certificado: volverlo temporariamente inficaz a partir de una determinada fecha.

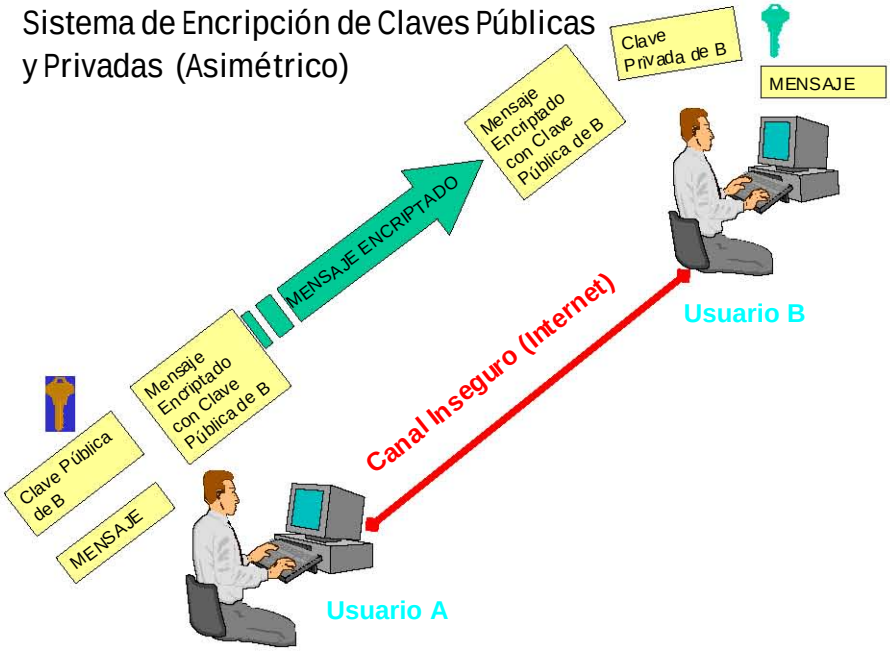
Timbre Fechador: Significa agregar a un mensaje, a una firma digital o a un certificado una anotación firmada digitalmente donde se indique como mínimo la fecha, la hora y la identidad de la persona que efectúa la anotación.

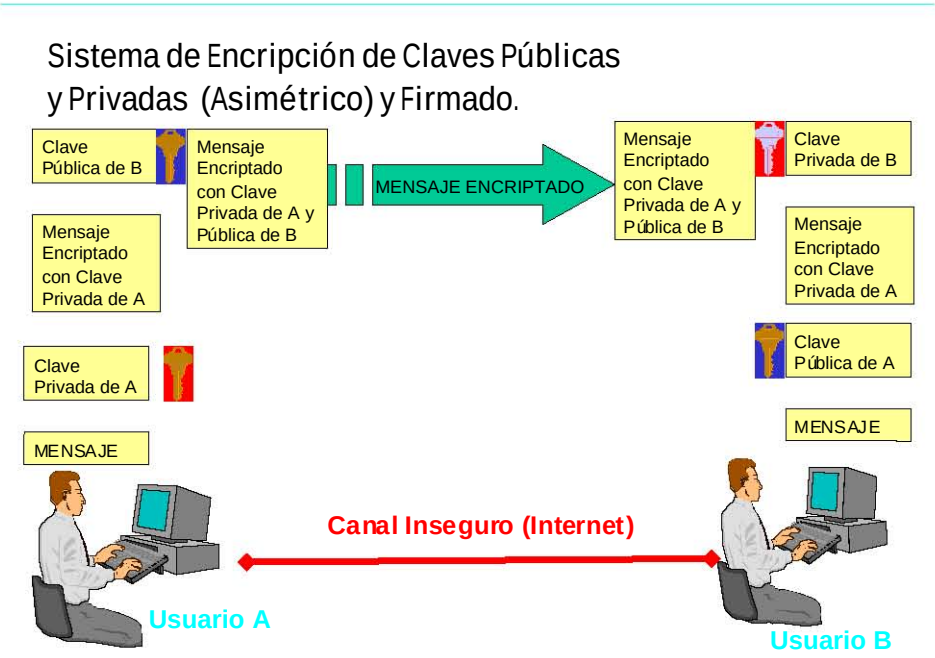
Sistema de Claves

Sistema de encripción de Clave única (Simétrico)



Sistema de Encripción de Claves Públicas y Privadas (Asimétrico)





AUTORIDADES CERTIFICANTES

Servicíos soportados por una Autoridad Certificante (AC)

- Existen dos maneras de realizar los servicios especificados:
  - **online** (La verificación se hace posible por medio servicio de Distribución y Verificación)
  - **offline** (La verificación se hace posible por medio de una SmartCard)
- Esto asegura un continuo flujo de trabajo en caso de problemas de comunicación con la entdidad certificante.

CAPITULO 4

LA NECESIDAD JURÍDICO LEGAL DE REGLAMENTAR LA FIRMA ELECTRÓNICA.

Hoy en día, la palabra “seguridad” ha tomado tal relevancia que por lógica ha llegado a formar parte de comentarios y estudio en todos los campos de esta importante actividad humana, de tal manera que, en materia de derecho informático, ha constituido un elemento de preocupación por parte de la comunidad mundial; pero también ha significado un impulso para el estudio y mejoramiento de los sistemas de encriptación de datos, así como de los mecanismos jurídicos que los deben resguardar.

Los ataques a sistemas informáticos y sitios de la Web, a través de virus, spyware o spam (**referirse al glosario**) hacen que los usuarios tengan verdadero temor y desconfianza al usar los medios cibernéticos para fines comerciales, bancarios, electorales o de cualquier otra índole, que tenga que ver con su patrimonio o incluso con su seguridad personal.

Todo esto ha urgido a que los diferentes organismos tanto gubernamentales como privados, realicen acciones tendientes a solucionar este problema tanto desde el punto de vista técnico como jurídico como ya se vio en el capítulo anterior.

Este esfuerzo por regular los actos jurídico-virtuales ha producido una serie de leyes, códigos, reglamentos y decretos tendientes a dar mayor certidumbre y confiabilidad a uso de los sistemas computacionales.

Ahora bien, con el fin de lograr una mayor explicación sobre el tema y poder sustentar la propuesta del anteproyecto de ley, veremos la forma en que nuestro derecho

mercantil ha llevado a cabo la protección sistemática de los actos que se realizan en el comercio electrónico; entre de estos, la regulación de la firma electrónica.

4.1.-LA REFORMA AL COMERCIO ELECTRÓNICO EN EL CÓDIGO DE COMERCIO.

Desde mayo del año 2000 hasta el 2002, se ha requerido desde el punto de vista legislativo, llevar acabo una serie de reformas al código de comercio para establecer una rubro en lo que es el libro segundo título segundo, y establecer reformas tendientes a regular la firma electrónica desde la perspectiva del comercio electrónico y su uso para los pagos de los contribuyentes. Mismas reformas que publicaron en el mes de agosto del 2003.

Así mismo, en la última reforma establecida, se puede observar que en el artículo 89, ya se empiezan a hablar sobre situaciones concretas de la firma electrónica.

Este artículo dice a la letra: “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.

El primer párrafo es relativo, pues el Código de Comercio es Federal. Se pretende tener en cuenta su origen internacional ya que fue creada por el legislador usando la ley modelo de la UNCITRAL.

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

Certificado: Todo mensaje de datos y otros registros 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 ficha 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 intercambio 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 este 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 adjudicados 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 la firma digital se considerará a ésta como una especia de firma electrónica.

Firmante: La persona que posee los datos de la creación de la firma y que actúa en nombre propia 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 propia, 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 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."[38]

Sin lugar a dudas, ya derivado de esta legislación mexicana, se puede decir que la firma electrónica en México empieza a tener una regulación específica.

Desde el punto de vista civil, podría llegar a ser aplicable, en una forma supletoria.

Evidentemente que hay una íntima relación entre lo que es el mensaje y el firmante.

[38] Código de Comercio: México; Editorial Sista, 2003, Pág. 14.

A través de esta posibilidad, se está manifestando una aprobación en la información contenida en el mensaje, y que produce los mismos efectos que la firma autógrafa.

Y más aún es admisible como prueba en juicio.

Esto definitivamente es ya trascendental, puesto que se denota un gran avance en lo que sería la calidad y la eficacia de la firma electrónica.

Por otro lado, al hablar de la **firma electrónica avanzada**, esta ya presupone una cierta certificación, y de hecho, empieza ya a relacionarse con lo que sería la naturaleza de la firma avanzada de la cual el artículo 97 del propio Código de comercio nos explica lo siguiente: "Cuando la ley requieran a las partes o las partes acuerden la existencia de una firma en relación por 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."[39]

La firma electrónica se considerará avanzada o fiable si cumple por lo menos los siguientes requisitos:

Fracción I.- Los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante.

Fracción II.- Los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante.

Fracción III.- Es posible detectar cualquier alteración de la firma electrónica hecha después del momento del momento de la firma, y;

[39] Código de Comercio: México; Editorial Sista, 2003

Fracción IV.- Respecto a la integridad de la información de un mensaje de datos, es posible detectar cualquier alteración de esta hecha después del momento de la firma.

No dispuesto en el presente artículo se entenderá sin prejuicio 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.

Se observará el cambio electrónico en la seguridad de los documentos, y la institución que se encargará de la certificación y registro, quién podrá generar una mayor fidelidad de la firma electrónica avanzada.

Ahora bien, es importante considerar el vínculo que se forma en base en los diversos principios de la misma informática.

Esto es, que la validez de la firma, necesariamente deberá estar dada a la luz de los diversos principios que rigen la creación de datos.

Ahora se habla de 2 sujetos en la relación del acto jurídico que se realiza, como son:

1.-El Emisor;

2.-El destinatario.

Entre estos, podría existir incluso un intermediario, el cual según se ha visto, será aquella persona que puede actuar a nombre de otra en una manera representativa.

Y, el objetivo de la comunicación es un cierto mensaje de datos, que el emisor manda al destinatario a través de la creación de una firma electrónica, que como ya se ha dicho, llena los principios fundamentales que rigen la formación informática de este tipo de manifestaciones del consentimiento.

Así, los datos de la creación de la firma, deben de estar basados a la luz de un control exclusivo del firmante, y con la posibilidad de una detección en la sustitución de la personalidad del firmante.
Ahora bien, el artículo 89-bis del propio código de comercio, establece lo siguiente:

"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."

Ahora bien, existe una cierta presunción de que un mensaje de datos ha sido enviado por el emisor en tanto que el destinatario, confía en ese mensaje de datos, y por lo tanto, se podrá actuar en consecuencia cuando ocurran las siguientes circunstancias:

1.- Cuando se aplica en forma adecuada el procedimiento acordado previamente con el emisor, con el fin de establecer el mensaje de datos que proviene efectivamente del emisor o;

2.- El mensaje de datos que reciba el destinatario o la parte que confía resulte de los actos de un intermediario que le haya dado acceso algún método utilizado por el emisor para identificar un mensaje de datos como propio.

Estas situaciones no se aplican en los siguientes dos casos:

a) A partir del momento en que el destinatario, la parte que confía, ha sido informado por el emisor que el mensaje de datos no provenía de éste, y que haya dispuesto de un plazo razonable para actuar en consecuencia o;

b) A partir en que el destinatario o la parte que confía, tenga conocimiento o debiere de tenerlo, de haber actuado como la debida diligencia o aplicar algún método convenido, que el mensaje de datos no provenía del emisor.

Así se tiene que salvo prueba en contrario, y sin perjuicio del uso de cualquier otro medio de verificación de la entidad del emisor, se presumirá que actuó con la debida diligencia si el método que uso el destinatario o la parte que confía cumple con los requisitos que establece este el código de comercio, para la verificación de fiabilidad de firmas electrónicas.

Ahora bien, es preciso continuar con el análisis de la legislación y la forma en que la actualidad el Código de Comercio ha estructurado una legislación específica para la utilización de la firma electrónica; de tal naturaleza, que la trascendencia sobre la cual se puede proceder, sería observar las situaciones dentro de la práctica jurídica y para esto, seguiremos utilizando a continuación, los diversos elementos que la legislación de comercio establece.

4.2.- CAMBIO ELECTRÓNICO EN LA SEGURIDAD DE DOCUMENTOS.

Para poder denotar una idea general del cambio electrónico en el documento, he diagramado la exposición, y si se observa la gráfica no. 1, se verá una íntima relación entre los tres elementos que podrían ser la confidencialidad, la integridad y la autenticidad; y la obligación de no repudio al documento que conlleva este tipo de formulaciones.

Cambio de Paradigma en el Documento

	Documento en Papel	Documento Electrónico
Confidencialidad	Sobres/Bóvedas	Encriptación
Integridad y autenticidad	Original y Copias	Firma Digital
No-repudio	Firma Autógrafa Sellos ...	Firma Digital

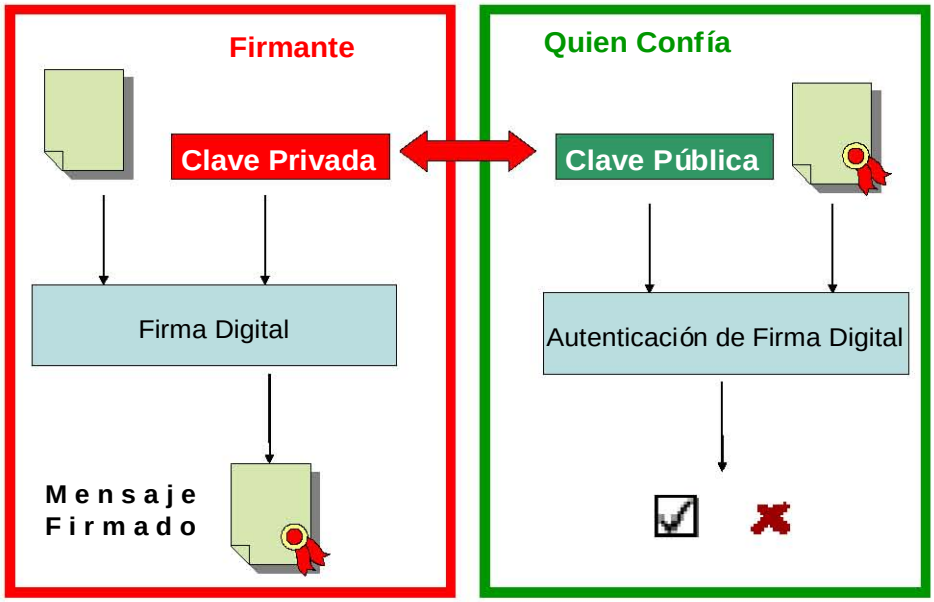
Gráfica No. 1

Pero insisto que esta legislación es meramente de ***carácter mercantil*** aunque no se deja de reconocer su carácter supletorio.

Por otro lado, si se observa la comparación que se hace en la gráfica No.1 sobre el documento en papel y el documento electrónico, resulta evidente que los archivos y las demás procedimientos se reducen logrando con esto mayor control de los documentos y un ahorro sustancial en tiempo, espacio físico y en costos de papel y de personal.

En la gráfica No. 2 muestra el proceso que se lleva a cabo para autenticar la firma Electrónica es decir, la relación entre lo que es la clave privada utilizada exclusivamente por el firmante, y otra que es la llave pública debidamente certificada y lo que le da la confianza al usuario receptor.

Firma y Autenticación Digital



Gráfica No. 2

En la siguiente gráfica se expresa el cambio de paradigma en la firma.

Es evidente, que la comparación que se hace, va en relación directa a los efectos que la firma tiene.

Y por el otro lado, también se pueden observar las fortalezas y debilidades que tienen ambos tipos de formas de expresión de la voluntad, haciendo la diferencia entre el “yo-

puedo” y el “yo-se”

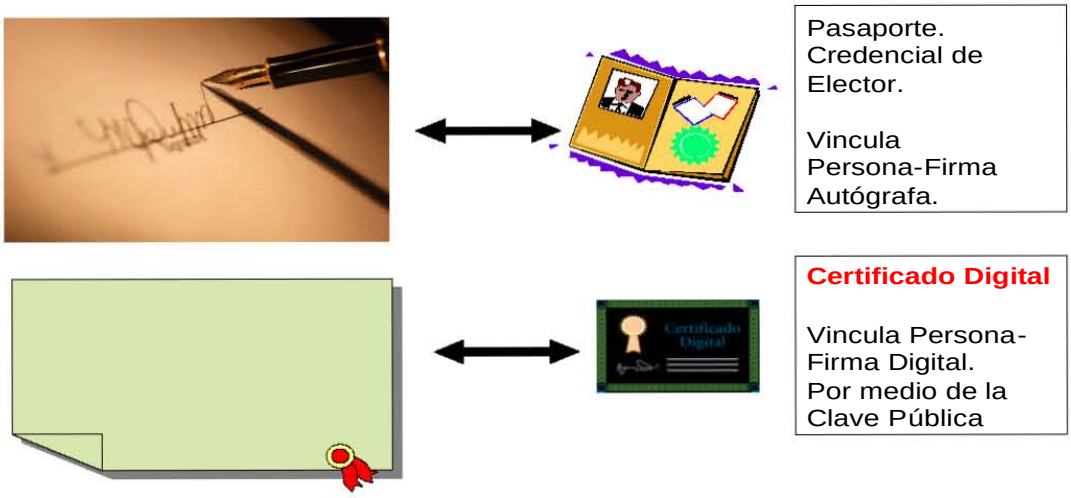
Cambio de Paradigma en la Firma

Firma Autógrafa	Firma Digital
Biometría – “Sólo yo puedo.”	Clave – “Sólo yo sé” *
No pueden robármela ni puedo perderla.	Sí pueden robármela y puedo perderla. Es temporal. *
Lo que veo es lo que firmo.	Lo que veo no necesariamente es lo que firmo.

Gráfica No. 3

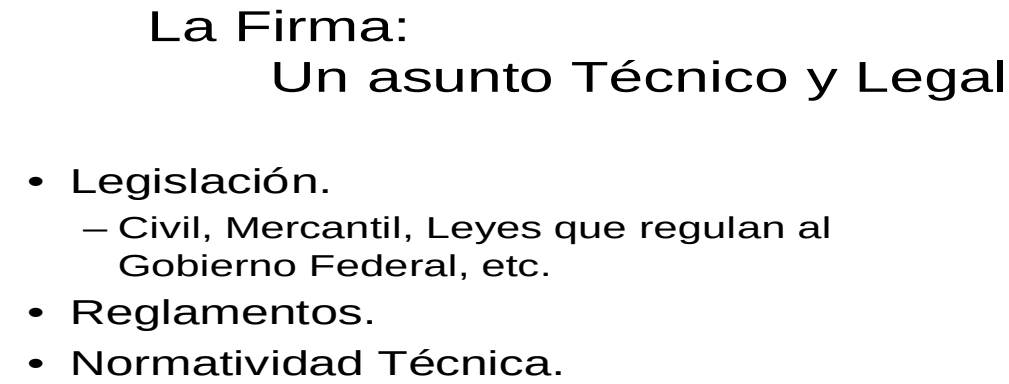
Por otro lado, al observar la gráfica No. 4 se explica cómo la certificación va a llevar a cabo una cierta vinculación en la forma de identificación del sujeto frente a su firma digital, que por supuesto está abalada por los certificados correspondientes.

La Vinculación del Firmante con su Firma : Medios de Identificación.



Gráfica No. 4

Ahora bien, los certificados digitales, basados en normas oficiales como es la número 151, van a proporcionar una infraestructura de clave publica (PKI) y como consecuencia de lo anterior, sugiere que las partes, para perfeccionar la manifestación de la voluntad, realicen previamente un intercambio de llaves o passwords, que les permita usar el sistema de forma segura.



Gráfica No. 5

Aún a pesar, dentro de lo que es la legislación gubernamental o administrativa, al observar la Ley Federal de Procedimientos Administrativos, en los artículos 35 y 69 c, se habla de la posibilidad de una firma electrónica, en la Ley de Adquisiciones, Arrendamientos y Servicios de Sector Público, se puede observar algunos indicios en los artículos 26, 27, 31 y 35; así mismo, en la Ley de Obras Publicas y servicios en los artículos 27, 28, 31 y 37, y en todo lo que son procedimientos administrativos a través de los medios de comunicación electrónica, principalmente de tipo de comercio, en donde se establecen diversos acuerdos, dentro de los cuales, se puede subrayar el acuerdo por el que se establece en las disposiciones que deberán observar las dependencias y organismos de la Administración Publica Federal, para la recepción de promociones que formulen los particulares en los procedimientos administrativos a través de medios de comunicación electrónica, así como para las notificaciones, citatorios, emplazamientos, requerimientos, solicitudes de informes o documentos y las resoluciones administrativas definitivas que se emitan por esa misma vía.

Otro acuerdo llamado oficio circular, que se puede citar es el que establece la Secretaría de Hacienda y Crédito Público, fijado en la publicación del 5 de Marzo del

2003, publicado en el Diario Oficial en esa fecha, intitulado como el oficio circular por el que se emiten los lineamientos para la operación de los sistemas electrónicos de la Subsecretaria de Egresos, mediante la utilización de la firma electrónica.

Legislación Gubernamental

- LEY FEDERAL DE PROCEDIMIENTO ADMINISTRATIVO, Artículos 35 y 69C.
- LEY DE ADQUISICIONES, ARRENDAMIENTOS Y SERVICIOS DEL SECTOR PUBLICO. Artículos 26, 27, 31 y 35.
- LEY DE OBRAS PUBLICAS Y SERVICIOS. Artículos 27, 28, 31 y 37.
- SECODAM.- PROCEDIMIENTOS ADMINISTRATIVOS A TRAVÉS DE MEDIOS DE COMUNICACIÓN ELECTRONICA.
  - Con fecha 17 de enero de 2002, se publicó en el Diario Oficial de la Federación el ACUERDO POR EL QUESE ESTABLECEN LAS DISPOSICIONES QUE DEBERÁN OBSERVAR LAS DEPENDENCIAS Y LOS ORGANISMOS DE LA ADMINISTRACIÓN PUBLICA FEDERAL, PARA LA RECEPCION DE PROMOCIONES QUE FORMULEN LOS PARTICULARES EN LOS PROCEDIMIENTOS ADMINISTRATIVOS A TRAVÉS DE MEDIOS DE COMUNICACÓN ELECTRÓNICA, ASI COMO PARA LAS NOTIFICACIONES, CITATORIOS, EMPLAZAMIENTOS, REQUERIMIENTOS, SOLICITUDES DE INFORMES O DOCUMENTOS Y LAS RESOLUCIONES ADMINISTRATIVAS DEFINITIVAS QUE SE EMITAN POR ESA MISMA VÍA.
- Subsecretaría de Egresos, SHCP. Publicación el 5 de marzo de 2003, en el Diario Oficial de la Federación
  - OFICIO CIRCULAR POR EL QUE SE EMITEN LOS LINEAMIENTOS PARA LA OPERACION DE LOS SISTEMAS ELECTRONICOS DE LA SUBSECRETARIA DE EGRESOS, MEDIANTE LA UTILIZACION DE FIRMA ELECTRONICA.

Gráfica No.6

Con lo anterior, es evidentemente que el uso de medios electrónicos implica tener mecanismos de seguridad tanto técnicos como jurídicos. Siendo esto una necesidad trascendental tanto hoy como en el futuro.

5.4.- LA FIRMA ELECTRÓNICA EN EL AMBITO INTERNACIONAL.

EN ESTADOS UNIDOS.

A finales de la década de los setenta, el gobierno de los Estados Unidos publicó el Data Encryption Standard (DES) para sus comunicaciones de datos sensibles pero no clasificados. El 16 de abril de 1993, el gobierno de los EE.UU. anunció una nueva iniciativa criptográfica encaminada a proporcionar a los civiles un alto nivel de seguridad en las comunicaciones: proyecto Clipper. Esta iniciativa está basada en dos elementos fundamentales:

- Un chip cifrador a prueba de cualquier tipo de análisis o manipulación (el Clipper chip o EES (Escrowed Encryption Standard) y

- Un sistema para compartir las claves secretas (KES -Key Escrow System) que, en determinadas circunstancias, otorgaría el acceso a la clave maestra de cada chip y que permite conocer las comunicaciones cifradas por él.

En EE.UU. es donde más avanzada está la legislación sobre firma electrónica, aunque el proyecto de estandarización del NIST (The National Institute of Science and Technology) no lo consiga. El NIST ha introducido dentro del proyecto Capstone, el DSS (Digital Signature Standard) como estándar de firma, si bien todavía el gobierno americano no ha asumido como estándar su utilización. El

NIST se ha pronunciado a favor de la equiparación de la firma manuscrita y la digital.

La ley de referencia de la firma digital, para los legisladores de los Estados Unidos, es la ABA (American Bar Association), **Digital Signature Guidelines**, de 1° de agosto de 1996.

El valor probatorio de la firma ha sido ya admitido en Utah, primer estado en dotarse de una Ley de firma digital. La firma digital de Utah (**Digital Signature Act Utah** de 27 de febrero de 1995, modificado en 1996) se basa en un "Criptosistema Asimétrico" definido como un algoritmo que proporciona una pareja de claves segura.

Sus objetivos son, facilitar el comercio por medio de mensajes electrónicos fiables, minimizar las incidencias de la falsificación de firmas digitales y el fraude en el comercio electrónico. Así como también, 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.

La firma digital es una transformación de un mensaje utilizando un criptosistema asimétrico, de tal forma que una persona que tenga el mensaje cifrado y la clave

pública de quien lo firmó, puede determinar con precisión el mensaje en claro y si se cifró usando la clave privada que corresponde a la pública del firmante.
El Criptosistema Asimétrico es aquel algoritmo o serie de algoritmos que brindan un par de claves confiable.

El Certificado, es 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.

Esta ley establece la presunción de que una firma digital tiene el mismo efecto legal que una firma manuscrita si se cumplen ciertas existencias; una de las exigencias es que la firma digital sea verificada por referencia a una clave pública incluida en un certificado válido emitido por una autoridad de certificación con licencia.

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.

El Estado de Utah ha redactado un proyecto de ley (**The Act on Electronic Notarization)** en 1997.

California define la firma digital como la creación por ordenador de un identificador electrónico que incluye todas las características de una firma válida, aceptable, como :

- única
- capaz de comprobarse
- bajo un solo control
- enlazándose con los datos de tal manera que si se cambian los datos se invalide la firma
- adoptada al menos como un standard por dos de las organizaciones siguientes:

- The International Telecommunication Unión.

- The American National Standards Institute.

- The Internet Activities Board.

- The National Institute of Science and Technology.

- The International Standards Organization.

No contempla sanciones.

ABA, Resolution concerning the CyberNotary: an International computer-transaction specialist, de 2 de agosto de 1994. 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.

- **The Electronic Signature Act Florida** ,de mayo de 1.996 que reconoce la equivalencia probatoria de la firma digital con la firma manual. En esta ley se usa el término de *"international notary"* en vez del *"cybernotary"* utilizado en otras leyes de EE.UU.
- **The Electronic Commerce Act**, de 30 de mayo de 1997, que hace referencia al *cybernotary.*

- **The Massachusetts Electronic Records and Signatures Act**, de 1996, que acoge todo mecanismo capaz de proporcionar las funciones de las firma manuscrita sin ceñirse a un tipo concreto de tecnología.

El 4 de agosto del 2000 se aprobó la "Uniform Computer InformationTransactions Act" (UCITA), la cual se encuentra en proceso de adopción por los diversos Estados de la Unión Americana.

PRESIDENCIA: El 30 de junio el 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).

EN CANADÁ:

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

EN JAPÓN:

1/04/2001 Ley sobre **firma electrónica** y Servicios de Certificación.

EN PANAMÁ:

3/08/2001 Ley 43 de Comercio Electrónico.

EN CHILE:

2002 Ley sobre documentos electrónicos, firma electrónica y servicios de certificación.

EN 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.

EN 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 equipara 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.

EN 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.

EN 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 Entidades 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.

En Europa:

La Comisión Europea está abocada a armonizar los reglamentos sobre Criptografía de todos sus estados miembros. Hasta el momento, sólo algunos países disponen de leyes sobre firma digital y/o cifrada:

EN ESPAÑA:

La legislación actual y la jurisprudencia, son suficientemente amplias para acoger bajo el concepto de firma y de escrito a la firma digital y a cualquier otro tipo de firma. Cierto es que por razones de seguridad y para ofrecer mayor confianza en los usuarios y jueces que a la postre deben juzgar sobre la firma digital, una reforma de ley cuyo objetivo fuera equiparar la firma manuscrita a cualquier otro medio de firma que cumpliera las mismas finalidades, sería una medida positiva.

El artículo 3° del RD. 2402/1985, de 18 de diciembre, al regular los requisitos mínimos de las facturas, no exige que se firmen. Bien es verdad que nuestro Código de Comercio no exige, por regla general, para una eficacia del contrato o de la factura, la firma ni ningún otro signo de validez, si bien muchos ordenamientos jurídicos requieren que los documentos estén firmados en forma manuscrita -de puño y letra- en orden a solemnizar la transacción o a efectos de su consideración como un documento privado. Creemos no existe inconveniente alguno en admitir la posibilidad de una firma electrónica.

La Circular del Banco de España 8/88 de 14 de Junio creando el reglamento del Sistema Nacional de compensación electrónica, se convirtió en pionera y marcó un hito para la protección y seguridad necesaria en la identificación para el acceso a la

información, al indicar que la información se cifrará, para que las entidades introduzcan un dato de autentificación con la información de cada comunicación, a lo que se le reconoce a este método el mismo valor que el que posee un escrito firmado por personas con poder bastante.

El artículo 45 de la Ley 30/1992 de régimen jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común incorporó el empleo y aplicación de los medios electrónicos en la actuación administrativa, de cara a los ciudadanos. Para su regulación, el Real Decreto 263/1996 de 16 de febrero, indica que deberán adoptarse las medidas técnicas que garanticen la identificación y la autenticidad de la voluntad declarada, pero no hace ninguna regulación legal de la "firma electrónica".

El Real Decreto Ley 14/1999, de 17 de septiembre, sobre Firma Electrónica (1999), establece como objetivo una regulación sobre el uso de firma electrónica, atribuyéndole eficacia jurídica, además de establecer lineamientos para los prestadores 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 doble 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.

EN ALEMANIA:

La ley de firma digital regula los certificados de las claves y la autoridad certificadora. Permite el seudónimo, pero prevé su identificación real por orden judicial. A la firma electrónica se la define como sello digital, con una clave privada asociada a la clave pública certificada por un certificador.

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 Nº 22, 22 May 2001. In Force 22 May 2001

EN FRANCIA:

La nueva Ley de Telecomunicaciones y disposiciones sobre uso interior de cifrado.

Décret nº 2001-272 du 30 mars 2001 pris pour lapplication de larticle 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 linformtion et relative à la signature électronique.

EN PORTUGAL:

Decree-Law 290-D/99.

EN 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

Estos ordenamientos jurídicos, recoge el principio de la plena validez de los documentos informáticos.

El reglamento aprobado por el Consejo de Ministros el 31 de octubre de 1997, si bien para el efectivo reconocimiento del valor jurídico de la documentación informática y de las firmas digitales será necesario esperar a que sea operativo en virtud de la emanación de los posteriores e indispensables reglamentos técnicos de actuación.

Se define la firma digital como el resultado del proceso informático (validación) basado en un sistema de claves asimétricas o dobles, una pública y una privada, que permite al suscriptor transmitir la clave privada y al destinatario transmitir la clave pública, respectivamente, para verificar la procedencia y la integridad de un documento informático o de un conjunto de documentos informáticos (artículo 1º apartado b). En el reglamento la firma digital está basada exclusivamente en el empleo de sistemas de cifrado llamados asimétricos.

El art. 2 del Reglamento italiano establece que los documentos informáticos serán válidos y eficaces a todos los efectos legales si son acordes a las exigencias del Reglamento; en concreto, el art. 10.2 equipara la firma digital sobre un documento informático a la firma escrita en soporte papel; y el art. 11.1 establece que los contratos realizados por medios telemáticos o informáticos mediante el uso de la firma digital según las disposiciones del reglamento serán válidos y eficaces a todos los efectos legales; pero téngase en cuenta que el art. 8 establece que cualquiera que pretenda utilizar la criptografía asimétrica con los efectos del art. 2 debe conseguir un par de claves adecuado y hacer pública una de ellas a través del procedimiento de certificación efectuada por un certificador.

Regulan la Ley y el Reglamento entre otras cosas: La validez del documento informático; el documento informático sin firma digital; el documento informático con firma digital; los certificadores; los certificados; autentificación de la firma digital; el "*cybernotary*"; los actos públicos notariales; la validación temporal; la caducidad, revocación y suspensión de las claves; la firma digital falsa; la duplicidad, copia y extractos del documento; y la transmisión del documento.

Está basada esta normativa en soluciones extranjeras y supranacionales.

EN REINO UNIDO:

En marzo del año 2002 se crea que regula la firma electrónica (**The Electronic Signature Regulations**).

Estos ordenamientos implementados por la directiva 1999/93/EC del Parlamento Europeo y El consejo comunitario para la construcción de la firma electrónica que es implementado por bajo la supervisión de los prestadores del servicio de certificación (certification-service-providers).

También se expiden las siguientes:

The Electronic Commerce (EC Directive) Regulations 2002 (2002 No. 2013, effective 21 August 2002). See also DTI resources page

Regulation of Investigatory Powers Act 2000 **(**Explanatory Notes to the Regulation of Investigatory Powers Act 2000**)**

EN DINAMARCA:

Act 417 of 31 May 2000 on Electronic Signatures. Bill L 229. Executive Order on Security Requirements etc. for Certification Authorities. Executive Order Nº 923 of 5 October 2000.

Executive Order on Reporting of Information to the National Telecom Agency by Certification Authorities and System Auditors. Executive Order Nº 922 of 5 October 2000.

EN BELGICA:

Loi fixant certaines règles relatives au cadre juridiqe pour les signatures électroniques et les services de certification (Moniteur belgue du 29 septembre 2001). Loi introduisant lutilisation 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.

EN IRLANDA:

Electronic Commerce Act, 2000 (Number 27 of 2000

EN LA COMUNIDAD EUROPEA:

El artículo 6 del Acuerdo EDI de la Comisión de la Comunidades Europeas, que determina la necesidad de garantía de origen del documento electrónico, no regula la firma electrónica.

No obstante Perales Viscasillas cree que no existe inconveniente alguno en admitir la posibilidad de una firma electrónica apoyada en las siguientes circunstancias:

1. La fiabilidad de la firma electrónica es superior a la de la firma manuscrita.

2. La equiparación en el ámbito comercial internacional de la firma electrónica y la firma manuscrita.
3. En el contexto de las transacciones EDI es habitual la utilización de la conocida como "firma digital" que se basa en "algoritmos simétricos" en los que ambas partes conocen la misma clave o en "algoritmos asimétricos" en los que, por el contrario, cada contratante tiene una clave diferente.

En el mismo sentido Isabel Hernando refiriéndose a los contratos-tipo en EDI indica que si los mensajes EDI se transmiten mediante procedimientos de autentificación como una firma digital, estos mensajes tendrán entre las partes contratantes el mismo valor probatorio que el acordado a un documento escrito firmado.

La Comisión Europea ha financiado numerosos proyectos (INFOSEC, SPRI, etc.) cuyo objetivo es la investigación de los aspectos técnicos, legales y económicos de la firma digital.

La Comisión Europea hizo pública en octubre de 1.997 una Comunicación al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones titulada "Iniciativa Europea de Comercio Electrónico", con un subtítulo de "Hacia un Marco Europeo para la Firma Digital y el Cifrado".

En el segundo trimestre del 1.998 se deberán encauzar las propuestas para nuevas medidas, una de las cuales podría ser la elaboración de una Directiva de firma digital.

Lo que pretende la Comisión Europea es encontrar un reconocimiento legal común en Europa de la firma digital, con el objeto de armonizar las diferentes legislaciones antes del año 2000, para que ésta tenga carta de naturaleza legal ante tribunales en materia penal, civil y mercantil, a efectos de prueba, apercibimiento y autenticidad. A efectos de dar cumplimiento a esta previsión, ha salido a finales de 1.998 un borrador de propuesta de directiva sobre firma electrónica y servicios relacionados. Pese a la seguridad ofrecida por la firma digital, el borrador de propuesta de directiva regula la firma electrónica en general, y no sólo la firma digital en particular, en un intento de abarcar otras firmas electrónicas, basadas en técnicas distintas de la criptografía asimétrica. Esta tendencia a la neutralidad tecnológica se ha acentuado a medida que se han ido sucediendo las distintas versiones del borrador de directiva, como pone de manifiesto el hecho de que la versión actual defina única y exclusivamente la firma electrónica (art. 2.1), mientras que en el primer borrador existía también una definición de firma digital, en el art. 2.2.; y del par de claves, pública y privada, en los art. 2.4 y 2.5. únicamente al establecer el concepto de elemento de creación de firma (definido, en el art. 2.3, como aquel dato único, como códigos o claves critpográficas privadas, o un elemento físico configurado de forma única, el cual es usado por el firmante para crear una firma electrónica) y elemento de verificación de firma (definido, en el art. 2.4, como aquel dato único, como códigos o claves criptográficas públicas, o un elemento físico configurado de forma única, el cual es usado para verificar una firma electrónica) existe una referencia a la criptografía asimétrica. Esta neutralidad es seguramente conveniente, para dejar abiertas las puertas a desarrollos tecnológicos futuros. Pero, por otra parte, llevada a ese extremo, deja sin resolver, porque no son siquiera abordados, muchos de los problemas planteados actualmente por las firmas digitales, únicas firmas electrónicas seguras hoy día.

Para conseguir una coherencia europea se deberá, sin duda, pasar por el establecimiento de una política europea de control armónica con otras potencias económicas como EE.UU., Canadá y Japón.

4.3.1. ORGANIZACIONES INTERNACIONALES.

EN NACIONES UNIDAS:

La Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI-UNCITRAL) en su 24º periodo de sesiones celebrado en el año 1991 encargó al Grupo de Trabajo denominado sobre Pagos internacionales el estudio de los problemas jurídicos del intercambio electrónico de datos (EDI: Electronic Data Interchange).

El Grupo de Trabajo dedicó su 24º periodo de sesiones, celebrado en Viena del 27 de enero al 7 de febrero de 1992, a este tema y elaboró un informe que fue elevado a la Comisión.

Se examinó la definición de "firma" y otros medios de autenticación que se han dado en algunos convenios internacionales. Se tuvo presente la definición amplia de "firma" que se contiene en la Convención de las Naciones Unidas sobre Letra de Cambio Internacionales y Pagarés Internacionales, que dice: "*El término firma designa la firma manuscrita, su facsímil o una autenticación equivalente efectuada por otros medios".* Por el contrario, la Ley Modelo sobre Transferencias Internacionales de Crédito utiliza el concepto de "autenticación" o de "autenticación comercialmente razonable", prescindiendo de la noción de "firma", a fin de evitar las dificultades que ésta pueda ocasionar, tanto en la acepción tradicional de este término como en su acepción ampliada.

En su 25º período de sesiones celebrado en 1992, la Comisión examinó el informe del Grupo de Trabajo y encomendó la preparación de la reglamentación jurídica del EDI al Grupo de Trabajo, ahora denominado sobre Intercambio Electrónico de Datos.

El Grupo de Trabajo sobre Intercambio Electrónico de Datos, celebró su 25º periodo de sesiones en Nueva York del 4 al 15 de enero de 1993 en el que se trató de la autenticación de los mensajes EDI, con miras a establecer un equivalente funcional con la "firma".

El Plenario de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI-UNCITRAL), el 14 de Junio de 1996 en su 29º periodo de sesiones celebrado en Nueva York, examinó y aprobó el proyecto de Ley Modelo sobre aspectos jurídicos de EDI bajo la denominación de Ley Modelo sobre el comercio electrónico. (Resolución General de la Asamblea 51/162 de 16 de diciembre de 1996). El artículo 7 de la Ley Modelo recoge el concepto de firma.

La Comisión encomendó al Grupo de Trabajo, ahora denominado "sobre Comercio Electrónico" que se ocupara de examinar las cuestiones jurídicas relativas a las firmas digitales y a las autoridades de certificación.

La Comisión pidió a la Secretaría que preparara un estudio de antecedentes sobre cuestiones relativas a las firmas digitales. El estudio de la Secretaría quedó recogido en el documento A/CN.9/WG.IV/WP.71 de 31 de diciembre de 1996.

El Grupo de Trabajo sobre Comercio Electrónico celebró su 31º periodo de sesiones en Nueva York del 18 al 28 de febrero de 1997 que trató de fijar las directrices sobre firmas digitales publicadas por la American Bar Association.

El Plenario de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional , que celebró su 30º periodo de sesiones en Viena del 12 al 30 de mayo de 1997, examinó el informe del Grupo de Trabajo, hizo suyas las conclusiones y le encomendó la preparación de un régimen uniforme sobre las cuestiones jurídicas de la firma numérica y de las entidades certificadoras.

El artículo 7 de la Ley Modelo sobre Comercio Electrónico (LMCE) regula el equivalente funcional de firma, estableciendo los requisitos de admisibilidad de una firma producida por medios electrónicos, que nos da un concepto amplio de firma electrónica, indicando "*cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos: a) si se utiliza un método para identificar a esa persona y para indicar que esa persona aprueba la información que figura en el mensaje de datos; y b) si ese método es tan fiable como sea apropiado para los fines para los que se creó o comunicó el mensaje de datos, a la luz de todas las circunstancias del caso, incluido cualquier acto pertinente".*

El apartado 3 del proyecto de articulo A del WP.71 indica que "una firma digital adherida a un mensaje de datos se considera autorizada si se puede verificar de conformidad con los procedimientos establecidos por una autoridad certificadora".

EN LA O.C.D.E.:

La Recomendación de la OCDE (Organización para la Cooperación y Desarrollo Económico) sobre la utilización de criptografía (Guidelines for Cryptography Policy) fue aprobada el 27 de marzo de 1997. Esta recomendación no tiene fuerza vinculante y señala una serie de reglas que los gobiernos debieran tener en cuenta al adoptar legislación sobre firma digital y terceros de confianza, con el fin de impedir la adopción de diferentes reglas nacionales que podrían dificultar el comercio electrónico y la sociedad de la información en general.

EN LA ORGANIZACIÓN INTERNACIONAL DE NORMAS ISO:

La norma ISO/IEC 7498-2 (Arquitectura de Seguridad de OSI) sobre la que descansan todos los desarrollos normativos posteriores, regula los servicios de seguridad sobre confidencialidad, integridad, autenticidad, control de accesos y no repudio.

A través de su subcomité 27, SC 27, trabaja en una norma de firma digital.

4.4.- PROPUESTA DE INICIATIVA DE LEY DE FIRMA ELECTRÓNICA.

TÍTULO ÚNICO
Disposiciones generales
CAPÍTULO I
Disposiciones generales

Artículo 1. Ámbito de aplicación

1. Esta Ley regula el uso de la firma electrónica, el reconocimiento de su eficacia jurídica y la prestación al público de servicios de certificación. Las normas sobre esta actividad son de aplicación a los prestadores de servicios establecidos en México.

2. Las disposiciones contenidas en esta Ley no alteran las normas relativas a la celebración, la formalización, la validez y la eficacia de los contratos y otros actos jurídicos ni al régimen jurídico aplicable a los derechos y obligaciones.

Las normas sobre la prestación de servicios de certificación de firma electrónica que recoge esta Ley no sustituyen ni modifican las que regulan las funciones que corresponde realizar a las personas facultadas, con arreglo a derecho, para dar fe de la firma en documentos o para intervenir en su elevación a públicos.

Artículo 2.- Las disposiciones de la presente ley, se regirán en toda la República Mexicana, sin perjuicio de lo dispuesto en los tratados internacionales de los que México sea parte, así como las normas relativas a la celebración, validez y la eficacia de los contratos y otros actos jurídicos aplicables a las obligaciones.

La presente ley tiene por objeto regular la utilización de la firma electrónica otorgándole la misma validez y eficacia jurídica al documento firmado de manera manuscrita u otra forma análoga que conlleve manifestación de voluntad.

En todos aquellos actos que conlleven la firma electrónica 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:

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 o que utilice cualquiera de los medios electrónicos, ópticos o cualquier otra tecnología pero que no esté actuando a título de Intermediario con respecto ha dicho Mensaje.

Emisor: Toda persona que, al tenor del Mensaje de Datos o que utilice cualquiera de los medios electrónicos, ópticos o cualquier otra tecnología, 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 (certificada) o Fiable: Aquella Firma Electrónica que cumpla con los requisitos contemplados en las fracciones I a VI del artículo 4.

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

Firmante: La persona que cuenta con un dispositivo de creación de firma, quien posee los datos de la creación de la misma y quien 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.

Artículo 3.- Las disposiciones de la presente Ley serán aplicadas de modo que no excluyan, restrinjan o priven de efecto jurídico cualquier método para crear una Firma Electrónica.

Artículo 4.- 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.

Artículo 5.- Los Prestadores de Servicios de Certificación determinarán y harán del conocimiento de los usuarios si las Firmas Electrónicas Avanzadas o Fiables que les ofrecen cumplen o no los requerimientos dispuestos en las fracciones I a IV del artículo 4.

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

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

Artículo 6.- El Firmante deberá:

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

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

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

El Firmante será responsable de las consecuencias jurídicas que deriven por no cumplir oportunamente las obligaciones previstas en el presente artículo, y

IV. Responder por las obligaciones derivadas del uso no autorizado de su firma, cuando no hubiere obrado con la debida diligencia para impedir su utilización, salvo que el Destinatario conociere de la inseguridad de la Firma Electrónica o no hubiere actuado con la debida diligencia.

IV. Deberá Almacenar de forma segura las claves privadas de los usuarios.

V. Deberá dar mantenimiento de las claves vigentes y revocadas.

VI. ofrecer servicios de directorio.

CAPÍTULO II
DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN

Artículo 7.- Podrán ser Prestadores de Servicios de Certificación, previa acreditación ante la Secretaría:

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.

La facultad de expedir Certificados no conlleva fe pública por sí misma, así los notarios y corredores públicos podrán llevar a cabo certificaciones que impliquen o no la fe pública, en documentos en papel, archivos electrónicos, o en cualquier otro medio o sustancia en el que pueda incluirse información.

Artículo 8.- Los Prestadores de Servicios de Certificación a los que se refiere la fracción II del artículo anterior, contendrán en su objeto social las actividades siguientes:

I. Verificar la identidad de los usuarios y su vinculación con los medios de identificación electrónica;

II. Comprobar la integridad y suficiencia del Mensaje de Datos del solicitante y verificar la Firma Electrónica de quien realiza la verificación;

III. Llevar a cabo registros de los elementos de identificación de los Firmantes y de aquella información con la que haya verificado el cumplimiento de fiabilidad de las Firmas Electrónicas Avanzadas y emitir el Certificado, y

IV. Cualquier otra actividad no incompatible con las anteriores.

Artículo 9.- Los Prestadores de Servicios de Certificación que hayan obtenido la acreditación de la Secretaría deberán notificar a ésta la iniciación de la prestación de servicios de certificación dentro de los 45 días naturales siguientes al comienzo de dicha actividad.

A) Para que las personas indicadas en el artículo 7 puedan ser Prestadores de Servicios de Certificación, se requiere acreditación de la Secretaría, la cual no podrá ser negada si el solicitante cumple los siguientes requisitos, en el entendido de que la Secretaría podrá requerir a los Prestadores de Servicios de Certificación que comprueben la subsistencia del cumplimento de los mismos:

I. Solicitar a la Secretaría la acreditación como Prestador de Servicios de Certificación;

II. Contar con los elementos humanos, materiales, económicos y tecnológicos requeridos para prestar el servicio, a efecto de garantizar la seguridad de la información y su confidencialidad;

III. Contar con procedimientos definidos y específicos para la tramitación del Certificado, y medidas que garanticen la seriedad de los Certificados emitidos, la conservación y consulta de los registros;

IV. Quienes operen o tengan acceso a los sistemas de certificación de los Prestadores de Servicios de Certificación no podrán haber sido condenados por delito contra el patrimonio de las personas o que haya merecido pena privativa de la libertad, ni que por cualquier motivo hayan sido inhabilitados para el ejercicio de su profesión, para desempeñar un puesto en el servicio público, en el sistema financiero o para ejercer el comercio;

V. Contar con fianza vigente por el monto y condiciones que se determinen en forma general en las reglas generales que al efecto se expidan por la Secretaría;

VI. Establecer por escrito su conformidad para ser sujeto a Auditoria por parte de la Secretaría, y

VII. Registrar su Certificado ante la Secretaría.

B) Si la Secretaría no ha resuelto respecto a la petición del solicitante, para ser acreditado conforme al artículo 100 anterior, dentro de los 45 días siguientes a la presentación de la solicitud, se tendrá por concedida la acreditación.

Artículo 10.- Las responsabilidades de las Entidades Prestadoras de Servicios de Certificación deberán estipularse en el contrato con los firmantes.

Artículo 11.- Los Prestadores de Servicios de Certificación deben cumplir las siguientes obligaciones:

I. Comprobar por sí o por medio de una persona física o moral que actúe en nombre y por cuenta suyos, la identidad de los solicitantes y cualesquiera circunstancias pertinentes para la emisión de los Certificados, utilizando cualquiera de los medios admitidos en derecho, siempre y cuando sean previamente notificados al solicitante;

II. Poner a disposición del Firmante los dispositivos de generación de los Datos de Creación y de verificación de la Firma Electrónica;

III. Informar, antes de la emisión de un Certificado, a la persona que solicite sus servicios, de su precio, de las condiciones precisas para la utilización del Certificado, de sus limitaciones de uso y, en su caso, de la forma en que garantiza su posible responsabilidad;

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

V. Guardar confidencialidad respecto a la información que haya recibido para la prestación del servicio de certificación;

VI. En el caso de cesar en su actividad, los Prestadores de Servicios de Certificación deberán comunicarlo a la Secretaría a fin de determinar, conforme a lo establecido en las reglas generales expedidas, el destino que se dará a sus registros y archivos;

VII. Asegurar las medidas para evitar la alteración de los Certificados y mantener la confidencialidad de los datos en el proceso de generación de los Datos de Creación de la Firma Electrónica;

VIII. Establecer declaraciones sobre sus normas y prácticas, las cuales harán del conocimiento del usuario y el Destinatario, y

IX. Proporcionar medios de acceso que permitan a la Parte que Confía en el Certificado.

a) La identidad del Prestador de Servicios de Certificación;

b) Que el Firmante nombrado en el Certificado tenía bajo su control el dispositivo y los Datos de Creación de la Firma en el momento en que se expidió el Certificado;

c) Que los Datos de Creación de la Firma eran válidos en la fecha en que se expidió el Certificado;

d) El método utilizado para identificar al Firmante;

e) Cualquier limitación en los fines o el valor respecto de los cuales puedan utilizarse los Datos de Creación de la Firma o el Certificado;

f) Cualquier limitación en cuanto al ámbito o el alcance de la responsabilidad indicada por el Prestador de Servicios de Certificación;

g) Si existe un medio para que el Firmante dé aviso al Prestador de Servicios de Certificación de que los Datos de Creación de la Firma han sido de alguna manera controvertidos, y

h) Si se ofrece un servicio de terminación de vigencia del Certificado.

Artículo 12.- La Secretaría coordinará y actuará como autoridad Certificadora, y registradora, respecto de los Prestadores de Servicios de Certificación, previstos en este Capítulo.

Artículo 13.- Para la prestación de servicios de certificación, las instituciones financieras y las empresas que les prestan servicios auxiliares o complementarios relacionados con transferencias de fondos o valores, se sujetarán a las leyes que las regulan, así como a las disposiciones y autorizaciones que emitan las autoridades financieras.

Artículo 14.- Serán responsabilidad del Destinatario y de la Parte que Confía, en su caso, las consecuencias jurídicas que entrañe el hecho de que no hayan tomado medidas razonables para:

I. Verificar la fiabilidad de la Firma Electrónica, o

II. Cuando la Firma Electrónica esté sustentada por un Certificado:

a) Verificar, incluso en forma inmediata, la validez, suspensión o revocación del Certificado, y

b) Tener en cuenta cualquier limitación de uso contenida en el Certificado.

Artículo 15.- Los Certificados, para ser considerados válidos, deberán contener:

I. La indicación de que se expiden como tales;

II. El código de identificación único del Certificado;

III. La identificación del Prestador de Servicios de Certificación que expide el Certificado, razón social, su domicilio, dirección de correo electrónico, en su caso, y los datos de acreditación ante la Secretaría;

IV. Nombre del titular del Certificado;

V. Periodo de vigencia del Certificado;

VI. La fecha y hora de la emisión, suspensión, y renovación del Certificado;

VII. El alcance de las responsabilidades que asume el Prestador de Servicios de Certificación, y

VIII. La referencia de la tecnología empleada para la creación de la Firma Electrónica.

Artículo 16.- Un Certificado dejará de surtir efectos para el futuro, en los siguientes casos:

I. Expiración del periodo de vigencia del Certificado, el cual no podrá ser superior a dos años, contados a partir de la fecha en que se hubieren expedido. Antes de que concluya el periodo de vigencia del Certificado podrá el Firmante renovarlo ante el Prestador de Servicios de Certificación;

II. Revocación por el Prestador de Servicios de Certificación, a solicitud del Firmante, o por la persona física o moral representada por éste o por un tercero autorizado;

III. Pérdida o inutilización por daños del dispositivo en el que se contenga dicho Certificado;

IV. Por haberse comprobado que al momento de su expedición, el Certificado no cumplió con los requisitos establecidos en la ley, situación que no afectará los derechos de terceros de buena fe, y

V. Resolución judicial o de autoridad competente que lo ordene.

Artículo 17.- El Prestador de Servicios de Certificación que incumpla con las obligaciones que se le imponen en el presente Capítulo, previa garantía de

audiencia, y mediante resolución debidamente fundada y motivada, tomando en cuenta la gravedad de la situación y reincidencia, podrá ser sancionado por la Secretaría con suspensión temporal o definitiva de sus funciones. Este procedimiento tendrá lugar conforme a la Ley Federal de Procedimiento Administrativo.

Artículo 18.- Las sanciones que se señalan en este Capítulo se aplicarán sin perjuicio de la responsabilidad civil o penal y de las penas que correspondan a los delitos en que, en su caso, incurran los infractores.

Artículo 19.- Las autoridades competentes harán uso de las medidas legales necesarias, incluyendo el auxilio de la fuerza pública, para lograr la ejecución de las sanciones y medidas de seguridad que procedan conforme a esta Ley. Incluso, en los procedimientos instaurados se podrá solicitar a los órganos competentes la adopción de las medidas cautelares que se estimen necesarias para asegurar la eficacia de la resolución que definitivamente se dicte.

Artículo 20.- En el caso de que un Prestador de Servicios de Certificación sea suspendido, inhabilitado o cancelado en su ejercicio, el registro y los Certificados que haya expedido pasarán, para su administración, a otro Prestador de Servicios de Certificación, que para tal efecto señale la Secretaría mediante reglas generales.

CAPÍTULO III
RECONOCIMIENTO DE CERTIFICADOS Y FIRMAS ELECTRÓNICAS EXTRANJEROS

Artículo 21.- Para determinar si un Certificado o una Firma Electrónica extranjeros producen efectos jurídicos, o en qué medida los producen, no se tomará en consideración cualquiera de los siguientes supuestos:

I. El lugar en que se haya expedido el Certificado o en que se haya creado o utilizado la Firma
Electrónica, y

II. El lugar en que se encuentre el establecimiento del Prestador de Servicios de Certificación
o del Firmante.

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

Toda Firma Electrónica creada o utilizada fuera de la República Mexicana

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

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

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

CONCLUSIONES.

La evolución de la tecnología en los últimos diez años, sobre todo en el terreno electrónico y digital, ha supuesto una enorme transformación en la operatividad de la industria, del comercio, del sector servicios, de los profesionales, e incluso a nivel doméstico. Los cambios operados en el ámbito de la información y de la comunicación han contribuido a la modernización de los instrumentos utilizados por los distintos operadores obteniéndose los consiguientes beneficios de eficacia y rapidez. Asimismo, en la actualidad son muchos los hogares que se encuentran conectados a la red por las múltiples ventajas que conlleva su utilización, dado que permite realizar desde operaciones bancarias o financieras a encargar la adquisición de todo tipo de productos. Por todo ello, la sociedad ha ido experimentando de forma paralela un cambio tan trascendente y decisivo como lo hayan podido suponer los grandes descubrimientos acontecidos a lo largo de la Historia. La comunicación en Internet tiene lugar a través de ordenadores enlazados de forma dinámica, por lo que el trayecto de un correo electrónico remitido entre dos ciudades cercanas puede haber viajado a cualquier país distante de ambas localidades antes de llegar a su destino. Lo que actualmente preocupa en Internet son el anonimato y el carácter abierto de las comunicaciones. En Internet no es posible, sin los instrumentos necesarios, verificar que la persona que se comunica con nosotros por ejemplo, mediante el correo electrónico, es realmente quien dice ser. Sabemos que la comunicación, ingrediente sustantivo de la convivencia humana, es el punto de partida del hacer colectivo, y la ley es la herramienta imprescindible para convivir con el menor grado de conflictividad posible. La ley cumple la misión de regular derechos y obligaciones. Es todo ello lo que justifica la sanción de una ley que permita estructurar y organizar el desenvolvimiento y desarrollo de las nuevas tecnologías en nuestro país. Los principios rectores en los cuales consideramos que se debe inspirar este marco normativo y sus principales directrices son los de libre competencia, neutralidad tecnológica, compatibilidad internacional y equivalencia de la firma digital a la firma manuscrita.

Principios rectores:

1. Promover la compatibilidad con el marco jurídico internacional. Este principio refiere a la dimensión global o internacional del tema desde el punto de vista legislativo y tecnológico, a fin de permitir la inserción de la Argentina en el mercado mundial del comercio electrónico.
2. Asegurar la neutralidad tecnológica: Se hace referencia aquí a la no discriminación entre distintas tecnologías y, en consecuencia la necesidad de producir normas que regulen los diversos entornos tecnológicos. Este principio refiere a la flexibilidad que deben tener las normas, es decir, que las mismas no estén condicionadas a un formato, una tecnología, un lenguaje o un medio de transmisión específico.
3. Establecer la equivalencia de la firma digital a la firma manuscrita, considerando que la misma satisface el requerimiento de firma respecto de los datos consignados en forma electrónica y tiene los mismos efectos jurídicos que la firma manuscrita con relación a los datos consignados en papel.
4. Establecer la libre competencia con respecto a todos los servicios relacionados con la certificación de las firmas electrónicas.

TERMINOLOGÍA UTILIZADA Y CONCEPTO DE FIRMA ELECTRÓNICA.

La firma es una forma de exteriorización de la voluntad humana. La voluntad puede manifestarse por diferentes formas, por un gesto, palabras, escritura, fax, etc. La manifestación de la voluntad en relación a un documento electrónico no puede ser la firma manuscrita. Por ello la ley debe reconocer una forma electrónica de consentir como válida y eficaz para la suscripción de documentos electrónicos. Esta forma de consentir - que no es un consentimiento electrónico sino una forma más de manifestación no legislada en nuestro país - es la llamada firma electrónica. La doctrina jurídica conviene en que la firma es el género, la firma electrónica una especie y dentro de ésta encontramos subespecies, tales como las denominadas en algunas legislaciones como firma digital, firma electrónica avanzada, ó firma electrónica certificada. Concluimos que: a.- La firma es la prueba de la manifestación de la voluntad que permita imputar la autoría e identificar al firmante de un instrumento. b.- firma electrónica: es un método o símbolo basado en medios electrónicos utilizado o adoptado por una persona con la intención de vincularse o autenticar un documento. Es una forma de manifestar la voluntad mediante medios electrónicos. c.- firma digital: es la firma electrónica que utiliza una técnica segura que permite vincular e identificar fehacientemente al firmante del documento electrónico garantizando la autenticación, integridad y no repudio del documento firmado. Es una forma segura y verificable de manifestar la voluntad mediante medios electrónicos. ***La propuesta de anteproyecto de ley*** que presento no se refiere exclusivamente al valor jurídico de la firma en si misma, sino con relación al instrumento en el cual dicha firma está estampada, y en líneas generales establece que un documento firmado es un instrumento privado, con validez jurídica, y que quien se oponga al contenido de un instrumento por el firmado es quien debe probar que las declaraciones u obligaciones que se encuentran en él no son las que ha tenido intención de hacer o contratar. Por otro lado prevé la posibilidad de una firma en blanco. Pero cuando analizamos la firma digital vemos que la realidad es diferente: - En primer lugar porque sería imposible encontrar una firma electrónica sobre un documento en blanco, ya que la firma solo existe con el conjunto de datos a los cuales se vincula. La firma digital no existe si la disociamos de su mensaje. - En

segundo lugar, porque el mismo procedimiento que verifica la firma está verificando la inalterabilidad o autenticidad del documento, o sea que la validez de la firma depende de que el documento no haya sido alterado. - Cuando hablamos de firma manuscrita puede suceder que un perito calígrafo determine que una determinada persona ha suscripto el documento, pero si éste está escrito a máquina, dicho perito no podrá establecer que ese documento es auténtico y que se encontraba en esa hoja en el momento de la firma. Quien niegue el contenido del documento deberá probarlo por otros medios. En materia de firma Electrónica Avanzada, el mismo procedimiento que verifica la titularidad de la firma, está acreditando también la autenticidad e inalterabilidad del documento. Ambos términos son inseparables. En esta materia las diferentes legislaciones le han dado a la firma digital o electrónica avanzada dos tratamientos diferentes: 1.- Otorgarle simplemente validez probatoria, sujeta a la valoración según los criterios comunes de apreciación establecidos en las normas procesales. Esto implicaría que quien quiere sostener la validez de la firma digital deberá probar los extremos necesarios. 2.- Otorgarle un juego de presunciones, en virtud de las cuales: a.- se presume que la firma Electrónica Avanzada ó Certificada, pertenece efectivamente al titular del certificado digital correspondiente. b.- que el documento digital firmando digitalmente no ha sido modificado desde el momento de su escritura c.- que la firma fue añadida por dicha persona con la intención de manifestar su acuerdo con los datos obrantes en el documento. Considero que la incorporación legislativa de la segunda opción, otorgando la presunción iuris tantum de validez y autenticidad a la firma electrónica es adecuada y beneficia la seguridad jurídica en el tráfico mercantil y para cualquier otro uso, por medios electrónicos. La primera opción se aplicaría a las firmas electrónicas, que deberían ser probadas por quien las alega.

CONCEPTO Y VALIDEZ DEL DOCUMENTO ELECTRONICO.

El documento en general es el género, mientras que el instrumento es el documento firmado. En este sentido instrumento privado es todo escrito que da constancia de un hecho u acto con consecuencias jurídicas que ha sido firmado por particulares sin intervención de un funcionario público competente, que no tiene otro requisito que la

firma. Un documento electrónico no podría considerarse un instrumento privado sin los efectos jurídicos que otorga la ley a la firma y al procedimiento de firma electrónica o digital. Es decir que la eficacia jurídica del documento informático viene condicionada por la necesidad de suscripción digital del mismo. Verificada la firma, el documento electrónico sería eficaz desde el punto de vista probatorio. Es por ello que creo adecuado validar mediante ley al documento electrónico firmado, para brindar el marco legal necesario, otorgándole eficacia probatoria Pero el documento electrónico no es un "escrito" , sino un cúmulo de información almacenada en un soporte magnético , representación en forma informática o electrónica de actos, hechos o datos jurídicamente relevantes.

LOS SERVICIOS DE CERTIFICACIÓN

Para asegurar el buen funcionamiento de los servicios de certificación, que serán los que permitan la existencia de la firma digital, es necesario precisar las exigencias esenciales a cumplir por dichos proveedores de servicios de certificación, incluida su responsabilidad y obligaciones.

IMPLEMENTACION DE LA FIRMA ELECTRONICA

Por ultimo opino que la implementación de la firma electrónica debe ser realizada en forma paulatina, respetando las formalidades que la legislación ha establecido para rodear de seguridad jurídica a determinado tipo de actos a través de las ***leyes Especiales*** siendo estas de aplicación general. En este sentido se debe circunscribir la utilización de la firma digital al ámbito del instrumento privado y a los actos administrativos, así como dentro del amplio espectro que abarca el Derecho, estableciendo posiciones de la ley no son aplicables a los actos jurídicos que se instrumenten bajo una forma incompatible con el documento electrónico como la escritura pública, por ejemplo, ya sea esta forma impuesta por las leyes u adoptada por las partes.

BIBLIOGRAFÍA

ABENDAÑO LOPEZ, Raúl Eduardo; "La Constitución Explicada"; México, Pac: 1° edición, 1995.

ALCOVER GARAU, Guillermo; "La Firma Electrónica como Medio de Prueba (Valoración Jurídica de los Criptosistemas de Claves Asimétricas)", Cuadernos de Corredores de Comercio, Madrid. Pags. 11 a 41.

ALVAREZ-CIENFUEGOS SUÁREZ, José María; "Las Obligaciones Concertadas por Medios Informáticos y la Documentación Electrónica de los Actos Jurídicos", Informática y Derecho n° 5, UNED, Centro Regional de Extremadura, Aranzadi, Mérida, 1994. Pags. 1273 a 1298.

BARRIUSO RUIZ, Carlos, "Interacción de Derecho y la Informática", Dykinson, Madrid, 1996.

BARRIUSO RUIZ, Carlos; "Contratación Electrónica", Marco legal y deontológico de la Informática, Mérida, 17 de septiembre de 1997.

BARRIUSO RUIZ, Carlos; "La Contratación Electrónica", Dykinson, Madrid, 1998.

BONNECASE, Julián; "Tratado Elemental del Derecho Civil"; México, Harla vigésima octava edición. 1998.

CAMPS LLUFRIÚ, Mateo; JOYANES AGUILAR, Luis; SANTAELLA LÓPEZ, Manuel; "Aspectos Socio-Jurídicos de la Contratación Electrónica", XII Encuentro sobre Informática y Derecho, Instituto de Informática Jurídica Facultad de Derecho de la Universidad Pontificia Comillas (ICADE), Madrid, 12 de mayo de 1998.

CARRANCAY RIVAS, Raúl; "La Constitución, Hoy"; México, El Día en Libros, Tercera edición, 1999.

CARRASCOSA LÓPEZ, Valentín; BAUZA REILLY, Marcelo; GONZÁLEZ AGUILAR, Audillo; "El Derecho de la Prueba y la Informática. Problemática y Perspectivas", Informática y Derecho n°2, UNED, Centro Regional de Extremadura, Mérida, 1991.

CARRASCOSA LÓPEZ, Valentín; POZO ARRANZ, Asunción; RODRIGUEZ DE CASTRO, Eduardo Pedro; "El Consentimiento y sus Vicios en los Contratos Perfeccionados a través de Medios Electrónicos", Informática y Derecho n° 12, 13,

14 y 15, UNED, Centro Regional de Extremadura, Mérida, 1996. Pags. 1021 a 1037.

CARRASCOSA LÓPEZ, Valentín;POZO ARRANZ, Asunción; RODRIGUEZ DE CASTRO, Eduardo Pedro; "Valor Probatorio del Documento Electrónico", Informática y Derecho n°8, UNED, Centro Regional de Extremadura, Mérida, 1995. Pags. 133 a 173.

CÓDIGO CIVIL PARA EL DISTRITO FEDERAL, México, Sista, 2002.

CÓDIGO FEDERAL CIVIL, MÉXICO, Sista, 2002.

CÓDIGO DE COMERCIO, Sista, 2003.

CONCHA MALO, Miguel; "Los Derechos Políticos como Derechos Humanos"; México, Comisión Nacional de los Derechos Humanos, Centro de Investigaciones Interdisciplinarias en Humanidades de UNAM, primera edición, 1994.

CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS, México, Sista, 2002.

FIX ZAMUBIO, Héctor; "Justicia Constitucional en Derechos Humanos"; México, Comisión Nacional de Derechos Humanos, 2° edición, 1999.

FLORESGOMEZ GONZALEZ, Fernando; CARVAJAL MORENO, Gustavo; "Nocionesde Derecho Positivo Mexicano"; México, Porrúa S.A, Vigésima primera edición, 1998.

GALINDO GARFIAS, Ignacio; "Derecho Civil"; México, Porrúa S.A. décimo primera edición, 2001.

IHERING RUDOLF, Von; "La Lucha por el Derecho"; México, Porrúa S.A., 4° edición, 2002.

JALIFE DAHLE, Mauricio; "Marcas"; México; Sista, segunda edición, 2002.

LOZANO NORIEGA, Francisco; "Contratos"; México, Asociación Nacional del Notariado Mexicano; México, octava edición, 1999.

MONTERO DUHALT, Sara; "Derecho de Familia"; México, Porrúa S.A., cuarta edición, 1990.

NUTO SALAZAR, Efraín; "Elementos de Derecho"; México, Porrúa S.A. Trigésimo sexta edición, 2001.

OCHOA OLVERA, Salvador; “La Demanda por Daño Moral”; México, Monte Alto, tercera edición, 2001.

OCHOA SANCHEZ, Miguel Angel; BANDEL MARTINEZ, Jacinto; “Derecho Positivo Mexicano”; México, Mc Graw Hill, 2° edición, 2000.

PEREZ FERNANDEZ del CASTILLO, Bernardo; “Representación, Poder y Mandato”; México, Porrúa S.A., novena edición, 1996.

RABASA, Emilio; CABALLERO, Gloria; “Mexicano, Ésta es tu Constitución”; México, Miguel Ángel Porrúa Grupo Editorial, vigésima cuarta edición, 1998.

RAQUIALES, Eduardo; “Derecho Procesal Civil”; México, Porrúa S.A., vigésimo primera edición, 1994.

ROJINA VILLEGAS R.E.; “Compendio de Derecho Civil”; México, Porrúa S.A. vigésimo octava edición, Tomo 1 al 5, 1999.

SERRANO MIGALLON, Fernando; “La Propiedad Industrial en México”; México, Porrúa S.A., segunda edición, 1995.

http://www.opsi.gov.uk/si/si2002/20020318.htm