RESUMEN

El mundo ha experimentado un proceso de globalización, especialmente económica y cultural, rompiéndose paradigmas políticos, económicos e ideológicos que actuaban como barreras separadoras entre los pueblos. Hemos entrado en una etapa de mundialización que exige adaptarnos a los cambios de mercado, en donde los servicios han suplantado a las industrias. Este escenario se ha dado gracias a los veloces avances en la ciencia y la tecnología, dentro de una sociedad marcada por la información y el conocimiento. En este entorno nos encontramos frente al reto de dotarles de valor jurídico a las actividades que se llevan a cabo por medios telemáticos, donde las Entidades Certificadoras de Firma Electrónica cumplen un papel esencial y preponderante. A estas entidades se las conoce también como terceras partes de confianza, cuya principal misión es la de certificar que determinada clave pública pertenece a una persona y que ésta se encuentra vigente. En el Ecuador, para que la firma electrónica tenga validez jurídica es indispensable que posea un certificado de firma digital, que debe ser emitido por una “Entidad Certificadora de Firmas Digitales” legalmente acreditada ante el CONATEL.

PALABRAS CLAVE:

Sociedad de la Información, Documentos Electrónicos, Firma Manuscrita, Firma Electrónica, Entidades Certificadoras de Firma Electrónica, Seguridades, Criptografía Simétrica, Criptografía Asimétrica

AUTORA:
DIANA MALO GONZALEZ.

INDICE

UNIVERSIDAD DE CUENCA

FACULTAD DE JURISPRUDENCIA

MAESTRIA EN DERECHO INFORMATICO, MENCION COMERCIO ELECTRONICO

TEMA

ENTIDADES CERTIFICADORAS DE FIRMA ELECTRONICA

AUTORA: DIANA MALO GONZALEZ.

DIRECTOR: Dr. JUAN PEÑA AGUIRRE

MARZO 2009

CUENCA – ECUADOR

UNIVERSIDAD DE CUENCA

DECLARACIÓN

Yo, Diana Isabel Malo González, declaro que los contenidos del presente trabajo son de mi propia autoría y bajo las referencias bibliográficas que constan en el documento.

…….....

DIANA ISABEL MALO GONZALEZ.

AGRADECIMIENTO

La consecución de este trabajo no hubiera sido posible sin la ayuda, paciencia y tiempo entregado por parte de mis padres, a quienes agradezco infinitamente.

Agradezco además al Dr. Juan Peña Aguirre por su dirección y asesoría, pero sobre todo por haber creído en mi y haberme dado la confianza de que lo podía lograr.

DEDICATORIA

Dedico este trabajo a los seres que complementan mi vida: Santiago y Matías, quienes envuelven de felicidad todo lo que hago.

CAPITULO I

INTRODUCCIÓN.

1.- Sociedad de la Información.

Fuente:http://images.google.com.ec/imgres?imgurl=http://andresgranada.files.wordpress.com/2009/12/sociedad-de-la-informacion.jpg&imgrefurl=http://andresgranada.wordpress.com/2009/12/16/sociedad-de-la-informacion/&usg=__pAOgKN0u5_E0IzHpa7PpUfrwGOI=&h=288&w=432&sz=40&hl=es&start=3&um=1&itbs=1&tbnid=iXY9wL6mkkOZUM:&tbnh=84&tbnw=126&prev=/images%3Fq%3DSociedad%2Bde%2Bla%2Binformaci%25C3%25B3n%26hl%3Des%26sa%3DX%26um%3D1

Quisiera iniciar este trabajo con algo que leí en un artículo elaborado por Oscar Picaro[1], y donde se manifestaba que a lo largo del desarrollo histórico de la humanidad se han evidenciado significativas épocas cuyo punto crucial de partida estigmatiza el pensamiento y las circunstancias de la gente. En el mundo occidental han existido cinco grandes períodos:

1.- El Cristianismo, imperante entre los siglos I y III, cuyo símbolo histórico lo representa la crucifixión de Jesús y las persecuciones martiriales.

2.- La Catolización Medieval, con la inquisición, las cruzadas y la colonización, siglos IV al XV.

3.- La Reforma protestante y la Ilustración, entre los siglos XVI y XVIII, que dan paso a las primeras revoluciones nacionales e independistas.

4.- El Modernismo, de los siglos XIX y XX, en los que se fraguan las bases tecnológicas e ideológicas de los grandes holocaustos mundiales.

5.- La Globalidad Informacional, en el siglo XXI, que no tenía bien definida su identidad o su espíritu del tiempo y al parecer comienza a delinear sus características. Se presenta el siglo XXI y el inicio del tercer milenio, como todo principio de siglo milenarista, con un quiebre histórico; el microchip y sus vertiginosas aplicaciones, unido al desarrollo de las nuevas tecnologías de información y comunicaciones, dan pie para catalogar a esta nueva etapa como la gran revolución informacional

[1] PICARO Oscar. La Sociedad de la Información, Debate, Servicios y Aplicaciones. URL. http://www.oei.es/revistactsi/numero1/debate1c.htm acceso 07-02-10

Por otra parte, Miguel Angel García, en su estudio titulado Sociedad de la Información[2], recopila las siguientes definiciones de la sociedad de la información:

"Sociedad que crece y se desarrolla alrededor de la información y aporta un florecimiento general de la creatividad intelectual humana, en lugar de un aumento del consumo material". Yoneji Masuda, La sociedad informatizada como sociedad post-industrial, Tecnos, 1994.

"La Sociedad de la Información, más que un proyecto definido, es una aspiración: la del nuevo entorno humano, en donde los conocimientos, su creación y propagación son el elemento definitorio de las relaciones entre los individuos y entre las naciones. El término ha ganado presencia en Europa, donde es muy empleado como parte de la construcción del contexto para la Unión Europea". Raúl Tejo Delarbre, La nueva alfombra mágica, Fundesco, 1996.

"Las sociedades de la información se caracterizan por basarse en el conocimiento y en los esfuerzos por convertir la información en conocimiento. Cuanto mayor es la cantidad de información generada por una sociedad, mayor es la necesidad de convertirla en conocimiento. Otra dimensión de tales sociedades es la velocidad con que tal información se genera, transmite y procesa. En la actualidad, la información puede obtenerse de manera prácticamente instantánea y, muchas veces, a partir de la misma fuente que la produce, sin distinción de lugar". Julio Linares et alii. Autopistas Inteligentes, Fundesco, 1995.

[2]GARCIA Miguel Angel. La Sociedad de la Información, Debate, Servicios y Aplicaciones. URL. http://www.oei.es/revistactsi/numero1/debate1c.htm acceso 07-02-10

“Nuevo sistema tecnológico, económico y social. Una economía en la que el incremento de productividad no depende del incremento cuantitativo de los factores de producción (capital, trabajo, recursos naturales), sino de la aplicación de conocimientos e información a la gestión, producción y distribución, tanto en los procesos como en los productos. “Manuel Castells, La era de la información, 1998.

“Se entiende por Sociedad de la Información aquella comunidad que utiliza extensivamente y de forma optimizada las oportunidades que ofrecen las tecnologías de la información y las comunicaciones como medio para el desarrollo personal y profesional de sus ciudadanos miembros”. Gobierno Vasco, Plan para el desarrollo de la Sociedad de la Información para el período 2000-2003.

“El término Sociedad de la Información se refiere a una forma de desarrollo económico y social en el que la adquisición, almacenamiento, procesamiento, evaluación, transmisión, distribución y diseminación de la información con vistas a la creación de conocimiento y a la satisfacción de las necesidades de las personas y de las organizaciones, juega un papel central en la actividad económica, en la creación de riqueza y en la definición de la calidad de vida y las prácticas culturales de los ciudadanos”. Misión para la Sociedad de la Información, Libro verde sobre la Sociedad de la Información en Portugal, 1997.

“Entorno en el que la información es un factor clave del éxito económico y en el que se hace un uso intenso y extenso de las Tecnologías de la Información y de las Comunicaciones”. Iniciativa para la Sociedad de la Información, Reino Unido, 1998.

El concepto de sociedad de la información hace referencia a la transformación que están provocando los nuevos medios de creación y transmisión de información mediante tecnologías digitales, lo que está provocando la aparición de nuevas formas de organización en la sociedad y en la producción de la misma.

La mayoría de autores están de acuerdo que en el año 1970 se marcó el inició de un cambio en el funcionamiento de las sociedades. Las industrias que eran las generadoras de riqueza, poco a poco han sido remplazadas por las tecnologías de la información y la comunicación, donde el eje central corresponde a la producción, almacenamiento y procesamiento de la información. Es decir, hemos pasado de la sociedad industrial a la sociedad de la información.

Es claro que el mundo ha experimentado un proceso de globalización, especialmente económica y cultural, donde se han roto muchos paradigmas políticos, económicos e ideológicos que actuaban como barreras separadoras entre los pueblos. Hemos entrado en una etapa de mundialización que nos exige adaptarnos a los cambios de mercado, en donde los servicios han suplantado a las industrias. Este escenario se ha dado gracias a los veloces avances en la ciencia y la tecnología.

Desde esta perspectiva globalizada de la economía, la sociedad de la información coloca a las nuevas tecnologías de la información y la comunicación TIC, como el motor del desarrollo y el progreso. Si antes la sociedad marcaba su desarrollo

económico en base a los procesos de industrialización fabriles, bajo un concepto de economía de mercadeo, desde principios de siglo XXI, hablamos de las industrias sin chimenea, donde el sector de los servicios se impone, y sobre todo la industria de la informática. Los ciudadanos del siglo XXI convivimos con materiales tecnológicos que nos brindan la posibilidad de un desarrollo personal y social, como son entre otras, las computadoras que nos proporcionan modernos instrumentos para el procesamiento de información y las redes telemáticas como el internet que nos brinda nuevos canales para comunicarnos y acceder al conocimiento. Debemos tener presente que el internet ha desempeñado un papel primordial como un medio de acceso a la información y de intercambio de datos, sin embargo, la sociedad de la información no se limita al internet.

Todos estos avances científicos que marcan la dinámica social en la actualidad originan que los conocimientos se vuelvan obsoletos rápidamente y provocan continuas transformaciones estructurales, exigiendo así, una rápida actuación para adaptarse a los cambios. La permanente formación se vuelve una necesidad indiscutible en nuestro tiempo.

En este entorno de cambio tecnológico continuo, donde existe la posibilidad de comunicarse de forma inmediata con cualquier persona, de acceder desde cualquier rincón del planeta a información dispersa por medio de redes de comunicación, es muy importante saber manejar la información, es decir, localizarla, valorarla, seleccionarla y aprovecharla, puesto que en la red existe todo tipo y clase de información. El reto estaría marcado en aprender a vivir de acuerdo a las exigencias de esta nueva sociedad de la información; saber estar

informados y actualizados; innovar y generar propuestas y conocimiento, todo aprovechando los millones de datos que circulan en la red.

Hay quienes critican a la sociedad de la información catalogándola como una réplica del imperialismo cultural de los países ricos a los pobres, sobre todo porque esta sociedad se desarrolla bajo parámetros de una dependencia tecnológica; bajo este principio y a pesar de que se pretende una sociedad globalizada, efectivamente se crea una brecha tecnológica entre los países desarrollados y los subdesarrollados económicamente.

Por su parte quienes defienden a la sociedad de la información, manifiestan que la integración de las TIC en los procesos productivos, nos facilitan ingresar a los mercados globales, en los que la creciente competencia obliga a bajar los costos y ajustarse a las condiciones del mercado.

Las dos posiciones tienen su razón muy cierta y justificada, sin embargo, para países que pudieran estar en desventaja tecnológica, es inútil negarse a la realidad ya impuesta y que sigue su marcha; esto representaría no sólo estancarse sino retroceder. Se debe sumar esfuerzos y marchar hacia adelante en un proceso de desarrollo dirigido a cumplir con los objetivos de la sociedad de la información, en base a los principios que se establecieron en la Cumbre de la Sociedad de la Información llevada a cabo en Ginebra en el año 2003, donde se dejo sentado que la Sociedad de la Información debe concentrarse en la persona, integradora y orientada al desarrollo, así como, orientarse en que todos puedan crear, consultar, utilizar y compartir información y el conocimiento para que las

personas, las comunidades y los pueblos puedan emplear plenamente sus posibilidades en la promoción de su desarrollo sostenible y en la mejora de su calidad de vida, sobre la base de los propósitos y principios de la Carta de las Naciones Unidas.[3]

En nuestro país se creó la Comisión Nacional de Conectividad, constituyéndose en el ente oficial encargado de promover políticas de la sociedad de la información y los proyectos concernientes a su desarrollo, donde se incluye infraestructura, conectividad, contenido y difusión. El principal objetivo de la Comisión es el de formular y desarrollar la Agenda Nacional de Conectividad, misma que pretende un lineamiento de cinco ejes básicos que son la infraestructura, teleducación, telesalud, gobierno en línea y comercio electrónico, aspectos que se han visto limitados aparentemente por ciertos aspectos de estructura organizacional de la Comisión y falta de continuidad.

En el año 2006, con iniciativa del Consejo Nacional de Telecomunicaciones, se implementó, un proceso tendiente a reformular las guías y objetivos que debe alcanzar nuestro país para insertarse en la llamada era del conocimiento y así parar el crecimiento de la brecha digital o lograr disminuirla. En esta actividad participaron diferentes sectores sociales que se organizaron en tres ejes:

1.- Infraestructura, acceso y servicio universal.

2.- Contenidos y aplicaciones locales.

3.- Sociabilización, apropiación y entorno habilitador.

[3] http://es.wikipedia.org/wiki/Sociedad_de_la_informaci%C3%B3n acceso 06-02-10

El resultado de estas labores se traduce en El Libro Blanco de la Información del Ecuador, que se halla a la espera de una política pública que lo ponga en marcha.[4]

2.- Firma Manuscrita y Firma Electrónica.

En Roma existía una ceremonia solemne llamada Manufirmatio, en la que, luego de leído el documento se lo colocaba sobre la mesa del escribano y luego de un acto de pasar la mano abierta por sobre éste a manera de juramento, el autor o el funcionario en su nombre, estampaba el nombre, signo, o cruces, al igual que lo hacían los testigos del acto.

En la Edad Media, se escribía una cruz acompañada de distintas letras y rasgos que se utilizaban como firma. Esta práctica fue reemplazada por los nobles, con el uso de sellos, debido a que no sabían leer ni escribir.

Las distintas firmas y signos que se estampaban fueron revelando que aquello significaba más que simples signos, la inscripción manuscrita del nombre y de los apellidos y esto representaba una identificación de la persona con el documento.

[4] http://www.gobiernoelectronico.org/node/5326 acceso 06-02-10

En aquel tiempo, muy pocas personas sabían leer y escribir, por eso se suscribían los documentos con diferentes signos; sin embargo, el desarrollo de la instrucción y de las transacciones comerciales, influyeron para que la firma fuera adquiriendo mayor importancia y se generalice su uso, y es así que con el pasar del tiempo se fue imponiendo como un fuerte símbolo de identificación y relación entre el autor de lo escrito o estampado en el documento y su persona.

El Diccionario de la Real Academia de la Lengua, le da un significado a la firma como 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.

A pesar de que específicamente el uso de la firma no lo regula ninguna legislación, podemos colegir que la firma manuscrita o autógrafa se la utiliza y ha utilizado a lo largo del tiempo, para que las partes expresen su consentimiento sobre un contrato.

La firma manuscrita cumple con ciertas características como son;

1.- Identificativa: sirve para identificar al autor del documento.

2.- Declarativa: representa la voluntad del firmante, quien asume el contenido del mensaje o la obligación contenida en el contrato.

3.- Probatoria: es posible identificar si el autor de la firma es el mismo que ha sido identificado como tal en el acto de firmar.

Por otra parte, a la firma la conforman ciertos elementos, que son los siguientes:

1.- Formales: Como su palabra lo dice son aquellos de forma o materiales, que se relacionan con los procedimientos utilizados para firmar y el grafismo mismo de la firma. Dentro de los elementos formales debemos caracterizar lo siguiente:

1.1. La firma como signo personal y distintivo, que debe ser expresada por puño y letra de su autor. Particularidad esta de la firma manuscrita que puede ser eliminada o sustituida en la firma electrónica por otros medios.

1.2. El animus signandi, que es la intención o intelectualidad de la firma, consistente en la voluntad de asumir el contenido del documento.

2.- Funcionales: La firma cumple una doble función:

2.1. Identificadora, porque determina la personalidad de su autor y aquellos derechos y obligaciones que del convenio se desprenden; es decir, vincula a la persona con el acto jurídico. La firma manuscrita expresa la identidad, aceptación y autoría del firmante; sin embargo no podemos asegurar que sea un medio fiable, siempre habrá el riesgo de que el documento sea modificado en su contenido. Tampoco podríamos decir que sin la firma autógrafa o manuscrita, no existe la posibilidad de otro modo de autenticación.

2.2. De Autenticación, porque revela ciertos aspectos de la identidad de la persona que la estampa, quien además de expresar su consentimiento, toma como suyo el mensaje.

Con estas consideraciones podemos aseverar que la firma es aquel lazo que une a una persona con el documento, y para que tal vínculo se dé, no es necesario que la firma sea legible en cuanto al nombre del propietario de ésta.

Por lo tanto, al ser el nexo personal y documental, se requiere únicamente que haya sido puesta en el documento por el firmante en persona, lo que nos demuestra que lo que suele expresarse o exigirse como manuscrita, no tiene un total sentido, puesto que puede adaptarse a cualquier otra grafía que ponga en el documento el firmante y que no rompa con ese vínculo del firmante con el documento, lo que representaría una autografía; término en base al cual nace la "firma autógrafa".

Es decir, la firma manuscrita puede ser sustituida por cualquier otra grafía personal del firmante, como lo es la huella digital. Es importante recalcar la calidad de "personal", puesto que, no cabe la idea de que pueda ser impuesta la firma por un tercero o por procedimientos que permitan a terceros imponerla. A este respecto es evidente que en la práctica mercantil y bancaria la firma puede estamparse por medios mecánicos como el facsímil o las máquinas de firma, sin embargo, para que aquello se dé es necesario que previamente exista un acuerdo entre las partes donde conste que el supuesto firmante asume cualquier responsabilidad que se genere del acto. En este sentido se han emitido ciertos cuestionamientos referentes a que no se podría considerar como firma a un

símbolo estampado por un tercero, lo cual tiene efectivamente su lógica, pero, eso no deja de lado que se trata de una práctica común.

En base a todo lo anotado, podemos recalcar que la función principal de la firma responde a ser un instrumento de la declaración de voluntad del firmante, en la que, por medio de la intervención personal de éste, expresa que asume todas y cada una de las manifestaciones o acuerdos contenidos en el documento, el mismo que al constar con la firma nos demuestra que ya no se trata de un mero proyecto o un borrador, sino de un verdadero documento.

Si la firma es la exteriorización de la declaración de la voluntad de un individuo, no tiene que ser exclusivamente de forma manuscrita, ya que esa exteriorización puede efectuarse por cualquier otro medio, como es el electrónico, sólo se necesitaría que lo haga el propio firmante o que legalmente sea atribuida a él.

Estamos listos para mencionar la existencia de la firma electrónica, la que nace de igual forma que todas aquellas prácticas evidenciadas en la historia; en este caso, en un entorno marcado por la era digital, donde se desarrollan las nuevas tecnologías. La firma electrónica se presenta como una exigencia para darle valor jurídico y fuerza probatoria a aquellos documentos que se los elabora utilizando los medios electrónicos e informáticos. La seguridad es esencial para el desarrollo del comercio electrónico, pues estamos hablando de relaciones donde ya no existe contacto físico entre las partes; ante lo que resulta necesario tener seguridad de la identidad de con quien se está tratando y certeza de que la información no ha sido alterada ni conocida por otras personas.

Siendo que el documento electrónico o informático es considerado como un medio de expresión de la voluntad que utiliza la electrónica con efectos de creación, modificación o extinción de derechos y obligaciones, la firma electrónica sería, el conjunto de códigos o claves criptográficas que se asocian de forma inequívoca a un documento electrónico, permitiendo identificar al autor o emisor y garantizando la integridad del mensaje en el trayecto de la comunicación.

Según la definición de la UNCITRAL, la firma electrónica se entiende como los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos.

Es decir, la firma electrónica es el conjunto de datos electrónicos, anexos o asociados a otros datos electrónicos que nos permite verificar al firmante como autor del documento y nos brinda la seguridad necesaria de que el autor del documento no pueda retractarse de lo manifestado en éste; lo que nos refleja las cualidades de autenticación y no repudio. Además nos presenta la garantía de integridad total durante la transmisión del documento, evitando así cualquier alteración o modificación que no sea detectada.[5]

[5] REYES KRAFT Alfredo Alejandro. *La Firma Electrónica*. URL. http://www.razonypalabra.org.mx/libros/libros/firma.pdf acceso 18-01-10

CAPITULO II

DOCUMENTOS ELECTRONICOS

1.- Origen de los Documentos Electrónicos

Con el nacimiento del internet y el desarrollo de las llamadas tecnologías de la información y el conocimiento, así como del comercio electrónico, empezamos a experimentar nuevas formas de manifestación y expresión de las distintas actividades de los seres humanos; obligándonos a romper la práctica habitual y bastante arraigada donde el papel es considerado el único instrumento que nos brinda seguridad. Todavía la tendencia se mantiene en gran parte a identificar al documento con aquella escritura sobre el soporte papel; y esto es porque hasta ahora muchas de las transacciones u operaciones son realizadas en este soporte, puesto que la materia documental era casi exclusivamente el papel.

Sin embargo, si partimos de un principio en el que el documento es toda aquella expresión del pensamiento, de la voluntad o del conocimiento que conste por escrito, podemos darnos cuenta que no tiene la calidad de documento únicamente aquel que conste sobre papel, sino que éste puede ser cualquier soporte donde se encuentren palabras u otros signos que identifiquen las ideas y lo que se quiere manifestar. Si retrocedemos en la historia podemos ver que antiguamente se utilizaba como soporte, ladrillos cocidos, tablas de madera encerada, el mismo papiro y el pergamino, entre algunas otras que podrían existir. Entonces, la

materia de la que se forme o pueda formar el documento podrá ir variando de acuerdo a los adelantos de la sociedad que marque la técnica.[6]

Es así que, actualmente existe el documento electrónico, mismo que se origina con las nuevas tecnologías, el desarrollo del software, y muchas otras innovaciones que han surgido y van surgiendo con el pasar del tiempo, con los que creamos constantemente documentos electrónicos, cuyo soporte material vienen a ser el disco duro, el disquete, el cd, las memorias, etc.

El documento electrónico es aquel que contiene información que puede constar en texto, sonido o imagen, que se lo transmite por medios electrónicos y se halla contenido en un mensaje de datos.

El principal temor manifiesto ante el documento electrónico es siempre el tema de la seguridad; ante esto, es importante mencionar que los documentos electrónicos o documentos transmitidos con soporte electrónico requieren efectivamente de un procedimiento lógico mediante un programa que convierta la codificación informática con la que se transmite, a la misma expresión en lenguaje natural para que pueda ser visualizada directamente. Para garantizar el contenido original del documento y su inalterabilidad existen medios tecnológicos que nos garantizan la coincidencia con el contenido original. Es lógico que la conservación de los documentos electrónicos tiene que hacerse bajo parámetros que permitan comprobar su originalidad, veracidad de su contenido y fiabilidad de la información, así como los procesos a los que se han sometido electrónicamente.

[6] RODRIGUEZ ADRADOS Antonio. *Firma electrónica y documento electrónico*. Edita Consejo General del Notariado. Madrid-España. pag. 14 y 15

Seguridad jurídica en nuestras relaciones y transacciones mediante documentos electrónicos podemos conseguir además con la firma electrónica y más aun con la firma electrónica certificada, aspectos todos que serán tratados más adelante.

Al referirnos a esta clase de documento se alude a que el lenguaje magnético constituye la acreditación, materialización o documentación de una voluntad ya expresada en las formas tradicionales, y la actividad de una computadora o de una relación jurídica o una regulación de intereses preexistentes. Se caracterizan por que sólo pueden ser leídos o conocidos por el hombre gracias a la intervención de sistemas o dispositivos traductores que hacen comprensibles las señales digitales. El ejemplo más común lo constituyen los documentos especialmente construidos para el uso de las terminales de un sistema, como es el caso de las tarjetas magnéticas para acceder a las cuentas bancarias, vías cajeros automáticos.

Abordando técnicamente el documento electrónico podemos explicarlo como los impulsos electrónicos que se transmiten de computador a computador, de manera que el documento se encuentra en los bits en los que se ha transformado el lenguaje natural. En este estado, ciertamente el documento no puede ser percibido directamente por los seres humanos, puesto que se trata de un lenguaje, si cabe el término informático, ajeno al que reconoce nuestros sentidos. Es decir, el documento creado con lenguaje natural, no es almacenado tal cual por el disco duro, sino que éste lo elabora con arreglo a su lenguaje mediante un programa; y a la vez, el mensaje almacenado en el disco duro solo podrá ser leído en lenguaje natural, por medio de una pantalla o impreso en papel, mediante un computador y a través de un programa.[7]

[7] Ibídem. pag. 20

Por lo tanto, hablando en un sentido estricto, el documento electrónico no es directamente reconocible, puesto que es un conjunto de ondas o impulsos electrónicos, que para ser presentado como prueba necesita ser transformado a alfabeto natural; debido a que está elaborado en forma digital y depositado en la memoria central del computador.

Sin embargo, apegándose a un criterio amplio se puede concebir al documento electrónico como aquel producido por la computadora a través de su entrada y salida y que resulta visible y comprensible para los seres humanos; es decir, es un objeto físico cuyo propósito es conservar y transmitir información. Este podría ser asimilado a un documento en soporte papel desde un punto de vista jurídico e interpretativo.

Los principales soporte informáticos son:

1.- Soportes magnéticos que almacenan la información digitalmente. Aquí podemos mencionar el disco duro que viene integrado en el hardware del computador y el disco extraíble que es un dispositivo externo que puede intercambiarse.

2.- Soportes ópticos de lectura láser, que son los CDs.

3.- Soportes o códigos ópticos impresos, que los conocemos como códigos de barra.

4.- Dispositivos electrónicos portátiles, como son las memorias.

5.- Dispositivos biométricos.

2.- Características.

El documento electrónico posee ciertas características propias y esenciales que lo conforman, mismas que se traducen en:

1.- El documento está escrito en lenguaje binario

2.- Debe ser almacenado en soporte informático, magnético, óptico u otra clase que pueda ser desarrollado para tales fines.

3.- El documento debe poder ser transformado a lenguaje comprensible por el ser humano.

A la par de aquello el documento electrónico posee idénticos elementos que uno escrito sobre papel, y esto es que:

1.- Constan en soporte material (como son las cintas, cd, discos duros, chip de memoria, etc.)

2.- Contiene un mensaje (que en este caso consta en un lenguaje binario no perceptible como tal por los sentidos del hombre)

3.- Están escritos en un idioma o código en este caso.

4.- Son atribuibles a determinada persona (empleando la firma electrónica o digital).

Partiendo de estas primeras consideraciones, abordaremos aquellas conocidas características, importantes para darle valor probatorio al documento:

1.- Inalterabilidad:

Cuando un documento no ha sido objeto de alteraciones decimos que es auténtico. A la vez que, será más seguro a medida que resulte difícil modificarlo y mientras sea más fácil identificar si ha sufrido alguna alteración.

Como en todo documento, para darle el valor y efectos jurídicos, esta característica resulta indispensable también en aquellos documentos electrónicos, cuyo contenido, como lo expresa el Ing. Héctor Revelo, no debe poder ser manipulado libremente luego de concluido, a no ser que las partes así lo acuerden y sea voluntad de ellas.

El temor latente, respaldado por los doctrinarios clásicos, de que los documentos electrónicos puedan ser alterados o modificados, ya sea en su contenido o

reutilización de los soportes, reduce su seguridad y confianza, volviéndose un freno para la plena aceptación probatoria de éstos.

2.- Autenticidad:

Esta característica va estrechamente ligada con la inalterabilidad, puesto que, un documento será auténtico cuando no haya sufrido alteraciones que varíen su contenido.

Para asegurar que el documento electrónico cumple con esta característica, debe ser guardado en un sistema encriptado que demuestre su autenticidad.

Debemos tener muy en cuenta algo que al respecto manifiesta el Dr. Miguel Angel Davara, y es que, las posibilidades de protección de la información por medios tecnológicos son mayores y más seguras que las que se ofrecen por los medios tradicionalmente empleados.

3.- Durabilidad:

Al hablar de durabilidad se pretende que el documento se mantenga en el tiempo sin sufrir alteración o modificación; característica que para mucho sólo poseen los documentos en soporte papel. Sin embargo, no es ajeno a nosotros el poder comprobar que en muchas circunstancias este soporte puede sufrir deterioros o incluso en casos extremos ser objeto de modificaciones; supuesto que no está

ajeno a los documentos electrónicos, pero que a mi criterio, es menos probable, bajo parámetros de seguridad que nos brinda la informática.

4.- Seguridad:

Constantemente se ha cuestionado a los documentos electrónicos, aduciendo que éstos carecen de seguridad con respecto a las tres características precedentes. Sin embargo, esto pierde fundamento al contar en la actualidad con varios sistemas de seguridad como claves de cifrado y otras medidas criptográficas en general. La propia firma electrónica nos brinda plena seguridad y validez probatoria en los documentos informáticos.

Además de todo lo anotado, me parece interesante trasladar a este trabajo algo que mencionó en clases el Dr. Julio Téllez al respecto de los documentos electrónicos y encaja perfectamente en el tema que estamos tratando. Esto es que, los documentos electrónicos como parte de su contenido deben permitir la identificación del lugar, nombres, dirección, fecha de redacción, de envío y de recepción, lo cual es perfectamente dable.

Concluyendo podríamos decir que para que el documento electrónico cumpla con la validez jurídica y probatoria de los otros documentos, es importante poder demostrar que al momento de insertar la información al computador, esta era cierta; que esta no ha sufrido manipulación desde que se la insertó; y, que la información leída en el computador de destino tiene correspondencia con aquella que se encuentra en el computador de origen.

3.- Clasificación de los documentos electrónicos.

A lo largo de esta investigación me he encontrado con algunas clasificaciones que les dan distintos autores a los documentos electrónicos, sin embargo, haré referencia unas pocas, que a mi criterio son las más interesantes y que están planteadas desde dos ópticas distintas.

El autor español Antonio Rodríguez Adrados [8] clasifica a los documentos electrónicos de de la misma forma que los documentos tradicionales, y es así que, fundamentalmente son públicos y privados. Partiendo de aquello expone que, el documento electrónico será soporte de:

1.- Documentos públicos, que estén firmados electrónicamente por funcionarios que tengan la facultad legal de dar fe pública, sea esta judicial, notarial o administrativa; siempre que ellos actúen en el ámbito de sus competencias y que cumplan con los requisitos que la ley exija para cada caso.

2.- Documentos expedidos y firmados electrónicamente por funcionarios o empleados públicos en el ejercicio de sus funciones públicas.

3.- Documentos privados.

En base a estos puntos de vista, se desprende que, existen tres clases de documentos electrónicos: los públicos, los oficiales y los privados.

[8] Ibídem

Por su parte Giannantonio considera que los documentos electrónicos pueden dividirse en: Documentos formados por la computadora y Documentos formados mediante la computadora.

Los primeros resultan ser cuando el computador no materializa únicamente una voluntad ya formada, sino que en base a ciertos parámetros y datos y con un adecuado programa, decide el contenido de una regulación de intereses.

Es decir, el computador determinará el contenido de una voluntad, sin limitarse a simplemente documentarla. El lenguaje electrónico no constituye simple documentación de una voluntad en las formas tradicionales, sino que constituye la forma entendida como elemento expresivo necesario de tal voluntad, la manifestación exterior necesaria de la regulación de intereses.

En la segunda clase de documentos electrónicos, expresada por este autor, la actividad del computador se orienta únicamente a comprobar y no a constituir; es decir, simplemente documenta una regulación de intereses ya expresados en otras instancias o en otras formas.

A esta clase es a la que en sentido estricto llamamos documentos electrónicos, mismos que no pueden ser percibidos por el ser humano sino gracias a la actividad de una máquina que transforme la señal digital que los constituye, en lenguaje comprensible para el hombre. Estos se encuentran contenidos en el disco duro, cdroom, memorias, etc., como ya habíamos mencionado en algún momento.

De Prada menciona una clasificación para los documentos informáticos, de acuerdo al soporte que los contiene: Documentos informáticos sobre soporte papel y Documentos informáticos sobre soporte electrónico.

Los documentos informáticos sobre soporte papel son aquellos producidos o elaborados por medio de la computadora, a los que se les dota de un soporte papel por medio de la impresora, en los que, se puede plasma la firma ológrafa de las partes.

Los documentos informáticos sobre soporte electrónico por su parte, son los documentos producidos en la computadora y ya no por su intermedio y pueden ser leídos únicamente con la aplicación de la técnica informática.

Los documentos electrónicos pueden también ser clasificados en base a su grado de conservación, y es así que tenemos los siguientes:

1.- Documentos de carácter volátil: Aquellos datos que se pierden al cortar la energía del computador, al encontrarse en las memorias de circuitos RAM.

2.- Documentos de carácter permanente: Como están contenidos en memorias de masa, sólo se pierden si éstos son borrados.

3.- Documentos de carácter inalterable: Son los que al ser grabados se dispone que sólo serán para lectura, lo que no permite su alteración. Esta particularidad la

encontramos en las memorias RAM, que es un chip integrado al computador y en los cd-room, que es una memoria en masa contenida en un disco.

4.- Naturaleza y validez jurídica.

En cuanto a la naturaleza jurídica del documento informático podríamos decir que éste constituye una nueva forma, originada bajo las técnicas de la electrónica, que se adapta a las teorías civil y mercantil en temas de contratación. Por lo tanto, con las adaptaciones pertinentes, su valor probatorio es similar que el documento sobre papel.

De esta manera, este tipo de documento, debe considerarse bajo los parámetros de documento público o privado, en la medida en la que cumpla con los requisitos que cada legislación contemple. Es perfectamente aceptable pensar que este documento pueda constituirse como instrumento público notarial, mediando para ello, una adecuación técnica de la informática dirigida a satisfacer los requerimientos jurídicos, y a la vez, una adecuación del Derecho frente a las condiciones de la informática.[9]

Debemos tener claro que el documento no es lo mismo que el soporte o el contenido. El soporte es el que contiene el documento y el contenido es la información constante. Una vez que los datos se ingresan al computador, se

[9] Gaete González, Eugenio Alberto; *Documento Electrónico e Instrumento Público*, Revista de Derecho Informático. URL. http://www.alfa-redi.org/rdi-articulo.shtml?x=511 acceso 18-02-10

registran y el documento ya está creado. Entonces, la computadora no forma sino comprueba, en base a un programa que la hace funcionar, a manera de su cerebro. El computador cumple órdenes del hombre, en base a instrucciones pre establecidas por este.

Los datos se originan por el hombre en una máquina o llegan a otra máquina por distintos medios pero siempre gracias a la actividad u orden humana de los programas. Cuando los datos son elaborados se convierten en información.

Conforme se incrementan las actividades en la Red, surgen controversias, que al igual que en las relaciones tradicionales, en muchos de los casos requieren de la intervención judicial. A este respecto se presentan las dudas sobre la validez de los documentos electrónicos como medio de prueba e inclusive los mismos jueces la cuestionan. Esto podría responder a factores como el rechazo tecnológico del Poder Judicial, tal vez al desconocimiento y temor ante los retos impuestos por las nuevas tecnologías o simplemente al hecho de que muchas legislaciones pueden no contemplar a los documentos electrónicos como medios de prueba.

De aquí, nace la necesidad de contar con una reglamentación que reconozca el valor jurídico y probatorio de los documentos electrónicos y una reglamentación que permita y garantice el ejercicio de las transacciones y contrataciones por estos medios en cumplimiento de todas las formalidades amparadas para las formas tradicionales. De la mano con lo anotado, es importante contar con infraestructura física y conocimiento en cuanto a las capacidades de las nuevas tecnologías de la información y sus límites.

Se debe tener en cuenta que en la valoración de la prueba que realizan los jueces, en un alto grado responden a apreciaciones basadas en la razón y la experiencia, que hasta cierto punto podría decirse que son subjetivas. De esta manera se estudia elementos como la integridad, inalterabilidad, veracidad y exactitud.

Es indiscutible que los documentos electrónicos pueden cumplir con los requisitos exigidos para tener validez jurídica, e inclusive pueden llegar a superar a los documentos tradicionales presentando mayores garantías de integridad e inalterabilidad, circunstancias muy importantes a ser consideradas por los jueces.

Ante el desarrollo e impacto que va teniendo la práctica del Comercio Electrónico, es preciso un adecuado reconocimiento jurídico de los acuerdos celebrados electrónicamente, para poderlos utilizar como medio probatorio válido en los procesos judiciales. Todas las modificaciones que puedan realizarse deberán ser flexibles con el objeto de que puedan adaptarse a la evolución electrónica, de tal forma que estos documentos puedan ser en todo momento considerados como vías seguras de contratación y tengan obligatoriedad jurídica, constituyéndose como medios de prueba idóneos.[10]

En nuestra legislación, el Código de Procedimiento Civil, admite como medios de prueba a los "…de otra naturaleza técnica o científica".

Con respecto al documento electrónico nuestra Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos lo regula en los siguientes términos: Art. 1.- Objeto de la ley.- Esta ley regula **los mensajes de datos**, la firma electrónica,

[10] PAEZ RIVADENEIRA Juan José; *Manual de Firmas Electrónicas y Mensajes de Datos*. Edit. Corporación de Estudios y Publicaciones. pag. 5 y 6

los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas."

Como se desprende de este artículo se le equipara al documento electrónico con el mensaje de datos, y es así, porque el documento electrónico está contenido en un mensaje de datos.

El artículo 2 del mismo cuerpo legal le da valor jurídico al documento electrónico o mensaje de datos al manifestar que "Los mensajes de datos tendrán igual valor jurídico que los documentos escritos. Su eficacia, valoración y efectos se someterá al cumplimiento de lo establecido en esta ley y su Reglamento.". De aquí podemos darnos cuenta que en nuestro país está plenamente reconocida la validez jurídica de los documentos objeto de nuestro análisis, de idéntica manera como se reconoce a aquellos que utilizan como soporte el papel.

Continuando con la revisión a nuestra ley, ésta hace mención a la posibilidad de darle validez jurídica a cierta información que no conste directamente en el documento electrónico, siempre que conste en éste a manera de remisión o de anexo. Es importante que el anexo o la información a la que se remita el documento tenga la plena aceptación de las partes y sea accesible directamente por medio de un enlace electrónico. A esto la ley lo llama "incorporación por remisión".

La ley ecuatoriana obliga a que los mensajes de datos, en temas referentes a propiedad intelectual se sometan a lo que la ley específica de esta materia lo

disponga y su reglamento, así como a los acuerdos internacionales a los que nuestro país esté obligado.

Con respecto a la confidencialidad y reserva de los documentos electrónicos o mensajes de datos se dice en el artículo 5 que “Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta Ley y demás normas que rigen la materia.”

Cuando por ley se disponga que la información deba constar por escrito, nuestra Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, manifiesta que esta condición estará cumplida con un mensaje de datos, siempre que la información contenida en él sea accesible a su posterior consulta. Cuando se requiera u obligue por ley que la información sea presentada o conservada en su forma original, también quedará cumplida con un mensaje de datos, siempre que pueda comprobarse que ha conservado la integridad de la información desde el momento en que se generó por primera vez en su forma definitiva y como mensaje de datos.

Se considera de acuerdo a la ley que permanece íntegro un mensaje de datos, cuando su contenido se mantiene completo e inalterable, con la salvedad de algún cambio de forma, propio del proceso de comunicación, archivo o presentación.

Los documentos que deban ser instrumentados físicamente podrán desmaterializarse con acuerdo previo de las partes y en cumplimiento de las obligaciones de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

Una cosa muy interesante para el objeto de este trabajo y que demuestra la utilidad de las certificadoras de firma electrónica es aquello que dispone la ley con referencia a los documentos desmaterializados respecto a que “Art. 7.-…Los documentos desmaterializados deberán contener las firmas electrónicas correspondientes debidamente certificadas ante una de las entidades autorizadas según lo dispuesto en el artículo 29 de la presente Ley, y deberán ser conservados conforme a lo establecido en el artículo siguiente.”

El artículo 29 expresa lo concerniente a las Entidades de certificación de la información, aspecto que será tratado en el capítulo correspondiente a este tema.

Por otra parte, la conservación de los mensajes de datos se cumplirá con el archivo del mismo, debiendo tener presente lo siguiente:

1.- Que la información que contenga sea accesible para su posterior consulta.

2.- Que el mensaje de datos sea conservado con el formato en el que se haya generado, enviado o recibido, o con algún formato que sea demostrable que reproduce con exactitud la información generada, enviada o recibida.

3.- Que se conserve todo dato que permita determinar el origen, el destino del mensaje, la fecha y hora en que fue creado, generado, procesado, enviado, recibido y archivado.

4.- Que se garantice su integridad por el tiempo que se establezca en el reglamento de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

Toda persona podrá cumplir con la conservación de mensajes de datos, usando los servicios de terceros, siempre que se cumplan las condiciones antes enumeradas. A la vez, la información que tenga por única finalidad facilitar el envío o recepción del mensaje de datos, no será obligatorio aplicar lo establecido.

La procedencia e identidad de un mensaje de datos, salvo prueba en contrario se entenderá que un mensaje de datos proviene de quien lo envía y autoriza a quien lo recibe, para actuar conforme el contenido.

Nuestra ley en su artículo 11 manifiesta también que, salvo que las partes pacten lo contrario, se presumirá que el tiempo y lugar de emisión y recepción de los mensajes de datos, son los siguientes:

1.- Momento de emisión: Cuando el mensaje de datos ingrese en un sistema de información o red electrónica que no esté bajo control del emisor o de la persona que envió el mensaje en nombre de éste o del dispositivo electrónico autorizado para el efecto.

2.- Momento de recepción: Cuando el mensaje de datos ingrese al sistema de información o red electrónica señalado por el destinatario. Si el destinatario designa otro sistema de información o red electrónica, el momento de recepción se presumirá aquel en que se produzca la recuperación del mensaje de datos. De

no haberse señalado un lugar preciso de recepción, se entenderá que ésta ocurre cuando el mensaje de datos ingresa a un sistema de información oral electrónica del destinatario, independientemente de haberse recuperado i no el mensaje de datos.

3.- Lugar de envío y recepción: Los acordados por las partes, sus domicilios legales o los que consten en el certificado de la firma electrónica, del emisor y del destinatario. Si no se les pudiere establecer por estos medios, se tendrá por tales, el lugar de trabajo, o donde desarrollen el giro principal de sus actividades o la actividad relacionada con el mensaje.

Finalmente nuestra ley en lo referente a los documentos electrónicos, hace referencia a la duplicación de los mensajes de datos y manifiesta que se considerará diferente a cada mensaje de datos y en caso de duda las partes pedirán la confirmación del nuevo mensaje y tendrán la obligación de verificar técnicamente la autenticidad del mismo

CAPITULO III

FIRMA ELECTRONICA

1.- Firma electrónica: generalidades

Con el desarrollo de la sociedad evoluciona constantemente la tecnología, dando paso a la aparición de nuevas herramientas que facilitan las actividades personales y empresariales.

El crecimiento de la llamada sociedad de la información aporta al crecimiento competitivo, resultando indispensable el uso de estas herramientas tecnológicas para fortalecer el comercio electrónico.

Como consecuencia, se requiere brindar la confianza necesaria a los usuarios de la Red sobre el uso estas herramientas, así como brindarles seguridad jurídica a quienes van percibiendo que el futuro de los negocios está manejado a través de estas redes.

En este contexto viene desarrollándose la firma electrónica y posicionándose exitosamente dentro de las medidas de seguridad aplicables a las operaciones, transacciones o transmisiones en la Red.

Siendo que la tendencia mundial va en torno al desarrollo económico basado en la globalización de las transacciones electrónicas, lo que permite aminorar costos y aumentar la productividad a nivel empresarial y de negociación, la firma electrónica juega un papel interesante desde la perspectiva de la seguridad que pueden alcanzar las redes.

En este sentido, cabe destacar a la firma electrónica como todo medio derivado del desarrollo de la técnica, que por el uso de ciertos sistemas de carácter también técnico, permite proteger bienes inmateriales y asegurar el cumplimiento de los elementos de integridad, autenticidad, disponibilidad, aceptación y validación; brindando seguridad a las partes que contratan con intermedio de redes, y, consecuentemente a la contratación electrónica, a la informática y a la telemática.

Se dice que la firma electrónica constituye un firmware, ya que combina el uso de bienes materiales como lo es el hardware, con bienes inmateriales como lo es el software, originando así un conjunto idóneo de elementos técnicos, que nos permiten conseguir medidas de seguridad apropiadas.

En este sentido, cabe destacar la definición de firma electrónica como aquel conjunto de datos que identifican a una persona o empresa en particular, mismos que suelen unirse al documento que se envía por medio telemático como si se tratara de una firma manuscrita, de tal manera que el receptor del mensaje tiene plena seguridad de quien ha sido el emisor y la garantía de que se trata de un mensaje original que no ha sido alterado.

La firma electrónica constituye el mensaje mismo una vez que ha sido ya codificado mediante el dispositivo de creación de firma. Según un autor Zagami, la firma electrónica es un conjunto de caracteres alfanuméricos resultante de complejas operaciones matemáticas de criptografía efectuadas por un ordenador sobre un documento electrónico. Por su parte Forcada Miranda la define como un resumen cifrado de un mensaje, al decir que, firmar electrónicamente un documento, supone cifrarlo para convertirlo en otro distinto e ilegible pero relacionado con el documento original gracias al algoritmo de cifrado.

La firma electrónica está representada por una clave o conjunto de claves, dependiendo de la clase de firma que se utilice, cuya función va en el sentido de cifrar el mensaje de datos; por lo tanto, es errado pensar que una firma manuscrita escaneada y superpuesta en un documento electrónico pueda considerarse como firma electrónica, o el hecho de firmar directamente en la pantalla del computador por medio de un lápiz electrónico con el que se pueden firmar documentos digitales, o cualquier otra clase o mecanismo que provoque la digitalización de la firma manuscrita.

Es más, resulta muy interesante saber que hablando en un sentido estricto una firma electrónica no siempre será la misma; pues al aplicar la clave o llave al mensaje de datos se producirá una fórmula distinta para cada texto cifrado. Es decir la clave secreta que nosotros ingresamos a manera de firma siempre será la misma en la práctica, sin embargo, en el proceso que experimenta dentro del computador está podrá representar resultados diferentes, dependiendo del texto al al que se le aplique. A este resultado lo denominamos algoritmo de cifrado.

La firma electrónica al prestarnos las mismas garantías que la firma manuscrita y en ciertos casos aun mayores, se la puede utilizar en infinidad de actividades comerciales en el ámbito privado, desde el caso de adquisición de bienes o servicios hasta relaciones entre empresas. En el sector público se la puede utilizar para las relaciones de la propia administración, así como en relaciones entre ésta y sus administrados en un sin número de actividades que ayudarían a ahorrar tiempo y dinero.

La implementación y regulación de la firma electrónica nos abre un abanico de oportunidades, desde el hecho de otorgarle pleno valor probatorio a los documentos electrónicos hasta procurar una actividad notarial y registral por medios electrónicos, sin necesidad que las partes se encuentren presentes físicamente.

La firma electrónica puede emplearse en todo tipo de documentos y actividades, y al ser un conjunto de caracteres que acompañan al documento, dentro de sus objetivos, a mas de asegurar la información contenida, está el de acreditar quienes son el autor y el receptor de éste. Por esto, siempre será necesario la existencia de un emisor y un receptor.

Garantías que nos presta la Firma Electrónica

1.- La utilización de la firma electrónica nos garantiza la integridad del mensaje, es decir la seguridad de que aquellos datos contenidos en el mensaje no han sido alterados ni modificados desde la emisión hasta la recepción del mensaje.

2.- Nos garantiza la identidad de los intervinientes, puesto que las dos partes cuentan con información verdadera de ellos; lo que además garantiza el no repudio por parte del emisor.

3.- Como mencionamos anteriormente le otorga plena validez al documento firmado electrónicamente, lo que proporciona seguridad a las transacciones en la Red.

4.- La firma electrónica a través de mecanismos como lo representan los sistemas criptográficos, especialmente la criptografía asimétrica, proporciona confidencialidad al mensaje, imposibilitando a terceros tener conocimiento del mensaje.[11]

2.- Clases de la Firma Electrónica

Existen principalmente dos clases de firma electrónica conocidas por la doctrina, que son: La firma electrónica y la firma electrónica avanzada.

La **firma electrónica como tal**, es decir aquella firma electrónica no avanzada, es aquella que posee todos los elementos requeridos y comúnmente utiliza la

[11] www.derechoecuador.com/index.php?option=comcontent&task=view&=id=4766&Itemid=130 acceso 04-12-09

encriptación simétrica, en base a una clave secreta, pero sin embargo, podría ser susceptible de romper las seguridades y ser interceptada por terceros.

Los documentos que conlleven este tipo de firma electrónica, en principio serían admisibles como prueba, teniendo un valor jurídico gradual.

Por su parte la **firma electrónica avanzada** es aquella a la que se la conoce generalizadamente como firma digital. Es una firma electrónica que usa técnicas de cifrado asimétrico, en base a un conjunto de claves, pública y privada. Esta firma electrónica avanzada es producida por un dispositivo seguro de creación de firmas, basada en un certificado de firma electrónica reconocido. Para que este tipo de firma tenga efectos jurídicos el certificado deberá ser expedido por una entidad Certificadora de Firma Electrónica debidamente acreditada; con este respaldo la firma electrónica provocará los mismos efectos jurídicos que la manuscrita.

Esta firma funciona otorgándole tanto al emisor como al receptor un número entero que funciona como su clave pública, a la vez, cada uno posee una clave privada que solo él conoce. Cuando el emisor envía el mensaje lo encripta con la clave pública del receptor, y emite la firma utilizando su propia clave privada. El receptor podrá abrir el mensaje únicamente con la clave pública del emisor para constatar la veracidad de la firma y podrá descifrar el mensaje con su clave privada.

De acuerdo al criterio de la UNCITRAL, para que una firma electrónica sea considerada como fiable debe cumplir con:

1.- Que los datos de creación de la firma, en el contexto en que son utilizados, correspondan exclusivamente al firmante;

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

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

4.- Cuando uno de los objetivos del requisito legal de firma consista en dar seguridades en cuanto a la integridad de la información a que corresponde, es posible detectar cualquier alteración de esa información hecha después del momento de la firma.

Cumplido aquello es posible garantizar la imposibilidad de suplantación, puesto que, la firma es creada por medios que están bajo el control exclusivo del signatario, como lo es su clave privada; la integridad, puesto que las firmas digitales por medio del cifrado que utilizan permiten percibir si el mensaje ha sido modificado luego de la firma. Nos ofrece seguridad inquebrantable que asegura el no repudio por parte de autor del documento, así como la no reusabilidad, es decir, que el documento no pueda duplicarse en lo posterior. Otra garantía importante es la privacidad, puesto que solo aquellos autorizados podrán intervenir en la comunicación. Finalmente la auditabilidad, con lo que se permite rastrear las operaciones efectuadas por el usuario de un sistema informático.

La firma digital no avanzada y la firma digital avanzada corresponden a la clasificación más generalizada dentro de la firma electrónica, sin embargo hay autores que han mencionado otras posibles clasificaciones donde incluyen clases como:

La firma electrónica alegal, que es una forma básica con un mecanismo de seguridad mínimo en el aspecto jurídico y con una economía también mínima, que funciona con acuerdo entre las partes.

La firma electrónica legal básica y avanzada que conforma uno varios mecanismos de seguridad jurídica básica y un costo más elevado por transacción.

La firma electrónica legal cualificada, que es una forma técnicamente más compleja, con elementos como requisitos de operación de dispositivos seguros y evaluaciones de conformidad que dan una mayor seguridad y mayores costos en la transacción.

Y finalmente la firma electrónica legal y legitimada donde los requisitos de los documentos y la firma se combinan con procedimientos y actuaciones de profesionales, que dan una gran seguridad jurídica y suponen un altísimo consto que se justifica únicamente en transacciones igualmente de costos elevadísimos.

El empleo de cada una de estas firmas corresponderá un análisis económico que justifique su actuación, sin embargo, es necesario al menos utilizar un mecanismo que brinde una seguridad básica jurídica.

3.- Equivalencia Funcional.

El mayor reto ante la aplicación de las nuevas tecnologías ha sido el de equiparar la firma electrónica a la firma manuscrita, otorgándole los mismo atributos y la misma validez jurídica; a eso se le conoce como equivalencia funcional, y es así que, en todos los países donde existe una ley al respecto se establece esa equivalencia funcional a favor de la firma electrónica que cumpla con los requisitos de seguridad y demás formalidades exigidas para el efecto.

A este respecto la Ley Modelo de la UNCITRAL manifiesta que: “Cuando la ley exija la firma de una persona, ese requisito quedará cumplido en relación con un mensaje de datos si se utiliza una firma electrónica que, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo aplicable, sea fiable y resulte igualmente apropiada para los fines con los cuales se generó o comunicó ese mensaje”.

Nuestra Ley Ecuatoriana a su vez expone dentro de los efectos de la firma electrónica que: “La firma electrónica tendrá igual validez y se le reconocerá los mismos efectos jurídicos que a una firma manuscrita en relación con los datos consignados en un documento escrito, y será admitida como prueba en juicio.”

Neutralidad Tecnológica

Debemos ser consientes de que la tecnología avanza de una forma muy rápida y lo que hoy nos resulta nuevo o moderno en poco tiempo podría tener un carácter obsoleto; por esta razón no podemos limitar el cumplimiento de las normas legales

a una determinada tecnología, es decir, regular en base a lo que tenemos ahora, porque estaríamos limitando el desarrollo tecnológico.

La creación de las leyes es un proceso claramente lento, por lo que éstas deben redactarse bajo un principio de neutralidad tecnológica, con apertura a las posibles nuevas modalidades. Con esto se pretende mantener un equilibrio entre las leyes y el dinámico proceso que implica la tecnología.

La Ley Modelo establece lo siguiente con respecto a preservar esta dinámica, al manifestar que: “Convencida de que la armonización tecnológicamente neutral de ciertas normas relativas al reconocimiento jurídico de las firmas electrónicas y el establecimiento de un método para evaluar de un modo tecnológicamente neutral la fiabilidad práctica y la idoneidad comercial de las técnicas de firma electrónica darán una mayor certidumbre jurídica al comercio electrónico.”

4.- Marco Jurídico Ecuatoriano.

La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, conocida también como la Ley 64, promulgada en el año 2002, es el cuerpo legal que regula en el Ecuador la correcta aplicación de la firma electrónica. La firma electrónica normada en nuestro país es aquella firma electrónica que la analizamos como avanzada o la que se le conoce en la doctrina como firma digital.

El art. 13 del mencionado cuerpo legal define a la firma electrónica como: “Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos.”

Recordemos que en nuestra ley acertadamente el mensaje de datos es lo mismo que decir documento electrónico.

En el Art. 14 equipara la validez de una firma manuscrita con la firma electrónica, con lo que le otorga admisibilidad probatoria dentro de un juicio, puesto que, se puede aportar como prueba un documento que contenga firma electrónica siempre y cuando esté contenida en un certificado legalmente reconocido por las autoridades de certificación y haya sido creada mediante un dispositivo seguro y legal.

Y es así, que la normativa establece requisitos básicos de validez para la firma electrónica, dejando abierta la posibilidad de que entre las partes se impongan otros además de los detallados a continuación:

Art. 15.-“…a) Ser individual y estar vinculada exclusivamente a su titular; b)Que permita verificar inequívocamente la autoría e identidad del signatario, mediante dispositivos técnicos de comprobación establecidos por esta Ley y sus reglamentos; c) Que su método de creación y verificación sea confiable, seguro e inalterable para el propósito para el cual el mensaje fue generado o comunicado;

d) Que al momento de creación de la firma electrónica, los datos que se creare se hallen bajo control exclusivo del signatario; y, e) Que la firma sea controlada por la persona a quien pertenece.

En este caso, para que la firma electrónica se dote de aquellas particularidades exigidas por la ley, resulta importante la labor que cumplen las entidades Certificadoras de Firma Electrónica, como lo veremos más adelante.

Nuestra ley prevé también que en un mensaje de datos la firma electrónica será parte integrante de éste o deberá estar asociada lógicamente al mismo, con lo que, se presumirá que el mensaje de datos contiene la voluntad del emisor, asumiendo y obligándose a su contenido.

Por su parte los titulares de una firma electrónica, son responsables de su manejo y deberán cumplir con ciertas obligaciones, a más de aquellas derivadas del uso mismo de la firma. Es el titular de la firma quien deberá preocuparse de tomar las medidas necesarias en cuanto a seguridad, ya que es responsable de cualquier uso indebido de la misma; deberá asegurarse de mantener la firma electrónica exclusivamente bajo su control y así evitar cualquier utilización no autorizada por su parte. Siendo su obligación también el notificar a todas aquellas personas vinculadas, cuando presuma o tenga la certeza de que la firma pueda estar controlada o utilizada indebidamente por terceros.

A este respecto, la Ley responsabiliza al titular de la firma electrónica, cuando no haya obrado con la debida diligencia, por cualquier obligación que se derive del

uso no autorizado de la firma. Pero lo exceptúa de tal responsabilidad, cuando el destinatario hubiese conocido de la inseguridad de la firma electrónica, o cuando la falta de diligencia pueda ser atribuida al destinatario.

Dentro de las obligaciones del titular de la firma, nuestra ley también prevé el hecho de notificar a la entidad de certificación de la información cualquier riesgo sobre su firma, así como solicitar de forma oportuna la cancelación de los certificados. Adicionalmente a todo lo que estipula específicamente la Ley 64 para el titular de la firma electrónica, éste está obligado a cumplir todas aquellas disposiciones que existan en otras leyes de la República con respecto al empleo de la firma manuscrita.

En nuestra legislación la firma electrónica tiene una vigencia indefinida, sin embargo, pueden ser revocadas, anuladas o suspendidas, siguiendo procedimientos que establece la misma ley, los cuales mencionaremos mas adelante cuando tratemos sobre las Entidades de Certificación.

La firma electrónica puede extinguirse por cuatro circunstancias que son:

1.- La simple voluntad del titular de ésta.

2.- De ocurrir el fallecimiento de su titular o una incapacidad del mismo.

3.- En caso de que el titular de la firma sea una persona jurídica, la firma se extinguirá si se da la disolución o liquidación de la persona.

4.- Si se declara judicialmente la extinción.

Cabe anotar que cualquier obligación contraída previamente a la extinción de la firma electrónica se mantiene hasta su cumplimiento.

El tema de neutralidad tecnológica también se halla presente en nuestra legislación, y es así que la firma electrónica es aceptada bajo este principio; sin restringir la autonomía privada de usar otras firmas electrónicas fuera de la infraestructura de clave pública.

Bajo este concepto veamos cuales son los principios y elementos que de acuerdo a nuestra ley respaldan a la firma electrónica:

1.- No discriminación a cualquier tipo de firma electrónica, así como a los medios de verificación o tecnología que se empleen en ella. Lo que nos asegura que la evolución de la tecnología no tendrá limitantes en la ley.

2.- Prácticas de certificación basadas en estándares internacionales o compatibles a los empleados internacionalmente. Lo que nos permite avanzar y no estancarnos en un solo tipo de tecnología.

3.- Con respecto a los estándares internacionales, también se establece como principio de la infraestructura de la firma electrónica, que se apegarán a éstos tanto los soportes lógicos o conjunto de instrucciones para los equipos de cómputo y comunicaciones, así como, los elementos físicos y demás componentes

adecuados al uso de las firmas electrónicas, las prácticas de certificación y condiciones de seguridad adicionales.

4.- Otro principio es el referente al sistema de gestión que permita el mantenimiento de las condiciones señaladas en los literales anteriores, así como la seguridad, confidencialidad, transparencia y no discriminación en la prestación de sus servicios.

5.- Finalmente la existencia de órganos de promoción y difusión de los servicios electrónicos, y de regulación y control de las entidades de certificación.

Indudablemente resultan nulas las posibilidades de alteración o falsificación de una firma electrónica, puesto que ésta conlleva seguridades y algoritmos imposibles de descifrar, como lo hemos analizado ya, situación que convierte a la firma electrónica en un mecanismo altamente seguro para las transacciones económicas.

La firma electrónica tiene una importancia fundamental para el desarrollo de las tecnologías en nuestro medio y la armonización social, lo que provoca darle primordial atención a esta figura. Por esta razón, organismos como el Consejo Nacional de Telecomunicaciones (CONATEL), se preocupan constantemente en crear el ambiente legal propicio para la plena aplicabilidad a la firma electrónica en el Ecuador, circunstancias que evidenciaremos más adelante.

Es importante saber que para utilizar la firma electrónica en nuestro medio, es necesario que, tanto las sociedades como las personas naturales interesadas

acrediten sus datos ante el Banco Central del Ecuador, que es el organismo encargado de emitir las certificaciones correspondientes.

Finalmente cabe manifestar que a pesar de que el porcentaje de la población que tiene acceso a internet en el Ecuador sigue siendo bastante bajo, la firma electrónica juega un papel muy importante para el desarrollo económico, puesto que, impulsa una expansión del comercio, en base al comercio electrónico, a la vez que brinda una herramienta efectiva a la administración, que puede emitir documentos y certificados a un costo bajo, permitiendo a los administrados obtenerlos fácilmente.

CAPITULO IV

ENTIDADES CERTIFICADORAS DE FIRMA ELECTRONICA.

1.- Antecedentes: generalidades.

Hasta el momento hemos concluido con un procedimiento de firma electrónica en base a una doble clave, privada y pública, con las que se cifra y decifra el mensaje de datos. Sin embargo, en cierto momento bastaba con generar un intercambio manual de aquellas claves públicas, situación que funcionaba mientras se trataba de grupos pequeños y sectoriales, pero ahora, cuando nos encontramos frente a un global y masivo tráfico por medio de internet, donde el intercambio es en redes abiertas y en muchos casos redes inseguras, ya no podemos continuar con aquel intercambio manual, puesto que, nos podría resultar inseguro.

Es frente a esto que aparece una figura de gran importancia como lo constituyen las Entidades de Certificación, que se las conoce también como terceras partes de confianza, cuya principal misión es la de certificar que determinada clave pública pertenece a una persona y que ésta se encuentra vigente.

En el Ecuador, para que la firma electrónica tenga validez jurídica es indispensable que posea un certificado de firma digital, que debe ser emitido por una “Entidad Certificadora de Firmas Digitales” legalmente acreditada ante el CONATEL.

2.- Importancia y función.

Las medidas que nos ofrece la técnica nos permiten contar con un alto grado de seguridad, no obstante, frente a la fuerza que ha adquirido la contratación electrónica nace la interrogante de que si la persona que se encuentra del otro lado de la red es efectivamente quien ha emitido determinada información. Esta necesidad de seguridad al respecto es muy justa, puesto que el conjunto de claves que se utiliza para crear una firma digital, por si solo no tiene una asociación intrínseca con alguien en especial.

Entonces, la solución de que un tercero confiable certifique a determinada persona innegablemente asociada con el par de claves, es lo que complementa la seguridad de todo el sistema de firma electrónica basada en criptografía asimétrica de clave pública. La importancia que adquieren las Entidades Certificadoras de Firma Electrónica es por su principal labor de asociar de modo inequívoco la identidad de una persona a una clave determinada.[12] Para que la firma electrónica avanzada sea reconocida, se necesita que la acompañe un certificado digital igualmente reconocido que lo emite una entidad certificadora, quien garantiza que la clave pública pertenece a determinada persona.

Podríamos decir, que las entidades certificadoras son quienes hacen posible en la realidad el empleo de la firma electrónica, constituyéndose entes importantes e indispensables en todo el proceso de reconocimiento y validez jurídica de todos aquellos documentos o contratos electrónicos.

[12] RIPPE S. CREIMER I. DELPAZZO C. HARGAIN D. MATTEO V. MERLINSKI R. BAUZA M. CAFFERA G. BALARINI P. PIAGGIO J. PEREZ N. *Comercio Electrónico*. Edit. B de F. Buenos Aires-Argentina. 2003. Pag. 82

La entidad de certificación es una institución técnica de validación y verificación de las partes intervinientes en una relación o contratación electrónica. Vale mencionar que esta institución debe ser ajena a los titulares de firma que se deben certificar y validar.

La certificadora de firma electrónica permite que se pueda conocer plenamente las fuentes de donde proviene la información, evitando los fraudes y desconfianza de quienes intervienen en transacciones en la red. Además otorga una mayor confidencialidad a los actos efectuados por las partes, ya que ésta se encarga de certificar si las firmas utilizadas realmente corresponden a las partes. También permite la integridad en las transacciones, puesto que al ser un ente especializado está en la capacidad de recomendar a las partes medios técnicos de seguridad altamente fiables.

Como todas las medidas de seguridad técnicas, las entidades certificadoras permiten estándares que aseguren una efectiva contratación electrónica, como la autenticidad de la información transmitida por un mensaje de datos, garantizando el no repudio y brindando la debida confidencialidad y seguridad.

Las entidades certificadoras de firma electrónica emiten documentos que son conocidos como certificados, los cuales constan cifrados para evitar intrusiones, y se adjuntan al documento. Estos certificados contienen información a cerca de la clave pública, pueden tener datos como el número del certificado, fechas de creación y caducidad, entre otros, de tal manera que se pueda confirmar y verificar

la identidad de las partes. De aquí que es muy importante que exista un adecuado reconocimiento jurídico y normativa que otorgue a esta institución la importancia necesaria.

A pesar de que una Entidad Certificadora como parte de su actividad puede prestar otros servicios o bienes relacionados con la emisión de una firma electrónica, es principalmente en busca de la intervención de un tercero que proporcione confianza a la transacción electrónica, por lo que un suscriptor acude a una entidad certificadora.

La Certificadora como primer paso efectúa un procedimiento tendiente a la verificación de la identidad de aquella persona a la que se le va a expedir el certificado digital. Son acciones cuya finalidad es comprobar los datos que han sido proporcionados a la entidad de certificación, por parte de aquella persona que le interesa ser un suscriptor de firma electrónica. Cabe mencionar que a este respecto nuestra ley no establece los mecanismos que deberá emplear la certificadora para cumplir con esta misión, sin embargo es una acción necesaria para la entidad y ésta deberá ingeniarse las formas de verificación.

Una vez que se haya verificado la identidad de la persona, la certificadora tomará la decisión de expedirle un certificado digital donde consta tal identidad. Debemos tener muy en claro que el certificado digital comprende un archivo electrónico que va incorporado a un soporte físico, el que encierra contenidos emitidos por la certificadora, relacionados con la identidad del suscriptor. Las declaraciones hechas por la entidad en este certificado tienen sentido únicamente dentro del

contexto del sistema de certificación digital implementado por la certificadora y dentro del marco jurídico que corresponde.

Por su parte el ahora suscriptor y terceras personas pueden verificar si el certificado ha sido revocado, puesto que las entidades de certificación deben tener actualizada su lista de revocación de certificados digitales, de tal manera que, se pueda confiar plenamente en un certificado que no consta en dicha lista, puesto que, aquello implica que el certificado se halla vigente.

El certificado como tal es un producto que provee la certificadora, sin embargo es el sistema de certificación digital que ofrece la entidad el que genera confianza y permite efectuar las transacciones sin temor.

La certificación digital es una actividad especializada que requiere de un amplio conocimiento sobre el complejo funcionamiento de la infraestructura de clave pública, que se lo conoce como PKI. Se debe saber cómo aplicar esa tecnología a los distintos sistemas de información. La actividad de las entidades certificadoras de firma electrónica conlleva una infraestructura tecnológica idónea y una gran cantidad de estrictos procedimientos que permiten el uso simplificado de un certificado digital.

Por todo lo anotado es importante fortalecer las entidades de certificación de firmas electrónicas, puesto que así se podría conseguir una legalización y legitimación de los procesos emprendidos en el comercio electrónico; controlar la transmisión de la información con características de confidencialidad,

autenticación e integridad y previniendo pérdidas de datos. Se puede lograr que se de fe pública en el intercambio de información y en el comercio electrónico mismo.

Fortaleciendo este tema se puede provocar un análisis de los medios probatorios que protejan a los usuarios para cualquier reclamo en caso de sentirse perjudicados; así como procurar técnicas de seguridad en la publicidad de datos personales, para un acuerdo electrónico que brinde tranquilidad a las partes.

3.- Legislación

Las leyes que se han expedido en los distintos países con respecto a comercio electrónico, son basadas en alguno de los siguientes modelos:

a) La ley de Utah, en Estados Unidos, denominada “Utah Digital Signature Act.”, publicada en el año 1995. Esta ley es la pionera en la historia y consta de cinco partes:

1.- La primera que corresponde a la interpretación de la ley y los propósitos de la misma que se traducen en: a) facilitar el comercio por medio de mensajes electrónicos confiables; b) minimizar la incidencia de falsificaciones de las firmas digitales y fraudes en el comercio electrónico; y, c) establecer reglas uniformes relacionadas con la autenticación y confiabilidad de los mensajes electrónicos.

Esta ley contiene una definición de criptografía asincrónica como un algoritmo o serie de éstos que proveen un par de claves seguras. Al par de claves lo define

como una clave privada con una correspondiente clave pública en un sistema de criptografía asincrónica, con la propiedad de que la clave pública puede verificar la firma digital que ha sido creada por la clave privada. Finalmente a la firma digital la concibe como la transformación de un mensaje usando un sistema de criptografía asincrónica de tal manera que, teniendo el mensaje inicial y la clave pública del firmante, se puede determinar con precisión si la transformación ha sido creada usando la clave privada que corresponde a la clave pública, y determinar si el mensaje ha sido alterado desde su transformación (o firma digital).

La segunda parte de la ley se refiere a la concesión de licencias y la regulación de las autoridades certificantes, donde se establecen requisitos para quienes consideren desempeñarse como tales autoridades.

La tercera parte trata sobre los deberes de las autoridades certificantes y el contenido de los certificados.

La cuarta parte se refiere a los efectos de la firma digital cuando por norma legal se requiera, equiparándola a cualquier otra modalidad de firma, cuando ésta esté contenida en
un certificado extendido por una autoridad certificante, o si la firma ha sido estampada por el firmante con la intención de hacerlo.

Finalmente su quinta parte menciona sobre los servicios estatales de archivo de claves públicas y aquellos requisitos que debe cumplir.[13]

[13] PAEZ RIVADENEIRA Juan José. Ob. Cit. Pag.57 y 58

b) La Ley Modelo de la UNCITRAL, a la cual la hemos mencionado en algunas ocasiones a lo largo del presente trabajo, puesto que, nuestro país la tomó como referente. Esta ley es la sugerida por la Organización de Naciones Unidas ONU.

En el campo del derecho mercantil internacional, la UNCITRAL es el principal órgano jurídico del sistema de las Naciones Unidas. Se dedica a modernizar y armonizar las reglas en cuanto al comercio internacional.

De acuerdo al criterio de la UNCITRAL un prestador de servicios de certificación es quien expide certificados y puede también prestar otros servicios que tengan relación con las firmas electrónicas. Lo considera un tercero de confianza que acredita el vínculo entre una determinada clave y su propietario. El certificado de firma electrónica que extiende el prestador de servicios de certificación debe estar firmado con la clave propia de la entidad para garantizar que la información en él contenida es auténtica.

El certificado digital para la UNCITRAL es un archivo que incorpora la clave pública de un sujeto y la relaciona con su clave privada. Su validez consiste en que actúa como tercero de confianza y verifica la identidad del firmante y da certeza sobre tal información.

Menciona también que la existencia de varios y diversos prestadores de servicios de certificación, otorga la posibilidad de que sea el mismo usuario quien elija a la entidad que le genere confianza y seguridad.

c) **El modelo de normativa Europea**, que se estableció en el año de 1999, creando un marco común referente al reconocimiento de la firma electrónica y a ciertos servicios de certificación. Esto fue emitido por decisión del Parlamento Europeo y el Consejo, cuya principal finalidad es la de garantizar un funcionamiento armónico con respecto a la firma electrónica, en base a un marco legal uniforme para toda la Comunidad.

Este modelo define a la firma electrónica como aquella firma expresada en forma digital que es empleada por un signatario para manifestar su aceptación con respecto al contenido del os datos, cumpliendo los requisitos que a continuación se detallan:

1.- Estar vinculada al signatario de manera única.

2.- Permitir la identificación del signatario.

3.- Haber sido creada por medios que el signatario pueda mantener bajo su exclusivo control.

4.- Estar vinculada a los datos relacionados de modo que se detecte cualquier modificación ulterior de los mismos.

Estableciendo que el dispositivo de verificación de la firma son los datos únicos, tales como códigos o claves criptográficas públicas, o un dispositivo físico de configuración única, utilizado para verificar la firma electrónica.

Con respecto a los proveedores de servicios de certificación se dice que es la persona o entidad que expide certificados o presta otros servicios al público en relación con la firma electrónica. El Certificado reconocido es el certificado digital que vincula un dispositivo de verificación de firma a una persona y que confirma su identidad.

Existe un Comité de Firma Electrónica que apoya a la Comisión en labores de supervisión. La firma electrónica será considerada como firma que cumple los requisitos legales de una firma manuscrita y por lo tanto produce los mismos efectos que la firma manuscrita, cuando cumpla con los requisitos establecidos, situación que deberá ser velada por cada estado miembro.

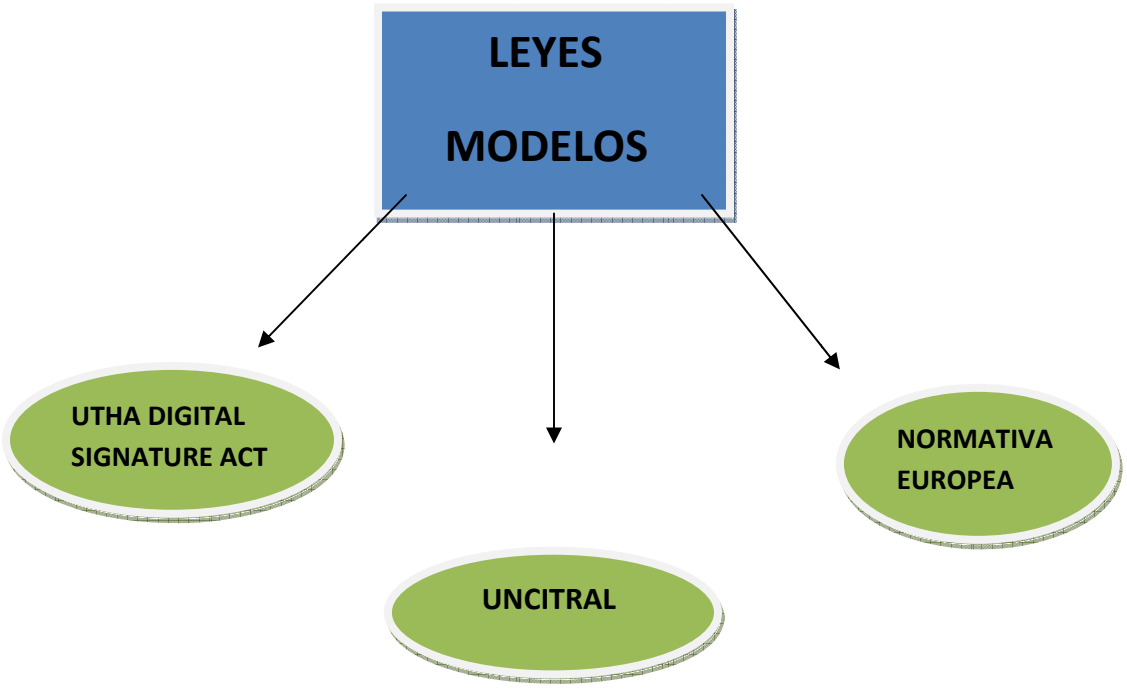
A los estados miembros les compete además el velar que los certificados que sean expedidos por un proveedor de servicios de certificación establecido en un tercer país, tengan la misma validez que un local, siempre que cumpla con los requisitos detallados.

Bajo este esquema, los certificados serán válidos si se dan las siguientes consideraciones:

1.- El proveedor de servicios de certificación cumple los requisitos establecidos en la Directiva y ha sido acreditado en el bajo el marco de un sistema voluntario de acreditación establecido por un Estado miembro.

2.- Un proveedor de servicios de certificación establecido en la Comunidad, que cumpla las prescripciones, avala el certificado en la misma medida que los suyos propios;

3.- El certificado o el proveedor de servicios de certificación están reconocidos en virtud de un acuerdo bilateral o multilateral entre la Comunidad y terceros países u organizaciones internacionales.



Mencionados los tres modelos de leyes, veamos brevemente lo que legislaciones de ciertos países manifiestan con respecto a nuestro tema de estudio.

En **Estados Unidos** el certificado digital es considerado o definido como aquel registro basado en la computadora que identifica a la autoridad certificante que lo emite. Este certificado identifica a quien lo suscribe y va firmado digitalmente por la autoridad certificadora, además contiene la clave pública del suscriptor.

La American Bar Association es una entidad que cuenta con una División de Comercio Electrónico, donde hay un Comité de Seguridad de la Información. Esta división es la encargada del control y la supervisión, a la vez que actúa como autoridad certificadora. La emisión de los certificados lo hace la autoridad certificadora que sea acreditada.

La normativa de los Estados Unidos concede igual valor probatorio a los documentos electrónicos o mensajes de datos que a aquellos que se encuentran en soporte papel, siempre y cuando los acompañe una firma digital de clave pública que esté contenida en un certificado debidamente emitido por una autoridad certificadora autorizada. No hay un reconocimiento expreso de certificados extranjeros, sin embargo da la facultad a la División de reconocer autorizaciones emitidas por autoridades certificadoras de otros Estados.

Por su parte **Colombia** se apega al modelo UNCITRAL; define a la entidad de certificación como aquella persona que, autorizada conforme a la Ley de Colombia, está facultada para emitir certificados en relación con las firmas digitales, 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. Estas entidades son las encargadas de dar seguimiento a la firma electrónica, respondiendo hasta por culpa leve.

En la normativa colombiana un mensaje de datos tendrá igual valor probatorio que un documento tradicional, cumpliendo los siguientes requisitos:

1. Es inherente 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.

Las entidades de certificación autorizadas están sometidas al control y supervisión de la Superintendencia de Industria y Comercio, quien tiene la facultad de imponer sanciones según la naturaleza y gravedad de la falta, desde la amonestación al a revocación de la autorización.

Perú tiene su normativa basada en el modelo europeo y otorga igual validez a la firma electrónica que a cualquier otra forma que exprese la voluntad, sin establecer valor probatorio para la firma electrónica. Define al certificado digital como el 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.

En cuanto a las entidades de certificación, expone que éstas intervienen en la emisión de certificados y pueden asumir las funciones de entidades de registro o verificación; deberán contar con un registro.

Existe una figura de entidad de registro o verificación que es la encargada de recolectar y comprobar la información del solicitante del certificado, quien además identifica y autentica al suscriptor de firma digital y acepta y autoriza las solicitudes de emisión y cancelación de certificados digitales.

En cuanto a los certificados otorgados por una certificadora extranjera se manifiesta que éste debe contar con el aval de una entidad nacional.

La supervisión y el control corresponden a la autoridad administrativa que sea designada por el poder Ejecutivo.

La normativa **Argentina** es un esquema que otorga a la firma digital una utilización completamente voluntaria, sin mencionar nada que la equipare a la manuscrita. Preserva una libertad contractual, permitiendo que las partes establezcan la modalidad en sus transacciones, de aquí que, serán ellas las que decidan la utilización de la firma digital y le provean de total validez.

Se manifiesta un reconocimiento legal a las firmas digitales y a los servicios de certificación en base a clave pública, proponiendo que un documento digital firmado digitalmente no deje de tener validez jurídica.

El documento digital en Argentina es la representación digital de actos, hechos o datos jurídicamente relevantes, con independencia del soporte utilizado para almacenar o archivar esa información.

Aquellos certificadores de clave pública no tienen responsabilidad por inexactitudes en los certificados por ellos emitidos, que sean generadas a causa de la información que les haya facilitado solicitante, siempre que el certificador demuestre que ha actuado diligentemente de acuerdo a las circunstancias y el tipo de certificado de que se trate. Los certificadores cuentan con la facultad de limitar su responsabilidad, señalando en los certificados emitidos, las restricciones para su utilización.

Se define al certificado como un documento digital firmado digitalmente por un certificador de clave pública, que asocia una clave pública con su titular durante el período de vigencia del certificado.

En la legislación de **España** se define 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.

Entonces, la firma firma electrónica avanzada tiene valor probatorio cuando conste en un certificado reconocido y que haya sido producida por un dispositivo seguro de creación de firma.

Define como certificado la certificación electrónica que vincula unos datos de verificación de firma a un determinado individuo o entidad, conocidos como signatario y confirma su identidad. Se exige como requisitos del certificado los siguientes:

1.- La indicación de que se expide como tal.

2.- El código identificativo único del certificado.

3.- La identificación del prestador del servicio de certificación.

4.- La firma electrónica avanzada del prestador del servicio de certificación.

5.- La identificación del signatario.

6.- Los datos de verificación de firma equivalentes a aquellos de creación de firma.

7.- El plazo de validez del certificado.

8.- Los límites de uso del certificado y del valor de las transacciones para las que puede utilizarse, si se establecen

El prestador de servicios de certificación se lo considera a aquella persona física o jurídica que expide certificados, pudiendo prestar, además, otros servicios en relación con la firma electrónica. Estas entidades tienen responsabilidad administrativa, con infracciones que van de muy graves, graves y leves.

Se establece que el Ministerio de Fomento por medio de la Secretaría General de Comunicaciones son los encargados de supervisar las actividades. Antes de iniciar las actividades las entidades certificadoras deberán registrarse en el Ministerio de Justicia.

4.- Marco jurídico Ecuatoriano respecto a las Entidades de Certificación y certificados de firma electrónica.

El cuerpo legal que norma lo relativo a nuestro tema de estudio es la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, cuyo objeto es el de regular los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas. Además, contamos con un Reglamento a la mencionada ley y ciertas resoluciones de organismos competentes como el CONATEL, que en muchos de los casos han sido promulgadas mediante decretos, que apuntan a un fin común de armonizar,

proteger y regular el reto presentado con la aparición de las nuevas tecnologías de la información y el conocimiento.

La ley ecuatoriana dentro de las Disposiciones Generales establece un glosario de términos dentro del cual define al comercio electrónico como toda transacción comercial realizada en parte o en su totalidad, a través de redes electrónicas de información. En este marco, debemos considerar que para que la actividad del comercio electrónico tenga una trascendencia jurídica y una consecuente validez probatoria se requiere que los documentos electrónicos estén integrados con la base de una firma electrónica, que deberá estar respaldada por un certificado de firma electrónica emitido por una Entidad Certificadora legalmente acreditada. En nuestra legislación la potestad de acreditación de estas entidades de certificación la tiene el CONATEL, es decir, para poder operar al público, deberán previamente cumplir con las disposiciones legales y someterse a la aprobación por parte de este organismo.

Un certificado de firma electrónica normalmente es un documento digital que nos cerciora la vinculación entre una persona o entidad con una clave pública, de manera que no haya duda con respecto a la identidad de la otra parte con la que estamos comunicándonos.

En el Art. 20 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos se define al certificado de firma electrónica de la siguiente manera: “Es el mensaje de datos que certifica la vinculación de una firma electrónica con una persona determinada, a través de un proceso de comprobación que confirma su identidad.”

El siguiente artículo menciona el uso del certificado de firma electrónica estipulando que: “El certificado de firma electrónica se empleará para certificar la identidad del titular de una firma electrónica y para otros usos, de acuerdo a la ley y su reglamento.”

Como ya hemos analizado anteriormente, un mensaje de datos es exactamente lo mismo que un documento electrónico, por lo tanto, el certificado de firma electrónica es un documento que acredita la identidad del propietario de una firma.

Para que el certificado de firma electrónica sea considerado válido deberá contener los requisitos que para el efecto nos establece la ley en su Art. 22 que son los siguientes:

a) Identificación de la entidad de certificación de información.
b) Domicilio legal de la entidad de certificación de información.
c) Los datos del titular del certificado que permitan su ubicación e identificación
d) El método de verificación de la firma del titular del certificado
e) Las fechas de emisión y expiración del certificado.
f) El número único de serie que identifica el certificado.
g) La firma electrónica del a entidad de certificación de información.
h) Las limitaciones o restricciones para los usos del certificado
i) Los demás señalados en esta Ley y los reglamentos.

La identificación de la entidad certificadora se cumple normalmente con una señal distintiva, con lo que podemos identificar quien respalda la firma que viene acompañando al documento o mensaje de datos.

El domicilio de acuerdo a nuestro Código Civil es la residencia, acompañada, real o presuntivamente, del ánimo de permanecer en ella. En el caso de una entidad de certificación sería el lugar donde ésta se halle constituida y ejerza sus funciones; el lugar donde cumpla sus obligaciones y se le pueda exigir las mismas.

Los datos del titular serían aquellos que lo identifiquen y haya comprobado la entidad certificadora.

El método de verificación que será establecido por la certificadora.

Las fechas de emisión y expiración ayudan a la constatación de vigencia del certificado.

El número de serie que deberá ser único para ese certificado, será el que le imponga la entidad certificadora de acuerdo a su registro.

La firma electrónica de la entidad certificadora es claramente necesaria para abalizar su existencia como tal.

Pueden existir ciertas limitaciones o restricciones impuestas para el uso de un certificado como el hecho de que sólo podrá emplearse en ciertos lugares, particularidad que resulta importante hacerla constar.

Como ya se dijo anteriormente, estos certificados se originan en unas entidades de certificación, a las que nuestra ley define como: Las empresas unipersonales o personas jurídicas que emiten certificados de firma electrónica y pueden prestar otros servicios relacionados con la firma electrónica, autorizadas por el CONATEL.

A este respecto vale mencionar que pueden existir dos maneras de prestar los servicios de certificación en nuestro país. Una de ellas son las entidades de certificación que poseen domicilio en el Ecuador, funcionan bajo un título habilitante y trabajan bajo un esquema de infraestructura propia, cuya razón social va dirigida a la emisión de firmas electrónicas y certificados, sellado de tiempo, registro de datos, certificación electrónica de documentos, almacenamiento de información, operación de infraestructura de clave pública. Otra forma es como entidades de registro con relación a una entidad de certificación; en este caso prestan servicios de registro de datos, como conservación, almacenamiento y custodia de la información, así como respaldo, recuperación y servicios relacionados. En los dos casos se detalla el Registro y Permiso.

Las entidades de certificación acreditadas bajo el esquema de nuestra ley deben cumplir con obligaciones como las siguientes que se establecen en el Art. 30:

a) Encontrarse legalmente constituidas, y estar registradas en el Consejo Nacional de Telecomunicaciones (CONATEL)
b) Demostrar solvencia técnica, logística y financiera para prestar servicios a los usuarios
c) Garantizar la prestación permanente, inmediata, confidencial, oportuna y segura del servicio de certificación de la información
d) Mantener sistemas de respaldo de la información relativa a los certificados
e) Proceder de forma inmediata a la suspensión o revocatoria de certificados electrónicos previo mandato de la Superintendencia de Telecomunicaciones, en los casos que se especifiquen en esta ley.
f) Mantener una publicación del estado de los certificados electrónicos emitidos
g) Proporcionar a los de certificados de firmas electrónicas un medio efectivo y rápido para dar aviso que una firma electrónica tiene riesgo de uso indebido
h) Contar con una garantía de responsabilidad para cubrir daños y perjuicios que se ocasionen por el incumplimiento de las obligaciones previstas en la presente Ley, y hasta por culpa leve en el desempeño de sus obligaciones. Cuando certifiquen límites sobre responsabilidades o valores económicos, esta garantía será al menos del 5% del monto total de las operaciones que garanticen sus certificados
i) Las demás establecidas en esta Ley y los reglamentos

Es oportuno en este momento manifestar que de acuerdo al Art. 38 de la Ley 67 el organismo de control de las entidades de certificación de información acreditadas es la Superintendencia de Telecomunicaciones cuyas siglas son SUPTEL, y como lo manifiesta el Art.37 del mismo cuerpo ñlegal, el CONATEL es la entidad encargada de la autorización, registro y regulación de las entidades de certificación acreditadas y dentro de sus funciones puede además:

a) Cancelar o suspender la autorización a las entidades de certificación acreditadas, previo informe motivado de la superintendencia de Telecomunicaciones
b) Revocar o suspender los certificados de firma electrónica, cuando la entidad de certificación acreditada los emite con inobservancia de las formalidades legales, previo informe motivado por la SUPTEL.

El CONATEL en uso de sus funciones aprobó la normativa relacionada a la acreditación de las entidades de certificación y servicios relacionados, además ha derogado ciertas resoluciones inconsistentes y ha emitido algunas referentes al tema que nos compete. Una de ellas, la Resolución 477-20-CONATEL-2008 en la que se aprueba el modelo de Acreditación como Entidad de Certificación de Información y Servicios Relacionados, de acuerdo a los términos presentados por la SUPTEL al CONATEL, en la que se establecen las siguientes obligaciones que tendrán las entidades de certificación acreditadas, además de aquellas que ya menciona la Ley 67:

1. Atender oportunamente las solicitudes y reclamaciones hechas por los usuarios.

2. Comprobar la veracidad, autenticidad, exactitud y validez de la información suministrada por los solicitantes del servicio, respecto de su identidad y otros datos relevantes, previo a la provisión efectiva de los servicios requeridos.

3. Garantizar la protección y conservación segura de los datos personales de los usuarios, obtenidos en función de sus actividades.

4. Verificar el contenido de todos los datos que consten en los certificados de firma electrónica y actuar con diligencia a fin de que toda la información constante en los mismos sea exacta, cabal y esté en función de lo los términos y condiciones acordados en el contrato de prestación de servicios.

5. Mantener la confidencialidad de toda información que no figure en los certificados electrónicos.

6. Mantener actualizada toda la infraestructura técnica empleada para la prestación de servicios de certificación de información y servicios relacionado con la firma electrónica, en función de la evolución de estándares tecnológicos internacionalmente reconocidos como fiables y que cumplan con las exigencias de seguridad necesarias a fin de garantizar la prestación de los servicios a sus usuarios.

7. Abstenerse de tomar conocimiento o acceder bajo ninguna circunstancia, a la clave privada de los usuarios titulares de Certificados de firma electrónica.

8. Publicar en su página WEB en forma permanente e ininterrumpida lo siguiente: listado de certificados emitidos, revocados y suspendidos, declaración de prácticas de certificación y políticas de seguridad, dirección de atención al público, dirección de correo electrónico, números telefónicos de contacto y el modelo de contrato de prestación de servicios de certificación de información y servicios relacionados con la firma electrónica a suscribir con los usuarios.

9. Proporcionar a los usuarios mecanismos automáticos de acceso y verificación de las listas de certificados revocados o suspendidos.

10. Poner a disposición de los solicitantes de una firma electrónica, toda la información relativa a su tramitación.

11. Remitir a la Secretaría Nacional de Telecomunicaciones, con una periodicidad mensual y conforme a los formularios que ésta establezca para el efecto, la siguiente información:

a. Número de solicitudes de servicio y trámite conferido a cada una de ellas

b. Número de certificados emitidos y revocados en el mes

c. Número de usuarios de servicios relacionados con la firma digital

d. Facturación total del mes

12. Suministrar la información que le requieran los entes de regulación y control, así como las entidades administrativas competentes o judiciales en relación con las Firmas Digitales y certificados emitidos y, en general, sobre cualquier Mensaje de Datos que se encuentre bajo su custodia y administración.

13. Informar a la Secretaría Nacional de Telecomunicaciones y a la Superintendencia de Telecomunicaciones de manera inmediata, la ocurrencia de cualquier evento que comprometa la disponibilidad y la seguridad en la prestación de los servicios de certificación de información y servicios relacionados con la firma electrónica.

14. Mantener actualizado en su totalidad, el registro de los certificados electrónicos revocados. Las entidades de certificación de información acreditadas, serán responsables de los perjuicios que se causen a terceros por incumplimiento de esta obligación.

15. Disponer de mecanismos de atención permanente e inmediata para consultas y solicitudes de revocación de certificados.

16. Informar al usuario dentro de las 24 horas siguientes, la suspensión del servicio o revocación de su certificado.

17. Proporcionar a los terceros que confían en los certificados emitidos por la Entidad de Certificación de Información y Servicios Relacionados Acreditada, medios razonablemente accesibles que permitan a éstos determinar mediante el certificado:

a. La identificación de la Entidad de Certificación de información y Servicios Relacionados Acreditada que presta los servicios;

b. Que el firmante nombrado en el certificado tenía bajo su control 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 o antes de ella".

En general y a manera de criterio, podríamos decir que la principal obligación de las entidades de certificación es la de garantizar la veracidad de la información contenida en el certificado.

Con respecto a las responsabilidades de las entidades de certificación acreditadas, la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, manifiesta en su Art. 31 que éstas serán responsables hasta por culpa leve y responderán por los daños y perjuicios que causen a cualquier persona natural o jurídica, en el ejercicio de su actividad, cuando incumplan las obligaciones que les impone esta Ley o actúen con negligencia, sin perjuicio de las sanciones previstas en la Ley Orgánica de Defensa del Consumidor. Serán también responsables por

el uso indebido del certificado de firma electrónica acreditado, cuando éstas no hayan consignado en dichos certificados, de forma clara, el límite de su uso y del importe de las transacciones válidas que pueda realizar.

Además, el artículo mencionado manifiesta que la carga de la prueba le corresponderá a la entidad de certificación de información, a la vez que expone, que los contratos con los usuarios deben incluir una cláusula de responsabilidad que reproduzca lo que señala la Ley respecto a la responsabilidad.

Finalmente el Art. 31 concluye expresando que cuando la garantía constituida por las entidades de certificación de información acreditadas no cubra las indemnizaciones por daños y perjuicios, aquellas deberán responder hasta con su patrimonio.

Por su parte y a este respecto, la resolución 477-20-CONATEL-2008 establece además de las responsabilidades contenidas en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, su Reglamento General de aplicación y regulaciones que emita el CONATEL con respecto a las entidades de certificación, las siguientes:

1. Contar con una declaración de Prácticas de Certificación, donde se especifiquen las condiciones, políticas y procedimientos aplicables a la solicitud, emisión, uso, suspensión y revocación de los certificados de firma electrónica así como para la prestación de servicios relacionados. Esta declaración deberá contener como mínimo:

a. Datos de identificación de la Entidad de Certificación de Información y Servicios Relacionados Acreditada.
b. Condiciones de manejo de la información suministrada por los usuarios.
c. Límites de responsabilidad en la prestación de servicios de certificación de información y servicios relacionados con la firma electrónica.
d. Obligaciones de la Entidad de Certificación de Información y Servicios Relacionados Acreditada en la prestación de *servicios* de certificación de información y servicios relacionados con la firma electrónica
e. Obligaciones de los usuarios y precauciones que deben observar en el manejo, uso y custodia de certificados y claves.
f. Políticas de manejo de los certificados de firma electrónica.
g. Políticas y condiciones de manejo de servicios relacionados con la firma electrónica.
h. Garantías en el cumplimiento de las obligaciones que se deriven de sus actividades
i. Costos y tarifas de los servicios de certificación de información y servicios relacionados con la firma electrónica.

2. Contar con una declaración de Políticas de Seguridad, donde se especifiquen las condiciones y procedimientos relativos a la seguridad de la infraestructura de la Entidad de Certificación de Información y seguridad en la prestación de servicios de certificación de información y servicios relacionados con la firma electrónica. Esta declaración deberá contener como mínimo:

a. Procedimientos de seguridad para el manejo de posibles eventos, cuando:
   i. La seguridad de la clave privada de la Entidad de Certificación de Información y Servicios Relacionados Acreditada se vea comprometida.

ii. El sistema de seguridad de la Entidad de Certificación de Información y Servicios Relacionados Acreditada ha sido vulnerado.

iii. Se presenten fallas en el sistema de la Entidad de Certificación de Información y Servicios Relacionados Acreditada que comprometan la seguridad, disponibilidad y prestación de los servicios.

b. Plan de contingencia para garantizar la continuidad y disponibilidad y de los servicios de certificación de información y servicios relacionados con la firma electrónica.

c. Procedimientos y mecanismos de seguridad para resguardo y conservación segura de la información relativa a la emisión de Certificados e información proporcionada por los usuarios.

3. Gestionar y suscribir convenios o acuerdos de reconocimiento mutuo con Entidades de Certificación regionales, nacionales e internacionales, a fin de otorgar el respectivo reconocimiento y validez a las firmas electrónicas creadas sobre la base de los certificados emitidos por la Entidad de Certificación de Información y Servicios Relacionados acreditada.

4. Contar con el personal idóneo que posea los conocimientos técnicos y la experiencia adecuada para manejar y gestionar sobre la base de los procedimientos de seguridad pertinentes, la provisión de servicios de certificación de información y servicios relacionados con la firma electrónica.

5. Implementar y operar mecanismos de ejecución inmediata para revocar los certificados emitidos a los usuarios, a petición de éstos o por las causas previstas en la normativa aplicable.

6. Contar con una infraestructura segura para la creación y verificación de firma electrónica así como de los servicios relacionados con la misma, que permita asegurar y garantizar la protección contra toda alteración.

7. Garantizar al usuario la prestación permanente, inmediata, oportuna, ágil y segura de los servicios de certificación de información y servicios relacionados con la firma electrónica, en los términos y condiciones acordados en el contrato de prestación de servicios.

8. Emitir certificados únicos e induplicables, que contengan un identificador exclusivo que lo distinga de forma unívoca ante el resto. Los certificados se emitirán a personas mayores de edad, con plena capacidad jurídica.

9. Informar a los solicitantes y usuarios de los certificados electrónicos, sobre el nivel de confiabilidad de los mismos, los límites de uso y sobre las responsabilidades y obligaciones que el solicitante asume como usuario del servicio de certificación.

10. Capacitar, advertir e informar a los solicitantes y usuarios de servicios de certificación de información y servicios relacionados con la firma electrónica,

respecto de las medidas de seguridad, condiciones, alcances, limitaciones y responsabilidades que deben observar en el uso de los servicios contratados.

Por otra parte, la normativa en aras de proteger los datos personales, establece que las entidades de certificación garantizarán la protección de éstos datos que sean obtenidos en función de sus actividades, de conformidad con lo que establece el Art. 9 de la misma ley 67, cuyo texto es el siguiente:

Art.9.- Protección de Datos: “Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros.

La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta Ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente…”

Cabe mencionar que los servicios de certificación de información pueden ser proporcionados y administrados en todo en parte por terceros, siempre que éstos demuestren su vinculación con la Entidad de Certificación de la Información y bajo los términos que establezca el CONATEL.

Nuestra ley en el Art. 28 ampara el reconocimiento de certificados y firmas electrónicas extranjeras que cumplan con los requisitos señalados en la Ley 67 y su Reglamento con respecto a los certificados nacionales, siendo el CONATEL el encargado de reglamentar lo pertinente a su aplicación.

Al momento no existe reglamentación al respecto por parte del CONATEL, sin embargo, el Decreto 1356 emitido el 29 de septiembre del año 2008, manifiesta que los certificados de firma electrónica emitidos en el extranjero tendrán validez legal en el Ecuador una vez obtenida la revalidación por parte de una Entidad de Certificación de Información y Servicios Relacionados acreditada ante el CONATEL, la misma que deberá comprobar el grado de fiabilidad de tales certificados y de quien lo emite.

El Art. 28 continúa manifestando que cuando las partes acuerden entre sí la utilización de determinados tipos de firmas electrónicas y certificados, se reconocerá que ese acuerdo es suficiente en derecho. Salvo aquellos casos en los que el Estado, en virtud de convenios o tratados internacionales haya pactado la utilización de medios convencionales, los tratados o convenios que sobre esta materia se suscriban, buscarán la armonización de normas respecto de la regulación de mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico, la protección a los usuarios de estos sistemas, y el reconocimiento de los certificados de firma electrónica entre los países suscriptores.

Esto nos demuestra la intención de la ley de no limitar el ejercicio del uso de una firma electrónica, pero dotarle siempre de la seguridad debida.

Los certificados de firma electrónica tienen su vigencia de acuerdo a lo que se establezca entre el titular de la firma electrónica y la entidad de certificación. De no haberlo establecido, el Reglamento a la Ley 67 manifiesta que tendrá una validez de dos años a partir de su expedición.

Al tratarse de certificados de firma electrónica emitidos con relación de cargos públicos o privados, la duración del certificado podrá ser superior a los dos años pero no podrá exceder el tiempo de duración del cargo, a menos que exista una de las prórrogas de funciones establecidas en las leyes.

Los certificados de firma electrónica son susceptibles de extinción, suspensión y revocación. La extinción puede darse por:

1.- Solicitud del titular

2.- Extinción de la firma electrónica en los términos en los que establece la ley, esto es:

a) Voluntad del titular

b) Fallecimiento o incapacidad de su titular

c) Disolución o liquidación de la persona jurídica, titular de la firma

d) Por causa judicialmente declarada

3.- Expiración del plazo de validez del certificado de firma electrónica

La ley ecuatoriana manifiesta que la extinción de firma electrónica se producirá desde el momento de su comunicación a la entidad de certificación de información, excepto en el caso de que ocurra el fallecimiento del titular de la firma, caso en el que se extingue a partir de su deceso. También se expone que en el caso de personas secuestradas o desaparecidas, el certificado se extingue a partir de que se denuncie el hecho ante las autoridades competentes. En todos los casos, la extinción del certificado no exime al titular de la firma electrónica y consecuente certificado, de las obligaciones contraídas previamente derivadas de su uso.

Por su parte, la entidad de certificación podrá suspender temporalmente el certificado de firma electrónica cuando se den las siguientes circunstancias:

1.- Se disponga por el CONATEL

2.- Se compruebe por parte de la entidad de certificación falsedad en los datos consignados por parte del titular del certificado.

3.- Se produzca el incumplimiento del contrato celebrado.

La suspensión temporal que disponga la entidad de certificación de información debe ser notificada inmediatamente al titular del certificado y al organismo de

control que en este caso es la SUPTEL, señalando la causa de la suspensión. De esta manera se previene al titular del certificado de hacerlo uso mientras dura la suspensión.

La suspensión deberá ser levantada una vez desvanecida la causa o causas que la produjeron, o cuando mediare resolución del CONATEL al respecto.

Los certificados de firma electrónica pueden revocarse por parte del CONATEL, de conformidad a lo previsto en la ley cuando la entidad de certificación de información cese en sus actividades y los certificados que se hallen vigentes no sean asumidos por otra entidad similar o cuando se produzca la quiebra técnica judicialmente declarada de la entidad de certificación. Tanto la revocatoria como sus causas tienen que ser notificadas de inmediato al titular del certificado.

La ley nos establece en el Art. 27 los efectos de la suspensión y la revocatoria, expresando que: " Tanto la suspensión temporal , como la revocatoria, surtirán efectos desde el momento de su comunicación con relación a su titular; y respecto de terceros, desde el momento de su publicación que deberá efectuarse en la forma que se establezca en el respectivo reglamento…" A su vez el reglamento expone que la revocación tendrá también como consecuencia la respectiva publicación y la desactivación del enlace que informa sobre el certificado.

De igual manera la ley impone que el titular del certificado de firma electrónica está obligado frente a todo lo contraído previamente. La entidad de certificación

será responsable por los perjuicios que ocasionare la falta de comunicación, de publicación o su retraso.

Por su parte el Reglamento a la Ley manda a que las entidades de certificación de información proporcionen mecanismos automáticos de acceso a listas de certificados revocados o suspendidos. Los períodos de actualización de las listas están sujetos a la decisión contractual. Si la verificación de la validez de los certificados de firma electrónica no es posible en tiempo real, la entidad de certificación de información deberá comunicar este hecho tanto al emisor como al receptor del mensaje de datos.

En el Reglamento también se estipula que en caso de que las actividades de certificación vayan a cesar, la entidad de certificación deberá notificar con por lo menos noventa días de anticipación a los usuarios de los certificados de firma electrónica y a los organismos de regulación y control sobre la terminación de sus actividades.

En caso de cesión de certificados de firma electrónica de una entidad de certificación a otra, se deberá contar con la expresa autorización del titular del certificado, siendo que la entidad que asuma dichos certificados deberá cumplir con los mismos requisitos tecnológicos exigidos por la Ley 67 y su Reglamento a las entidades de certificación.

La notificación inmediata a la que se refiere la ley en los casos de extinción, suspensión o revocación del certificado de firma electrónica de la deberá hacer a

la dirección electrónica y a la dirección física que hubiere señalado en el contrato de servicio.

Por su parte la publicación debe hacer por los siguientes medios establecidos en el Reglamento a la Ley:

1.- A la página electrónica determinada por el CONATEL en la que se reporta la situación y la validez de los certificados, así como en la página WEB de la entidad certificadora.

2.- Mediante un aviso al acceder al certificado de firma electrónica desde el hipervínculo de verificación, sea que éste forme parte de la firma electrónica, que conste en un Directorio electrónico o por cualquier procedimiento por el cual se consulta los datos de certificado de firma electrónica.

3.- Opcionalmente de creer conveniente la entidad certificadora o de registro, se podrá publicar en uno de los medios de comunicación pública.

Como podemos ver tenemos sentadas las bases jurídicas propicias para el funcionamiento de las entidades certificadoras de firma electrónica, que provean a las relaciones electrónicas de una seguridad apta para su desarrollo. Lo más importante ahora es no detenerse en el camino y procurar en el día a día el fortalecimiento de estas actividades.

5.- Breve referencia a las Entidades de Certificación en el Ecuador.

De las certificadoras que han sido acreditadas por el CONATEL para prestar sus servicios de Certificación de la Información y otros relacionados, solo una, El Banco Central del Ecuador ha logrado cumplir con los requisitos y las garantías respectivas para operar, lo que les impide a las demás funcionar legalmente.

Lo mencionado se debe a que en un inicio por disposición del CONATEL en la resolución324-17-CONATEL-2006 , se establecían rubros extremadamente altos a las entidades aspirantes a funcionar como entidades de certificación. Es así que, para conseguir el título habilitante tenían que cumplir con la cancelación de los valores que implicaban un monto total de USD $56.000,00, al brindar todos los servicios relacionados a una entidad certificadora, y además extender una garantía de responsabilidad que ascendía al menos a USD $1.000.000,00, misma que sería reajustable anualmente de acuerdo a los informes por concepto de supervisión que emita la SUPTEL.

Los USD $56.000,00 se desprenden de lo siguiente:

1.- USD $10.000,00 valor de registro y autorización

2.- USD $ 10.000,00 por concepto de acreditación

3.- USD $6.000,00 por cada servicio a ser prestado, como son:

a) emisión de firmas electrónicas y certificados de firma electrónica

b) sellado electrónico de tiempo

c) certificación electrónica de documentos a cargo de un Notario Público o autoridad competente empleando firma electrónica.

d) conservación de mensajes de datos

e) otros

4.- USD $3.000,00 por costos y gastos de administración del CONATEL y SENATEL

5.- USD $3.000,00 costos y gastos de control de la SUPTEL

Posteriormente, cuando surgió la idea de constituirle al Banco Central como Entidad de Certificación se efectuó un nuevo análisis sobre económico para la acreditación. Es así que mediante la resolución No. 480-20-CONATEL-2008 el CONATEL dispone que:

Los valores que se deberán cancelar en la Secretaría Nacional de Telecomunicaciones, por la Acreditación de una Entidad de Certificación de Información y Servicios Relacionados, previo a que se realice el registro respectivo, es de USD $ 22.000,00, que corresponden a:

1.- USD $10.000,00 emisión de acreditación y registro
2.- USD $6.000,00 por concepto de prestación de servicios de certificación de información y servicios relacionados, sonde se incluye la emisión de firmas electrónicas, sellado electrónico de tiempo, conservación segura de mensajes de datos y otros.

3.- USD $3.000,00 por costos y gastos de administración del CONATEL y SENATEL

4.- USD $3.000,00 Costos y gastos de control de la SUPERTEL

Además en el Decreto No. 1356 del 29 de septiembre del 2009 se establece con respecto a la garantía de Responsabilidad que ésta será incondicional, evocable y de cobro inmediato y podrá consistir en pólizas de seguro de responsabilidad previstas en el artículo 43 de la Codificación de la Ley General de Seguros u otro tipo de garantías que están autorizadas conforme lo dispuesto en el artículo 51, letra c) de la Ley General de Instituciones del Sistema Financiero. Estableciendo de manera genera lo siguiente:

a) Para el primer año de operaciones, la Entidad de Certificación de Información y Servicios Relacionados Acreditada, deberá contratar y mantener, a favor de la Secretaría Nacional de Telecomunicaciones, una garantía de responsabilidad para asegurar a los usuarios el pago de los daños y perjuicios ocasionados por el posible incumplimiento de las obligaciones, cuyo monto será igual o mayor a cuatrocientos mil dólares de los Estados Unidos de América (USD $ 400.000, oo). En el contrato de prestación de servicios que suscriba la Entidad de Certificación de información con los usuarios, se deberá incluir una cláusula relacionada con los aspectos de esta garantía, tales como: monto asignado a cada usuario, mecanismos de reclamación y restitución de valores.

b) Para el segundo año de operaciones y hasta la finalización del plazo de la acreditación, la Entidad de Certificación de Información y Servicios Relacionados Acreditada deberá contratar a favor de la Secretaría Nacional de Telecomunicaciones, una garantía, cuyo monto estará en función de un valor base de garantía por certificado y que será determinado por el CONATEL.”

Todo aquello nos demuestra que se ha considerado enormemente una reducción en los distintos costos y garantías, lo que tal vez les permitirá a las entidades de certificación acreditadas concretar la obtención del título habilitante para funcionar legalmente en el Ecuador.

Una de estas entidades es **Ecuacert** que trabaja con alianzas internacionales con compañías como E-Sign S.A. que es una prestadora de servicios de certificación chilena que opera para Chile, Perú, Ecuador y Colombia y se encuentra avalada por firmas como Verisign, bastante reconocida internacionalmente y que se ha constituido en una empresa líder dentro de los servicios de seguridad transaccional en Internet, procurando la absoluta confianza a las personas al utilizar internet.

Los siguientes son los productos que Ecuacert podría ofrecer por intermedio de sus alianzas:

1.- Certificados de firma electrónica personales

2.- Certificados para proteger sitios Web

3.- Consultorías de seguridad para detección de vulnerabilidades.

4.- Servicios para proteger el robo/suplantación de Identidad.

5.- Aplicaciones para la emisión y distribución de documentación electrónica.

Otra certificadora acreditada pero que tampoco cuenta con el título habilitante para operar en el Ecuador es Esdinámico o idSegura cuya propuesta de productos son principalmente aquellos destinados a brindar seguridad para los datos que viajan en la red, además de certificar información digital. La tecnología con la que cuentan hace posible cifrar los datos que viajan por la red.

Esta entidad provee certificados de correo seguro por la Corporación Aduanera Ecuatoriana CAE, así como Certificados Digitales para Sitios Web E-commerce e E-business.

Para que esta entidad nos otorgue una firma electrónica se requiere llenar un formulario, comprar la firma electrónica y validar la información.

Finalmente mencionemos al **Banco Central del Ecuador**, que es la primera entidad que recibe la acreditación como Certificadora de Información por parte del Estado Ecuatoriano. De acuerdo a la reforma al Reglamento General a la Ley de Comercio Electrónico, Firma Electrónica y Mensaje de Datos, todas las instituciones del sector público deben obtener del Banco Central los certificados de firma electrónica.

Este constituye un paso muy importante dentro del intento armonizador de las nuevas tecnologías en el esquema jurídico, y es así que, bajo este esquema, al estar plenamente acreditada y con el respaldo necesario, y brindarnos el servicio de emisión de certificados de firma electrónica, nos permite efectivizar el uso de la firma electrónica en iguales criterios de validez que la manuscrita.

El procedimiento para acceder a una firma electrónica emitida por la Entidad Certificadora de Información Banco Central es el siguiente:

1.- Llenar un formulario de solicitud de emisión de certificado
2.- Entregarlo de forma personal en cualquiera del as oficinas de la Entidad, y
3.- Firmar el respectivo contrato para la prestación del servicio.

El certificado de firma electrónica emitido por el Banco Central tiene una vigencia de dos años. Se cancela un monto total de USD $69,00 que corresponden a la

emisión del certificado de firma electrónica (USD $43,00) y al costo del dispositivo portable seguro TOKEN USB (USD $26,00). Se puede renovar el certificado por dos años más cancelando el monto de USD $22,00.

6.- Ventajas de la Firma Electrónica certificada.

Luego de analizar todo lo relativo a la firma electrónica y a la importancia de una entidad de certificación, podemos establecer claramente algunas de las ventajas que claramente nos presenta una firma electrónica certificada por una entidad de certificación:

1.- Realizar actividades con plena seguridad en la Red, lo que produce confianza en las transacciones.

2.- Garantizar la autenticidad, confidencialidad, integridad y no repudio.

3.- Lograr plena aplicabilidad de la firma electrónica, dotándole de características que le otorgan plena validez jurídica.

4.- Aminorar costos y evitar un innecesario desgaste humano y natural

5.- Con el fomento de su aplicación y el debido sustento legal se puede lograr una plena actividad jurídica electrónica, donde se integren tanto actividades judiciales como notariales y registrales de forma electrónica.

CAPITULO V

SEGURIDADES

1.- Consideraciones Generales.

La importancia que va obteniendo la contratación electrónica dentro de un mundo globalizado, exige que se generen seguridades para las transacciones, las mismas que deben combinar un desempeño tanto técnico como jurídico, basado en políticas de Estado.

A este respecto, se hace indispensable la intervención del Derecho, como rector y regulador de los actos que afectan a las relaciones del ser humano. El Derecho, mediante el Derecho Informático se preocupa en analizar la problemática que se origina por el uso de la computadora.

El Derecho Informático, busca a la vez, las soluciones a aquellos retos planteados por la creciente actividad en la Red. Esta nueva rama del Derecho se encuentra en constante estudio y seguimiento de aquellos adelantos y transformaciones tecnológicas, con el objetivo de ir diseñando las medidas adecuadas que permitan una armoniosa convivencia social.

Dentro de los mecanismos técnicos de seguridad existentes tenemos desde sistemas técnicos de auditoría informática, sistemas de seguridad física, de

seguridad lógica, sistemas de seguridad de redes, sistemas criptográficos, sistemas de firmas electrónicas y digitales, estos dos últimos que ya hemos hecho mención anteriormente.

Las medidas técnicas de seguridad, como ya lo dijimos, deben ir de la mano con un respaldo legal que permita su evolución y un camino abierto para aquellos sistemas de seguridad que vayan surgiendo en función al desarrollo de la técnica.

La contratación electrónica tiene su sustento doctrinario a través del Derecho Informático y un importante apoyo en la Informática Jurídica, ya que esta última tiene la función de instrumentar los medios electrónicos al servicio del Derecho.

Gran parte de la contratación electrónica depende de las medidas de seguridad que se adopten en las redes de transmisión de bienes y servicios informáticos, puesto que éstas son susceptibles de intercepción por medio de módems técnicamente preparados para el efecto o por medio de sistemas de grabación de señales que permitan recomponer éstas con el objetivo de conseguir claves de acceso al sistema.

Las transmisiones en un inicio se las hacían por medio de cables de cobre, hoy en día se las realiza a través de fibras ópticas construidas en bases a fibras de vidrio por donde circulan emisiones de rayo láser que hacen posible la transmisión de contenidos inmateriales a través de bits, siendo ésta una transmisión digital. Otra forma de transmitir es con la intervención de un satélite debidamente equipado

con repetidoras que se encuentren en contacto con una estación en tierra, y que trabajan en base a microondas para el efecto.

Pero estos medios pueden generar intromisiones u hechos no contratados que alteren las transacciones en línea, por lo que una vez más, se hace necesaria la implementación y aplicación de medidas técnicas de seguridad actualizadas.

Una medida técnica de seguridad que es elemental, es el resguardo y protección de los datos e información que sea derivada de las transacciones electrónicas, que deben mantener aquellos principios de integridad, confidencialidad y disponibilidad.

A manera de prevención es importante mantener los datos e información en distintos lugares y con copias de seguridad. De igual forma, aunque podría estar demás decirlo, las instalaciones deben contar con mínimas medidas de seguridad para que evitar un fácil acceso a la información.

Es claro que quien pretende acceder de forma ilícita a un sistema, emplea todo el tiempo necesario en hacerlo, por eso es importante implementar medidas de seguridad que posean adecuados controles de calidad, que brinden una verdadera seguridad al usuario de la Red, aquellas que son poco conocidas en el mercado no proporcionan una seguridad confiable.

Otra medida básica de protección de la información que surgió hace una década más o menos es la de implementar seguridades en una computadora principal que se encarga del procesamiento centralizado de la información remitida desde distintas computadoras. A esta computadora central se la denominó el anfitrión. A la vez, existe un método conocido como seguridad para redes, que permite a los encargados de la seguridad monitorear y controlar los distintos accesos a la red que se realizan a través de los llamados anfitriones. Es conocido como firewall y proporciona un alto grado de confianza a nivel de redes internas y permiten reducir el riesgo en incursiones no deseadas desde el exterior. En sentido estricto son unos routers a través de los cuales fluye el tráfico de datos.[14]

2.- La Criptografía

El sistema de seguridad que merece mayor atención y estudio es aquel que data de hace miles de años y que ha ido perfeccionándose con el desarrollo de la sociedades, siendo hasta la actualidad el más utilizado e importante, estamos hablando de la criptografía, que es la técnica de encriptar, aplicable a redes abiertas y cerradas; constituye el sistema óptimo para garantizar el comercio electrónico y la transmisión de documentos electrónicos de forma segura, ayudando a cumplir todos aquellos requisitos exigidos en el tráfico tradicional.

El ser humano se ha caracterizado a través de la historia por mantener ciertas actividades en forma confidencial, lo que le ha llevado a ingeniar mecanismos que le permitan dicho objetivo. Al inicio se utilizaban signos y símbolos que eran

[14] ESPINOZA CESPEDES José Francisco. *Contratación Electrónica, Medidas de Seguridad y Derecho Informático*. Edit. RAO S.R.L. Lima-Perú. 2000. pag. 79-98

manejados por determinados círculos de personas, luego con la aparición de la escritura se va perfeccionando, hasta convertirse en una herramienta fundamental para las actividades modernas de la informática.

Se dice que las primeras civilizaciones que utilizaron la criptografía fueron la Egipcia, Mesopotámica, la India y la China. Los espartanos utilizaban un cilindro donde le enrollaban un papiro en espiral y escribían sobre éste desde arriba hacia abajo, de modo que al desenrollar el papiro únicamente se evidenciaba una serie de letras dispersas. Para leer exactamente el mensaje, era necesario colocar el papiro en idéntica posición de cómo cuando fue creado el mensaje.

Se dice que textos judíos se encriptaron utilizando un método de sustituir la primera letra del alfabeto por la última, la segunda por la penúltima y sucesivamente. Pero es a Julio César a quien se le atribuye documentalmente como el primero en implementar un método criptográfico, a través de un sistema de sustitución de letras en el cual se utilizaba la tercera letra que siguiera a la que realmente correspondía, creando así un documento codificado.

Como definición podemos decir, que la criptografía es el proceso de transformación del texto original en texto cifrado o criptograma; el contenido de información del texto cifrado es igual al del texto original pero sólo es inteligible para las personas autorizadas.

También se habla de una tecnología que consiste en el uso de una fórmula o algoritmo que permite firmar de forma no tradicional, relacionando una clave privada, con la que se genera la firma, con una clave pública atribuida a una persona.

En la Edad Media se incrementa el uso de la encriptación, pero sobresale en la historia el religioso Johannes Trithemius, quien escribió el primer libro sobre criptografía, introduciendo un concepto de tabla ajustada en el que se permuta el alfabeto para codificar mensajes. Basándose también en métodos de sustitución del alfabeto, los legendarios piratas codificaban la localización de los tesoros, esto entre los siglos XVII y XVIII.

Es un sistema ancestralmente utilizado por los ejércitos, para comunicarse o mandar mensajes a sus aliados sin que éstos puedan ser interceptados y conocidos por los enemigos. Esta estrategia se halla presente en los tiempos modernos.

La criptografía era considerada como un arte de cifrar, sin embargo, con los avances tecnológicos y estudios científicos hoy en día la criptografía constituye toda una ciencia del cifrado, de mantener en secreto los mensajes utilizando sistemas electrónicos que le permiten cumplir eficientemente su labor. Esta ciencia, estudia los procesos de cifrado y desifrado de los mensajes, así como el análisis para descubrir la clave y texto original, aspecto este último que recibe el nombre de criptoanálisis.

En aras de cumplir con su misión, la criptografía utiliza técnicas de cifrado y codificación, de tal manera que los datos sean transportados de forma segura por las redes, pudiendo detectar si éstos han sido alterados. Nos permite además determinar si el remitente es realmente quien ha realizado la operación; proteger la intimidad de las partes, evitando que aquella información confidencial pueda

interceptarse por terceros, puesto que esta tecnología con el uso adecuado de las claves de seguridad, mediante algoritmos, provoca que los datos sean ilegibles para terceros.

Este tipo de criptografía que está basado en claves seguras permite realizar un proceso eficiente de protección de la información, además de prestar las condiciones para emitir una clave adecuada que provoque o permita el proceso inverso de descifrar los datos encriptados.

Hemos enunciado ya algunos métodos tradicionales que se han usado a lo largo de la historia para encriptar mensajes, técnicas éstas que han sido superadas con la criptografía moderna, que se caracteriza por dos técnicas claramente definidas en el proceso de cifrado; una de ellas corresponde al sistema de cifrado simétrico conocido también como de clave secreta, y la otra que se refiere al sistema de cifrado asimétrico o de clave pública.

Cabe mencionar la etimología de la palabra criptografía y esta viene del griego Kriptos que significa Oculto y Graphos que significa Escribir, es decir, la escritura oculta o en clave.

A su vez la ciencia conocida como Criptología abarca lo siguiente:

1.- Criptografía: que se refiere a datos, textos e imágenes.

2.- Criptofocía: que hace referencia a la voz

3.- Criptoanálisis: que es la rama de la ciencia que estudia a partir de los textos cifrados, los métodos para descubrir la clave.

La firma electrónica que es uno de los aspectos de mayor interés en el objeto de nuestro estudio, tienen su fundamento en la criptografía como disciplina matemática que además de cifrar los textos protegiéndoles de terceros y proporcionándoles confidencialidad, ofrece mecanismos para asegurar la integridad de los datos y la identidad de las personas que participan en las transacciones. En este sentido la criptografía de cifrado se encarga de transformar un texto en lenguaje natural entendible a un texto cifrado mediante un algoritmo y gracias a una clave de cifrados, de esta manera resulta incoherente o inentendible, si cabe el término, para todas las personas excepto aquel legítimo destinatario.

Por su parte el algoritmo es un sistema complejo de operaciones matemáticas que se basan en sustituciones y permutaciones de bits en función de una clave. Cabe recalcar que el conocer el algoritmo no permite descifrar la información cifrada.

1.1. Cifrado simétrico o de clave secreta:

La calidad de simétrico corresponde a que la llave o clave para encriptar y desencriptar es la misma. En este tipo de criptografía es necesario dar a conocer la clave secreta a todas las partes que se encuentren involucradas en determinada transacción electrónica; entonces, la parte emisora debe cifrar la información con

la clave secreta, la misma que debe ser conocida por la otra u otras partes, en este caso las receptoras, para que la utilicen en decifrar el mensaje.

La debilidad expuesta con respecto a esta llave ha provocado que no se la use mayormente, a no ser que se la combine con otro tipo de técnicas.

1.2. Cifrado asimétrico o de clave pública:

Este cifrado ha sido catalogado como el mejor sistema para ser utilizado en la contratación electrónica, ya que se lo hace en base a algoritmos asimétricos, permitiendo así que cada parte obtenga un par de claves, de las cuales la una es pública y la otra privada. Esta última se mantiene en poder y conocimiento exclusivo de su dueño y no tiene porque ser conocida por nadie más, a diferencia de la clave pública que se la deja abiertamente en la red.

Entonces en este caso, las claves para cifrar y descifrar son diferentes. Cada persona tiene un par de claves, una pública y otra privada, la primera conocida por todos, y la segunda que se mantiene bajo la confidencialidad de su propietario. Así el emisor par enviar el mensaje al receptor lo encripta usando su clave privada y la clave pública del receptor; a su vez el receptor, usa su clave privada para desencriptar el mensaje y la clave pública del emisor para verificar la identidad.

Es decir, el cifrado asimétrico existe cuando concurre una pareja de claves para separar los procesos de cifrado y descifrado. Hablando en términos generales la clave pública sirve para cifrar y la privada para descifrar, sabiendo que, a partir del conocimiento de la llave pública, no es posible determinar la clave privada ni decifrar el texto que fue cifrado.

Estos sistemas de clave pública son más lentos en relación a los simétricos, pero presentan mayor seguridad para los servicios de autenticación y distribución de claves de sesión y firmas digitales.

En términos generales sería suficiente cifrar los datos con la clave privada que sólo conoce su dueño y obtener una firma digital segura, para que luego cualquiera pueda decifrarlos con la clave pública y así confirmar la identidad del remitente o firmante.

Para asegurar la integridad del mensaje, evitar altos costos y ahorrar tiempo, se suele codificar solo un resumen del mensaje y no la totalidad de éste. Los algoritmos de clave pública requieren un tiempo considerable para cifrar documentos voluminosos, por lo que, los protocolos de firma digital se implementan conjuntamente con funciones unidireccionales de resumen, como lo es el algoritmo Hash, de tal manera, se firma únicamente un resumen del documento que se envía. Este documento aplicado la función hash y luego codificado de manera inversa al documento constituye la firma digital. El algoritmo hash es una función que sirve para generar claves o llaves que representen de manera casi unívoca a un documento.

Repasemos este sistema tal como funciona en la práctica:

1.- El emisario de un mensaje sigue los siguientes pasos:

a) Mediante la función hash obtiene un resumen del mensaje.

b) Codifica este resumen mediante su propia clave privada.

c) Codifica con la clave pública del destinatario conjuntamente el mensaje y el resumen.

d) Lo remite electrónicamente al destinatario.

2.- El destinatario o receptor del mensaje, cuando lo recibe, hace lo siguiente:

a) Lo descodifica con su propia clave privada, con lo que obtiene ya desifrado el texto del mensaje, pero el resumen aun se encuentra codificado con la clave privada del emisor.

b) Obtiene mediante la misma función hash otro resumen del mensaje recibido, es decir, un nuevo resumen.

c) Desencripta el resumen con la clave pública del emisor, asegurándose así de la identidad del emisor o firmante.

d) Comprueba la identidad de ambos resúmenes, el que le fue enviado por el emisor y el que él mismo obtuvo, con lo que queda garantizada la integridad del mensaje.[15]

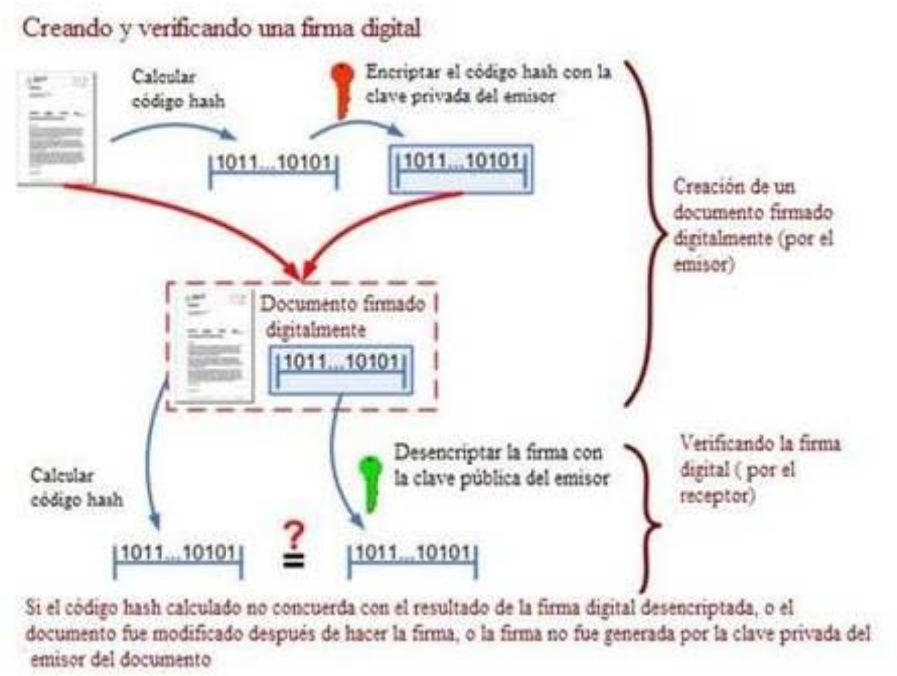
[15] RODRIGUEZ ADRADOS Antonio. Ob.Cit. pag. 12

Debemos tener claro que todos estos pasos no se los cumple uno a uno, sino que el programa del computador se encarga de hacerlo ágil y automáticamente.

Resumiendo podríamos decir que las primeras criptografías eran en base a combinaciones de rotación de caracteres, cuya seguridad dependía en alto grado de la confidencialidad con la que se maneje el algoritmo utilizado. Estos sistemas ya no se utilizan mayormente en la actualidad.

Los criptosistemas utilizados en la actualidad responden a funciones matemáticas en base a parámetros o claves con los cuales los datos de entrada no se los puede obtener a partir de los de salida, y si se llegara a pasar, sería en tan largo plazo que la información ya no tendría valor alguno. La seguridad de estos sistemas ya no dependen de poder mantener en secreto el algoritmo, sino los parámetros claves del mismo.

Entonces, firmar digitalmente un documento radica en pasar un determinado algoritmo sobre el texto que se desea cifrar, esto en base a la clave privada del firmante o remitente. Cuando el texto debe transmitirse firmado, el algoritmo recorre todos sus datos electrónicos y, junto a la clave privada, obtiene un valor (“Hash”), que es la llamada firma digital.



Fuente: http://www.informatica.gov.ec/index.php/sistemas/transversales/firma-digital

CONCLUSIONES Y RECOMENDACIONES

Como hemos podido analizar, nuestro país cuenta con un ordenamiento jurídico que reconoce plenamente la validez de los documentos electrónicos, de la firma electrónica y entidades certificadoras de información, entre otros temas.

En base a la legislación ecuatoriana podemos ver que los documentos electrónicos son plenamente válidos y se los puede emplear como prueba dentro de un juicio.

La firma electrónica avanzada por su parte nos ayuda a proporcionarle a esos documentos las cualidades probatorias necesarias, equiparándose a la firma manuscrita.

A la vez las entidades certificadoras de información le dan características muy importantes a las transacciones en la red, apoyándole a la firma electrónica en su utilización y proporcionando además otros servicios relacionados con ésta.

Las Certificadoras de Firma Electrónica constituyen el eslabón final en todo este proceso de implementación de las nuevas tecnologías en el desarrollo social, el paso con el que se puede concretar de forma segura este gran reto. La legalización y legitimación de los procesos son unas de las principales finalidades de las entidades certificadoras, razones aquellas, por las que se crearon estas figuras.

Sin embargo hemos podido evidenciar que su gran limitante en nuestro medio, para poder desarrollarse como tales, ha estado radicado en los altos costos que implicaba el poder brindar estos servicios. Es por esto que, resulta trascendental aquella normativa que produjo ese cambio tendiente a fortalecer el contexto de las entidades de certificación, bajo el cual se originó la primera certificadora de firmas electrónicas aprobada, en cumplimiento con todos los requisitos impuestos por la Ley, el Reglamento y las Resoluciones del CONATEL. Esta normativa ha generado el patrón inicial para un fortalecimiento de las entidades certificadoras y para que la firma digital se convierta en una realidad palpable en nuestro medio.

Aun existen ciertos paradigmas por romper, como son, el presente rechazo a las nuevas tecnologías, el desconocimiento y desconfianza a las nuevas formas de desarrollo social, y obviamente la falta de infraestructura y acceso con la que cuenta nuestro país. A pesar de aquello, es también verificable el creciente uso que experimenta el internet y la práctica del comercio electrónico.

Por todo ello es muy importante no sólo legislar, pues ante algo tan nuevo no se puede esperar que únicamente se aplique por el sólo hecho de existir. Es importante un acercamiento a la realidad local, para así poder instrumentar la aplicación de la ley e irla adaptando a esa realidad.

Las políticas de Estado siempre son importantes, debiendo producirse en este caso con miras a un entorno facilitador, donde se armonice las nuevas tecnologías con los ciudadanos, para propiciar el uso de las primeras por parte de los

segundos. Empleando mecanismos que concienticen sobre la preservación de los recursos naturales y la consecuente reducción del uso del papel, medidas que abaraten el acceso a servicios como el internet; acompañados de un impulso a las transacciones en línea.

BIBLIOGRAFIA.

RODRIGUEZ ADRADOS, Antonio. Firma Electrónica y documento electrónico. Madrid, España: Consejo General del Notariado 2004.

ESPINOZA CESPEDES, José Francisco. Contratación Electrónica, Medidas de Seguridad y Derecho Informático. Lima, Perú. Edit. RAO S.R.L. 2000

RIPPE S. CREIMER I. OTROS. Comercio Electrónico. Buenos Aires, Argentina. B de F 2003

DAVARA RODRIGUEZ, Miguel Angel. Seguridad en lãs Transacciones Electrónicas. La Firma Electrónica. Madrid, España. Comillas Madrid. 2005

PAEZ RIVADENEIRA, Juan José. Manual de Firmas Electrónicas y Mensajes de Datos. Corporación de Estudios y Publicaciones.

DEVOTO, Mauricio. Comercio Electrónico y Firma Digital. Buenos Aires, Argentina. La Ley 2001.

CREMADES, Javier. Régimen Jurídico de Internet. Madrid, España. La Ley. 2002.

TELLEZ VALDEZ, Julio. Derecho Informático. Mexico. Mc Graw Hill. 2003

La Sociedad de la Información http://www.oei.es/revistactsi/numero1/debate1c.htm acceso 07-02-10

REYES KRAFT Alfredo Alejandro. *La Firma Electrónica*. URL. http://www.razonypalabra.org.mx/libros/libros/firma.pdf acceso 18-01-10
http://www.gobiernoelectronico.org/node/5326 acceso 06-02-10

Gaete González, Eugenio Alberto; *Documento Electrónico e Instrumento Público*, Revista de Derecho Informático. URL. http://www.alfa-redi.org/rdi-articulo.shtml?x=511 acceso 18-02-10

www.derechoecuador.com/index.php?option=comcontent&task=view&=id=4766&Itemid=130 acceso 04-12-09