UNIVERSIDAD DE EL SALVADOR

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

SEMINARIO DE GRADUACION EN CIENCIAS JURÍDICAS AÑO 2005

PLAN DE ESTUDIO 1993

LA FIRMA DIGITAL COMO MEDIO DE SEGURIDAD Y CONSENTIMIENTO EN LAS TRANSACCIONES DEL COMERCIO ELECTRÓNICO.

TRABAJO DE GRADUACION PARA OPTAR AL TITULO DE:

LICENCIADA EN CIENCIAS JURIDICAS

PRESENTAN:

GALÁN CORTEZ, JEANNIE ELIZABETH.
GARCÍA MEJÍA, LAURA AZUCENA.
GÓMEZ BARAHONA, VILMA VERÓNICA.

DIRECTORA DE SEMINARIO:

LICENCIADA ALICIA ZELAYA QUINTANILLA

CIUDAD UNIVERSITARIA, SAN SALVADOR, SEPTIEMBRE DE 2006.

UNIVERSIDAD DE EL SALVADOR

RECTORA
DRA. MARIA ISABEL RODRIGUEZ

VICE-RECTOR ACADEMICO
ING. JOAQUIN ORLANDO MACHUCA GOMEZ

VICE-RECTORA ADMINISTRATIVO
DRA. CARMEN ELIZABETH RODRIGUEZ DE RIVAS

SECRETARIA GENERAL
LICDA. ALICIA MARGARITA RIVAS DE RECINOS

FISCAL GENERAL
LIC. PEDRO ROSALIO ESCOBAR CASTANEDA

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

DECANA
LICDA. MORENA ELIZABETH NOCHEZ DE ALDANA

VICE-DECANO
LIC. OSCAR MAURICIO DUARTE GRANADOS

SECRETARIO
LIC. FRANCISCO ALBERTO GRANADOS HERNANDEZ

COORDINADORA DE LA UNIDAD DE SEMINARIO DE GRADUACION
LICDA. BERTA ALICIA HERNANDEZ AGUILA

DIRECTORA DE SEMINARIO
Licda. ALICIA ZELAYA QUINTANILLA

AGRADECIMIENTOS

A DIOS: Por haberme dado la vida, paciencia, fuerza y sabiduría para culminar un paso más. Porque sin tu ayuda, nada de esto hubiera sido posible, porque me levantaste cuando creí caer, porque me diste ánimo cuando creí que esto no iba a ser posible. GRACIAS SEÑOR.

A MARIA AUXILIADORA: Porque como buena Madre que eres, estuviste siempre a mi lado guiando mis pasos, nunca me dejaste sola y me consolaste cuando más lo necesitaba. GRACIAS MADRECITA.

A MIS PADRES: Miriam y Jorge, porque siempre me apoyaron, creyeron en mí, en que podía lograr cualquier cosa que me propusiera. Porque supieron comprenderme y estar junto a mí cuando más los necesite a pesar de todas las dificultades. Porque yo sé que serán mis eternos compañeros, Gracias por ser parte de este primer logro, porque de no ser por ustedes dos, tampoco hubiera sido posible. INFINITAMENTE GRACIAS.

A MIS HERMANOS: Jorge y Willian, por ser parte de mi vida, por haber sido tan comprensivos y apoyarme en todo momento.

A MI NOVIO: Marlon, porque con este logro, es un paso menos para llegar a nuestra meta. Porque a pesar de las dificultades has estado ahí para mí en todo momento y me has apoyado sin dudarlo. Porque este logro es de los dos y porque cuento contigo en mi vida, soy una mejor persona. T.A.M.H.I.Y.D.R.

A MIS COMPAÑERAS DE TESIS: Que más que mis compañeras de tesis o mis amigas, son mis hermanas, porque sin ellas, esta carrera no hubiera sido igual, sin ellas este triunfo no hubiera sido el mismo y porque sin ellas mi vida no estaría completa.

JEANNIE ELIZABETH GALÁN CORTEZ.

A DIOS: por la vida que me regala, por enseñarme que ningún sueño es posible sin su ayuda, por darme la fuerza para alcanzar esta meta, por la sabiduría para aceptar mi historia y por el amor que hoy llena mi vida.

A MARIA AUXILIADORA: porque desde niña ha sido mi guía, ha estado conmigo en mis alegrías y tristezas y por ayudarme a aceptar con humildad los planes que Dios tiene conmigo.

A MIS PADRES: por hacer de mi, lo que hoy soy; por cuidarme y educarme siempre con amor, por su paciencia y sobre todo la comprensión que tuvieron conmigo, aún cuando los había defraudado. Los Amo!

A MIS HERMANOS: por su apoyo y comprensión, y por cuidarme, aquí y desde el cielo, te extraño hermanito!

A MI HIJO: Danito, porque desde que supe que llegabas a mi vida, te convertiste en lo mas importante, y como te lo prometí, todo lo que haga es para ti.

A MI ESPOSO: Gerardo, todo esto no sería posible sin tu amor y comprensión, porque desde que llegaste a mi vida me enseñaste a sonreír y tu lo sabes, gracias por quedarte con nosotros y hacer nuestras vidas tan felices. Te Amo!

A MIS COMPAÑERAS DE TESIS: por la amistad incondicional que durante todos estos años nos ha unido, porque crecimos juntas y aprendí mucho de ustedes; y aún en los momentos difíciles, supimos reírnos y salir adelante. Gracias!

A MI FAMILIA Y LA FAMILIA DE MI ESPOSO: por su ayuda, apoyo y por alegrarse de mi triunfo.

LAURA AZUCENA GARCÍA MEJÍA.

AGRADEZCO A DIOS TODOPODEROSO Y A LA VIRGEN MARIA: por haberme dado sabiduría para culminar con éxitos mis estudios y lograr el primero de mis propósitos.

A MIS PADRES RAMIRO Y VILMA: por todo su amor, confianza, apoyo, oraciones y todo el esfuerzo que ha lo largo de mi vida han hecho por mi y con ello hacer realidad este sueño, gracias por todo, los amo.

A MIS HERMANOS: Silvia por brindarme su apoyo en todo momento y sabiduría en este proyecto y a mi hermano Walter por su tolerancia y paciencia.

A MI NOVIO: Oswaldo Alexander por su amor, conocimiento, comprensión y apoyo incondicional, gracias...

A MIS COMPAÑERAS: Jeannie Elizabeth y Laura Azucena por haberme permitido trabajar con ellas estos cinco años y por dejarme trabajar a su lado en este proyecto tan importante; Gracias por su comprensión, tolerancia y apoyo en todo momento.

Así como también a la Licda. Zelaya por su conocimiento en este proyecto y maestros, amigos que siempre estuvieron pendientes de este logro.... A todos MUCHAS GRACIAS…

VILMA VERÓNICA GÓMEZ BARAHONA.

INDICE

Página

CAPITULO II. LA FIRMA DIGITAL COMO MEDIO DE SEGURIDAD Y CONSENTIMIENTO EN LAS TRANSACCIONES DEL COMERCIO ELECTRONICO.

INTRODUCCIÓN

La rápida difusión y el gran interés en el mundo de la informática, ha permitido la creación del Internet, que sirve como una herramienta para las empresas, ya que han comenzado a usar Internet como un nuevo canal de ventas, sustituyendo las vías tradicionales del comercio por el denominado comercio electrónico. Sin embargo, la aparición del comercio electrónico obliga ha replantearse muchas cuestiones, ya que surgen nuevos problemas desde la seguridad de las transacciones hasta la validez legal de dichas transacciones.

En razón de lo antes relacionado el presente trabajo de investigación denominado "La Firma Digital como medio de seguridad y consentimiento en las transacciones del comercio electrónico" tiene como finalidad analizar los aspectos generales del comercio electrónico, prestando una mayor atención en como la incorporación de la firma digital a documentos electrónicos representa un medio de seguridad y consentimiento en las transacciones que se llevan a cabo frente al auge del comercio electrónico.

El trabajo de investigación se encuentra estructurado en cuatro capítulos los cuales se concentran de la siguiente manera:

En el capítulo primero se señala aspectos generales del comercio electrónico y firma digital, es decir, el origen y evolución del comercio electrónico y de la firma digital a

nivel mundial y a nivel de nuestro país, definiciones y las ventajas y desventajas que el comercio electrónico plantea; también los tipos, principios y características de la firma digital.

El segundo capítulo denominado la firma digital como medio de seguridad y consentimiento en las transacciones del comercio electrónico, en dicho capitulo se desarrolla la base fundamental del trabajo de investigación ya que en el se explica como se desenvuelve la firma digital por los medios criptográficos y como alcanza a producir seguridad a través de las entidades certificadoras; asimismo como las contrataciones electrónicas que se realizan con documentos electrónicos producen consentimiento y validez legal.

En el tercer capítulo se desarrolla mecanismos jurídicos y medios de prueba en caso de reclamos judiciales sobre documentos con firma digital en transacciones del comercio electrónico, es decir, que este capitulo se puede determinar la eficacia de los mecanismos jurídicos como la mediación, conciliación y arbitraje en relación a los medios de prueba electrónica, pero solo aquellos medios que el anteproyecto de comercio electrónico de nuestro país retoma y que podrán ser utilizados en caso de controversia de un documento con firma digital en transacciones del comercio electrónico; además se encuentra todo lo concerniente sobre la regulación jurídica de la prueba electrónica en El Salvador.

Finalmente en el cuarto capitulo se presenta las similitudes y diferencias de la regulación de la firma digital en España, Argentina y Colombia con El Salvador, asimismo las ventajas y desventajas que existen en estos países, es decir, que comparamos las leyes de estos países que contienen una ley especifica para el comercio electrónico y sobre todo una de firma digital, con nuestro país que no posee una ley especifica solo regulaciones aisladas.

Posteriormente se señalan las conclusiones y recomendaciones que al terminar la investigación se manifiestan, la bibliografía utilizada para la exploración del tema y los anexos que se han señalado a lo largo del trabajo.

CAPITULO I

ASPECTOS GENERALES DEL COMERCIO ELECTRONICO Y FIRMA DIGITAL.

Las redes mundiales de información están transformando al mundo y acercando más a la gente a través de la innovación de las comunicaciones mundiales, lo cual posibilita cambios en todos los ámbitos de la actividad humana, por ejemplo la competitividad, el empleo y la calidad de vida de las naciones, incluidas en ellas el comercio electrónico.

El comercio en todos los países del mundo ha sido muy importante para sus economías, tanto es así que ha evolucionado de una forma tal, que ya no es necesario estar frente a la presencia física de las partes para realizar actos de comercio, es decir que los comerciantes puedan hacer sus contratos, compras, transacciones económicas a través del Internet. Con estas nuevas tecnologías, el tiempo y la distancia dejan de ser obstáculos, los contenidos se pueden dirigir a una audiencia masiva o a un pequeño grupo y se busca un alcance mundial o local.

1.1 ORIGEN Y EVOLUCIÓN DEL COMERCIO ELECTRÓNICO.

El comercio es una actividad antigua del ser humano, ha evolucionado de muchas maneras pero su significado y fin es siempre el mismo, según el Diccionario Económico el comercio es: *"El proceso y los mecanismos que son elaborados para colocar las mercancías que son elaboradas en las unidades de producción, en los centros de*

consumo en donde se provisionan los consumidores, ultimo eslabón de la cadena de comercialización."[1]

El comercio implica la investigación de mercado, la publicidad, la posibilidad de adquirir el producto, métodos de persuasión, venta al por menor y la adquisición por parte del público.

A través de los años han aparecido diferentes formas o tipos de comercio, tal es el caso que a finales del año 1960 y principios del año 1970 la Agencia para Proyectos de Investigación Avanzada (ARPANET) de Estados Unidos de América**,** había sentado las bases para el desarrollo de lo que sería Internet, a través de la cual empleando la tecnología se enlazan documentos científicos provenientes de diferentes computadoras a los que se les puede integrar texto, música, entre otros.

En el año de 1970, la futura Internet ya había desarrollado los reglamentos o protocolos para la transferencia de datos entre computadoras con diferentes sistemas operativos. A finales de 1980 y principio de la década de los noventas, al mismo tiempo que ARPANET dejaba de existir para ceder el paso a la Fundación Nacional para la Ciencia (NSFNET), aparecieron los primeros intentos de clasificar y ordenar los recursos de la red que había crecido a un ritmo acelerado. *"Pero quizá el acontecimiento más importante fue el desarrollo de la red mundial o World Wide Web (WWW) en*

[1] Enciclopedia Básica Visual. Tomo III. Grupo Editorial Océano. Barcelona, España, 1998.

1991"[2] , lo característico de esta red es su alto nivel de accesibilidad lo que significa que el usuario no necesita un alto nivel de informática para poder hacer uso de esta red.

Al tener los países (Comunidad Europea, Estados Unidos de América, Canadá) una mayor accesibilidad a la red, se conectaban con más facilidad a otras redes internacionales y es así como en 1995, surge el Comercio Electrónico, siendo el punto de partida el Intercambio Electrónico de Datos (EDI), entre empresas de un mismo sector, y que fueran inicialmente fomentados por asociaciones industriales y adoptadas por las empresas, para elevar la calidad de la información empleada e intercambiada.

En la práctica, las empresas están comenzando a utilizar el comercio electrónico como un nuevo canal de ventas ya que gestionar un pedido por Internet cuesta menos que hacerlo por las vías tradicionales, lo cual resulta en una reducción de costos.

El Comercio Electrónico en El Salvador, tuvo como pionero en 1999 a Almacenes Simán S.A. de C.V. A mediados del año 2000, el Banco Cuscatlán, Banco Salvadoreño y Banco Agrícola lanzaron las primeras tarjetas de crédito orientadas a realizar compras a través de Internet.

[2] Alfaro Najarro, Rene Adonai y otros, Plan de implementación sobre comercio electrónico para la mediana empresa salvadoreña, Tesis, Universidad Tecnológica, 2001, Pág. 35.

En Enero de 2002, las agencias aduanales empezaron a realizar transacciones por Internet con la Dirección General de la Renta de Aduanas, utilizando la firma digital, agilizando en gran medida el procesamiento de información para importación de mercadería.

En Agosto de 2002, surge el primer Centro Comercial en Línea de El Salvador, implementado por NetCom S.A. de C.V.

La aparición del comercio electrónico obliga a replantear cuestiones del comercio tradicional las cuales van desde la validez legal de las transacciones, contratos sin papel hasta la necesidad de acuerdos internacionales que armonicen las legislaciones sobre comercio.

1.2 DEFINICIÓN DE COMERCIO ELECTRÓNICO.

"El comercio electrónico es un concepto amplio que involucra cualquier transacción comercial efectuada por medios electrónicos, implica un amplio rango de operaciones, incluyendo: intercambio de información, ventas, pagos electrónicos, distribución y asociaciones virtuales; además incluye niveles de alta tecnología de informática y de telecomunicaciones, por tal razón las empresas ven al comercio como

una manera de modernizar las operaciones actuales, alcanzar nuevos mercados y servir mejor a los clientes."[3]

Para tener una visión más amplia de la conceptualización del comercio electrónico se plantean diferentes definiciones:

- Según el gobierno de Canadá el Comercio Electrónico es *"la conducción de actividades de negocios-compra, ventas y transacciones de todo tipo-, por medio de comunicaciones."*[4]
- Para Estados Unidos de América, el Comercio Electrónico "es cualquier transacción completada mediante una red de computadoras e incluye la transferencia de la propiedad o de derechos de bienes y servicios."[5]
- El comercio electrónico es "una metodología moderna para hacer negocios que detecta la necesidad de las empresas, comerciantes y consumidores de reducir costos, así como mejorar la calidad de los bienes y servicios, además de mejorar el tiempo de entrega de los bienes o servicios."[6]

Tomando en cuenta las anteriores definiciones, podemos resumir el concepto de comercio electrónico, a efectos de unificar el criterio para la investigación como: cualquier forma de transacción comercial en la cual las partes involucradas interactúan de manera electrónica, en lugar de hacerlo de la manera tradicional, con

[3] www.utem.sl/cyt/derecho/firma.html
[4] Sarra, Andrea Viviana. Comercio Electrónico y Derecho, Editorial Astrea, Buenos Aires, Argentina, 2000, Pág. 281.
[5] Ib Ídem Pág. 281.
[6] www.monografias.com

intercambios físicos, permitiendo a las compañías ser mas eficientes y flexibles en sus operaciones internas, para así, trabajar de una manera mas cercana con sus proveedores y estar mas pendiente de las necesidades y expectativas de sus clientes.

"Para que se desarrolle auténticamente el comercio electrónico, deben darse las siguientes condiciones:

1. *Creación de redes de distribución, para la entrega física de los productos requeridos digitalmente.*
2. *Promoción de mercados competitivos en las telecomunicaciones, para provocar bajos precios en los sistemas de tarifación del costo de conexión a Internet.*
3. *Introducción a las tecnologías seguras(firma digital, certificados digitales) y a los sistemas de pago de alta confiabilidad.*
4. *Fortalecimiento de la confianza en este tipo de comercio por parte de los consumidores y las empresas.*
5. *Consolidación de los temas conexos al comercio electrónico, tales como: seguridad de la información; protección a los derechos de propiedad intelectual; y privacidad en general.*

6.Armonización de las regulaciones existentes o el establecimiento de marcos jurídicos coordinados internacionalmente."[7]

[7] Op. Cit. Sarra. Pág.289 y 290.

1.3 VENTAJAS Y DESVENTAJAS DEL COMERCIO ELECTRÓNICO.

1.3.1 VENTAJAS

El uso del comercio electrónico favorece a sus usuarios, en cuanto que:

- Permite el acceso a más información; ya que la naturaleza de la red faculta al usuario para realizar búsquedas profundas, que ellos mismos inician y controlan, en consecuencia, las actividades de mercadeo electrónico, son impulsadas por los clientes quienes son los que buscan el producto deseado.
- Facilita la investigación y comparación de mercados; ya que la red tiene la capacidad de acumular, analizar y controlar grandes cantidades de datos, permitiendo al usuario confrontar el producto que desea comprar y acelera el proceso para encontrar exactamente lo que busca.
- Rebaja los costos y precios; conforme aumenta la capacidad de los proveedores para competir en un mercado electrónico, abierto, se produce una baja en los costos y precios, de hecho tal incremento en la competencia, mejora la calidad y variedad de los productos y servicios.

Así como el uso del comercio electrónico, representa ventajas para los usuarios, también incorpora ventajas a las empresas, entre las cuales tenemos:

- Mejoras en la distribución; la posibilidad de participar en un mercado interactivo en el que los costos de distribución o ventas tienden a reducirse, dando fin de manera progresiva al intermediarismo. También compradores y vendedores se contactan entre si de manera directa, de igual forma se puede disminuir el tiempo

que se tardan en realizar las transacciones comerciales, incrementando la eficiencia de las empresas.

- Comunicaciones de mercadeo; las empresas utilizan la red para informar a los clientes sobre la compañía, de sus productos o servicios, y facilitar las relaciones de mercadeo, además ofrece otro tipo de beneficios para desarrollar la relación con los clientes las 24 horas del día, permitiendo que el cliente solicite tanta información como desee y al mismo tiempo que la empresa obtenga información relevante de sus clientes con el fin de servirles en cuanto a sus necesidades y beneficios que buscan.
- Beneficios operacionales; los proveedores disminuyen sus costos al acceder de manera interactiva a las bases de datos de oportunidades de ofertas, y enviar éstas por el mismo medio, revisar de igual forma las concesiones, además se facilita la creación de mercados y segmentos nuevos, es decir, mayor facilidad para entrar a mercados nuevos, y alcanzarlos con mayor rapidez. Todo esto se debe a la capacidad de contactar de manera sencilla y a un costo menor a los clientes potenciales.

1.3.2 DESVENTAJAS.

El comercio electrónico también presenta desventajas, tales como:

- Entorno empresarial y tecnológico cambiante: Aunque anteriormente señalamos como una ventaja la rebaja en los costos y precios del producto, podemos ver que la empresa necesita hacer una inversión inicial y constante en la implementación

de un sistema operativo que cumpla con los requisitos mínimos para ofrecer a sus clientes una buena calidad en sus sistemas de compras y financieros.

- Privacidad y seguridad: una mas de las desventajas del comercio electrónico es que la mayoría de los usuarios no confían en la red como un canal de pago; ya que las compras y pagos de servicios se realizan utilizando el número de la tarjeta de crédito, cualquiera que transfiera datos de una tarjeta de crédito mediante la red no puede estar seguro de la identidad del vendedor, en forma similar no lo está sobre la del comprador, es decir que quien paga no puede asegurarse de que su número de tarjeta de crédito no sea utilizado para algún propósito malintencionado, por otra parte el vendedor no puede asegurarse que el dueño de la tarjeta rechace lo que compró.
- Cuestiones legales, políticas y sociales: existen algunos aspectos que son extensivos en torno al comercio electrónico, por ejemplo validez de la firma digital, legalidad de un contrato electrónico, perdida de derechos sobre las marcas. Esto puede tomarse como una desventaja ya que en muchos países de Latinoamérica no se cuenta con una legislación específica de comercio electrónico que pueda regular todos los aspectos anteriormente mencionados. Esto sin contar con la poca promoción de parte de los gobiernos para el comercio electrónico; ya que este vendría a aumentar y desarrollar las economías de nuestros países.

1.4 LEY MODELO DE LA COMISIÓN DE LAS NACIONES UNIDAS PARA EL DERECHO MERCANTIL INTERNACIONAL (CNUDMI) SOBRE COMERCIO ELECTRÓNICO.

Debido al auge del comercio electrónico a nivel internacional y la trascendencia del mismo en la economía de los países, la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional advirtió la necesidad de la creación de un marco regulatorio internacional que armonizara las legislaciones internas de cada país miembro.

Es así que el 16 de Diciembre de 1996 fue aprobada la Ley Modelo sobre Comercio Electrónico, ésta ley que consta de diecisiete artículos está dividida en dos partes: Una sobre el comercio electrónico en general y otra sobre el comercio electrónico en áreas específicas.

El objetivo esencial de la ley es elaborar un marco jurídico seguro capaz de ser adoptado por los distintos Estados al momento de la adecuación de sus legislaciones, al mismo tiempo se constituye como un instrumento internacional para interpretación de convenios y tratados entre naciones.

Un aspecto importante que contempla esta ley es el reconocimiento jurídico de los mensajes de datos, en el Art. 5 se establece que no se negarán efectos jurídicos,

validez o fuerza probatoria a los mensajes de datos por el solo hecho de que estén en formato digital.

Esto toma relevancia al momento de brindarle seguridad tanto a compradores y vendedores ya que en caso de controversia cuentan con un respaldo para sus pretensiones.

Otro punto relevante dentro de la ley es lo relativo a la formación y validez de los contratos celebrados en el medio del comercio electrónico ya que uno de los principales inconvenientes que presenta la contratación, es en cuanto a determinar con certeza el momento y el lugar en donde debe considerarse realizada y aceptada la oferta.

El Art. 15 de dicha ley presenta la solución a este inconveniente al disponer que el mensaje de datos se tendrá por expedido cuando entre en un sistema de información que no esté bajo el control de quien lo ha enviado, salvo disposición expresa de las partes.

1.5 PROBLEMÁTICA GENERAL DEL COMERCIO ELECTRÓNICO.

Existen grandes facilidades y alcances que el comercio electrónico ofrece, pero también podemos encontrar diversas problemáticas, principalmente el de la seguridad y la confiabilidad en el comercio electrónico.

Tradicionalmente el documento por escrito ha sido la prueba por excelencia de las convenciones o negocios jurídicos, pero no la única, pues nada impide que la voluntad de contratar o extinguir una relación jurídica sea acreditada a través de otros medios de prueba.

Hoy en día el problema jurídico que se genera con la utilización del comercio electrónico donde se desmaterializa los documentos escritos, es que no en todos los casos el usuario puede solicitar el envío físico del contrato que documenta la transacción, esto ocurre entre usuarios separados por grandes distancias; es de mencionar el hecho de que en la mente de un comerciante la exigencia del documento en papel atenta contra la celeridad de las transacciones electrónicas que él ofrece, ya que ésta desmaterialización es una práctica del Comercio Electrónico, derivada de las ventajas de reducción de costos, por lo que se busca que las personas obvien los documentos escritos.

La seguridad en este medio lleva ciertos riesgos, tanto en el sistema como en el dato, a la posibilidad de alteraciones o destrucciones de datos informáticos, es decir a la violación de la confidencialidad e integridad y disponibilidad de la información.

Además la confiabilidad de la información obtenida puede también ser materia de riesgo. De ahí que sea necesario la creación de diversos mecanismos de verificación de la información.

Según Rosa Julia Barceló y Thomas Vinje *"el crecimiento del Comercio Electrónico depende de la capacidad de los mensajes electrónicos para ser confidenciales y seguros"*[8]; en virtud de que los mensajes y documentos electrónicos constituyen la forma en que los comerciantes y usuarios de los medios electrónicos realizan la mayoría de sus transacciones comerciales.

En la actualidad los Estados tienen la necesidad de obtener un medio confiable que se vea reflejado en tratados bilaterales, legislaciones internas o la enunciación sobre autentificación, integridad y confidencialidad de la información, encontrando como mecanismo a utilizar la firma digital.

1.6 GENERALIDADES DE LA FIRMA.

En el ámbito legal, siempre ha existido la necesidad de hacer constar el consentimiento de las personas sobre actos y declaraciones de las cuales tomen parte, es por eso que las normas jurídicas le dan validez a la firma manuscrita, la cual puede definirse de la siguiente manera: *"nombre, apellido o titulo que se pone al pie de un escrito para acreditar que procede de quien lo escribe, para autorizar ahí lo manifestado u obligarse a lo declarado en el documento"*[9] , es decir que se trata de un rasgo o conjunto de rasgos gráficos, que tienen existencia desde que el sujeto las emplea

[8] Barceló, Rosa Julia y Vinje Thomas, Hacia un marco europeo sobre firmas digitales y criptografía. Revista de Derecho Mercantil. Número 228, Abril-Junio, 1998. Madrid. www.vlex.com.
[9] Cabanellas de Torres, Guillermo. Diccionario Jurídico Elemental, Editorial Heliasta S.R.L, Buenos Aires, Argentina, 1994. Pág. 115

como individualización; y demostrar su presencia, propiedad, titularidad o autoría del documento al que se incorpora.

Particularmente dentro de los procesos jurídicos una de las decisiones mas acudidas es demostrar la identidad de una persona. Este procedimiento puede encontrarse en verificación de la autoría de documentos. Así tenemos que para saber si un documento fue emitido por un individuo, la relación que existe entre el documento y el individuo legalmente se establece con la firma autógrafa.

Por décadas la firma autógrafa ha servido para identificar la autoría de documentos, sin embargo desde que se creó ha acarreado defectos. Uno de estos es la falsificación y el procedimiento de verificación de la firma. A pesar de estas imperfecciones, la firma autógrafa ha servido como el método más aceptado para verificar la identidad de una persona.

La firma tradicional tiene varias características, la principal de ellas es que es aceptada legalmente, esto quiere decir que si alguna persona firmó un documento adquiere tanto los derechos como las obligaciones que de él deriven, y si éstas obligaciones no son respetadas, el portador del documento tiene el derecho de reclamación mediante un litigio. La autoridad competente acepta las responsabilidades adquiridas con solo calificar a la firma como válida.

La firma manuscrita, implica dos acciones; una que es la acción de firmar y otra que es la verificación de la firma. La primera consiste en que un individuo escriba su nombre o rúbrica, o algún conjunto de caracteres particulares: no es necesaria autorización para su uso y tiene validez legal en todo el mundo. La segunda es mas complicada, el proceso de verificación de la firma se realiza de forma visual, comparando la firma con otra que se encuentre en un documento de identificación, y así, acepta o rechaza la firma. En casos más complejos, se puede llegar hasta una verificación realizada por perito.

Es importante hacer notar que la firma comprueba la identidad de una persona, de tal manera que así se sabe quien es la persona que firmó, y que ésta persona no puede negar responsabilidades que adquiere en un documento firmado. Con la firma manuscrita queda resuelto legalmente el problema de la autenticidad o el de comprobar la identidad de una persona.

Precisamente nuestro tema principal es desarrollar la nueva tecnología que pueda reemplazar a la firma autógrafa y que se ha denominado Firma Digital.

En el año de 1976, dos investigadores norteamericanos, descubren lo que se denomina la criptografía de clave pública, y como consecuencia de ésta la firma digital. En 1978, R. Rivest, A. Shamir y L. Adleman, proponen hasta hoy el método mas usado de firma digital, denominado RSA, de sus iniciales proviene el nombre del algoritmo,

(Rivest, Shamir y Adleman). Este método obedece a los mismos principios que la firma autógrafa, es decir, tiene una acción de firmar y otra de verificación de la firma. Este proceso de verificación de firma es exacto, y es prácticamente imposible que hayan falsificaciones.

El uso de la firma digital, se considera un medio técnico para que algunas o todas las funciones identificadas como características de la firma manuscrita se cumplan en un entorno electrónico brindando seguridad a todos los usuarios.

La seguridad como elemento fundamental del comercio, se ha logrado en parte con la Firma Digital y sus diferentes clases, aunque no es el único medio; permitiendo a las partes involucradas en el negocio jurídico tener las herramientas para hacer valer sus derechos y ejercer las acciones pertinentes. De esta forma, el comercio electrónico, pese a la falta de documentos y firmas escritas, ofrece la misma seguridad jurídica a los participantes en las transacciones electrónicas.

1.7 DEFINICIONES DE FIRMA DIGITAL.

Definir un concepto de firma digital no es fácil, aún más cuando no existe una noción clara sobre el mismo y se está utilizando distintamente en muchos países del mundo, sin alcanzar una denominación global.

Es por eso que profundizaremos en conceptos tanto doctrinarios como jurídicos de diferentes autores y legislaciones para tener una visión amplia del tema.

1.7.1 DOCTRINARIO.

Para Andrea Sarra, la firma digital es *"una firma electrónica realizada mediante la transformación de un registro electrónico utilizando criptosistemas asimétricos y función hash, de modo que la persona que tiene el mensaje de origen y la clave pública del signatario puede determinar si la transformación se efectuó por medio de la clave privada que se corresponde con la clave pública que él tiene, y si el mensaje original fue alterado desde que se hizo la transformación."*[10]

Según Apol-Lonia Martínez Nadal, la firma digital es: *"la que se crea en un sistema de criptografía asimétrica o de clave pública basados en el uso de un par de claves asociadas: una clave privada, que se mantiene en secreto, y una clave pública, libremente accesible para cualquier persona."*[11]

Ramiro Cubillos Velandia, define la firma digital como: *"los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, y todo método relacionado con un mensaje de datos que puedan ser utilizados*

[10] Op. Cit, Sarra. Pág. 389.
[11] Martínez Nadal, Apol-Lonia. Comercio Electrónico, Firma Digital y Autoridades de Certificación, Tercera Edición, Editorial Civitas, Madrid, España. 2001. Pág. 42

para identificar al titular de la firma en relación con el mensaje de datos e indicar que el titular de la firma aprueba la información contenida en el mensaje de datos."[12]

También podemos encontrar definiciones de firma digital en Internet, tales como:

- *"La firma digital está formada por una serie de caracteres de lo mas variado –letras, números, signos, etc.- elaborados con un programa informático, los cuales, al asociarse a otros datos, también de tipo electrónico permite entre otras cosas, identificar al firmante de los mismos."*[13]

- *"La firma digital es una cadena de caracteres, generados mediante un algoritmo matemático que se obtiene utilizando como variables la clave privada y la huella digital del texto a firmar, de forma que permite asegurar la identidad del firmante y la integridad del mensaje"*[14]

- *"La firma digital puede ser definida como una secuencia de datos electrónicos que se obtienen mediante la aplicación a un mensaje determinado de un algoritmo, o de cifrado asimétrico o de clave pública, y que equivale funcionalmente a la firma autógrafa en orden a la identificación del autor del que procede el mensaje."*[15]

---

[12] Cubillos Velandia, Ramiro y otro, Introducción Jurídica del Comercio Electrónico, Ediciones Jurídicas Gustavo Ibáñez, Bogotá, Colombia. 2002. Pág.215
[13] www.tuguialegal.com/firma digital/1.htm
[14] www.iec.csic.es/criptonomicon/seguridad
[15] www.espanol.groups.yahoo.com/groups/

- *"La firma digital es un conjunto de caracteres que se añaden al mensaje que enviamos a través de Internet, con el objeto de proteger la integridad de los datos que se trasmiten, evitando que sean interceptados y falsificados. A través de esta codificación, el receptor del mensaje puede comprobar no solo el origen de los datos que se han remitido, sino su integridad y la identidad de la persona que los envió."*[16]

1.7.2 JURÍDICO.

Según la Comisión de las Naciones Unidas para el Desarrollo del Derecho Mercantil Internacional (CNUDMI), en la Ley Modelo sobre Firma Electrónica Articulo 2 literal a), se entenderá por tal: *"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".*

Según el Real Decreto-Ley 14/1999, en el cual se regula la firma electrónica en el derecho español, el Articulo 2 literal a), establece que la firma electrónica: *"es el conjunto de datos, en forma electrónica anexos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que las recoge."*

[16] www.html.net/seguridad/varios/firma-certificado

En la Ley 25.506 de Firma Digital de la República Argentina, en el Articulo segundo se entiende por Firma digital: *"el resultado de aplicar a un documento digital, un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permite identificar al firmante y detectar cualquier alteración al documento digital posterior a su firma."*

El Articulo segundo en su inciso tercero de la Ley 527/1991: Del Comercio Electrónico y de las firmas digitales de la República de Colombia, define a la firma digital como: *"un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje, permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador que el mensaje inicial no ha sido modificado después de efectuada la transformación."*

Para el Decreto Legislativo Número 529 del 13 de Enero de 1999, sobre Reformas a la Ley de Simplificación Aduanera, constituye la firma digital o electrónica: *"una pareja de claves o llaves únicas correspondientes entre sí, una pública y otra privada que se corresponden de manera exclusiva y excluyente; en la que existe una autoridad certificadora que debe administrar un sistema de publicidad de las llaves públicas."*

Después de lo anteriormente expuesto y según nuestra investigación, podemos concluir como grupo que la firma electrónica o digital es: un conjunto de datos electrónicos que identifican a una persona en concreto, suele unirse al documento que se envía por medio telemático, como si de la firma tradicional se tratara, de esta forma el receptor del mensaje está seguro de quien ha sido el emisor; este mecanismo permite la confidencialidad y la seguridad de la información tanto enviada como recibida por Internet.

1.8 TIPOS DE FIRMA DIGITAL.

Después de haber definido y analizado el concepto de firma digital, doctrinaria y jurídicamente, podemos distinguir dos tipos de firma digital en función del formato técnico que se emplea para construirla, una básica y una avanzada.

1.8.1 FIRMA DIGITAL BASICA.

"Esta firma contiene un conjunto de datos recogidos de forma electrónica que formalmente identifican al autor y se incorporan al propio documento."[17] Es decir que esta firma únicamente autentifica la identidad de la persona, se puede entender como lo que se hace al mostrar un documento de identidad, para confirmar que es la persona quien dice ser.

[17] www.ingenieroseninformatica.org/recursos/tutoriales/firmaelectronica/cap4.php

Esto significa que podemos estar seguros de la identidad del emisor del mensaje pero queda en tela de juicio que el contenido del mensaje no ha sido modificado o alterado por terceras persona.

1.8.2. FIRMA DIGITAL AVANZADA.

Como se dijo anteriormente podemos elegir la tecnología que deseamos, siempre y cuando nos garantice que la firma digital nos va a brindar seguridad, todo esto lo podemos encontrar en la firma digital avanzada.

" Esta firma permite la identificación del signatario, que 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 anterior de éstos. Debe basarse en un certificado reconocido, aquel que contiene determinadas informaciones y que ha sido emitido respetando determinadas cautelas, el certificado reconocido, tiene que haber sido expedido por un prestador de servicios de certificación acreditado. Además, ésta firma tiene que haber sido generada empleando un dispositivo seguro de creación de firma, debidamente certificado."[18]

Los medios que el signatario mantiene bajo su exclusivo control, a los que se refiere el Real Decreto-Ley, son los datos de creación de firma digital que están

[18] Real Decreto-Ley 14/1999

compuestos por el "**signatario** que es *persona física que cuenta con un dispositivo de creación de firma y que actúa en nombre propio o en el de una persona física o jurídica a la que representa; y el* **dispositivo de creación de firma** *que es un programa o un aparato informático que sirve para aplicar los datos de aplicación de firma, siendo éstos, códigos o claves criptográficas privadas, que el signatario utiliza para crear la firma digital."*[19]

La firma digital avanzada, además de cumplir la función de la firma digital básica, que es identificar al emisor, también vincula de manera única al que firma el documento con los datos que incorpora, debido a que él es el único que posee el control exclusivo de las claves, además de que permite saber si éstos datos han sido alterados posteriormente al envío del mensaje.

Otra diferencia entre éstos tipos de firmas, es en cuanto a los efectos jurídicos que producen, ya que el Art. 3 del Real Decreto Ley 14/1999, establece que los datos consignados de forma electrónica, en una firma digital avanzada, tienen el mismo valor jurídico que la firma manuscrita y es admisible como prueba en juicio, es decir, que se le confiere plena eficacia jurídica y probatoria.

En la Ley de Simplificación Aduanera, se regula el uso de la Firma Digital Avanzada, ya que el Art. 8 inc. 3 establece que "*Para el intercambio de la información*

[19] www.internautas.org

en general, cada usuario autorizado, contará con una pareja de claves o llaves únicas y correspondientes entre sí, una pública y otra privada, de manera tal que ambas se correspondan de manera exclusiva y excluyente, debiendo además la Entidad Certificadora, administrar un sistema de publicidad de las llaves públicas. La vinculación de ambas llaves o claves constituye la Firma Digital, que para todos los efectos legales se constituye en el sustituto digital de la firma manuscrita."

1.9 PRINCIPIOS Y OBJETIVOS DE LA FIRMA DIGITAL.

PRINCIPIOS DE LA FIRMA DIGITAL

"1.Principio de no discriminación:

No se le negarán efectos jurídicos, validez o fuerza obligatoria a la información por la sola razón de que esté en forma de mensaje de datos.

2.Principio de la autonomía de la voluntad:

Entendiéndose como la facultad que tienen las partes en un contrato de auto regularse, teniendo como límites el orden público, las buenas costumbres, las leyes prohibitivas y los derechos de terceros.

3. Principio de compatibilidad internacional:

De acuerdo al cual las disposiciones sobre el comercio electrónico serán aplicables en arreglo a las leyes internacionales que se hayan expedido con anterioridad y no contravenga a otras normas que dificulten su aplicación.

4. Principio de equivalencia funcional:

La información y el soporte electrónico surte los mismos efectos que si el soporte fuese en papel, para lo cual se deben cumplir los siguientes requisitos:

a) Identificación de la persona;

b) Imputación de la información a esa persona; y

c) Utilización de un método fiable en la creación y certificación.

La base de este principio es el análisis de los objetivos y funciones del requisito tradicional de la presentación de un escrito sobre papel, con miras a estipular el modo de satisfacer sus objetivos y funciones con técnicas que utiliza el comercio electrónico.

En virtud de este principio no se debe dar lugar a que se impongan a los usuarios del comercio electrónico normas de seguridad más estrictas que las aplicables a la documentación consignadas sobre papel.

OBJETIVOS DE LA FIRMA DIGITAL

Los objetivos de la firma digital son:

a. Identificar fehacientemente a los signatarios del mensaje enviado por medios telemáticos, de manera tal, que no quepa duda a los intervinientes que cada uno de ellos es quien dice ser.

b. Permitir a los intervinientes en el acto o contrato transmitido, tener la razonable seguridad de que ningún tercero no autorizado tenga acceso a dicho acto o contrato.”[20]

1.10 CARACTERÍSTICAS DE LA FIRMA DIGITAL.

El comercio electrónico empezó a ser seguro a mediados de 1990, actualmente avanzados sistemas de seguridad ofrecidos por Internet, pueden asegurar el éxito de todas las transacciones económicas que se llevan a cabo en este medio, con el fin de que exista una celebración válida de negocios jurídicos que impliquen la viabilidad de expresar la voluntad de una persona y con ello la posibilidad de celebrar contratos válidos y exigibles.

Existen también riesgos derivados de los problemas inherentes a los mismos sistemas electrónicos a través de los que se desarrollan en una red abierta e insegura como Internet.

Los riesgos mas importantes derivados de un intercambio de información a través de Internet son:

- Que el autor y fuente del mensaje haya sido suplantado, es el problema de la autoría de los mensajes electrónicos.

[20] Galindo Sifuentes, Ernesto. Derecho Mercantil, Comerciantes, Comercio electrónico, Contratos mercantiles y Sociedades Mercantiles. Editorial Porrua. México D.F. 2004. Pág.50.

- Que el mensaje sea alterado, de forma accidental o intencional durante la transmisión o incluso una vez recibido, es el problema de la integridad de los mensajes electrónicos.
- Que el emisor del mensaje niegue haberlo transmitido o el destinatario haberlo recibido, es el problema del repudio de los mensajes electrónicos.
- Que el contenido del mensaje sea leído por una persona no autorizada, es el problema de la confidencialidad de los mensajes electrónicos.

En esta transición de un sistema comercial basado en el papel a un sistema de comercio electrónico se hace necesario que la sustitución del papel y de las firmas escritas por sus equivalentes electrónicos pueda generar la misma confianza y ofrecer seguridad jurídica a los usuarios. Por lo tanto, para minimizar los riegos derivados del intercambio de información a través de Internet se utiliza la firma digital la cual proporciona una amplia gama de servicios de seguridad al cumplir con las siguientes características:

1.10.1 INTEGRIDAD.

La integridad es una de las características con las cuales se le da plena validez jurídica al documento electrónico, y es por esto que se confía en la firma digital, ya que *"asegura la información de manera que ésta, no pueda ser modificada o alterada, ya*

sea intencionalmente o accidentalmente. El mensaje debe llegar a su destino sin alteraciones en su contenido o en el orden de la recepción de las unidades.”[21]

Doctrinariamente, muchos autores coinciden en la relevancia de ésta característica, principalmente porque se trata de datos firmados y enviados entre personas que en ningún momento llegan a tener un contacto directo entre ellos, y gracias a la característica de la integridad que tiene la firma digital, se presume que el mensaje recibido es el que se ha enviado.

Es por lo anteriormente dicho, que la integridad permite que sea detectada cualquier modificación por pequeña que sea, de los datos firmados, proporcionando así, una garantía ante alteraciones accidentales o provocadas, durante el manejo de documentos o datos firmados.

1.10.2 AUTENTICIDAD.

Al igual que la firma manuscrita se presume que ésta pertenece a la persona que la estampa con su puño y letra, la firma digital no es ajena a ésta manera de firmar, ya que expresa la autoría de la declaración de voluntad del signatario y que pertenece exclusivamente a la persona que consta como titular del certificado.

[21] Polanco Villalobos, José Antonio y otros, La regulación sobre comercio electrónico en el ordenamiento jurídico salvadoreño, Tesis, Universidad José Simeón Cañas, 2001. Pág. 45.

A ésta característica de la firma digital se le conoce como autenticidad, la cual consiste en que: *"el mensaje ha sido generado por la parte identificada en el documento como emisor del mismo, no pudiendo alguna otra entidad suplantar a un usuario del sistema."*[22] Esto se logra mediante la inclusión en el documento transmitido de un valor de autenticación (MAC, Message Autentication Code).

Es decir que la autenticación permite identificar y sin equivocaciones quien es el signatario, ya que el hecho de que la firma ha sido creada por él, mediante medios que mantiene bajo su propio control, como por ejemplo, contraseñas, tarjetas inteligentes, etc., aseguran la imposibilidad de su suplantación, aspecto de especial relevancia, ya que el medio utilizado para la difusión de los mensajes es el Internet, el cual por si solo no brinda la confianza y seguridad en los usuarios como la proporciona el uso de la firma digital.

1.10.3 NO REPUDIO.

Cuando se firma un documento, lo que se hace es manifestar que está acorde con el contenido del mismo, por ende cuando un documento electrónico se encuentra firmado por medio de firma digital, se deduce que el autor del mensaje que consta en el certificado, debidamente expedido, está manifestando que su voluntad es la consignada en dicho documento y por lo tanto no puede negarse a los efectos que del mismo derivan.

[22] www.scba.gov/fdweb.swf

La figura del no repudio puede por tanto, ser definida como *"una de las características resultantes de los contratos y documentos electrónicos, la cual protege a las partes de la negación de que dicha comunicación haya ocurrido, es decir que protege al receptor del documento de la negación del emisor de haberla enviado."*[23]

Esta característica, es más fuerte que las anteriores ya que el emisor no puede negar bajo ninguna circunstancia que ha generado dicho mensaje. A pesar de que no se puede conseguir el no repudio sin la autenticación y la integridad de los datos, el no repudio consiste en algo más, ya que es la capacidad de probar a un tercero que una determinada transmisión de información ha sido originada, admitida y enviada a determinada persona.

En el Derecho Norteamericano, el no repudio es el principio general del derecho probatorio, porque permite evadir la negativa tanto de haber recibido como de haber enviado el mensaje.

1.10.4 CONFIDENCIALIDAD.

El comercio se desarrolla por medios electrónicos, a través de una red abierta como Internet, la cual no proporciona seguridad a los usuarios, y se hace necesario garantizar la confidencialidad, ya que existen empresas que utilizan Internet para el

[23] Op. Cit. Pág 22

envío y recepción de información sumamente importante y que no puede ser interceptada por otra empresa, ya que esto implicaría un peligro para su seguridad.

Por confidencialidad entenderemos, *"el mayor o menor grado de secreto al que la persona quiere someter a un dato o una información; lo cual va a depender de los intereses particulares o personales del poseedor del dato e independientemente de cuestiones puramente jurídicas o de relaciones contractuales."*[24]

La aplicación de las tecnologías de firma digital hace posible, que esta característica de confidencialidad, sea cubierta ya que un mensaje cifrado con firma digital *"protege los datos de revelaciones o accesos de personas no autorizadas."*[25]

La obtención de confidencialidad en la transmisión de datos, implica el uso de tecnologías basadas en la criptografía, como el cifrado, aspecto que desarrollaremos mas adelante.

[24] Escuela Judicial Concejo General del Poder Judicial. Problemática jurídica en torno al fenómeno de Internet. Cuadernos de Derecho Judicial. Imprime: LERKO PRINT, S.A. 2000. Pág. 152
[25] Op. Cit. Martínez Nadal. Pág. 38.

CAPITULO II

LA FIRMA DIGITAL COMO MEDIO DE SEGURIDAD Y CONSENTIMIENTO EN LAS TRANSACCIONES DEL COMERCIO ELECTRONICO.

A lo largo de la historia, el ser humano ha desarrollado sistemas de seguridad que le permiten en una comunicación, comprobar la identidad del interlocutor; como por ejemplo la firma, asegurando de que solo obtendrá la información el destinatario seleccionado, y que además ésta no podrá ser modificada e incluso que ninguna de las dos partes podrá negar el hecho ni cuando se produjo. En la mayor parte de los casos el sistema de seguridad se basa en la identificación física de las personas, información que se verifica con el documento de identidad.

Actualmente, cada vez es mayor el número de actividades que se están trasladando al mundo electrónico a través de Internet, se hace por lo tanto necesario trasladar también los sistemas de seguridad a este contexto, en que la seguridad en las transacciones económicas es la preocupación más angustiante para los responsables de los sistemas de información, ya que existe una fragilidad en el sistema, en el sentido que cualquier persona entrenada en computación podría llegar a tener acceso a documentaciones, aún durante la elaboración, si se está conectado a Internet o durante la transferencia electrónica.

Por ésta y muchas más razones la Firma Digital es el sistema más seguro para enviar datos con la certeza de que nadie mas que el receptor autorizado será capaz de

leerlo, ya que hoy por hoy es el mejor método para garantizar la seguridad en las transmisiones de datos a través de la red porque aplica el máximo nivel en el encriptamiento de la información que protege.

Para proteger la información antes mencionada, se ha recurrido a la criptografía, que es actualmente la herramienta más conveniente para lograr la seguridad y confiabilidad en las comunicaciones electrónicas, y de este modo favorecer el desarrollo de las redes abiertas.

2.1 CRIPTOGRAFÍA.

2.1.1 ANTECEDENTES HISTÓRICOS DE LA CRIPTOGRAFÍA.

La historia de la criptografía data desde las primeras civilizaciones, ya que desarrollaron técnicas para enviar mensajes durante las campañas militares de forma que sí el mensajero era interceptado, la información que portaba no corría peligro de caer en las manos del enemigo.

El primer criptosistema que se conoce fue realizado por el historiador griego Polybios, el cual consistía en un *"sistema de sustitución basado en la posición de las letras en una tabla."*[26]También los romanos utilizaron este sistema de sustitución, siendo conocido el método como César, porque supuestamente Julio César lo utilizó en sus campañas.

[26] www.internauntas.org

Otro de los métodos criptográficos utilizados por los griegos fue la Escitala Espartana, *"un método de transposición basado en un cilindro que servía como clave en el que se enrollaba el mensaje para poder cifrar y descifrar."*[27]

En 1465 el italiano León Batista Alberti inventó un nuevo sistema de sustitución poli alfabética que fue un gran avance en la época. Otro de los criptógrafos más importantes del siglo XVI fue el francés Blaise de Vigenere que escribió sobre la escritura secreta y que diseñó una cifra que ha llegado hasta nuestros días.

"Durante los siglos XVII, XVIII, XIX el interés de los monarcas por la criptografía fue notable ya que los ejércitos en campaña de Felipe II utilizaron durante mucho tiempo una cifra con un alfabeto de mas de quinientos símbolos, que los matemáticos del rey consideraban invencible, pero el matemático francés Francois Viete consiguió criptoanalizar aquel sistema, el rey impulso una queja de la corte española ante el Papa Pío V acusando a Enrique IV de utilizar magia negra para vencer a sus ejércitos. Por su parte la reina Maria Estuardo reina de los escoceses fue ejecutada por su prima Isabel I de Inglaterra al descubrir un complot de aquella tras un criptoanálisis exitoso por parte de los matemáticos de Isabel."[28]

[27] Ib idem
[28] Op. Cit. Pág 41

"El uso de la criptografía moderna basada en medios informáticos, comenzó durante la segunda guerra mundial donde las figuras mas importantes fueron la del holandés Auguste Kerckhoffs y la del prusiano Friedrich Kasiski, donde la criptografía se usó para fines no bélicos o militares, el sistema era una máquina de calculo, la mas conocida de las máquinas de cifrado, la cual consistía en una máquina de rotores que automatizaba considerablemente los cálculos que eran necesarios realizar para las operaciones de cifrado y descifrado de mensajes, ésta se llamaba máquina alemana Enigma."[29]

Tras la conclusión de la segunda guerra mundial, la criptografía tiene un desarrollo teórico importante, siendo Claude Shannon y sus investigaciones sobre teoría de la información, esenciales en dicho desarrollo.

Además los avances en computación automática, suponen tanto una amenaza para los sistemas existente como una oportunidad para el desarrollo de nuevos sistemas.

En esas mismas fechas ya se empezaba a gestar lo que sería, hasta ahora la última revolución de la criptografía en lo teórico y lo práctico que son: los sistemas asimétricos; estos sistemas supusieron un salto cualitativo importante ya que permitieron introducir a la criptografía en otros campos que hoy en día son esenciales, como el de la firma digital.

[29] Op. Cit. Martínez Nadal. "Comercio Electrónico..." Pág 45

2.1.2 DEFINICIÓN DE CRIPTOGRAFÍA.

La criptografía es un tema que contempla todo lo relacionado con la firma digital, aunque en muchas ocasiones se trate por separado.

Es así que se define como *"la ciencia que se ocupa de transformar mensajes en formas aparentemente ininteligibles y devolverlos a su forma original"*[30]

Sin embargo a raíz del desarrollo normal de la sociedad, esta ciencia se ha convertido en una técnica especializada a través de la cual se procura establecer lenguajes especiales que solo pueden ser leídos por ciertos grupos de personas. Es importante tener en cuenta que el término criptografía se emplea tanto para desarrollar códigos de lenguaje como para descifrarlos.

Otra definición de criptografía es:*"ciencia que estudia la ocultación, disimulación o cifrado de la información, así como el diseño de sistemas que realizan dicha función."*[31]

Del análisis de las definiciones anteriores podemos concluir, para efectos de nuestra investigación que la criptografía es: la rama de las matemáticas aplicadas que se ocupa de transformar mensajes en forma aparentemente ininteligibles y devolverlos a su

[30] Op. Cit. Martínez Nadal. "Comercio Electrónico..." Pág 45
[31] Cornejo López, Valentino. Revista Electrónica de Derecho Informático, Número 33. www.vlex.com.2001

forma original, decimos que se trata de una rama de las matemáticas porque se basa en el empleo de funciones algorítmicas para generar dos claves diferentes pero matemáticamente relacionadas entre sí.

El fundamento de las firmas digitales es la criptografía, disciplina matemática que no solo se encarga del cifrado de textos para lograr su confidencialidad, protegiéndolos de terceros ajenos a la información, sino que también proporcionan mecanismos para asegurar la integridad de los datos y la identidad de los participantes en la transacción.

2.2 SISTEMAS CRIPTOGRÁFICOS.

En el uso del comercio electrónico, la problemática de la seguridad comenzó a ser el punto débil, y para evitar este problema se han creado varios sistemas de criptografía, tales como: el Sistema Simétrico y el Sistema Asimétrico, los cuales desarrollaremos posteriormente.

El objetivo de la criptografía es proporcionar comunicaciones seguras sobre canales no seguros; es decir permite que dos entidades, bien sean personas o bien aplicaciones, puedan enviarse mensajes por un canal que puede ser interceptado, de modo que solo los destinatarios autorizados puedan leer los mismos.

La criptografía no constituye la seguridad en si misma, solo es la herramienta que utilizan mecanismos mas complejos para proporcionar, además de confidencialidad, otros servicios de seguridad.

Los criptosistemas que basan su seguridad en mantener secreto el algoritmo, son fáciles de descifrar, por lo que ya no se utilizan y se han sustituido por sistemas de encriptación que basan su seguridad en mantener en secreto una serie de parámetros, llamados claves, de forma que el algoritmo no puede ser conocido.

Para que una persona pueda contar con su firma digital, es necesario que una Entidad Certificadora le genere su par de claves, previo cumplimiento de los requisitos exigidos para tal efecto, a través de un certificado digital que contiene datos personales del titular y su firma digital, el cual garantiza a los receptores del mensaje la correspondencia entre el par de claves y la autenticidad del mensaje. Es así, que la Entidad Certificadora actúa como tercera parte de confianza de la parte firmante y del receptor, cuyo funcionamiento será explicado posteriormente al desarrollo de los sistemas criptográficos.

Existen dos grandes grupos de cifrados: los algoritmos que utilizan una única clave tanto en el proceso de cifrado como en el de descifrado; y los que utilizan una clave para cifrar mensajes y una clave distinta para descifrarlos. Los primeros se denominan cifras simétricas o de clave simétrica y son la base de los algoritmos de

cifrado clásico. Los segundos se denominan cifras asimétricas o de clave pública y clave privada y es la base de las técnicas de cifrado moderno.

2.2.1 SISTEMA SIMÉTRICO.

Este sistema surge a finales de los años 1970 y se basa en los usuarios que quieren intercambiar mensajes, y disponen de una clave secreta que aplicada a un *algoritmo*[32] transforma el mensaje original en otro cifrado siendo responsabilidad de los usuarios conservar la clave.

Cuando se emplea la misma clave en las operaciones de cifrado y descifrado, se dice que el criptosistema es simétrico o de clave secreta. Estos sistemas son mucho más rápidos que los de clave pública, y resultan apropiados para el cifrado de grandes volúmenes.

"En este sistema dos operadores conocen el mismo código con el que acceden a la información encriptada, por ejemplo, las dos partes conocen la clave "x", la cual aplican a la hora de codificar o bien decodificar respectivamente un mensaje de datos."[33]

---

[32] Método de resolución de cálculos complicados mediante el uso repetido de otro método de cálculo más sencillo. En la actualidad, el término algoritmo se aplica a muchos de los métodos de resolución de problemas que emplean una secuencia mecánica de pasos, como en el diseño de un programa de ordenador o computadora.
Enciclopedia Microsoft® Encarta® 2003. © 1993-2002 Microsoft Corporation.

[33] Op. Cit. Pág 22

"Sin embargo este sistema genera dos problemas: el primero es que no se puede determinar quien es el emisor de la información como tampoco quien es el receptor, porque los dos tienen el mismo sistema de conocimiento del texto aplicado al mensaje de datos; y el segundo problema es que se tiene que mantener en absoluto silencio la clave por parte de ambos intervinientes, existiendo el problema del empleo de un mecanismo seguro para transferir la clave de una parte a la otra, haciendo posible a terceros entrar en el sistema."[34]

Este sistema es el mas simple y común, en él se usa una única llave o clave matemática tanto para la encriptación del mensaje como para su desencriptación. La encriptación simétrica asegura confidencialidad dado que el mensaje solo puede ser descifrado por el destinatario que conoce la clave secreta. El destinatario debe conocer, además de la llave simétrica, el algoritmo utilizado y algunos parámetros que dependan de éste. (VER ANEXO 1).

Para el cifrado simétrico que se utiliza para encriptar el cuerpo de los mensajes en el correo electrónico o los datos intercambiados en las comunicaciones digitales, se emplean algoritmos como: Data Encryption Standard (DES); este fue el primer algoritmo desarrollado comercialmente y surgió como resultado de la petición del departamento de defensa de Estados Unidos a IBM. El DES es un cifrado en bloques

[34] Op. Cit. Cubillos Velandia, Pág 209

que utiliza una clave de 64 *bits*[35] de longitud, de los cuales 8 son iguales entre si para encriptar bloques de 64 bits de datos.

Debido al actual desarrollo tecnológico la seguridad proporcionada por una clave de solo 64 bits de longitud está siendo cuestionada, lo que ha llevado a la búsqueda de otros sistemas simétricos como el Triple-DES, que utiliza una clave de 168 bits o el IDEA que utiliza una clave de 128 bits.

Para efectos de un mejor entendimiento de la aplicación del sistema simétrico en el uso electrónico de las comunicaciones podemos plantear el siguiente ejemplo:
Ana ha escrito un mensaje para Bernardo, pero quiere asegurarse de que nadie más que él lo lea. Por esta razón ha decidido cifrarlo con una clave. Para que Bernardo pueda descifrar el mensaje, Ana deberá comunicarle dicha clave. Bernardo recibe el mensaje y la clave y realiza el descifrado.

En El Salvador la tecnología que se utiliza para el sistema simétrico es el de 128 bits de longitud ya que este ofrece un sentido de seguridad pero no tanto como el que ofrece el sistema asimétrico, que desarrollaremos a continuación.

---

[35] En la comunicación de datos, en el intercambio de información entre computadoras. Los ordenadores sólo entienden un lenguaje binario, es decir, los valores 1 o 0. Cada uno de estos dos dígitos se llama bits. Una serie de bits forman un byte.
Enciclopedia Microsoft® Encarta® 2003. © 1993-2002 Microsoft Corporation.

2.2.2 SISTEMA ASIMÉTRICO.

Este sistema, también llamado criptosistema de clave pública, está basado en *"el uso de un par de claves asociadas: una clave privada o clave de firma, conocida solo por su titular que debe mantenerla en secreto, e incluso puede ocurrir que ni siquiera el titular conozca la clave privada, que probablemente se mantendrá en una tarjeta inteligente, o se podrá acceder a ella mediante un número de identificación o, mediante un dispositivo de identificación* biométrica[36]*; y una clave pública o clave de verificación, matemáticamente relacionada con la primera y libremente accesible por cualquier persona."* [37]

Por lo tanto esto se refiere a que la criptografía asimétrica usa dos claves, una para encriptar y otra para desencriptar, relacionadas de forma matemática de tal modo que los datos encriptados por una de las dos solo pueden ser desencriptados por la otra. Cada usuario tiene dos claves, una pública y otra privada pero solo se distribuye la primera.

El diseño y procedimiento en forma segura de un criptosistema asimétrico hace virtualmente imposible que las personas que conocen la clave pública puedan derivar de ella la clave privada.

---

[36] Biométrica, es un sistema en el cual a través de la identificación de la retina o huella digital, se produce la autentificación de los entes involucrados en las transacciones u operaciones. www.cybertesis/tesis/uchile/2003/maulen_i/html/index

[37] Martínez Nadal, Apol-Lonia, La Ley de Firma Electrónica, segunda edición, Editorial Civitas, Madrid(España), 2001, Pág 51 y 52.

La desventaja de este método es su lentitud para encriptar grandes volúmenes de información. En comparación al sistema simétrico, es cien veces más lento; a pesar de esta desventaja el sistema asimétrico es uno de los más seguros que existe actualmente.

Para la encriptación asimétrica se utilizan algunos algoritmos como: El algoritmo RSA. Lo importante de éste método es que es el mas usado actualmente. Para que sea seguro, la longitud de sus claves debe ser de 1024 bits, es decir un número de un poco más de 300 dígitos; lo que la hace ser indescifrable.

"El RSA emplea las ventajas proporcionadas por las propiedades de los números primos cuando se aplica sobre ellas operaciones matemáticas basadas en la función "Modulo". La robustez del algoritmo se basa en la facilidad para encontrar dos números primos grandes frente a la dificultad que presenta la factorización de su producto."[38]

"Otro algoritmo reconocido es el DSA, que significa Digital Signatura Algorithm, que es aceptado para las transacciones oficiales en el gobierno de los Estados Unidos. Este método usa también claves del mismo tamaño que RSA, pero está basado en otra técnica, la cual es la función exponencial del algoritmo discreta en un campo de elementos finito, la cual tiene la característica de ser difícilmente

[38] www.cne.es/firmadigital/seguro/sisicne1/index1.asp

reversible."[39] Este algoritmo fue propuesto por el U.S National Institute of Standard and Technology (NIST).

2.2.2.1 PROCEDIMIENTO DEL SISTEMA ASIMÉTRICO.

En este sistema cuando se aplica la clave privada del emisor sobre el mensaje, a efectos de firma, y se verifica éste por el destinatario con la clave pública de aquel y se obtiene un resultado positivo, se tiene la garantía de la autenticación e integridad del mensaje, así como del no repudio del mismo, ya que el mensaje verificado con la clave pública solo puede haber sido firmado con la clave privada que se atribuye a un solo titular, por lo tanto se dice que es autentica, y que dicho mensaje no ha sido cambiado en su transcurso, es decir que el mensaje está íntegro; y finalmente el emisor del mensaje no puede negar ser el autor de ese mensaje, y en esto se verifica la característica del no repudio.(VER ANEXO 2).

"El procedimiento de este sistema asimétrico es mas complicado ya que entra a formar parte un elemento nuevo: la función de HASH, que es un algoritmo que transforma una secuencia de bits en otra menor y que se aplica tanto para la creación como para la verificación de la firma digital."[40]

[39] Op. Cit. Pág 51
[40] Op. Cit. Martínez Nadal. "La Ley de Firma..." Pág 52 y 53

Debido a que la aplicación de la criptografía asimétrica sobre la totalidad del mensaje puede resultar costosa, especialmente si este es muy extenso, se aplica sobre el mensaje inicial con función de HASH, usualmente 128 ó 254 bits donde se obtiene un resumen del mismo. El resumen es cifrado con la clave privada del firmante y en último lugar ambos mensajes, el inicial y el resumen cifrado, son remitidos conjuntamente al destinatario.

"Finalmente, el receptor que cuenta con los dos elementos -el mensaje inicial y el resumen cifrado- debe proceder a la verificación de la firma. La verificación de la firma digital es el proceso de comprobación de ésta con referencia al mensaje original y a una clave pública dada, determinando de esta forma si la firma digital fue creada para este mismo mensaje utilizando la clave privada que corresponda a la clave pública. Para ello el verificador realizará dos operaciones descifrará el HASH firmado con la clave privada del emisor aplicando la clave pública del mismo, y aplicará la función de HASH sobre el mensaje completo que ha obtenido. Si el HASH recibido y descifrado y el segundo HASH obtenido coinciden, el destinatario tiene la seguridad de que el mensaje recibido ha sido firmado por el emisor con ese contenido."[41]

Para un mejor entendimiento de este sistema, planteamos el siguiente ejemplo:

[41] Op. Cit. Martínez Nadal. "La Ley de Firma..." Pág 53

Ana y Bernardo tienen sus pares de claves respectivas cada uno, es decir una pública y una privada. Ana escribe un mensaje a Bernardo, es necesario que Bernardo pueda verificar que realmente es Ana quien ha enviado el mensaje, por lo tanto Ana resume el mensaje original mediante una función HASH, cifra el resultado de la función HASH con su clave privada, y lo envía a Bernardo junto con el mensaje original. Bernardo recibe el mensaje original junto con el resumen cifrado, éste deberá comprobar su validez para dar por bueno el mensaje y reconocer al autor del mismo. Es así que descifra el resumen del mensaje mediante la clave pública de Ana, que ha sido proporcionada previamente por la Entidad Certificadora; aplica al mensaje original recibido la función HASH para obtener el resumen. Luego, compara el resumen recibido con el obtenido a partir de la función HASH, si son iguales Bernardo puede estar seguro que quien ha enviado el mensaje es Ana y que este no ha sido modificado.

En el momento en que Bernardo introduce la clave pública de Ana y se descifra el resumen, se considera que se materializa la firma digital, por la correspondencia entre las claves de Ana que da como resultado el resumen descifrado, de conformidad con lo establecido en el Art. 8 inc. 3 de la Ley de Simplificación Aduanera.

Podemos concluir que la criptografía contribuye a la seguridad de las transacciones comerciales, en una red abierta e insegura como Internet. Los criptosistemas de clave asimétrica son la mejor solución a la necesidad jurídica de autenticación, integridad y no rechazo del mensaje electrónico, a través de los

procedimientos de firma digital, y a la vez cumpliendo con la confidencialidad mediante los procesos de cifrado.

Con la criptografía se resuelve una parte del problema de seguridad en las transacciones del comercio electrónico. Por otro lado, se presenta el problema del rechazo en destino en comunidades amplias, ya que la criptografía no garantiza el vínculo entre la clave pública y el titular de la clave privada, es aquí donde surge la necesidad de una nueva entidad: una tercera parte de confianza, cuya actuación será fundamentalmente asegurar el vinculo entre la clave pública y el titular de la clave privada, así como otras funciones tales como: autenticar horas y fechas de determinadas acciones y transacciones y publicar electrónicamente las claves privadas que ya no son de confianza.

2.3 ENTIDADES DE CERTIFICACIÓN.

Cuando una parte contratante desea verificar la firma digital generada por la otra parte, la parte verificadora necesita una copia de la clave pública de la parte firmante y necesita tener la certeza de la correspondencia entre la clave pública y privada y que estas corresponden a una persona determinada. Este problema se resuelve con los certificados de clave pública emitidos por una autoridad de certificación que actúa como tercera parte de confianza de la parte firmante y de la parte verificadora.(VER ANEXO 3).

Una entidad certificadora es *"la encargada de emitir certificados digitales de las solicitudes que cumplan con los requisitos para su obtención. Realiza además funciones de revocación, publicación, almacenamiento y registro de certificados. Se constituye un tercero confiable para las partes involucradas en una transacción electrónica"*[42]

Las entidades de certificación son una pieza fundamental en el desarrollo del Comercio Electrónico, pues son los que brindan certeza sobre el autor y contenido de un mensaje de datos, y por lo mismo de ellas depende el desarrollo de este tipo de canales de comunicación dentro de un marco de seguridad jurídica esencial para la proliferación del comercio por esta vía.

2.3.1 GENERALIDADES DE LAS ENTIDADES DE CERTIFICACIÓN.

2.3.1.1 DEFINICIÓN DE ENTIDAD DE CERTIFICACIÓN.

La terminología utilizada para referirse a las terceras partes de confianza es muy variada, desde la expresión autoridad, proveedor de servicios, prestador de servicios de certificación, entidad certificadora o simplemente certificador.

En nuestro caso, adoptamos la expresión de entidades de certificación por su apariencia neutral.

[42] Op. Cit. Barceló. Pág 332

Existe una amplia gama de definiciones de entidades de certificación, para referirnos a ellas retomamos a algunos autores:

"La entidad certificadora es un organismo dedicado a la emisión de certificados que contiene información sobre algún hecho o circunstancia del sujeto del certificado, en los casos de los certificados de clave pública, son certificados que vinculan un par de claves con una persona determinada de forma segura, cubriendo así la necesidad de servicios de terceras partes de confianza en el comercio electrónico de los tenedores de pares de claves asimétricas."[43]

Otra definición de entidades de certificación es: *"Cualquier entidad de confianza de las partes intervinientes en una transacción para proporcionar servicios de seguridad; aquella específica tercera parte de confianza que desempeña de forma fundamental la función de emisión de certificados."*[44]

También podemos definir las entidades de certificación como: *"La persona física o jurídica, pública o privada, que expide, renueva y revoca certificados, pudiendo prestar, además, otros servicios en relación con la firma digital, como la validación de certificados."*[45]

[43] Op. Cit. Martínez Nadal, "Comercio electrónico..." Pág 149
[44] Op. Cit. Martínez Nadal. "La Ley de Firma..." Pág 100
[45] www.hfernandezdelpech.com.ar/leyes/trab/firma%20digital.deusto%202002.htlm

Nosotras como grupo podemos concluir que, la criptografía necesita de una tercera parte de confianza, es decir, una entidad certificadora que debe realizar la vinculación de una persona debidamente identificada con un par de claves determinadas y para ello necesita de una regulación que la controle y determine su responsabilidad, ya que para asociar un par de claves con un probable firmante, una entidad de certificación emite un certificado que liga una clave pública con el sujeto del certificado, y confirma que el probable firmante identificado en el certificado tiene la correspondiente clave privada.

2.3.1.2 IMPORTANCIA DE LAS ENTIDADES DE CERTIFICACIÓN.

Por la creciente participación de los negocios por medios electrónicos, es indispensable la creación y fundamentación de las entidades de certificación, ya que los negocios aumentan progresivamente y es necesario establecer una estructura que brinde confianza a las transacciones, no solo desde el punto de vista técnico sino también jurídico.

Es por eso que las entidades juegan un papel definitivo tanto para brindar seguridad en la red, como para asegurar la confianza en el mundo físico, respecto a algunos de los actos que tengan efectos jurídicos que en ella se den. *"Esto significa para un pequeño empresario que podrá realizar convenios y transacciones comerciales sin necesidad de viajar fuera del país e incluso sin moverse de su puesto de trabajo, pues*

todas las operaciones las podrá realizar desde su computadora. Obtendrá la seguridad de que conoce la identidad de aquel con quien está negociando, tendrá certeza de que el documento enviado no ha sido manipulado, ni alterado y una vez la otra persona recibe el mensaje, este hecho no podrá ser negado."[46]

Estas entidades de certificación se han convertido en una base importante para el comercio electrónico, ya que permiten conocer a los emisores de una oferta y aceptación de actos jurídicos y las partes intervinientes en un contrato. Permite además evitar que se cometan fraudes por falsificación de identidad o que se caigan en errores contractuales por falta de personería jurídica.

Estas entidades de certificación proveen seguridad al comercio electrónico, basado en la confianza y la honorabilidad que garantizan estas entidades.

Las entidades de certificación, por el vínculo que tienen en la transmisión de los mensajes de datos, llegan a ser parte fundamental de la estructura comercial, ya que son las que brindan precisión sobre el autor y contenido de un mensaje de datos, así mismo de ellas depende el desarrollo de canales de comunicación seguro en ésta era de aumento del comercio electrónico. *"Constituye además una especie de fedatario ya que se*

[46] Guerrero, María Fernanda. El notario virtual de los negocios en línea. Revista Ámbito Jurídico. Bogota, Colombia, Abril 2001. Pág 12

convierte en un tercero disipador de conflictos al determinar la originalidad y autoría de los mensajes de datos.''[47]

2.3.1.3 BASES DEL SISTEMA DE CERTIFICACIÓN.

El sistema de certificados ha de basarse en una serie de puntos esenciales, que son los siguientes:

- La vinculación de forma segura de una clave pública a una persona determinada es el papel central de toda entidad de certificación, que debe responder por esta actuación, y la función esencial de todo certificado.

La importancia de la correcta identificación del solicitante, es que en algunos casos ésta es defectuosa y puede llegar a darse la existencia de firmas falsas por suplantación de la persona del solicitante del certificado por parte de un tercero.

- El control de la correspondiente clave privada por parte del titular del certificado al que se ha vinculado con una determinada clave pública es también esencial para evitar supuestos de falsificación de firma por utilización no autorizada por parte de terceros en caso de pérdida y robo de la clave de firma.

[47] Op. Cit. Cubillos Velandia, Pág 257

De aquí deriva la importancia de una existencia de sistemas de revocación que permitan comunicar que una determinada clave deja de estar vinculada, y por tanto, no le son ya atribuibles los mensajes firmados con la misma.

- La existencia de sellos temporales digitales de confianza es esencial para el correcto funcionamiento, fundamentalmente, para determinar el momento de creación de mensajes electrónicos durante el período de validez del certificado.

- El sistema de certificados debe estructurarse, dada la naturaleza transfronteriza del comercio electrónico, de forma tal que sean a través de una adecuada jerarquización de las autoridades de certificación.

Es decir que existe un reconocimiento general de los certificados. Solo de ésta forma y teniendo en cuenta éstas bases se podrá conseguir un sistema útil, eficaz y seguro, y por lo tanto la tecnología de firma digital con la adecuada infraestructura legal e institucional, puede ser una alternativa poderosa de base informática a las firmas tradicionales.

2.3.1.4 NATURALEZA JURÍDICA DE LAS ENTIDADES DE CERTIFICACIÓN.

La naturaleza de las entidades de certificación está abierta de acuerdo a la legislación en la que radique, así podrán ser públicas o privadas, y su funcionamiento estar sometido a una autorización o ser de libre constitución.

Se señala como una ventaja el hecho de que la entidad de certificación sea pública, ya que su objetivo es el beneficio de la comunidad y por ende un mejor servicio.

Estas entidades de certificación pueden desempeñar funciones más importantes en el comercio electrónico en el país, como por ejemplo, ser la entidad de certificación raíz del Estado, certificando a las entidades de certificación privadas e inclusive a las públicas de menor jerarquía. Se presume que una administración o una entidad pública actuará en función del interés público, además de ser más estable que las privadas.

"Las autoridades de certificación públicas pueden desempeñar distintos papeles: pueden actuar como autoridad de certificación raíz de la estructura de autoridad de certificación de un país, certificando al resto de autoridades de certificación comerciales, o bien pueden actuar como autoridades de certificación para los ciudadanos, únicamente para las relaciones administrador-administrados."[48]

[48] Op. Cit. Martínez Nadal, "Comercio Electrónico..." Pág 151

Resulta lógico que para que una entidad de certificación pública funcione adecuadamente es necesario que el Estado tenga la voluntad de incorporar esa tecnología al organismo público que asuma esas funciones de certificadora, o delegarlas a algún organismo que cuente con la infraestructura y sea capaz de asumir esa responsabilidad.

Las autoridades de certificación pueden ser entidades privadas, dependiendo de la legislación en cada país. Una empresa privada fundamentalmente buscaría el lucro y se trata de un régimen de competencia en el que de acuerdo a la calidad de sus servicios pueden ampliar el número de usuarios de sus certificados, dependiendo de la seguridad que les ofrezca.

"Dentro de las funciones de las entidades privadas tenemos que pueden dedicarse a la certificación ofreciendo ese servicio a terceros como parte de su actividad empresarial principal, o bien únicamente de forma complementaria a esa actividad o a efectos internos puramente organizativos."[49]

Para que una empresa privada se constituya como entidad de certificación es necesario que cumpla con los requisitos que la ley ha previsto para garantizar la seguridad a los usuarios del comercio electrónico. Estos requisitos están consignados en las normas que regulan la prestación de estos servicios en cada país.

[49] Op. Cit. Martínez Nadal, "Comercio Electrónico..." Pág 151

2.3.1.5 REQUISITOS DE LAS ENTIDADES DE CERTIFICACIÓN.

Para que una entidad certificadora pueda considerarse confiable debe cumplir una serie de requisitos fundacionales, así como otros requisitos posteriores de funcionamiento que genera una confianza y seguridad en su organización y actividades. En la medida que la empresa certificadora cumpla con todos los requisitos exigidos tendrá mayor solidez ante la vista del usuario de que otra certificadora solo cumpla con algunos de ellos.

Doctrinariamente se logra un consenso sobre los requisitos que deben cumplir las entidades certificadoras; clasificándolas básicamente de la forma siguiente:

- Requisitos técnicos:

  Estos consisten en la utilización de sistemas seguros y de confianza por parte de la Autoridad de Certificación para el desarrollo de sus actividades. Por ejemplo, para emitir, suspender o revocar un certificado, publicar o dar noticia de la emisión, suspensión o revocación de un certificado, o para crear o salvaguardar su propia clave privada.

- Requisitos de personal:

  El personal que labora en la autoridad certificadora debe ser competente desde el punto de vista de gestión, técnica y confianza. El personal que tiene acceso a las

operaciones criptográficas, emisión, suspensión o revocación de los certificados digitales deberá someterse a una investigación inicial para determinar si puede acceder a una posición de confianza, con la finalidad de proporcionar seguridad y confiabilidad a sus usuarios.

- Requisitos financieros:

Es necesario que la entidad certificadora cuente con un capital base que servirá para desarrollar el negocio y para afrontar eventuales responsabilidades por daños, por error o negligencia, o como consecuencia de cualquier acción u omisión de la Entidad Certificadora.

- Auditoria:

Para mostrar la fiabilidad de la autoridad de certificación deberá someterse a una Auditoria.

- Documentación de actividades:

La documentación de actividades es indispensable para la actuación de una autoridad de certificación digna de confianza. Esta debe ser capaz de probar sus propias operaciones y actuaciones en el futuro. La documentación debe ser conservada durante un periodo adecuado, el cual debe estar fijado en el contrato de prestación

de servicios, la practica o incluso en la ley, y el cual puede ser variado de acuerdo a la necesidad del usuario.

- Planes de contingencia y de recuperación frente a desastres:

La entidad certificadora debe estar preparada ante la posibilidad de una paralización del funcionamiento de sus sistemas, lo cual de no poseer dichos planes acarrearía graves consecuencias para los usuarios de los certificados.

- Finalización de actividades con los mínimos perjuicios a sus usuarios:

Cuando una entidad certificadora finaliza sus actividades, es decir, que cesará en la prestación de sus servicios, deberá avisar anticipadamente a sus clientes a fin de evitarles perjuicios, a la vez que puede ofrecerles traspasar sus actividades a otra entidad certificadora previamente calificada.

2.3.1.6. OBLIGACIONES DEL PRESTADOR DE SERVICIOS DE CERTIFICACIÓN.

Como hemos citado anteriormente las bases y requisitos de las Entidades de Certificación, es el momento de hablar de las obligaciones que tiene en su rol de prestador de servicios de certificación.

Entre estas exigencias enfatizaremos el hecho de controlar en todo caso y en todo momento la fiabilidad del certificado, identificando a quien se le va a otorgar, y una vez otorgado, manteniendo un registro de los certificados emitidos y poniendo a disposición de los signatarios los dispositivos de creación y verificación, y no almacenar ni copiar los datos de creación de firma de la persona a la que hayan atendido.

Otras obligaciones están inclinadas a garantizar los certificados, en cuanto al contenido, tiempo, día y hora de emisión, además, emplear personal calificado y utilizar sistemas y productos viables para que se garantice las medidas de seguridad contra la falsificación de certificados.

Estas obligaciones se complementan con el deber que tiene el prestador de servicios de certificación de disponer de recursos económicos para afrontar el riesgo de la responsabilidad por daños y perjuicios.

2.3.1.7. RESPONSABILIDAD DE LAS ENTIDADES DE CERTIFICACIÓN.

La responsabilidad de las entidades certificadoras al desarrollar una verdadera vocación de servicio al público, debe adoptar la figura del buen padre de familia, respecto a la ejecución misma de su labor, de modo que todo incumplimiento por parte de la entidad se convierta en culpa o falla en la prestación del servicio, y por ende sea una causal de responsabilidad. Es decir, que el prestador de servicios de certificación

responde por los daños y perjuicios causados en el ejercicio de su actividad, con independencia de si su actuación fue diligente o negligente, o sea, que si el prestador de servicios tendrá que responder no solo en el caso de que se haya debido a la negligencia de sus empleados –por ejemplo, no exigieron el documento acreditativo de la identidad del titular- sino que el error se haya producido pese a haber actuado con diligencia; pero esto no quiere decir que el proveedor de servicios no será responsable si puede demostrar que no ha sido negligente, por ejemplo, probando que ha tomado medidas razonables para evitar errores en el certificado reconocido.

" Es por ello que se puede aplicar la responsabilidad objetiva, es decir, un régimen en el cual no se analiza al sujeto responsable (caso de responsabilidad subjetiva), si no exclusivamente a los hechos, sin entrar a examinar la condición subjetiva del agente".[50]

Tomando los dos supuestos de responsabilidad – objetiva y subjetiva – y teniendo en cuenta las dificultades que para el usuario de un certificado puede suponer la prueba de la negligencia de la entidad certificadora, se establece la carga de la prueba para las entidades certificadoras.

Una segunda responsabilidad está dada por su naturaleza contractual o extracontractual. La entidad certificadora tiene como obligación establecida el contrato

[50] Op. Cit. Cubillos Velandia, Pág 296

mismo, y como accesoria a éste la de dar información y por lo tanto en caso de incumplir con cualquiera de éstos, produciría una responsabilidad para la entidad certificadora; por desarrollar éstas el principio de buena fe, el cual incluye no sólo el tener la convicción por parte del contratante de actuar adecuadamente, si no que además implica el desarrollar aquellas actividades que el co-contratante requiera para que se dé cabal cumplimiento al objeto del contrato.

Por la evolución de la responsabilidad contractual se ha generado un debilitamiento en la autonomía de la voluntad ya que las empresas incluyen en sus contratos cláusulas exonerativas de responsabilidad. De tal manera que en caso de controversia de un contrato que incluya este tipo de cláusulas, el juez está en la obligación de analizar el fondo del contrato y determinar cuales son las obligaciones del mismo, y en caso de ser necesario deberá obviar la existencia de dichas cláusulas, si en virtud de ellas, la entidad certificadora está contraviniendo una obligación que pertenece a la naturaleza misma del contrato.

Como consecuencia de lo anterior el juez le otorga al contrato una serie de obligaciones que aunque no se encuentren presentes dentro del mismo deberían haber estado, son obligaciones implícitas a la ejecución del contrato mismo.

En conclusión, respecto a la responsabilidad contractual se debe en principio acudir al contenido estricto del instrumento, entendiéndose que dicho contenido incluya

las obligaciones esenciales y las obligaciones accesorias necesarias para el cumplimiento del mismo, de modo que si éste no las contiene deberán hacerse valer, en razón de la justicia, por tratarse de obligaciones implícitas a la ejecución del contrato.

2.4. ENTIDAD CERTIFICADORA SALVADOREÑA CERTICAMARA.

Desde Enero de 2002, existen mas de doscientos cincuenta usuarios realizando transacciones reales por Internet con la Dirección General de la Renta de Aduanas de El Salvador (Envío de la declaración de mercancía y póliza por Internet), agilizando en gran medida el procesamiento de información para la importación de mercadería. Los principales usuarios son empresas de courier, agencias aduanales, maquilas y empresas industriales.

Para la implementación de este proyecto, el rol de DIESCO EAN-El Salvador, fue decisivo tanto para el desarrollo de la plataforma tecnológica y operativa de TELEDESPACHO como por los servicios cerrados de emisión de certificados digitales a través de su Autoridad Certificadora CERTICAMARA. Esta entidad certificadora nace jurídicamente con el Decreto Legislativo Numero 523 del 30 de Agosto de 2001 publicado en el Diario Oficial Numero 353, del 5 de Octubre de 2001,de Reformas a la Ley de Simplificación Aduanera, con el que se autoriza el funcionamiento de entidades certificadoras y la prestación de servicios de certificación para el sistema de Teledespacho; es decir para el sistema de certificación cerrada, en el cual el certificado es válido únicamente para transacciones con la Dirección General de Rentas y Aduanas.

Para el sistema de Teledespacho por Internet, se ha implementado el uso de la firma digital y certificados digitales, con el objetivo de asegurar las transacciones electrónicas de dicho proyecto. Estos mecanismos aseguran el envío y la recepción de la información, ya que el emisor al firmar el documento electrónico y validarlo con su certificado digital, está dotando a dicho documento de la característica de seguridad. Esto le da certeza al receptor de que quien firma y envía es quien dice ser, adicionalmente este mensaje se codifica para que viaje por Internet en un lenguaje en que solo las partes involucradas podrán entenderlo.

Cabe aclarar que por el momento los certificados digitales emitidos por Certicamara solo certifican al usuario, no la información y su uso es únicamente para Teledespacho por Internet, es decir, tramites de importación por Internet con la Dirección General de la Renta de Aduanas.

Las prácticas realizadas por Certicamara, han sido elaboradas en el contexto de la declaración de prácticas de certificación a que se refiere el proyecto de régimen uniforme para las firmas digitales, en relación con la Ley modelo sobre comercio electrónico, elaboradas por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional y su finalidad es constituirse en el mecanismo formal de difusión y comunicación, para con los titulares de un certificado digital emitido por Certicamara, así como para con cualquier persona que pretenda usar y confiar en dichos certificados.

Certicamara es una autoridad certificadora de carácter privado y los certificados que emite son utilizados para el sistema de Teledespacho por Internet, facultad otorgada por el Ministerio de Hacienda, quien a su vez actúa como autorizador, fiscalizador y sancionador de la entidad certificadora, conforme lo preescrito en el Art. 8 de la Ley de Simplificación Aduanera.

La finalidad de los servicios ofrecidos por Certicamara, es constituirse en un tercero de confianza para las partes involucradas en una transacción electrónica con la aduana, creando de esta manera un marco de seguridad jurídica y tecnológica para sus usuarios.

- SERVICIOS

Dentro de los servicios de certificación digital prestados por Certicamara, se encuentran:

- Emisión de certificados: ya sea que se trate de personas naturales o jurídicas.
- Revocación de certificados: se da por terminada la vigencia de un certificado anticipadamente, cuando el titular así lo desee, o cuando concurra alguna causal de revocación.

- Publicación de certificados: los certificados digitales emitidos deben ser publicados en un directorio, de manera que terceros interesados puedan acceder a ellos.
- Almacenamiento de certificados: por seguridad, los certificados emitidos y la lista de revocados, son almacenados por un período determinado de tiempo debido a que el documento firmado digitalmente, puede poseer un período de validez o vigencia mas amplio que el del certificado utilizado para firmar.

- TECNOLOGÍA UTILIZADA

La tecnología aplicada en los productos utilizados por Certicamara han sido creados utilizando el mas alto nivel de criptografía, siguiendo el modelo de criptografía de clave pública mas reconocido y utilizado a nivel internacional, RSA. Con la implementación de esta tecnología, Certicamara ofrece a sus clientes el mas alto nivel de seguridad, consistentes en claves RSA de hasta 2048 bits de extensión y claves simétrica de 128 bits de longitud. Las claves privadas se generan y almacenan en dispositivos de seguridad que cumplen con las especificaciones internacionales.

- GENERACIÓN DE CLAVES

La generación de las claves publica y privada necesarias en la emisión de un certificado digital, se realiza bajo el absoluto control de quien será el titular de dicho

certificado y es de exclusiva responsabilidad de éste, el tomar las medidas de seguridad que considere necesarias para el resguardo de la clave privada y su respectiva contraseña de acceso.

- USO Y VERIFICACIÓN DE CERTIFICADOS

Gracias a la tecnología que sustenta la prestación de los servicios de certificación digital que ofrece Certicamara, el cliente puede tener la confianza que su certificado digital lleva impreso confidencialidad, autenticidad, integridad y no repudiación de la información que envíe o reciba a través de medios electrónicos. La responsabilidad sobre la adecuada utilización, alcance y repercusión en el uso de un certificado digital, recae exclusivamente sobre el titular del mismo.

- USO Y PUBLICACIÓN DE LA BASE DE DATOS

La información proporcionada por los usuarios de los servicios de certificación y la proporcionada por los titulares de los certificados digitales, no será revelada, compartida, rentada o vendida a terceras personas o empresas, bajo ninguna circunstancia.

Certicamara se reserva el derecho de revelar información, sin autorización del titular, cuando sea necesario para identificarlo, contactarlo o ejercer cualquier acción legal en su contra, o en caso de que alguna autoridad jurisdiccional o administrativa facultada para exigir dicha revelación, se lo solicite expresamente.

- CONTROLES DE SEGURIDAD

Para la prestación de los servicios de certificación digital, y en la emisión, administración, almacenamiento y revocación de certificados digitales, Certicamara cuenta con tecnología, mecanismos y procedimientos de seguridad del mas alto nivel, los cuales son revisados y actualizados con cierta regularidad. La seguridad es revisada y evaluada en términos de instalaciones físicas, de telecomunicaciones, de hardware, de software y de personal.

- GARANTIAS

Certicamara otorga garantías respecto a los certificados digitales emitidos, pero aplican única y exclusivamente a los usuarios y titulares de los mismos, más no incluye a cualquier otro tercero participante. Responderá en razón del tipo de certificado de que se trate, lo cual analizaremos al referirnos a los certificados digitales.

- RESPONSABILIDADES

Certicamara no ofrece garantía expresa ni tácita sobre sus servicios de certificación digital y no será responsable por los daños o perjuicios que sufran sus usuarios, cuando éstos se deriven de la mala utilización de los servicios o por la presentación de documentación falsa por parte del usuario.

En los casos en que Certicamara tendrá responsabilidad, ésta estará delimitada por las consecuencias legales y económicas que deriven del cumplimiento o incumplimiento de los requisitos establecidos para los distintos procesos y niveles de certificación.

- EXCLUYENTES

  Certicamara reconoce como excluyentes de responsabilidad las siguientes causas:

  - Cuando el daño o perjuicio se derive de la mala o indebida utilización de los servicios de certificación digital por parte de los usuarios finales; de la mala o incorrecta interpretación, análisis, síntesis o conclusión a que los usuarios finales lleguen en el uso de dichos servicios, e incluso si el solicitante de un certificado digital aporta datos o documentos falsos para la obtención de dicho certificado.
  - Cuando la interrupción o alteración temporal de los servicios de certificación sean por causas ajenas a su voluntad, fuerza mayor o caso fortuito, propiciada por condiciones climatológicas adversas, fallas en la energía eléctrica, fuego, actos vandálicos, huelga o cualquier otro motivo similar que afecte sus instalaciones, así como por errores, omisiones o negligencia que afecten las instalaciones de transmisión, enlace y bases de repetición de los proveedores de telecomunicaciones de Certicamara.

- Cuando la interrupción temporal del servicio sea ocasionada por acciones gubernamentales que coarten o restrinjan la libertad en las telecomunicaciones civiles o que impidan su transmisión privada o incluso, por cualquier otro motivo de naturaleza análoga.

- SOLUCION DE CONFLICTOS

Cualquier controversia que se suscite entre Certicamara y sus usuarios, se resolverá a través de la negociación entre sus representantes comerciales. Si no logra resolverse por este medio, se someterá a un arbitraje de derecho en El Salvador. Las reglas del arbitraje serán las del Centro respectivo de la Cámara de Comercio e Industria de El Salvador, o si no existiere, las reglas que contiene el reglamento de la UNCITRAL.

Los costos y honorarios razonables relacionados con el procedimiento arbitral serán cubiertos por ambas partes conjuntamente y por montos iguales.

2.5. CERTIFICADOS DIGITALES.

Al establecer la existencia de las entidades certificadoras y las funciones de éstas, podemos decir que para garantizar que una llave pública le pertenece a cierta entidad, se emite un documento electrónico denominado Certificado Digital, en el cual aparecen una serie de datos de la entidad, como el nombre que la identifica, etc. La autenticidad

de estos datos es asegurada, pues la entidad certificadora anexa en el mismo certificado su propia firma digital.

Así, podemos decir que las entidades certificadoras son terceros de confianza que, cumpliendo con determinados requisitos son reconocidos y autorizados para emitir un certificado digital que identifique a una persona o una entidad; pero no solamente emite los certificados, sino que también se ocupa de la gestión de los mismos, de forma que los puede revocar y renovar cuando se den determinadas circunstancias. Por lo tanto podemos definir a los Certificados Digitales como *"documentos digitales emitidos por un prestador de servicios de certificación, que dan fe de la vinculación entre una clave pública y una persona física o jurídica. Son como un documento de identidad electrónico que garantizan en Internet la identidad de las personas físicas o jurídicas."*[51]

Doctrinariamente podemos definir al Certificado Digital – también conocidos como Identificador Digital – como *"un documento electrónico, emitido por una autoridad de certificación reconocida, que asocia una clave pública con una persona, entidad, empresa u organización determinada; la autoridad de certificación, antes de emitir un certificado, realiza una serie de comprobaciones para asegurarse de que la persona a la que va a otorgar el certificado es quien dice ser."*[52]

[51] Op. Cit. Pág 51
[52] Op. Cit. "Escuela Judicial..." Pág 171

"Para la realización de los certificados digitales se tiene un formato estándar que se ha extendido para todas las aplicaciones, este es el llamado X.509. Este formato contiene los datos del poseedor del certificado, la clave pública del propietario, y la firma de una autoridad certificadora. La mejor propiedad del formato X.509 es que contiene el mínimo necesario de información para realizar muchas transacciones principalmente comerciales y financieras."[53] La existencia de estos certificados es lo que precisamente garantiza la identidad, integridad, la confidencialidad y la garantía del envío o el no repudio de la firma digital.

En cuanto a cuál sea su contenido, un certificado puede contener una amplia gama de informaciones, por lo tanto, los requisitos mínimos que debe contener son:

a) La identificación del signatario, por su nombre y apellido o a través de un seudónimo que conste como tal de manera inequívoca. Se podrá consignar en el certificado cualquier otra circunstancia personal del titular, en caso de que sea significativa en función del fin propio del certificado y siempre que aquél de su consentimiento.
b) La clave pública atribuida que ha de corresponderse con una clave privada que esté bajo el control del titular, es decir, un elemento de verificación de firma que se corresponda con un elemento de creación de firma bajo el control del titular.
c) Los algoritmos con los que firman el titular del certificado y la autoridad de certificación.

[53] ww.zonavirus.com/datos/articulos/44/firma_digital_certificados_digitales.asp

d) El número del certificado, que debe ser único, de forma que dos certificados distintos de una misma autoridad de certificación no tengan el mismo número.
e) El comienzo y el fin del período de validez del certificado, el certificado debe tener una vida limitada, en la práctica, los certificados que emite Certicámara tienen una vida útil de un año, finalizada ésta debe dejar de confiarse en el mismo.
f) La identificación del prestador de servicios de certificación que expide el certificado, indicando su nombre o razón social, su domicilio, su dirección de correo electrónico y su número de identificación fiscal.
g) La firma digital del prestador de servicios de certificación que expide el certificado.
h) Información de si el uso de una firma está limitado a específicos tipos y objetivos de aplicación.
i) Los límites del valor de las transacciones para las que puedan usarse los certificados, si se establecen.
j) En los supuestos de representación, la indicación del documento que acredite las facultades del signatario para actuar en nombre de la persona física o jurídica a la que representa.

Recapitulando, podemos decir que la misión fundamental de los certificados es permitir la comprobación de que la clave pública de un usuario pertenece realmente a ese usuario, ya que así lo hace constar el certificado de una entidad que da fe de ello.

Las entidades de certificación ofrecen tres niveles de certificados. Cada nivel o clase de certificado provee servicios específicos en cuanto a funcionalidad y seguridad; los interesados eligen entre estos grupos de servicios el que mas le conviene, según sus necesidades. Cumplidos los requisitos exigidos, se emite el certificado.

2.5.1. CERTIFICADO NIVEL 1.

Esta clase de certificados son emitidos y comunicados electrónicamente a personas físicas, y relacionan en forma indiscutible el nombre del usuario o sus "alias" y su dirección de e-mail con el registro llevado por Verising[54]. No autentican la identidad del usuario. Son utilizados fundamentalmente para Web Browsing y Correo electrónico, garantizando la seguridad de sus entornos. En general no son utilizados para uso comercial, donde se exige la prueba de identidad de las partes.

Para Certicamara los Certificados Nivel Uno son certificados personales para e-mail, su valor legal deriva del contrato entre las partes y se emiten por instrucción o bajo la responsabilidad de la entidad interesada.

Son emitidos con el único fin de facilitar la transmisión de información entre partes que utilizan Internet y desean un entorno mas seguro en el envío y recepción de mensajes, básicamente por medio de correo electrónico. La seguridad que proporciona

[54]Verising, es una de las empresas que brinda servicios de certificación. Estos servicios han sido diseñados básicamente para brindar seguridad al comercio electrónico y a la utilización de la firma digital. Op. Cit. Pág 59

solo está referida a la confirmación del nombre de una persona y la dirección de correo electrónico con la que esa persona ha sido vinculada. Ambos elementos constituyen el único objeto de validación que Certicamara le reconoce.

2.5.2 CERTIFICADO NIVEL 2.

Los certificados nivel dos son emitidos a personas físicas y confirman la veracidad de la información aportada en el acto de presentar la aplicación y que esta no difiera de la que surja de alguna base de datos de usuarios reconocida. Es utilizado para comunicaciones intra-inter organizaciones vía e-mail, transacciones comerciales de bajo riesgo, validación de software y suscripciones on-line.

Certicamara define a los certificados nivel dos como certificados personales, su valor legal deriva del contrato entre las partes y se emiten por instrucción o bajo la responsabilidad de la entidad interesada para entornos aplicativos.

Al surgir un proceso de identificación realizado por la entidad solicitante a la que pertenece el titular del certificado, solo poseen la propiedad de autenticar la identidad y facultades de un sujeto determinado en términos de su pertenencia a dicha entidad.

Ya se mencionó anteriormente de las garantías que otorga Certicamara a sus usuarios, pero tratándose de los certificados digitales niveles 1 y 2, Certicamara no

verifica la información suministrada en el requerimiento de certificación por parte de la entidad solicitante o por parte de quien será su titular.

Como consecuencia, Certicamara no es ni será considerada como responsable de la veracidad de cualquiera de los datos contenidos en dicho certificado y quienes pretendan confiar en los certificados digitales niveles 1 y 2 deberán reconocer que sus titulares o la entidad solicitante son responsables por cualquier declaración falsa hecha a Certicamara.

En este sentido, Certicamara no garantiza bajo ninguna circunstancia la no repudiación de las transacciones realizadas por el titular de un certificado nivel 1 y 2, dado que esa circunstancia queda regida exclusivamente por los términos y condiciones que las partes se hayan expresado mutuamente.

2.5.3. CERTIFICADO NIVEL 3.

Estos certificados son emitidos a personas físicas y organizaciones públicas y privadas. En el primer caso, aseguran la identidad del suscriptor; en el caso de las organizaciones, aseguran la existencia y nombre mediante el cotejo de los registros denunciados en los contenidos de la base de datos independientes. Son utilizados para determinadas aplicaciones de comercio electrónico como Electronic banking y Electronic Data Interchange (EDI).

En Certicamara los certificados nivel tres son certificados personales o jurídicos, con valor legal pleno, cuyos alcances serán explicados en el siguiente capítulo, y son emitidos en un entorno mas seguro y revestidos de ciertos formalismos no solo respecto del proceso de emisión, ya que para ello resulta indispensable la comparecencia personal del titular ante el agente certificador.

Estas formalidades, realizadas en el contexto del marco jurídico existente, proporcionan una mayor seguridad en las transacciones de Comercio Electrónico y garantizan al mismo tiempo la posibilidad de exigir su cumplimiento mediante los procedimientos jurisdiccionales tradicionales.

Tratándose de los certificados digitales nivel tres, la verificación de la información suministrada en el requerimiento de certificación por parte de quien será su titular, será realizada previa autorización de la Aduana y presentación de los documentos antes mencionados.

De igual forma la Cámara de Comercio e Industria de El Salvador, ha presentado una fianza de fiel cumplimiento por el servicio de Certificación Electrónica cerrada a favor del Ministerio de Hacienda.

2.6. REGULACIÓN JURÍDICA DE LA ENTIDAD CERTIFICADORA SALVADOREÑA.

La utilización de sistemas informáticos para el intercambio de información de trascendencia tributaria y la implementación de redes abiertas para dicho intercambio, hace necesaria la adopción de mecanismos de seguridad. Y dentro de este proceso de modernización, el Estado salvadoreño ha dictado disposiciones pertinentes a fin de dar cobertura legal a las nuevas figuras que se han generado en la implementación de Teledespacho y de la entidad certificadora Certicamara, es así que se crea la Ley de Simplificación Aduanera.

Esta normativa tiene por objeto establecer el marco jurídico básico para la adopción de mecanismos de simplificación, facilitación y control de operaciones aduaneras, a través del uso de sistemas automáticos de intercambio de información, de acuerdo al Art. 1 de esta ley.

El Art. 6 de la ley, introduce la declaración de mercancías mediante transmisión electrónica de la información, a lo cual se le denomina Teledespacho, el cual está definido en el inciso 2º del mismo artículo de la siguiente manera: *"conjunto sistematizado de elementos tecnológicos de carácter informático y de comunicaciones que permiten, dentro de un marco de mutuas responsabilidades y mediante los procedimientos autorizados, el intercambio por vía electrónica de información de trascendencia tributaria entre la Dirección General y los usuarios y auxiliares del servicio aduanero, bancos y en general, los operadores e instituciones contraloras del comercio exterior".*

El art. 7 inciso 1º de la ley de Simplificación Aduanera, establece que el intercambio de información que se brinda sobre las mercancías y otros documentos, así como para certificar el pago de lo adeudado por medios informáticos y de la vía electrónica goza de plena validez y produce los mismos efectos jurídicos que los entregados en soporte físico. El inciso 2º del mismo artículo plantea el caso de disconformidad de datos en un mismo documento registrado y presentado en la aduana, lo cual se resuelve considerando como correcto los datos sobre los cuales la entidad certificadora otorga fe publica, o si no, aquel que conste en documento escrito sin ninguna alteración, tachadura o borrón.

El establecimiento de los sistemas de certificación de la información para garantizar la autenticidad, confidencialidad, integridad y no repudio de la misma, está autorizada en el Art. 8 de la Ley, a través de la intermediación de empresas que proveen estos servicios, a los que denomina: Entidades Certificadoras.

Las entidades certificadoras operan bajo la autorización del Ministerio de Hacienda, quien además ejerce funciones de fiscalizador y sancionador, mientras no se dicte una ley específica al respecto.

Las entidades certificadoras que se autoricen para operar, se encargarán de emitir los respectivos certificados que permitan a los usuarios del sistema una interacción

segura en el intercambio de datos, debiendo al efecto proporcionar al usuario una certificación para acceder a la red, según lo establecido en el inciso 4º del Art.8 de la ley.

Las funciones de las entidades certificadoras, se encuentran establecidas en el Art. 8-A de la ley, dentro de las cuales tenemos:

- Ejercer la potestad jurídica de otorgar fe pública en el marco del intercambio electrónico de datos.
- Emisión de los certificados digitales.
- Generar el par de llaves, la pública y la privada, verificando el cumplimiento de los requisitos exigidos, la identidad y capacidad del solicitante.
- Llevar un registro público en línea de los certificados, de manera que cualquier persona interesada pueda acceder al directorio de los certificados emitidos y vigentes.
- Tomar medidas para evitar falsificación de los certificados.

La obligación de secreto y reserva de los datos personales de los titulares de los certificados que emitan, se encuentra regulado en el Art. 8-B de la ley. Esta información es considerada de acceso privado, con el objeto de asegurar la confidencialidad, los únicos autorizados a acceder a esta información son la Fiscalía General de la República o un Tribunal competente que con motivos fundados requiera de dicha información.

Dentro de los deberes de las entidades certificadoras, enumeradas en el Art. 8-C de la ley tenemos:

- Emitir certificados, implementar sistemas de seguridad, garantizar la protección de la información, garantizar la prestación permanente del servicio, permitir y facilitar la realización de auditorias, elaborar su reglamento y llevar un registro de los certificados emitidos.

Las sanciones que puede imponer el Ministerio de Hacienda a las entidades certificadoras se encuentran en el Art. 8-E de la ley. Dependiendo de la naturaleza y la gravedad de la falta, pueden ser:

- Amonestación
- Suspensión de autorización
- Revocación definitiva de autorización para operar.

2.7. CONTRATACIÓN ELECTRÓNICA.

Como se ha venido desarrollando el contenido respectivo al comercio electrónico donde el contacto físico ha sido reducido a su mínima expresión y como la firma digital permite garantizar la integridad del mensaje, su autenticidad y su no repudio, ya que al existir un número creciente de transacciones comerciales, nacionales e internacionales es necesario que conste algo que dé seguridad como la firma digital a todas estas obligaciones que se realizan por medio del intercambio electrónico de datos y por otros medios de comunicación, sin embargo la aparición del comercio electrónico obliga a

plantearse cuestiones del comercio tradicional donde las transacciones se realizan por medio de contrataciones, pactando mutuamente dichas obligaciones.

Es por esta razón que es preciso que nos refiramos a la contratación electrónica ya que es obligatorio conocer; puesto que todos los compromisos que se adquieran por medio del intercambio de información electrónico se deberán realizar a través de la contratación electrónica.

Por lo tanto podemos precisar que *"La contratación electrónica, desde un punto de vista jurídico, es un contrato a distancia que tiene notas distintivas como:*

- *La circulación de la información por canales abiertos, exige la adopción de importantes medidas de seguridad que garanticen la confidencialidad y la identidad de los que emiten los mensajes.*
- *La contratación sin presencia personal y sobre la base de condiciones generales, requiere medidas normativas que aseguren una debida formación de la voluntad contractual.*
- *Y en relación con lo anterior se impone un análisis de los supuestos en los que se debe restringir esta forma de contratación."*[55]

[55] Perales Sanz, José Luís, La Seguridad Jurídica en las Transacciones Electrónicas. Seminario Organizado por el Consejo General del Notariado de la UIMP. Editorial Civitas, Madrid (España) 2002. Pág 149

2.7.1. DEFINICIÓN DE CONTRATACIÓN ELECTRÓNICA.

Diversos autores han tratado de definir la contratación electrónica de la siguiente manera:

- *"La contratación realizada mediante la utilización de elementos electrónicos que tienen incidencia en la formación de la voluntad, el desarrollo e interpretación futura de algún acuerdo".*[56]

- *"Todo contrato celebrado sin la presencia física simultanea de las partes, prestando éstas su consentimiento en origen y destino por medio de equipos electrónicos de tratamiento y almacenamiento de datos, concretados por medio de cable, radio, medios ópticos o cualquier otro medio".*[57]

En base a las anteriores definiciones, como grupo podemos sintetizar como contratación electrónica: El acuerdo de voluntades en el que las partes se comprometen a realizar una obligación que consiste en dar, hacer o no hacer alguna cosa, caracterizado porque las declaraciones de voluntad que prestan los sujetos intervinientes se manifiestan a través de medios electrónicos.

[56] Patroni, Vizquerre, Úrsula. Contratación Electrónica y acuse de recibo. www.mailweb.udcap.mycontelect.html
[57] Davara Rodríguez, Miguel Angel. Manual de Derecho Informático. Ediciones Aranzandi. España. 1997. Pág 165

2.7.2. CARACTERÍSTICAS.

Este tipo de contratación, como ya se ha mencionado, es realizada a través de medios electrónicos y tiene como características principales las que a continuación señalaremos:

a) No existe presencia física de las partes, ya que se trata de contratos que se celebran entre ausentes en tiempo real.
b) Por la misma naturaleza de la transacción, el consentimiento expresado por las partes que intervienen en el mismo, es prestado a través de medios electrónicos.
c) Los contratantes pueden ser varias personas simultáneamente, (se puede realizar entre una gran cantidad de socios o clientes), sean éstas naturales o jurídicas, reduciendo en gran medida el costo de contratación.
d) Esta clase de actividad comercial deriva en relaciones transfronterizas, por lo que la contratación electrónica es en la mayoría de casos una contratación que trasciende las fronteras.

2.7.3. PRINCIPIOS.

Los principios que orientan a este tipo de contratación son los siguientes:

A. PRINCIPIO DE NEUTRALIDAD TECNOLOGICA DE LAS DISPOSICIONES REGULADORAS DEL COMERCIO ELECTRÓNICO.

Con este principio se busca evitar favorecer un tipo específico de tecnología, es decir, intenta dar un trato igualitario a las tecnologías existentes como a las que a futuro se puedan desarrollar.

Esta neutralidad permite que los estándares sean fruto de la oferta y de la demanda y no que sean impuesto por una ley, ya que si un cuerpo normativo apoya un tipo de tecnología especifica por sobre otras, quedará desfasado, puesto que si se observa la rapidez con que evoluciona la tecnología, se tendría en muy poco tiempo un cuerpo normativo obsoleto e inservible.

B. PRINCIPIO DE INALTERACION DEL DERECHO PREEXISTENTE DE OBLIGACIONES Y CONTRATOS.

Mediante este principio se busca que la incorporación de nuevas tecnologías a la legislación nacional no modifique las leyes existentes sobre obligaciones y contratos.

Si las nuevas tecnologías son reguladas la naturaleza de esta regulación daría como resultado una ley especial, la cual se aplicaría para las transacciones vía comercio electrónico, sin vernos en la necesidad de modificar la teoría contractual y obligacional vigente y legislada.

Es por este principio que se hace necesaria una regularización de dicha materia ya que no debe haber una obstaculización del desarrollo de nuevos productos y servicios, a causa de que las normas vigentes no contemplan estas nuevas realidades. La necesidad de una ley especial que regule el comercio electrónico en El Salvador es para que la sociedad salvadoreña despeje todas las inquietudes que plantea las transacciones electrónicas.

C. PRINCIPIO DE EXIGENCIA DE BUENA FE.

Este es un principio básico, ya que al tratarse de transacciones no físicas ni directas realizadas a través de medios electrónicos, añade la voluntad para complementarla, aclararla ó corregirla. La buena fe constituye uno de los fundamentos al régimen jurídico, aplicable al intercambio nacional e internacional de bienes y servicios. El que tal intercambio se haya convenido verbal, manual o electrónicamente, no es relevante en cuanto a la observancia necesaria de la buena Fe.

2.8 RELACIÓN CONTRACTUAL ELECTRÓNICA.

La contratación y los actos jurídicos en general, realizados por medios de la electrónica, la informática y la telemática, determinan el nacimiento de obligaciones tanto personales como patrimoniales de una determinada forma y manera, y este vínculo ha sido denominado Relación Contractual Electrónica.

La contratación y el comercio electrónico representan una nueva modalidad constitutiva de obligaciones, esto no quiere decir que no sean una fuente de estas, ya que se trata de una nueva forma de expresión de la voluntad derivada de los avances tecnológicos que hoy en día facilita la transmisión electrónica de mensajes de datos, agilizando las transacciones comerciales.

Las Relaciones Contractuales Electrónicas conservan los mismos elementos de aquellas consideradas comunes, son válidas y existirán jurídicamente desde que una o varias personas consientan sin error, libre y voluntariamente, ha obligarse entre ellas, a darse una cosa o prestarse un servicio licito ó con una causa; de modo que el concurso de la oferta y de la aceptación expresada por medios y sobre soporte electrónicos perfeccionara tal relación con base a la normativa tanto general como especifica de la materia.

2.8.1 LIBERTAD CONTRACTUAL Y LIBERTAD DE CONTRATAR.

En el sistema Jurídico Salvadoreño la materia contractual esta basada en la libertad y la autonomía de la voluntad, respectivamente garantizada en los artículos 2 y 8 de la Constitución de la República del Salvador, teniendo por entendido que las personas gozan de libertad para ejercitar sus facultades y derechos, y con esto dando vida a las diferentes relaciones jurídicas y ejerciendo su autonomía privada, que es una facultad concedida por el Estado a los particulares con la cual les confiere la potestad normativa de autorregularse y reglamentar sus intereses jurídicos, generando una relación

obligacional entre las partes contratantes. La autonomía privada se ejerce a través de dos principios: Libertad Contractual y Libertad de Contratar.

"La libertad de contratar, es aquella que tiene el particular para decidir por si mismo si contrata ó no, cuando los particulares deciden con quien contratar ejercen este derecho; que se encuentra regulado en los artículos 2, 3, 22,23 de la Constitución de la República."[58]

Este derecho garantiza que los sujetos puedan escoger libremente a las personas con quienes han de contratar, la Ley regula el ejercicio de esta libertad para defender el principio de justicia y evitar el abuso del derecho, y así impedir las modificaciones de los términos contractuales por ley o disposiciones de cualquier naturaleza.

La libertad contractual, es aquella por la cual las partes fijan el contenido de su contrato siempre y cuando este no atente contra el orden público y las buenas costumbres, esta libertad se encuentra garantizada en el artículo 1416 del Código Civil de El Salvador, el cual establece que: *"Todo contrato legalmente celebrado es obligatorio para los contratantes, y solo cesan sus efectos entre las partes por el consentimiento mutuo de estas o por causas legales."*[59]

[58] Recopilación de Leyes Civiles. Constitución de la República de El Salvador. Editorial Jurídica Salvadoreña.

[59] Recopilación de Leyes Civiles. Código Civil de la República de El Salvador. Editorial Jurídica Salvadoreña.

Según lo anteriormente expresado, se está en la posibilidad de celebrar cualquier tipo de contrato y establecer el contenido, aunque no se encuentre regulado por nuestra legislación, siempre y cuando cumpla con los requisitos que anteriormente señalamos, siendo de aplicación accesoria la voluntad de las partes con las disposiciones vigentes que tengan carácter de imperativa.

Ya que ha sido analizada la libertad de contratación de los sujetos se vuelve necesario el estudio de los aspectos que se ven incluidos dentro de la relación contractual electrónica.

2.8.2 CAPACIDAD DE LAS PARTES EN LA CONTRATACIÓN ELECTRÓNICA.

La autoría de las partes tiene que estar debidamente identificada y comprobada, se tiene que determinar si tienen la capacidad legal de obrar y de contratar necesaria y suficientemente vinculada con el consentimiento.

Este aspecto es especialmente delicado en la contratación electrónica puesto que hacen falta los datos obtenidos por apreciación directa entre las partes, que son de gran importancia en la determinación de la capacidad de los contratantes, ya que la presunción de la capacidad tiene mas base por conocimientos externos: Comprobación de la sede, la actividad que realiza, mayoría o no de edad, etc. Se supone que el problema se minimiza gracias al avance de las últimas tecnologías que permiten tener en

pantalla la imagen, la voz e incluso la escritura en directo de la otra parte, pero en países como el nuestro, en los que la tecnología de las comunicaciones inicia su trayecto, contar con el equipo necesario y suficiente para tal actividad es casi imposible.

No obstante debe de recordarse que en base al principio de Buena Fe Art. 1417 C.C. que expresa que *"los contratos deben ejecutarse de buena fe y por consiguiente obligan no sólo a lo que en ellos expresan, sino a todas las cosas que emanan precisamente de la naturaleza de la obligación, o que por la ley o la costumbre pertenecen a ella"*[60], es por este principio que se presume que todos los sujetos que intervienen en una relación contractual electrónica son capaces; pero que tal presunción queda desvirtuada si existe la declaratoria judicial que señala el artículo 292 del código de familia en la que se determina la incapacidad del sujeto para contratar.

Para comprobar esta capacidad en la Contratación Electrónica hay una serie de dificultades, teniendo en cuenta que las partes nunca están en presencia de la otra; en estos casos las precauciones para que no hayan defraudaciones estarán a cargo del proveedor de servicios a través de la red, lo acostumbrado sería que antes del momento de la Contratación Electrónica se llevarán a cabo actos para comprobar la capacidad, también debería ser comprobado en el momento de contratar el acceso a la red, al

[60] Recopilación de leyes Civiles. Código civil. Editorial Jurídica Salvadoreña.

suscribir el contrato de prestación de servicios con el usuario, de esta manera la única forma de contratar sería con el uso de claves.

2.8.3 EL CONSENTIMIENTO ELECTRÓNICO.

ALESSANDRI Y SOMARRIVA en su obra la fuente de las obligaciones define al consentimiento como *"El acuerdo de voluntades de dos ó más personas con un objeto licito; en el acto unilateral se denomina voluntad".*[61]

La formación del consentimiento en materia de contratación electrónica, puede regularse por las reglas generales que rigen nuestro ordenamiento jurídico, pero deberán considerarse ciertos puntos que se estimen convenientes al respecto.

El consentimiento que se otorga por medios electrónicos es válido, lo único que se necesitan es que sea determinante, claro e inequívoco, consagrándose con ello los principios de la autonomía de la voluntad y libertad contractual, pero esto siempre con la limitación que imponen las normas de orden público, moral, buena fe, utilidad pública e interés social recogidas en nuestra legislación.

[61] Rodríguez Alessandri, Arturo y otro. Curso de Derecho Civil, Tomo IV, Las Fuentes de las Obligaciones en particular. Editorial Nacimiento. Santiago de Chile. 1942. Pág 21

La voluntad que genera el consentimiento para que sea valida tiene que ser consiente y libre, así como lo dispone el artículo 1316 del Código Civil, y sobre el consentimiento de dicho acto no debe existir vicio alguno.

Las relaciones contractuales electrónicas son una nueva forma de expresar, trasmitir y de manifestar la voluntad y por tanto el consentimiento dista de la forma tradicional.

En la contratación tradicional, es decir con papel escrito, y con firma autógrafa, las distintas fases de la declaración de voluntad son continuas y no pueden diferenciarse una con la otra; en cambio en la contratación electrónica estas fases están claramente diferenciadas.

El consentimiento electrónico esta constituido por: motivación, intención, deliberación, decisión, expresión o manifestación, transmisión y conocimiento, por el oferente, y se manifiesten de la siguiente forma.

FASES	***FORMAS DE MANIFESTACION***
Motivación	*Solo Humana.*
Intención	*Por ser expresada únicamente por los contratantes es solo humana.*

Deliberación	*Humana con apoyo informático.*
Decisión	*De activación del sistema.*
Proceso	*De elección, posible procesamiento cibernético y previsión humana.*
Declaración	*Apoyo informático, definición humana.*
Expresión y comunicación	*Solo informática, mediante lenguajes informáticos que precisan transformaciones para su inteligibilidad en las telecomunicaciones digitales.*
Emisión/Recepción	*Sistemas informáticos a través de aplicación informática.*
Soporte	*Electrónico, informático.*
Almacenamiento	*Informático.*
Firma	*Electrónica.*
Pago	*Electrónico.* [62]

El sistema informático, una vez activado expresa la declaración de voluntad de un modo totalmente electrónico y telemático, es decir que si no hay un acuerdo de las partes no existirá contrato. El Código Civil señala un punto preponderante a la voluntad que es lo mismo que el consentimiento, sin olvidar las restricciones y limitaciones que señalamos anteriormente, así como también la igualdad o equilibrio entre las partes contratantes.

[62] www.htm/web.net/seguridad/varios/firma-jurídico.html

En la formación del consentimiento existen dos etapas, representadas cada una por la voluntad de los contratantes, los cuales son la oferta y la aceptación.

En la contratación electrónica, tanto como la oferta como la aceptación pueden ser realizados por medios electrónicos para que se considere el contrato como tal o bajo dicha denominación.

No obstante lo anterior, por tratarse de una oferta y una aceptación no suscrita o materializada en papel, es pertinente hacer algunas consideraciones sobre aquellas desde el punto de vista electrónico.

2.8.3.1 LA OFERTA ELECTRÓNICA.

Para que el consentimiento tradicional tome forma requiere de dos etapas que son la oferta y la aceptación, así mismo se pueden observar en el Consentimiento Electrónico. Podemos decir que para entender estos conceptos de una manera más clara nos referiremos en primer lugar a la oferta.

Para el autor chileno Somarriva *"La oferta es un acto jurídico por el cual una persona propone a otra la celebración de un contrato en términos tales, que para que este quede perfecto basta con que el destinatario de la oferta simplemente la acepte"*[63].

[63] Op. Cit. Rodríguez Alessandri. Pág 43

Para el autor Ramiro Cubillos *"La oferta es la manifestación unilateral de voluntad en virtud de la cual se propone la celebración de un contrato a una o mas partes"*[64], debe ir dirigida a una persona o a un grupo de personas determinadas.

Partiendo de este elemento general se puede decir que por Oferta Electrónica se entenderá: *"Aquella declaración unilateral de voluntad que una persona realiza a través de medios de comunicación y/o medios informáticos, proponiendo a otra persona la celebración de un contrato que quedará perfeccionada con la sola aquiescencia de ésta"*[65].

Cabe aclarar que la oferta electrónica constituye una oferta escrita, ya que integra un texto alfa numérico ó grafico en lenguaje de bits y por lo tanto no existe razón valida para no considerarla como una oferta escrita.

En cuanto a la oferta no hay inconveniente en establecer cual es el medio en que se realiza, siempre y cuando sea permitido por la ley, es decir, que en el caso de los contratos electrónicos, no importa si la oferta se realiza a través de medios electrónicos o no, pero tratándose de la declaración contractual que debe darse en primer lugar para formar el consentimiento y así formar el contrato, se debe tomar en cuenta que no toda

[64] Op. Cit. Cubillos Velandia. Pág 160
[65] Ib Idem.

declaración de voluntad implica una oferta porque para ello debe cumplir con ciertos requisitos:

A) Debe ser completa: de manera que el destinatario pueda limitarse simplemente a aceptar. Este punto es de mayor importancia en la contratación celebrada vía Internet, ya que en la mayoría de los casos el destinatario de la oferta se limita a "pulsar clic" sobre un icono de la pagina Web para emitir su aceptación, sin posibilidad de modificar las cláusulas de la oferta.

B) La oferta debe emanar de la voluntad del oferente o de un representante suyo, y ser dirigida a un destinatario o algún representante del mismo.

C) La oferta debe ser precisa y cumplir con todo los elementos esenciales del tipo de contrato que se desea llevar a cabo; en los casos de las ventas en Internet se deben cumplir los requisitos establecidos en la normativa sobre las ventas a distancia.

D) La oferta debe tener un plazo de duración, ya que es importante que los oferentes establezcan el periodo de validez de las ofertas con el objeto de otorgarle firmeza evitando de esta manera modificaciones de carácter unilateral a las condiciones incluidas en la página Web o bien en el correo electrónico.

Los principales problemas que se presentan con las ofertas incluidas en las páginas Web ó trasmitidas mediante E-mail se centran, por un lado, en la dificultad de localizar un lugar de la oferta y por otro en el hecho de la determinación de la naturaleza jurídica de los mensajes contenidos en estos instrumentos.

El primer punto podría resolverse, aunque de modo parcial, a través del sistema *DNS*[66], que permite identificar, a través del *CCTLD*[67], el país a la que pertenece la empresa o persona emisora de la oferta, presumiendo que la oferta se tendrá por hecha en el país incluido en el nombre de dominio respectivo.

Como observamos se trata de una solución de modo parcial, ya que el dominio no es fácilmente determinable en situaciones que solo incluye como primer nivel com, org, net, sin aludir a la posición grafica determinada por CCTLD.

El segundo punto pretende determinar si realmente los mensajes de datos transmitido por las compañías vía E-mail ó a través de sus paginas Web debe considerarse como verdaderas ofertas que obliguen al oferente ó si por el contrario, debe ser considerados como simples mensajes publicitarios constitutivos de una invitación a ofrecer, situaciones de importancia fundamental en el proceso de formación del contrato, ya que la oferta determina, en la mayoría de los casos, el lugar de donde se entiende celebrado el contrato con las implicancias jurídicas que esto conlleva.

La oferta electrónica que se realiza por Internet puede ser clasificada en los siguientes términos:

1) Aquella realizada vía E-mail ó correo electrónico.

[66] Domain Name System ó Sistema de Nombre de Dominio
[67] Country Code Top Level Domain ó Dominio Máximo de Código de país, en el caso de El Salvador se identifica a través de la partícula SV al final de las direcciones de Internet.

2) Aquella realizada On-line, en redes de comunicaciones como Internet.

1- La oferta realizada por E-mail ó correo electrónico es aquella enviada a ordenadores determinados por medios de cuentas de correo electrónico, aunque en la mayoría de los casos constituye mensajeria publicitaria y no son considerados oferta.

2- Estas son ofertas que se encuentran en forma permanente en las redes y a las cuales se tienen acceso navegando por diferentes paginas, pero estas no llegan a las computadoras, sino que se accede a ellas a través de visitas a ciertos sitios Web, características que permite englobarlas dentro de la ofertas a personas indeterminadas.

2.8.3.2 LA ACEPTACIÓN ELECTRÓNICA.

En segundo lugar, otra etapa para que el consentimiento tome forma es la Aceptación; la cual para el jurista Somarriva *"es el acto por el cual la persona a la que va dirigida la oferta manifiesta su conformidad con ella"*[68]. Por lo tanto puede definirse a la aceptación electrónica como: *"Aquella declaración de voluntad que una persona realiza a través de medios de comunicación y/o medios informáticos manifestando su conformidad a una propuesta recibida por ella"*[69]. Esto quiere decir que la aceptación electrónica comprende la declaración unilateral de voluntad realizada a través de medios

[68] Op. Cit, Rodríguez Alessandri, Pág 52
[69] Op. Cit. Cubillos Velandia, Pág 168

electrónicos dirigida al oferente en la cual aprueba los términos de la oferta antes recibida.

Existen ciertas circunstancias o requisitos que son necesarias para que se conforme el consentimiento en cuanto a la aceptación, y ellos son los siguientes:

1) Debe ser Congruente
2) Debe darse mientras la oferta este vigente
3) Debe ser oportuna
4) Debe ser pura y simple.

1- Debe ser Congruente: se refiere a que la aceptación debe tener completa relación con la oferta hecha sin variar en cuanto a los objetos, la cantidad, calidad o valor.

2- Debe darse mientras la oferta esta vigente: la oferta se encuentra vigente mientras no produzca dos hechos jurídicos; la retractación y la muerte o incapacidad sobrevenida del oferente, que se encuentra regulados en el Código de Comercio en el Art. 969.

a) Retractación: esto ocurre cuando el oferente puede dejar sin efecto la propuesta emitida mientras esta no haya sido aceptada; en las ofertas electrónicas realizadas por correo electrónico es fácil que se de esta figura, pero en las ofertas permanentes que se dan en línea resulta muy difícil por el hecho que el cliente compra en el mismo momento que accede a la pagina respectiva (ya que la aceptación se envía a través de formularios a los cuales se accede a través de hipertextos).

b) Muerte o incapacidad sobrevenida del oferente: esta ocurre cuando se pierde la vigencia de la oferta, debido a la muerte o incapacidad legal de uno de los sujetos intervinientes en la relación, quien es el ofertante.

El artículo 969 Inc. 2º, del Código de Comercio, no priva de eficacia a la oferta cuando sobrevenga esta circunstancia, a menos que se trate de un negocio que por su naturaleza, resulte lo contrario. En este sentido y en materia de contratación electrónica, no tiene validez ya que se trata de personas jurídicas o abstractas y el artículo está referido principalmente a personas naturales.

3- Debe ser oportuna: se entiende que la aceptación es oportuna cuando se otorga dentro del plazo legal que es el señalado como periodo de validez por la ley, o bien el plazo voluntario o convencional establecido por las partes, caso en el cual no existirían inconvenientes.

4- Debe ser pura y simple: en un contrato electrónico, en el cual la oferta es electrónica, la forma de la aceptación deberá de ser electrónica, y deberá ir dirigida al oferente, no puede dirigirse a persona diferente a este.

La respuesta de la oferta debe estar limitada a la aceptación o negación de la oferta, ya que si le incorpora modificaciones a la propuesta inicial se convierte en una contra oferta, figura contemplada en la parte final del Artículo 966 del Código de Comercio donde se establece que el contrato se perfeccionara hasta que se reciba la contestación aceptándolas. Las dificultades que se derivan de la aceptación en entornos electrónicos se relacionan directamente con la inclusión de condiciones generales de contratación, ya que se trata de contratos de adhesión que impiden la negociación de sus

cláusulas, las cuales por lo general no se encuentran insertadas en forma directa, clara y visible, lo que deriva en que el aceptante desconoce totalmente las condiciones generales que rigen el contrato, ocasionándole graves perjuicios, además de la dificultad de probar el asentimiento bajo conocimiento expreso del mismo, sobre la aceptación de las cláusulas de adhesión.

2.8.4 VICIOS DEL CONSENTIMIENTO ELECTRÓNICO.

En la contratación electrónica, la buena Fe, debe tenerse en cuenta para potenciar la protección de los contratantes, ya que estamos frente a acuerdos de intercambio. El artículo 1322 del Código Civil, enumera los vicios que pueden afectar el consentimiento prestado a través de medios electrónicos, los cuales son: el error, la fuerza y el dolo.

2.8.4.1 ERROR.

El error puede definirse como *"el falso conocimiento de la realidad o el desconocimiento de alguna circunstancia que sea determinante a la voluntad en el acto jurídico".*[70]

El error puede ocurrir en alguna de las fases de la contratación y afectar a todo el proceso, ya que si la voluntad no se genera de una manera libre, racional, conciente y sin

[70] Baqueiro Rojas, Edgar. Diccionario Jurídico Temático: Derecho Civil. Volumen I. Ediciones Oxford University Press. México 2000. Pág 43

vicios puede producir un consentimiento nulo, debido a que se quiere con error, desviando la verdadera realidad y naturaleza esencial del bien o servicio a contratar.

El contrato electrónico será anulable, si contiene errores acreditados en la fase de declaración, impidiendo que lo declarado, que era lo que se quería emitir, coincida con lo que realmente se emitió o recibió. Para lograr apreciar el vicio del error en el consentimiento, es necesario que éste se haya producido plenamente y estar perfeccionado el contrato con el error, porque si no, no habrá contrato que anular.

Dentro de las causas de errores que pueden ocurrir en la contratación electrónica, se pueden señalar las siguientes:

- Pérdida o demora: cuando el documento ha sido enviado y no fue recibido por la otra parte, debido a extravió o demora en la recepción.
- Repetición: es casi imposible distinguir un documento electrónico original de una copia, por lo que se hace necesario que se le dote de alguna marca o signo que permita diferenciarlos.
- Manipulación ilícita: el documento declarado no contiene los mismos caracteres que el recibido, debido a que las partes no detectaron la intervención en el momento de la perfección del contrato y lo hacen en una fase de cumplimiento posterior.
- Confidencialidad.

- Repudio: negar el envío o la recepción del mensaje.
- Fallos técnicos en la transmisión: da como resultado que se intento la transmisión pero no se consiguió o no es recibida por el destinatario; o hay transmisión errónea del contenido o en la identificación de las partes.
- Imposibilidad de comunicación: protocolos no adecuados o sistemas incompatibles.
- Contradeclaraciones: documentos electrónicos con fecha posterior al contrato.
- Software: manipulación intencionada, cambio del programa, virus devastador o con funciones especificas como recopilar datos, códigos o errores de programación.
- Indebida manipulación o errores del dueño.

Luego de clasificar las causas que pueden dar motivo al error, examinaremos los dos tipos de errores reconocidos en la doctrina y aplicables a la contratación electrónica.

-Error de derecho:

Ninguna persona puede alegar ignorancia de la ley y en consecuencia basar un error o equivocación cometida por ellos, con el fin de anular el consentimiento prestado en cierto momento, según lo dispuesto en los artículos 8, y 1323 del Código Civil. La ignorancia de la ley no excusa su cumplimiento y por tanto no puede invocarse error para eludir el cumplimiento de la obligación.

No puede invocarse como error de derecho para evitar sus consecuencias, el haber efectuado una contratación electrónica que pone en juego datos sensibles por desconocimiento de la legislación aplicable a tal tipo de contratación.

-Error de hecho:

El artículo 1322 del Código Civil, señala que uno de los vicios del consentimiento es el error, y los artículos 1324 y 1325 Del Código Civil manifiestan que para que el error invalide el consentimiento, deberá recaer sobre la sustancia de la cosa que fuere objeto del contrato, o sobre aquellas condiciones de la misma que principalmente hubiesen dado motivo a celebrarlo. El error sobre la persona sólo invalidará el contrato cuando la consideración de ella hubiere sido la causa principal del mismo.

2.8.4.2. FUERZA.

La fuerza, según el artículo 1327 del Código Civil, es *"el acontecimiento ajeno a la voluntad que infunde a una persona temor de verse expuesta a ella, su consorte o alguno de sus ascendientes o descendientes capaz de producir en quien la padece una impresión fuerte o un mal irreparable o grave"*.

En la contratación electrónica se puede forzar a una persona a dar una declaración no querida bien directamente forzando su realización o indirectamente, forzando la entrega de las claves, sistemas criptográficos o instrumentos necesarios al

titular para realizar la contratación. La fuerza en la contratación electrónica será todo acto que infunde un justo temor de verse expuesta a ella ya sea el sujeto que se pretende contrate por medios electrónicos o bien su familia.

Cabe aclarar que la fuerza no vicia el consentimiento, sino solo cuando es capaz de producir una impresión fuerte en una persona de sano juicio, tomando en cuenta sus condiciones particulares.

2.8.4.3 DOLO.

Del texto del artículo 1329 del Código Civil, se desprende que existe dolo, cuando con palabras o maquinaciones insidiosas de parte de uno de los contratantes, se induce a la otra parte a celebrar un contrato, que sin mediar tales acciones, no se hubiera hecho. El dolo como causa de la contratación, tiene como objetivo el engaño, y el ánimo de lograr la declaración mediante el artificio utilizado.

2.8.5. PERFECCIONAMIENTO DEL CONSENTIMIENTO EN TRANSACCIONES DEL COMERCIO ELECTRÓNICO.

El comercio electrónico no es sino una nueva modalidad para la formación del consentimiento, requisito esencial para la validez de los contratos. La validez de la contratación electrónica tanto en entornos abiertos como en entornos cerrados, ya sea de una contratación en Internet, mediante EDI, o cualquier otro medio electrónico, es susceptible de tratamiento legal.

De acuerdo a la forma, los contratos electrónicos y las estipulaciones en ellos contenidas, se consideran perfectamente válidas, por encontrarse amparadas, fundamentalmente en los principios de libertad y de autonomía de la voluntad.

La declaración de voluntad que acarrea el consentimiento debe ser manifestada con el propósito de crear un vínculo jurídico, para que pueda obligar a la persona que la emite; debe haber una relación jurídica formal, y no solo el propósito de servir, complacer o ayudar sin animo de obligarse seriamente.

Para que un contrato se perfeccione, tiene que pasar por el consentimiento de ambas partes contratantes, es decir por el concurso de la oferta y la aceptación sobre el objeto del contrato. Con respecto al momento en que se perfecciona el contrato electrónico, tenemos la figura del acuse de recibo, como una forma de acreditación de su perfeccionamiento, como por ejemplo en el Código Civil Peruano, con sus reformas para la aplicación de la contratación electrónica, dispone que opera la presunción de aceptación, de la realizada por medios electrónicos cuando el aceptante reciba acuse de recibo de su aceptación por parte del oferente facilitando con esto el medio de prueba de declaración de voluntad de aceptación hecha por el aceptante.

Así mismo la Directiva de la Unión Europea por medio de sus comisiones en fecha 18 de noviembre de 1998, al exponer sobre algunos aspectos jurídicos del comercio electrónico, comprende como punto importante el momento de la celebración

del contrato electrónico, en el cual dice: Cuando el consentimiento del cliente respecto a la aceptación de la oferta del proveedor se manifiesta a través de un clic en un icono, se aplicarán los siguientes principios:

1. El contrato se perfecciona en el momento en que el cliente recibe del proveedor por medios electrónicos, un acuse de recibo de la aceptación del cliente y confirma la recepción de dicho acuse de recibo.
2. El acuse de recibo se considera recibido y la confirmación se considera dada cuando las partes a las que se ha destinado están en disposición de acceder a los mismos.
3. El acuse de recibo y la confirmación deben ser enviados lo antes posible.

Se concluye entonces que el momento de perfeccionamiento del contrato electrónico es cuando el destinatario obtiene el acuse de recibo de la aceptación que este ha enviado.

El lugar de celebración tiene efectos importantes para fijar la competencia, la ley aplicable, el carácter nacional o internacional del contrato, y para interpretarlo conforme a los usos y costumbre del lugar de celebración del contrato. El lugar de celebración del contrato es el que fijen las partes, ya que tienen la libertad para hacerlo por ser un derecho dispositivo de estas; pero en ausencia de acuerdo de partes, el lugar del contrato lo designará el legislador.

2.8.5.1 REGLAS PARA DETERMINAR EL PERFECCIONAMIENTO.

La contratación electrónica como contratación entre ausentes se caracteriza porque entre la oferta y la aceptación existe un tiempo relevante en cuanto a la posibilidad de la ocurrencia de riesgos que hay que distribuir.

Para lograr determinar el momento en que ha de entenderse que el contrato ha quedado perfeccionado, existen cuatro teorías[71], que pueden ser resumidas de la siguiente manera:

- Regla de la declaración: considera concluido el contrato con el solo hecho de la aceptación de la oferta, sin que sea necesaria ninguna exteriorización de voluntad, ni el envío de ella al oferente. El aceptante que redacta una carta de aceptación perfecciona el contrato, y no cuentan el tiempo ni los riesgos que demanda su envío al oferente.
- Regla de la expedición: el contrato queda concluido con la expedición o envío de la aceptación por parte del aceptante. No se trata solamente de que se acepte, sino de que se exteriorice ese acto mediante el envío. El tiempo y los riesgos que existen desde el envío hasta que el oferente recibe la aceptación quedan a cargo del oferente, dado que el contrato ya está perfeccionado.

[71] Lorenzetti, Ricardo L. Comercio Electrónico, Editorial Abeledo Perrot, Buenos Aires, Argentina 2002, Pág 192

- Regla de la recepción: el contrato queda perfeccionado desde que la aceptación es recibida por el oferente. De modo que se precisa que el aceptante declare su voluntad de aceptar, la exteriorice mediante el envío y sea recibida por el oferente. El tiempo y los riesgos del envío son a cargo del aceptante.
- Regla del conocimiento: el contrato queda perfeccionado desde que la aceptación es conocida por el oferente. De modo que no solo requiere una declaración de voluntad recepticia, sino también el conocimiento de ella. El tiempo, los riesgos del envío y el de que la declaración no sea conocida por el oferente son a cargo del aceptante.

La regla de la recepción es la que mas se ha difundido, la Convención de Viena sobre Compraventa Internacional de Mercaderías, en los artículos 23 y 18.2, dispone que el contrato se perfeccionara en el momento de surtir efecto la aceptación de la oferta, y ello sucede en el momento en que la indicación del asentimiento llegue al oferente.

El artículo 966 del Código de Comercio señala que los contratos mercantiles celebrados por correspondencia, quedaran perfeccionados desde que el proponente recibe la respuesta en que se acepte lo que haya ofrecido.

CAPITULO III

MECANISMOS JURIDICOS Y MEDIOS DE PRUEBA EN CASO DE RECLAMOS JUDICIALES SOBRE DOCUMENTOS CON FIRMA DIGITAL EN TRANSACCIONES DEL COMERCIO ELECTRONICO.

3.1 MECANISMOS EXTRAJUDICIALES.

Internet se configura como un sistema de comunicación transnacional que permite el intercambio y obtención de información mediante la utilización de diversas modalidades de comunicación en línea, y como resultado de esto, constituye un sistema de comunicación global y descentralizado.

Por lo tanto, Internet se articula como una infraestructura universal sin tener en cuenta las fronteras nacionales, el espacio sobre el que extiende sus dominios es plurijurisdiccional, quedando limitada la jurisdicción de cada Estado a las fronteras de su territorio.

Debe considerarse que el comercio electrónico comprende no solo las ventas o adquisiciones que el empresario y el usuario realizan a través de Internet, sino que engloba todas las fases del negocio empresarial, así se puede incluir la oferta de productos, la publicidad, mensajes transmitidos entre los contratantes, etc.

Las transacciones del comercio electrónico revisten seguridad y certeza, pues las compañías cuentan con la tecnología necesaria para aplicarlo. Sin embargo, no están libres de enfrentarse a situaciones conflictivas debido a la dificultad de acordar transacciones o por el incumplimiento de alguna cláusula contractual.

También las personas físicas, quienes actúan como consumidores, se encuentran expuestos a situaciones conflictivas, ya que no cuentan con la información adecuada sobre el mercado en el que se desenvuelven, por lo que se hace necesario la presencia de un tercero que ayude a establecer una solución.

Este tercero, que interviene por voluntad de las partes, debe considerar una solución que satisfaga los intereses de cada uno de ellos. Para ello, debe mantener comunicación con las partes y proponer acuerdos equitativos. De no lograr la concertación, las partes pueden acudir a una nueva instancia en donde el tercero impondrá una solución imparcial, íntegra y objetiva.

Dado que los conflictos se originan en el ciberespacio, ningún país puede decir que tiene el monopolio para imponer las leyes de su país ya que en muchos casos las partes en conflicto se encuentran en diferentes partes del mundo.

Ante esta circunstancia, no se plantea la posibilidad de crear un único órgano judicial a nivel mundial para la resolución de las controversias que se puedan originar en

el ciberespacio, sino que mas bien se determina si los órganos judiciales de cada uno de los Estados pueden hacer frente a estas controversias, o si por el contrario, resultaría inconveniente sustituir la actuación de los jueces por fórmulas de solución extrajudicial, tales como la mediación, conciliación o arbitraje, mas acordes con lo característico que presenta la red y los conflictos derivados de su uso.

Los argumentos en contra de que sean los jueces tradicionales de cada uno de los Estados los que se ocupen de la resolución de este tipo de controversia son, el de estar fuera del territorio de la jurisdicción habitual de éstos y que existe la necesidad de aplicar un derecho nuevo, para que no sea motivo de controversia el origen y la ubicación del territorio de las partes que intervienen.

La resolución extrajudicial de conflictos, se convierte en una pieza esencial para el desarrollo de la contratación electrónica, puesto que se convierte en una respuesta necesaria para garantizar al consumidor una vía rápida de solución de los litigios que puedan surgir respecto a las transacciones comerciales efectuadas vía electrónica, tales como competencia desleal, defensa de la propiedad intelectual, incumplimiento de obligaciones contractuales, problemas con la firma digital, entre otros.

Actualmente, existe una tendencia a impulsar las vías de solución extrajudicial de controversias para este tipo de conflictos, por la razón de que estos procesos conllevan celeridad, eficacia, confidencialidad y menor costo económico. A estas cualidades debe

añadírsele la carencia de conocimientos técnicos y científicos de los jueces, circunstancia que conduce al constante y necesario auxilio pericial con el fin de completar los conocimientos de aquellos y poder fundamentar la resolución correspondiente.

Los sistemas de resolución extrajudicial generan confianza en los consumidores y usuarios que contratan vía electrónica, también se figuran como vías rápidas de resolución de conflictos. De esta forma, se convierte en un mecanismo esencial para la implantación y desarrollo del comercio electrónico, ofreciendo ventajas a los prestadores de servicios, ya que pueden ofrecer a quienes contraten con ellos, una vía alternativa a la jurisdicción de solución de conflictos, sin que ello suponga en modo alguno una renuncia a la misma.

La labor que desempeñan los terceros a los que acuden las partes para la resolución de los litigios existentes entre las mismas resulta fundamental, puesto que su intervención determinara en su caso la finalización del mismo. Estos terceros adquieren diferentes denominaciones y funciones, en virtud del procedimiento de resolución de conflictos concreto por el que opten las partes. Así pueden ser árbitros, mediadores y conciliadores, ellos tienen la potestad para resolver el litigio.

Los procedimientos principales están constituidos por el arbitraje, la mediación y la conciliación; en cualquier caso, mediante dichos mecanismos se pretende obtener una

solución al conflicto que se plantea, el cual podrá tener un mayor o menor grado de vinculación para las partes, así como suponer un mayor o menor grado de intervención por parte del tercero en que las partes delegan o solicitan ayuda para la solución del conflicto.

La elección del sistema de resolución de conflictos vendrá determinada por varios factores, las partes en función de la naturaleza del litigio surgido y de la necesidad de obtener una resolución especifica, acudirán a uno u otro procedimiento, debiendo garantizarse que el sistema seleccionado cumple los principios para obtener una resolución que ponga fin al conflicto surgido.

Con la finalidad de fomentar en la cultura jurídica, el acercamiento de las partes interesadas en la solución de sus diferencias, a través del diálogo y la utilización de medios alternativos que permitieran la búsqueda de soluciones creativas y ágiles a los asuntos tratados, con mayor privacidad y sencillez; el 30 de Agosto de 2002, se decreta en nuestro país la Ley de Mediación, Conciliación y Arbitraje, que en lo general contiene el procedimiento para dirimir conflictos a través de cada uno de estos mecanismos, que además lleva el objetivo de aliviar la carga judicial en los tribunales comunes.

3.1.1 MEDIACIÓN.

La administración de la justicia, es una actividad que corresponde al Estado, es él quien tiene que darle seguimiento y solucionar los conflictos que los particulares decidan someter a su conocimiento.

De lo anterior surge la idea de crear nuevas formas para resolver disputas, donde el Estado no es el principal interviniente, lo cual se da a través de los llamados métodos alternos de solución de controversias como la mediación.

Este mecanismo forma parte de los denominados métodos auto compositivos de solución de controversias, pues en ellos las partes resuelven sus diferencias por si mismas, es decir, se auto componen voluntariamente.

"La institución de la mediación tuvo su origen en el siglo pasado y se ha venido desarrollando a partir del surgimiento de los Estados Nacionales y los consecuentes conflictos dependentistas, es así que la mediación tuvo aplicación a los conflictos interestatales, de donde surge como una figura jurídica en el derecho internacional, teniendo luego aplicación en los conflictos sociales internos de los Estados."[72]

[72] Pallares Eduardo. Diccionario de Derecho Procesal Civil, Séptima Edición, Editorial Porrua, S.A. México, 1973. Pág. 471.

En el Artículo 3 literal “a” de la Ley de Mediación, Conciliación y Arbitraje (LMCA), establece que la mediación es un mecanismo de solución de controversias a través del cual, dos o mas personas tratan de lograr por si mismos la solución de sus diferencias con la ayuda de un tercero neutral y calificado que se denomina mediador.

Con base en lo anterior se dice que el mediador es un tercero que propone soluciones a las partes a fin de lograr un acuerdo entre ellos, de lo que se trata es de llegar a un punto en el que se satisfaga a ambas partes; el mediador debe contar con características de una persona creativa, original, que infunda confianza y principalmente neutral, pues se pretende que éste no favorezca a ninguna de las partes y no saque provecho alguno por su servicio en el procedimiento.

En el caso de los documentos con Firma Digital, si surgiera una controversia alrededor de éste en nuestro país, la mediación, como una forma de solucionar conflictos, no sería tan efectiva ya que el resultado que brinda este método no es vinculante para las partes y queda abierta la posibilidad de entablar un proceso. Es por esta razón que los usuarios de la firma digital, evitan esta vía.

3.1.2. CONCILIACIÓN.

La conciliación es otro método alterno de solución de conflictos; también forma parte de los métodos auto compositivos.

El Artículo 3 literal ¨b¨ de la LMCA, establece que es un mecanismo de solución de controversias a través del cual, dos o mas personas tratan de lograr por si mismas la solución de sus diferencias con la ayuda del juez o árbitro, según el caso, quien actúa como tercero neutral y procura avenir los intereses de las partes.

De lo anterior se puede observar que la conciliación es un acto mediante el cual el árbitro o el juez proponen a las partes en conflicto soluciones para que ellos mismos lleguen a un acuerdo mediante el cual se ponga fin al conflicto y se evite la iniciación o continuación de un proceso ante el Órgano Judicial. Se dice que en la conciliación interviene un tercero que propone a las partes una determinación, la cual pueden aceptarla, transformarla o discutirla libremente para que ellas mismas logren un convenio que armonice sus intereses y opiniones.

3.1.3 ARBITRAJE.

En El Salvador, el arbitraje ha sido reconocido formalmente como un medio alterno para solucionar las disputas entre las partes, ya que el Artículo 23 de nuestra Constitución ha reconocido la Autonomía de la voluntad, estableciendo que “ninguna persona que tenga la libre administración de sus bienes puede ser privada de terminar sus asuntos civiles o comerciales por transacción o arbitramiento”. En virtud de este principio, las personas capaces de obrar pueden obligarse según lo consideren y con las modalidades que convengan entre si.

La LMCA en su Artículo 3 literal “c”, expresa que el Arbitraje es “un mecanismo por medio del cual las partes involucradas en un conflicto de carácter transigible, difieren su solución a un tribunal arbitral, el cual estará investido de la facultad de pronunciar una decisión denominada Laudo Arbitral”.

De esta manera podemos decir que el arbitraje constituye una vía alterna que tienen los particulares para dirimir sus diferencias sometiéndolas al conocimiento de un árbitro para que éste las resuelva a través de un Laudo.

En el arbitraje debe existir la figura del convenio arbitral, el cual es un contrato en el que las partes manifiestan su voluntad de deferir la solución de sus conflictos de intereses actuales o futuros, originados en una relación contractual o una situación de derecho, a la justicia arbitral, quedando derogada la jurisdicción ordinaria.

La decisión que toma el árbitro se denomina Laudo Arbitral, que es una decisión definitiva que pone fin a la controversia que le ha sido sometida. El laudo es equiparable a una sentencia, pues participa de su mismo carácter imperativo y posee, una vez firme y ejecutoriada, autoridad de cosa juzgada. El laudo arbitral se encuentra regulado en los Artículos 59 al 65 de la LMCA.

Para nuestro trabajo de investigación, el arbitraje es el método mas utilizado para resolver controversias sobre documentos con firma digital, ya que Certicamara a través

de Diesco Ean ofrece un centro de arbitraje para dirimir conflictos entre esta institución y el titular de la firma digital; siempre y cuando se haya suscrito el convenio arbitral. Es por esta razón que los documentos que estén respaldados con un certificado emitido por Certicamara donde exista una controversia, el arbitraje es el único método, hasta ahora, para resolverlos.

3.2 LA PRUEBA EN LOS MEDIOS ELECTRÓNICOS.

Hoy en día, la utilización de la tecnología de la información y el desarrollo de la contratación electrónica esta haciendo disminuir la utilización del papel escrito, sustituyéndolo por documentos electrónicos. Es de esta manera que la firma manuscrita decae a favor de la digital.

Es el caso que, en la mayoría de las legislaciones se contempla de forma expresa y específica la valoración, cotejo y eficacia probatoria de los medios de prueba válidos en juicio, pero está inconclusa la valoración del documento electrónico –en su sentido más amplio- como una forma de almacenamiento de información.

La falta de regularización en dicha materia crea incertidumbre, obstaculizando el desarrollo de nuevos productos y servicios, pues las normas vigentes no contemplan estas nuevas realidades, lo cual hace evidente la necesidad de crear una normativa que regule todo lo relativo a los actos realizados por medios informáticos o telemáticos, adecuándolo a sus características propias, dinamizándola y modernizándola a fin de

adaptarla a los mercados internacionales cada vez mas globalizados. Es indispensable que existan leyes que faciliten el comercio electrónico, brindando seguridad a todos los actores participantes de esta nueva forma de hacer comercio.

En El Salvador, no existe una ley que regule claramente al comercio electrónico, pero existe una iniciativa de la Asamblea Legislativa a través del programa nacional de competitividad, del Ministerio de Economía, un Anteproyecto de Ley de Comercio Electrónico, que recoge y presenta el trabajo realizado por el Centro Nacional de Registros, en conjunto con reconocidos bufetes privados y abogados particulares. El Objeto de dicho Anteproyecto está plasmado en su Art. 1, el cual es normar la utilización de mensajes de datos y comunicaciones electrónicas, cualquiera sea la forma utilizada, en el contexto de actividades comerciales en el ámbito nacional e internacional, de tal manera que ellas puedan ser acreditadas válidamente, mediante procedimientos de seguridad electrónicos ya existentes y que a su vez permitan dar claridad, seguridad, autoría y autenticidad de las mismas.

Para la realización del presente Capítulo sobre la Prueba en los medios electrónicos, se tomará como base legal el Anteproyecto de Ley de Comercio Electrónico de El Salvador; que en lo sucesivo llamaremos el anteproyecto, aunque no se contempla como una ley en sentido estricto, en su debido momento puede llegar a constituirse como tal; puesto que el anteproyecto plantea la admisibilidad y fuerza probatoria de los mensajes de datos, en su Art. 12, estableciendo que “los mensajes de

datos serán admisibles como medio de prueba y su fuerza probatoria es la otorgada por la presente ley. Este medio y fuerza probatoria que da admisión a un mensaje de datos prevalecerá sobre cualquier otro que lo contraríe sin perjuicio de cualquier otra forma de prueba establecida en nuestra legislación común."

En el proceso, la apreciación de la prueba constituye una de las actividades más importantes que desarrolla el juez, a quien le corresponde examinar la prueba rendida y valorarla, determinando la eficacia de los diversos medios probatorios y la influencia que ejercen en la formación de su convicción, y de esta manera resolver el asunto controvertido.

Pero todo lo anteriormente mencionado solo puede realizarse dependiendo del sistema de valoración de prueba con el que cuente determinada legislación.

3.2.1 SISTEMAS DE VALORACIÓN DE LA PRUEBA.

Tenemos que dentro de los diferentes sistemas de valoración de la prueba, los más conocidos son: de la prueba legal, tasada o regulada; el de la libre convicción y, el de la sana crítica. De los cuales podemos decir lo siguientes:

a. <u>El sistema de valoración legal, tasada o regulada:</u> Este sistema es aquel en el cual la ley señala al tribunal competente por anticipado, el grado de eficacia justificativa de cada uno de los elementos probatorios admitidos.

b. El sistema de prueba de libre convicción: En este sistema se sigue un criterio distinto, un tribunal puede decidir en conciencia, evaluando libremente el merito de las pruebas rendidas.

c. El sistema de la sana crítica: Este sistema es aquel en el cual el tribunal debe aproximarse a la verdad judicial de la mano de sus conocimientos jurídicos, se razona sobre la ponderación de los aspectos técnicos, sobre su experiencia personal, la lógica, el sentido común, el buen juicio, todo esto sobre la base de los medios de prueba que señala la ley.

En los ordenamientos jurídicos que se rigen por medio del principio de prueba legal, como es el caso del ordenamiento jurídico salvadoreño, la misión del documento electrónico como medio de prueba, queda limitada, ya que requiere que el legislador lo considere de una forma expresa, directa o indirecta, como idóneo para acreditar un hecho. Por esta razón, el art. 13 del Anteproyecto, establece que "para la valoración de la fuerza probatoria de los mensajes de datos , se tendrán en cuenta las reglas de la sana crítica...", con lo cual deja al criterio del juzgador la valoración del documento, teniendo en cuenta la confiabilidad en la forma en que se haya generado, archivado o comunicado el mensaje, la confiabilidad en la forma en que se haya conservado la integridad de la información, la forma en que se identifique al iniciador, el tipo de procedimiento que se haya utilizado para mantener la seguridad y cualquier otro factor pertinente.

3.2.2. PRINCIPIOS PROBATORIOS.

En el ámbito electrónico, la constitución de la prueba es un aspecto sumamente importante, ya que para la celebración de cualquier acto por este medio se requiere que los derechos y obligaciones se establezcan para preconstituirlos, en virtud de que al momento de hacerla valer en juicio demuestre la veracidad de los hechos y pueda deducirse la responsabilidad por el cumplimiento o incumplimiento de la obligación.

Es por eso, que se hace necesario que se respeten los principios probatorios siguientes:

a. Asimilación de lo escrito bajo formato electrónico con lo escrito sobre un soporte papel.

Con este principio lo escrito bajo forma electrónica adquiere la misma fuerza probatoria que lo escrito en papel. Ya que en el comercio electrónico se desmaterializa la relación entre las partes, teniendo estas a su cargo la obligación de establecer en todo los casos un instrumento para preconstituir la prueba ya que no es posible hacerlo en forma tangible, puesto que toda la relación jurídica se realiza a través de medios electrónicos.

b. La equivalencia funcional plena entre el documento electrónico con firma digital y el documento con firma manuscrita.

Se debe reconocer plena validez a los actos y contratos otorgados por personas naturales y jurídicas, publicas o privadas, suscritos por medio de firma digital, los cuales serán validos de la misma manera y producirán los mismos efectos que los celebrados

por escrito y suscritos en forma manual. Existen cinco limitaciones en cuanto al valor probatorio de los documentos firmados por medios electrónicos, el art. 2 del Anteproyecto establece que el documento electrónico no puede ser aplicable en los siguientes casos y materias:

- Derecho sucesoral
- Derecho de familia
- Aquellos actos jurídicos o contratos para los cuales otras leyes exijan expresamente que, se realicen en escritura pública o requieran de la concurrencia personal de al menos una de las partes.
- Aquellas advertencias escritas que por disposición legal deban ir necesariamente impresas en cierto tipo de productos en razón del riesgo que implica su comercialización, uso o consumo.
- Obligaciones contraídas por el Estado de El Salvador en virtud de convenios o tratados internacionales.

c. Los documentos electrónicos podrán ser presentados en juicio.

Eso quiere decir que se debe admitir en forma igualitaria a unos y otros como prueba en juicio no importando que sean o no sean materiales o intangibles.

3.2.3. REGLAS PROBATORIAS.

En los países cuya legislación ha aceptado la presentación de los documentos electrónicos como medio de prueba en juicio, el Juez debe sujetarse a las reglas siguientes:

a. El juez aceptará su presentación como prueba, considerando los antecedentes de fiabilidad de la forma en que se generó, archivó o comunicó el respectivo documento y de la conservación de su integridad.

b. Los documentos cuya firma digital esté debidamente certificada por prestadores acreditados, tendrán el mismo valor que los instrumentos privados o públicos, según sea su naturaleza. Si se tratare de un documento privado, se tendrá por reconocida su autoría e integridad, pero en el caso de un instrumento público, los documentos electrónicos no tendrían el mismo valor, ya que deberán ser extendidos u otorgados por funcionario competente.

c. Los documentos electrónicos no comprendidos en los dos casos anteriores, solo podrán estimarse como base de una presunción judicial. El objeto de esta regla residual es que todo documento electrónico que no pueda ser considerado como un instrumento público o privado, pueda servir como base o antecedente para que el tribunal configure una presunción judicial a partir de este.

d. La producción de la prueba de los documentos electrónicos, se regirá por las normas generales que sean aplicables en consideración a la naturaleza del documento, y dándole amplitud a esta regla, también en todos aquellos medios de prueba que no sea la documental, siempre y cuando se adecue a las peculiaridades de la informática.

e. En los procedimientos en que el juez deba valorar el merito probatorio de acuerdo a su libre convicción o según las reglas de la sana critica, no regirán las reglas b y c, ya que el tribunal será soberano para asignar valor probatorio a los documentos electrónicos, tengan o no firma digital que los ampare.

3.3 VALOR PROBATORIO DEL DOCUMENTO ELECTRÓNICO.

En el contexto actual se vienen realizando importantes transacciones comerciales, bancarias y aduanales utilizando la vía informática o telemática, en las cuales desaparece el documento escrito, impreso en papel para ser reemplazado por el documento electrónico.

Tradicionalmente, el documento en sentido estricto, es considerado de igual manera que el escrito, es decir, como un *"conjunto o instrumento en el que queda plasmado un hecho que se exterioriza mediante signos materiales y permanentes del*

lenguaje".[73] En su significación amplia, el documento puede ser la representación de un hecho u objeto perceptible que puede servir de prueba en un proceso. Para el autor Cardoza Isaza, documento es *"cualquier cosa que siendo susceptible de ser percibida por la vista, el oído o ambos, sirve por si misma para ilustrar o comprobar, por vía de representación la existencia de un hecho cualquiera o la exteriorización de un acto humano".* [74]

En la tradición jurídica ha prevalecido la teoría del documento como escrito, impreso en papel y avalado mediante una firma. Desde este punto de vista se ha considerado al documento como prueba privilegiada, única e insustituible, ya que no se puede modificar fácilmente, y en tanto prueba preconstituida, se dice que el documento acredita, demuestra derechos y obligaciones, dentro y fuera del proceso. Así, todo acto que se ha formalizado en documento escrito se le reconoce fuerza probatoria.

El Anteproyecto recoge en el Art. 3 una definición de documento electrónico, instituyendo que "es un formato electrónico conteniendo información electrónica que se almacena, envía, comunica, recibe, archive o genere por cualquier medio electrónico".

Doctrinariamente el documento electrónico se entiende como *"toda expresión en lenguaje natural o convencional y cualquier otra expresión gráfica, sonora o en imagen,*

[73] www.geocities.com/capitolgil/cenate8569/html.
[74] Cardoza Isaza, Jorge. Pruebas Judiciales. Librería Jurídica Welches, Bogotá Colombia, 1985. Pág. 228

recogidos en cualquier tipo de soporte material, incluso los soportes informáticos, con eficacia probatoria".[75]

Para sustentar que el documento electrónico e informático es realmente un medio probatorio, haremos referencia a la teoría representativa, según esta corriente, prueba es todo objeto representativo que pueda informar sobre un hecho o sobre otro objeto. Bajo esta óptica el documento no esta restringido a la forma escrita, ni a la naturaleza del soporte, en este caso al papel o impresa. Esta teoría es retomada por el Art.8 del Anteproyecto, ya que "los mensajes de datos tendrán efecto, validez y fuerza obligatoria como cualquier otro acto o contrato en forma material".

El día 17 de diciembre del año 1996, las Naciones Unidas, mediante resolución 2205 (XXI) pidió a la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) que fomentara la armonización y unificación progresiva del derecho mercantil internacional, para que participara en el comercio internacional electrónico y por lo tanto sobre el valor jurídico de los documentos electrónicos, a fin de garantizar la seguridad jurídica en la utilización del procesamiento informático del comercio internacional.

[75] Rivas Hernández, Salvador Antonio y Otro. La Firma Electrónica. Monografía. Universidad Francisco Gavídia, 2004, Pág. 24.

Es así, como en el artículo 5 de la Ley Modelo de esta Comisión, sobre comercio electrónico, establece que no se negaran efectos jurídicos, validez o fuerza obligatoria a la información por la sola razón de que esté en forma de mensaje de datos. Este articulo recoge el principio denominado en doctrina, de la equivalencia funcional, tratado en el Capitulo II. Esto implica aplicar a los mensajes de datos un principio de no discriminación, respecto de las declaraciones de voluntad, independientemente de la forma en que hayan sido expresadas, en este sentido los efectos jurídicos deseados por el emisor de la declaración, deben producirse con independencia del soporte en papel o electrónico donde consta la declaración.

Lo importante a la hora de equiparar los efectos jurídicos de un documento contenido en soporte papel a un documento electrónico, es la posibilidad de recuperación del mensaje en el sentido de que su contenido sea accesible posteriormente y reconocido por las partes y por terceras personas, con esta exigencia se da cumplimiento al requisito solicitado para los documentos tradicionales de duración en el tiempo. Es importante observar los requisitos de validez, pues para que un documento electrónico sea equiparable a un documento tradicional y surta los efectos queridos, es necesario que las declaraciones no estén viciadas.

El documento electrónico tendría eficacia probatoria, si además de ser válido reúne lo requisitos de idoneidad y es conducente para probar un hecho, además deberá tener establecida su autenticidad.

Cabe recalcar que el documento electrónico debería apreciarse como documento escrito, y en el caso que nuestro sistema fuera el de la libre apreciación de la prueba, el juez en su libertad probatoria le otorgaría valor; y consideraría la confiabilidad del documento en tres aspectos, como son la forma como se generó, la forma en como se ha conservado y la forma en como se identifica el iniciador.

La ley modelo de la CNUDMI sobre comercio electrónico, en el artículo 9 establece que la información presentada en un mensaje de datos gozará de la debida fuerza probatoria, cuando la ley se refiere a "debida fuerza probatoria", lo hace en cuanto al valor relativo de su eficacia probatoria, es decir, que no intenta dicha prueba gozar de privilegio frente al resto del material probatorio, sino que todas deben valorarse bajo el criterio de la sana critica, es lo que en doctrina se conoce como dependencia de la prueba complementaria, en la cual, la eficacia probatoria del soporte informático depende del resultado de la prueba complementaria: pericial, testimonial, confesional, etc. Como por ejemplo en transacciones electrónicas de datos o de control, la información obtenida, procesada por programas de computación de usuarios diferentes, puede probar las operaciones y contrataciones realizadas entre dichos sujetos, en este caso, cabe acudir judicialmente al testimonio aquellos terceros, a presunciones y a peritajes o consultas para corroborar la verosimilitud del documento.

En relación a lo anteriormente dicho por la estructura del documento electrónico, se puede considerar que el medio más idóneo de prueba lo constituye el documental, sin

embargo otro medio probatorio que es factible; es la utilización de la prueba pericial, por cuanto puede requerirse de personas con conocimientos en informática para convertir la información en el sistema en datos inteligibles para que el juez llegue al documento de forma para que este lo pueda comprender, como es el caso de un documento que se encuentre encriptado.

La prueba instrumental tiene amplio valor probatorio porque en ella aparece expresada con exactitud la voluntad del otorgante, y la desmaterialización escrita de las ideas produce desconfianza en la mente del juzgador, es decir, que la ausencia de un escrito original firmado por las partes, trae muchos inconvenientes en materia probatoria, más aún en países como el nuestro, en que estamos acostumbrados a la existencia del documento escrito como soporte documental de una transacción comercial.

Es así que, el deseo de consumidores y comerciantes que utilizan Internet para realizar sus actividades, es tener la certeza de que su uso es seguro y confiable; y principalmente que tanto la información objeto del contrato como la identidad de las partes en una operación, será verificable.

Los mensajes y documentos electrónicos que constituyen la forma en que los comerciantes y usuarios de los medios electrónicos, realizan la mayoría de estas transacciones comerciales, según nuestro Código Civil y de Procedimientos Civiles, no

podrían ser admitidos como prueba en juicio, porque el sistema imperante es el de la prueba tasada; pero en base al Art. 12 del Anteproyecto, si sería posible hacer valer un mensaje de datos como prueba en juicio, pues a través de el se documentan hechos, actos o declaraciones con relevancia jurídica.

Es común que las nuevas tecnologías no sean recogidas de forma expresa por el legislador y que además no exista una regulación acerca de su aplicación práctica en el proceso, como es el caso del Anteproyecto, ya que no se encuentra disposición alguna que regule la forma en que ha de rendirse la prueba documental dentro de un juicio, lo que trae como consecuencia, por una parte, la incomprensión de parte de los ciudadanos, y por otro lado, la inseguridad y dificultad de los abogados a la hora de ofrecer los medios probatorios informáticos en el acto postulatorio de un proceso judicial, limitando el derecho de defensa. Es necesario llevar a juicio al documento electrónico, no como prueba documental, sino como prueba electrónica.

Según Rengel Romberg*,"es difícil imaginar algún tipo de prueba que no tenga alguna semejanza con los medios tradicionalmente admitidos; dado que por regla general, el principio de libertad probatoria concuerda con el de la semejanza con los medios legales a los efectos de la valoración de aquellos; siendo una labor importante y delicada de la jurisprudencia, determinar con prudencia la legalidad de dichos medios,*

sin caer en una interpretación estrecha de los medios que coloque al juez de espaldas al progreso técnico y científico de nuestro tiempo".[76]

El documento electrónico utilizado en sí como prueba, es muy complejo, ya que deben utilizarse otros medios probatorios para acreditar en un proceso aquellos actos instrumentales o privados que estando debidamente amparados bajo el régimen legal que los establece, pueden ser objeto probatorio de hechos substanciales adecuados por las partes, con el fin de producir la formación del juicio crítico de valor procesal en el juzgador.

La posibilidad de producir o de admitir los documentos electrónicos como medio de prueba, significa que no debería de haber norma alguna que inhiba al juez para utilizar los documentos electrónicos como medios de prueba, que prevea la admisibilidad sólo en el caso de falta de otros medios de prueba, o que imponga una determinada eficacia probatoria de ellos. Esto significa que al documento electrónico el juzgador debe atribuirle plena admisibilidad hasta después de una adecuada valoración de la autenticidad y de la seguridad del documento electrónico.

"Se debe entender que el análisis del documento electrónico debe efectuarse en forma sistemática con el de la firma digital, que hace parte del documento total y es ella la que le da validez; y por ende el valor del contenido de este se encuentra supeditado a

[76] www.virusprot.com/art.36html/trabajofirmavenezuela#.asp

la confirmación de autenticidad de la firma. Ya que la firma digital en términos de confiabilidad es superior a la manuscrita en la medida que no solo atestigua la identidad del firmante sino que además brinda una constancia sobre el contenido del mensaje de datos al que está fijada pues este no puede ser reformado posteriormente y en el caso que se llegase a hacer la firma quedaría invalida por haber sido vulnerada.''[77]

Finalmente, la problemática que se presenta con la admisibilidad y valoración de los documentos electrónicos en juicio en los casos en que la ley nada dice, debe resolverse con prudencia. Abordar en forma directa el tema del documento electrónico como medio de prueba, su valor y la validez de las firmas digitales, permitiría que el juez adopte una actitud distinta frente a su presentación en juicio, al sentirse respaldado para admitirlo y valorarlo, ya que estaría tratando con un medio de prueba legal expreso. Es necesaria una reforma a la legislación civil que admita las modalidades de prueba que se admiten en la legislación procesal penal, más todo aquellos medios técnicos que correspondan al concepto amplio de documento.

3.4 MEDIOS PROBATORIOS.

Podemos decir que la prueba electrónica se refiere, en un sentido meramente restringido, al documento electrónico o mensaje de datos en su esencia más pura y

[77] Op Cit, Cubillos Velandia, Pág. 228

simple, ya sea que éste se encuentre acompañada o no de firma digital o acompañada de certificación.

Es el caso que dentro del Comercio Electrónico cobran fuerza probatoria otros medios de prueba, tales como: la prueba pericial y las presunciones judiciales, ya que éstos también pueden ser de gran utilidad para acreditar el contenido o la firma de un documento electrónico, tomando como base el Anteproyecto, desarrollaremos los siguientes medios de prueba:

3.4.1 PRUEBA ELECTRÓNICA DOCUMENTAL.

- Documento Electrónico o Mensaje de Datos.

Actualmente, podemos afirmar que la prueba por instrumentos o por documentos electrónicos ha tomado un carácter natural, ya que se encuentran representados por cualquier sistema informático, electrónico o telemático.

En primer lugar cabe precisar, en cuanto al documento electrónico, que no constituye prueba electrónica el texto impreso en papel que proviene de una computadora y está acompañado de firma; en todo caso, este es un documento privado en sentido tradicional.

Como mencionamos anteriormente, el verdadero documento electrónico es el que se crea, conserva, transmite y que eventualmente se firma por medios electrónicos, sin

importar que pueda convertirse o reproducirse en papel, ya que se plasma en soporte papel con la única finalidad de facilitar su manejo y estudio.

Para garantizar la seguridad de los datos, se da la adopción de técnicas criptográficas para escribir los datos y programas de una manera ininteligible para quienes desconozcan la clave criptográfica y el algoritmo de transformación. De esta manera, el mensaje de datos será válido, siempre y cuando se garantice su seguridad, aún cuando la ley exija el requisito en papel; tal como se encuentra plasmado en el Art. 15 Inc. 1° del Anteproyecto, al indicar que, el mensaje de datos que se produce entre las partes tendrá efectos jurídicos, validez y fuerza obligatoria, por contener en el una manifestación de voluntad.

Podemos decir también que un mensaje de datos satisface los requerimientos tradicionales de la escritura, la firma y el original. Con relación a la escritura, en donde la información debe constar por escrito, queda cumplido con un mensaje de datos, pero siempre y cuando la información que él contenga pueda ser conocida posteriormente. En el caso de la firma, el requisito queda cumplido si el método que se utiliza para firmar reúne las siguientes características:

- Permite identificar a la persona y así determinar que ha consentido en el contenido del mensaje de datos y;

- Es fiable y apropiado a los fines para los cuales se generó o comunicó el mensaje de datos.

En cuanto al requisito del original, pareciera que los mensajes de datos no podrían cumplir con el, ya que se entiende por tal el soporte en el que por primera vez se plasma la información y los destinatarios del mensaje, en este caso, siempre reciben una copia de estos. En el artículo 8 de la Ley Modelo de la UNCITRAL se establece que cuando la ley incorpora el requisito de que la información sea presentada o conservada en su forma original, quedará cumplido siempre y cuando:

- Existan garantías fidedignas de que la información se ha mantenido inalterada desde el momento en que se generó y;
- La información esté disponible cuando sea requerida;

Es así como el Anteproyecto, retoma en su Art. 14 los dos requisitos anteriores, agregándole la que consiste en *"...que se conserve toda la información que permita determinar el origen, el destino del mensaje, la fecha y la hora en que fue enviado o recibido el mensaje o producido el documento."*

Es de esta manera que a través de estos requisitos que debe contener un documento o información electrónica queda cumplido la conservación del mensaje de datos.

"En cuanto a la aportación de los originales puede existir cierta dificultad de interpretación en cuanto a los registros electrónicos; ya que los documentos pueden estar o no en posesión de las partes, lo que se tendrá que resolver si el juez entiende que es trascendente para la sentencia. Si el juez determinare su exhibición, se hará una comprobación in situ de los dispositivos generadores del documento electrónico en el establecimiento u oficinas donde se encontraren"[78]

En los países en que ésta situación está regulada, los datos registrados electrónicamente tienen el mismo valor probatorio que los documentos privados en soporte papel, con tal que se encuentren firmados digitalmente; pero a falta de ésta, se apegan a la prueba por presunción judicial.

- El valor probatorio del documento electrónico certificado.

Una vez que el documento electrónico ha sido verificado y que cumpla con las cuatro condiciones que hacen posible que se asemeje con el documento escrito, es decir, autenticidad, fiabilidad, inalterabilidad y accesibilidad, a través de los mecanismos de seguridad en Internet, entonces, se podrá otorgar valor probatorio al mismo, además de cumplir con aspectos procesales como pertinencia, esencialidad, indubitabilidad, y que en su obtención no se ha violado ningún derecho, y no han sido contradichos por otros elementos probatorios.

[78] Lorenzetti, Ricardo L, Comercio Electrónico. Editorial Abeledo Perrot, Buenos Aires, Argentina, Pág. 86.

También gozará de legitimidad, si mediante prueba pericial, por medio de un análisis criptográfico de la firma digital u otro mecanismo conveniente se determine la autoría, autentificación e integridad del mismo, siempre y cuando se observe la ausencia de manipulaciones y la fidelidad de los procedimientos del registro electrónico con la manifestación de voluntad de las partes en su intención de obligarse.

3.4.2 PRUEBA ELECTRÓNICA PERICIAL.

La complejidad técnica de los conocimientos informáticos, exige que los jueces sean auxiliados por peritos en la materia, entonces el peritaje se convierte en el segundo medio de prueba que tiene características propias en el comercio electrónico.

La pericia electrónica es un tópico complejo ya que por el surgimiento rápido y constante de nuevas técnicas se plantean nuevas ideas sobre la metodología que debe aplicar un perito informático. El Anteproyecto plantea en su Art. 13 Inc. final que *"para la valoración de las pruebas, el juez, árbitro o mediador que juzga el caso deberá designar los peritos que considere necesarios pues en base a su conocimiento técnico e interpretación de las pruebas presentadas le servirán para su análisis y calificación."* Es por esto que la prueba pericial es considerada un medio de prueba electrónico complementario, ya que el resultado de la pericia refuerza la convicción del Juez.

Existen técnicas que se usan en el desarrollo de aplicaciones o en auditoria informática, pero que también pueden ser utilizadas en algún caso pericial concreto; después de todo, el perito habrá de elegir la técnica más adecuada o una combinación de varias, efectuando pruebas simples con datos específicamente preparados para ello o bien pruebas integradas, que pueden combinarse con la grabación de los datos leídos, que pueden permitir detectar codificación errónea o no autorizada.

El uso de ciertas técnicas periciales puede dar como resultado una conclusión sobre la existencia, integridad y probable origen de datos informáticos en particular, para determinar la veracidad de un hecho o de un acto jurídico sostenido en juicio.

En la contratación electrónica, la prueba pericial puede llegar a determinar el contenido y la autenticidad del documento electrónico e informático, siempre que éste sea relevante en la controversia, y más que nada, mediante el análisis criptográfico de la firma digital. Cabe recordar que la labor del perito consiste en brindarle al juez una base científica, técnica o práctica, para que éste sea capaz de juzgar la controversia sobre lo que versa el informe pericial.

3.4.3 LAS PRESUNCIONES ELECTRÓNICAS.

La prueba por presunción regulada en el Anteproyecto recoge tres presunciones, la primera referida al origen del mensaje de datos, la segunda sobre el contenido del mensaje de datos, y la tercera acerca de la recepción del mensaje de datos.

La presunción sobre el origen del mensaje de datos se refiere a que, se va a suponer que el mensaje ha sido enviado por el emisor cuando este haya acordado con el destinatario el procedimiento para descifrar el mensaje de datos, y cuando lo haya enviado una persona designada por el emisor para tal efecto; pero existen dos excepciones en cuanto a esta presunción ya que se tendrá como no enviado por el emisor cuando el destinatario haya sido informado que el mensaje de datos no fue enviado por el emisor y en el caso que sabiéndolo hubiera actuado con la debida diligencia o que de haber aplicado algún método convenido hubiera sabido que el mensaje de datos no provenía del iniciador, todo esto regulado en el Art. 17 del Anteproyecto.

Respecto a la segunda presunción podemos decir que en el comercio electrónico se presumirán válidos los documentos o registros informáticos, siempre y cuando sean una reproducción y registro fiel y completo de los documentos o registros originales y de su contenido, regulado en el Art. 18 del Anteproyecto.

En la tercera presunción podemos decir que si al enviar un mensaje de datos o antes de enviarlo, el emisor acuerda con el destinatario que este ultimo avise que el mensaje ha sido recibido, estamos hablando del acuse de recibo, regulado en el Art. 20 del Anteproyecto; ahora bien cuando el emisor reciba este acuse de recibo de parte del destinatario se presumirá que este ultimo ha recibido el mensaje, pero esto no implica que el mensaje de datos recibido corresponda con el mensaje enviado, salvo prueba en contrario, tal y como lo establece el Art. 21 del Anteproyecto.

Excepto en los casos en que la Ley lo prohíba expresamente, la presunción admitirá prueba en contrario, dirigida a probar la inexistencia del hecho presunto como a demostrar que no existe el enlace que ha de haber entre el hecho que se presume y el hecho probado o admitido que fundamente la presunción. Pretendiendo demostrar que si alguna prueba en contrario acredita completamente que el documento original del que se deduce, está manipulado o no es auténtico queda desvirtuada la presunción.

3.5 REGULACIÓN JURÍDICA DE LA PRUEBA ELECTRÓNICA EN EL SALVADOR.

Al momento de enfrentar un proceso judicial, los medios probatorios típicos son elementos fundamentales para determinar y configurar los hechos y valorar los mismos para establecer la sentencia sobre el caso en la investigación.

Sin embargo, al aportar documentos electrónicos como prueba electrónica se plantea una revisión diferente de los medios, dado que los jueces no cuentan con suficiente conocimiento para analizarlo y por ende, valorarla.

Como ya se dijo anteriormente, el documento electrónico es admisible en aquellos países donde está consentido el sistema de libre apreciación de la prueba, es decir, siguiendo las reglas de la sana crítica para aquellos medios de prueba que no están excluidos de forma expresa en la ley. Es en ese sentido, donde el juzgador deberá

atribuirle a ese medio de prueba, validez y fuerza probatoria, luego de la adecuada valoración del mismo.

Es por ello que algunos países han tomado a bien la admisión de los medios electrónicos como instrumentos probatorios, afirmando que *"los computadores y los medios electrónicos deben sumarse a las herramientas jurídicas procesales, puesto que son una expresión de la realidad que el derecho no puede desconocer."*[79]

En nuestro país, el código civil adopta el sistema de la prueba tasada, en el cual, la ley establece los medios de prueba, la forma de rendirla en juicio y la valoración que debe darle el juez. Es por ello que la prueba tiene un valor inalterable y constante donde se prescinde del criterio o apreciación del juez.

En el Código Civil, este sistema esta tratado en el Titulo XXI del Libro IV; así tenemos que en el articulo 1569 de este cuerpo normativo señala: *"Las pruebas consisten en instrumentos públicos o privados, testigos, presunciones, confesión de parte, juramento deferido e inspección personal del juez y peritos."* El Código de Procedimientos Civiles, de igual manera, enumera los medios de prueba y reglamenta la manera como se produce esta ante los tribunales, en el Título IV del Libro I.

[79] Vargas Frontera, Ginay del Valle. Valor Probatorio de los Medios Electrónicos en el Derecho Comparado, particularmente en la legislación mexicana, española, francesa y venezolana. Informe de Investigación Jurídica, Guayana, 2003, Pág. 75.

En materia mercantil, de acuerdo con el articulo 999, las obligaciones mercantiles se prueban por los medios siguientes: instrumentos públicos, autentico y privado, factura, correspondencia postal y telegráfica reconocida, registros contables, testigos y demás admitidos por la ley. Y en el caso de contratos, se aplicaran supletoriamente las disposiciones del código civil, según lo estipulado en el articulo 945 C.Com.

De lo anterior podemos señalar que en nuestra legislación civil y mercantil, no existe norma alguna que otorgue valor probatorio al documento electrónico. Sin embargo, existen leyes especiales que si le reconocen valor probatorio, las cuales son: la Ley de Bancos, Ley de Anotaciones Electrónicas de Valores en Cuenta, Ley del Mercado de Valores, la Ley Orgánica de la Superintendencia de Valores, Ley General Marítimo Portuaria, Ley de Mediación, Conciliación y Arbitraje, Ley de Simplificación Aduanera, Anteproyecto de Ley de Comercio Electrónico del Ministerio de Economía.

LEY DE BANCOS

Esta Ley tiene por objeto regular la función de intermediación financiera y las otras operaciones realizadas por los bancos, propiciando que estos brinden a la población un servicio transparente, confiable y ágil, que contribuya al desarrollo del país, esta ley en su Capitulo II, de las OPERACIONES PASIVAS, articulo 56 literal “l”, denominado “Términos de referencia aplicables”, establece que:

"Art. 56 Para la elaboración de las normas a que se refiere el articulo precedente los bancos tomarán en cuenta:

l) Que los bancos podrán celebrar operaciones y prestar servicios con el público mediante el uso de equipos y sistemas automatizados, estableciendo los contratos respectivos, las bases para determinar las operaciones y servicios cuya prestación se pacte; los medios de identificación del usuario y las responsabilidades correspondientes a su uso; y los medios por los que se hagan y obligaciones inherentes a las operaciones y servicios que se trate.

El uso de los medios de identificación que se establezca conforme a lo previsto en este literal, en sustitución de la firma autógrafa, producirá los mismos efectos que los que las leyes otorguen a los documentos correspondientes y en consecuencia, tendrán el valor probatorio; cuando estas operaciones se realicen mediante contratos de adhesión, los modelos de dichos contratos deberán ser previamente depositados en la Superintendencia, quien podrá, mediante decisión fundamentada, en un plazo no mayor de treinta días a partir de la fecha del depósito del modelo, requerir los cambios necesarios cuando contengan cláusulas que se opongan a la legislación o cuando se consideren violatorios a los derechos del cliente. En todo caso el banco estará obligado a explicar al cliente las implicaciones del contrato, previo a su suscripción."

Esta disposición es la única que en toda la legislación salvadoreña otorga la misma validez de la firma manuscrita a la firma digital, y a la vez permite la implementación de medios informáticos o telemático en transacciones bancarias.

En el Capitulo III, de las OPERACIONES ACTIVAS, Art. 60 inciso 1°, "De los sistemas de pagos y las transacciones electrónicas", de la misma ley, también establece que:

"Las operaciones activas y pasivas que efectúen los bancos y otras instituciones a través de las cuentas que se manejan en el Banco Central, podrán realizarse mediante el intercambio electrónico de datos. Para tal efecto, tendrá validez probatoria los registros o bitácoras contenidas en los sistemas informáticos, las impresiones que reflejan las transacciones efectuadas por los mismos registros de firmas digitales o de números de identificación personal de los participantes autorizados en dichos sistemas. Las certificaciones extendidas, por el funcionario autorizado por el Banco Central, serán de carácter irrevocable"

Este artículo establece los registros que se llevarán de firmas digitales.

LEY DE ANOTACIONES ELECTRONICAS DE VALORES EN CUENTA

Esta Ley establece como objeto la regulación de la creación, administración, y demás actos que recaen sobre las anotaciones electrónicas en cuenta, consiguiendo así garantizar a los ciudadanos, bajo una perspectiva constitucional, la libre contratación con la bolsa de valores y las centrales de depósitos y custodia de valores, y así garantizar a las instituciones legalmente autorizadas la realización de dichas operaciones, concediéndoles por medio de este cuerpo normativo, las herramientas jurídicas necesarias para hacer uso de las tecnologías de la información para tal efecto.

LEY DEL MERCADO DE VALORES

Este cuerpo normativo tiene como objeto regular la oferta pública de valores y a estos, sus transacciones, sus respectivos mercados e intermediarios y a los emisores, con la finalidad de promover el desarrollo eficiente de dichos mercados y velar por los intereses del público inversionista, disponiendo en sus artículos 27 literal "b" y 45, que las transacciones se pueden llevar a cabo por medios electrónicos, y estos expresan literalmente que:

"Autorización de operaciones

Art. 27 Cada bolsa, para obtener autorización de operar, debe acreditar, ante la Superintendencia que:

b)Tiene la organización, los medios y procedimientos adecuados para la realización de transacciones que permitan a los inversionistas la buena ejecución de sus ordenes e instrucciones. Los medios y procedimientos podrán ser electrónicos.

Operaciones Bursátiles

Art. 45 Las operaciones en una bolsa podrán realizarse de viva voz o por medio de sistemas de negociación electrónica y podrán ser:

a)Al contado;

b)A plazo;

c)Operacionales, de compra o venta; y

d)Otro tipo de operaciones que autorice previamente la Junta Directiva de cada bolsa mediante la correspondiente incorporación a su reglamento"

Estas disposiciones otorgan plena validez a las transacciones bursátiles que sean realizadas por medios o procedimientos informáticos o telemáticos, y como consecuencia de la misma, la necesidad de su respectiva y efectiva regulación, es así como en el reglamento de esta ley se establecen los requisitos que deberán reunir los registros electrónicos para brindar la seguridad necesaria a todos los sujetos intervinientes dentro de las actividades del mercado de valores.

LEY ORGANICA DE LA SUPERINTENDENCIA DE VALORES

Esta Ley establece y regula las funciones de la Superintendencia de valores, y dentro de ellas establece en su articulo 38 la facultad que ésta tiene de fiscalizar las contrataciones bursátiles que sean realizadas por medios electrónicos y telemáticos, que son representantes del comercio electrónico como una forma de contratación y actividad mercantil.

LEY GENERAL MARITIMO PORTUARIA

Este cuerpo normativo tiene por objeto regular las actividades relacionadas a la promoción, desarrollo y defensa de los intereses marítimos, al control y vigilancia de los asuntos relativos al mar y al ejercicio de la soberanía y jurisdicción en el territorio marítimo y aguas continentales de El Salvador; y para realizar ciertas transacciones tales como la recepción de mercancías contemplada en su Art. 88, ésta permite que se realicen por medio de intercambio electrónico de datos y que la firma de éstos se puede dar por medios electrónicos, lo cual contempla el articulo 90 de esta ley, y que literalmente dice:

"Intercambio electrónico de datos

Art. 90 Para la emisión de los documentos a que se refieren los artículos anteriores, podrá emplearse cualquier medio por el que quede constancia de la información que contenga. Cuando el usuario y el armador o transportador hayan convenido en comunicarse electrónicamente, dichos documentos podrán ser sustituidos por un mensaje de intercambio electrónico de datos.

La firma podrá ser manuscrita, o bien estampada mediante facsímil o autenticada por un código electrónico."

Con esta disposición, la ley declara la importancia de la introducción de los medios electrónicos en todos los ámbitos de la sociedad que ayudan a su desarrollo.

LEY DE MEDIACION, CONCILIACION Y ARBITRAJE

Este marco normativo establece el régimen jurídico aplicable al arbitraje, sin perjuicio de lo dispuesto en los tratados o convenios internacionales vigentes, así mismo reconoce la eficacia de otros medios alternativos, que opcionalmente pueden adoptar las personas naturales o jurídicas capaces, en asuntos civiles o comerciales, sobre los cuales tengan la libre disposición de sus bienes y que sean susceptibles de transacción o desistimiento; así como lo establece el Art. 23 de nuestra Constitución donde expresa que *"ninguna persona que tenga la libre administración de sus bienes puede ser privada del derecho de terminar sus asuntos civiles o comerciales por transacción o arbitramiento."*

Dentro de lo referente al arbitraje que regula la presente ley al referirse a las modificaciones y comunicaciones permite que éstas sean por medios electrónicos así como lo establece el Art. 27 literal "d":

"Art. 27 Las notificaciones y comunicaciones escritas previa la iniciación del procedimiento arbitral se regirá por las siguientes reglas:

d)Las notificaciones serán igualmente válidas cuando se hicieren por correo certificado, telex, facsímil, o cualquier otro medio de comunicación de la cual pueda quedar una constancia respecto de haber sido recibido por su destinatario."

También cuando esta ley se refiere al convenio arbitral en su Art. 29 inciso 3° expresa que *"el convenio se ha formalizado por escrito cuando esté contenido en documento único suscrito por las partes, sino también cuando resulte del intercambio de cartas o de cualquier otro medio de comunicación y correspondencia que inequívocamente deje constancia documental de la voluntad de las partes de someterse al arbitraje....."*

Esta disposición no establece específicamente que los medios por los cuales se puede exteriorizar el convenio arbitral sean electrónicos ya que deja la posibilidad abierta para que sea cualquier otro medio de comunicación o correspondencia, concluyendo que sí es posible utilizar cualquier otro medio de comunicación como los informáticos o telemáticos.

LEY DE SIMPLIFICACION ADUANERA

En nuestro país, esta normativa y para efectos de nuestro trabajo, es la que más claramente establece un sistema para la implementación del uso de la firma digital porque tiene por objeto establecer el marco jurídico básico para la adopción de mecanismos de simplificación, facilitación y control de las operaciones aduaneras, ya que plantea el uso de sistemas automáticos de intercambio de información. Constituye la base jurídica para el funcionamiento del sistema de Teledespacho, la cual consiste principalmente en intercambiar información específicamente de la declaración de mercancías con la Dirección General de la Renta de Aduanas, tal como lo establece el Art. 6 inciso primero de este cuerpo normativo al expresar que: *"La declaración para destinar aduaneramente las mercancías, deberá efectuarse mediante transmisión electrónica de la información, conforme los lineamientos y formatos físicos y electrónicos establecidos por la Dirección General, a través del sistema conocido como Teledespacho, el cual, para asegurar la integridad de los flujos de información, deberá estar estructurado por procedimientos que aseguren la autenticidad, confidencialidad, integridad y no repudiación de la información transmitida...."*.

El tercer inciso de este mismo artículo reconoce que: *"Los documentos contenidos en un soporte magnético, digital o electrónico producirá los mismos efectos jurídicos que los escritos en un soporte de papel.....Cuando la ley requiera que la información conste o que la misma sea presentada y conservada o archivada en su*

forma original, ese requisito quedará satisfecho con un mensaje de datos, siempre que la información contenida en este sea accesible para su ulterior consulta."

De acuerdo al último inciso de éste artículo *"En todo trámite legal, no se dará aplicación a disposición alguna que sea óbice para la admisión como prueba de un mensaje de datos".*

El Art. 8 de este cuerpo normativo establece que la firma digital o electrónica sustituye la firma manuscrita y a la vez le otorga los mismos efectos legales.

ANTEPROYECTO DE LEY DE COMERCIO ELECTRONICO DEL MINISTERIO DE ECONOMIA.

Debido al desarrollo del comercio electrónico en El Salvador, el Ministerio de Economía y la Fundación Salvadoreña para el Desarrollo Económico y Social (FUSADES) a través de su departamento de estudios legales, ha sido invitada para la revisión de este anteproyecto, el cual establece el marco regulatorio que vendría a normar la contratación electrónica y por ende la validez y eficacia del documento electrónico, firma digital y el valor probatorio de los mismos.

CAPITULO IV

SIMILITUDES Y DIFERENCIAS DE LA REGULACION JURIDICA DE LA FIRMA DIGITAL EN EL SALVADOR, ESPAÑA, COLOMBIA Y ARGENTINA; ASI COMO LAS VENTAJAS Y DESVENTAJAS DE SU USO.

4.1 EL SALVADOR Y ESPAÑA

La Ley 59/2003 entró en vigor el 19 de Diciembre del año 2003.

4.1.1 SIMILITUDES

CONCEPTO

La Legislación española recoge un concepto amplio de Firma Digital, plasmado en el Art. 3 numeral 2 de la Ley 59/2003, según el cual *"La firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control"*. En la legislación salvadoreña, tomando como punto de referencia la Ley de Simplificación Aduanera con sus reformas, encontramos un concepto de Firma Digital en su Art. 8 inc. 4°: *"Para la ejecución de las distintas actuaciones que conforman el sistema de teledespacho y para el intercambio de la información en general, cada usuario autorizado, contará con una pareja de claves o llaves únicas y correspondientes entre si, una pública y otra privada, de manera tal que*

ambas se correspondan de manera exclusiva y excluyente... La vinculación de ambas llaves o claves constituye la firma digital... que permite al receptor de un mensaje electrónico verificar con certeza la identidad proclamada por el transmisor, impidiendo a este ultimo desconocer en forma posterior la autoría del mensaje." Con esto podemos concluir que ambas legislaciones aportan un concepto relativo a la Firma Digital.

VALOR PROBATORIO

En este punto queda claro que al tomar en cuenta el valor probatorio de la Firma Digital, la legislación española proporciona una fuerte aseveración al otorgarle total y pleno valor probatorio a la Firma Digital en caso de controversia, tal y como lo podemos contemplar en el Art. 3 numeral 8, que dice que *"los datos firmados electrónicamente serán admisibles como prueba documental en juicio"*, ya que una vez emitido el cerificado por el prestador de servicios, se constituye en un garante de la integridad del flujo de información, así como de su autenticidad, confidencialidad, integridad, y la mas importante de todas, el no repudio, que juntas son la base del valor probatorio.

En la Ley de Simplificación Aduanera se le otorga valor probatorio a los documentos contenidos en el intercambio electrónico de información, ya que le otorga el mismo efecto jurídico que lo escrito en soporte papel, tal y como lo establece el Art. 6 Inc. 1 y 3, así como el Art. 7 Inc. 1. Pero principalmente está plasmado y tiene su objeto en el Art. 6 Inc. Último en el cual plantea que "*no será ningún obstáculo la admisión como prueba de un mensaje de datos"*. Así como también esta contemplado en el Art. 9

Inc. 1° al establecer que *"los datos y registros recibidos y archivados en el sistema informático constituirán plena prueba de que el usuario del servicio aduanero realizó los actos que le corresponden y que el contenido de esos actos y registros fue suministrado por éste, haciendo uso de su clave de acceso confidencial".*

AUTORIDADES DE CERTIFICACION

Este apartado es importante debido a que la Legislación española establece en su Art. 2 numeral 2 que un prestador de servicios de certificación es "*la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica"*.

En la Ley de Simplificación Aduanera en su Art. 8 Inc. 1° establece que *"se autorizará la intervención de empresas que provean servicios de certificación....., llamadas en adelante entidades certificadoras".*

Así mismo establece que el encargado de autorizar dichas entidades será el Ministerio de Hacienda, pero dada la situación en la que el país se encuentra, en lo relativo al atraso en lo que a Comercio Electrónico respecta, El Salvador solo cuenta con una entidad certificadora, Certicamara, que es una entidad de naturaleza privada regulada por la Cámara de Comercio.

CERTIFICADOS DIGITALES

La legislación española en su Art. 6 numeral 1°, establece que "*un certificado electrónico es un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma y un firmante y confirma su identidad"*.

En la Ley de Simplificación Aduanera podemos observar en el Art. 8 Inc. 1° que se emitirán certificados para *"garantizar la autenticidad, confidencialidad e integridad de la información y de impedir su posterior repudiación".*

REGULACION DE CONDUCTAS DELICTIVAS

Pudimos observar que en ninguna de las dos legislaciones se encuentra una regulación que penalice conductas delictivas.

EQUIPARACION DE LA FIRMA DIGITAL CON LA FIRMA MANUSCRITA

La legislación española le da, en su Art. 3 numeral 4 la misma validez a la firma electrónica con la firma manuscrita, ya que establece que *"la firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel"*.

De igual forma , la legislación salvadoreña, en su Art. 7 Inc. 1° expresa que: *"El uso de medios informáticos y de la vía electrónica para el intercambio, gozará de plena*

validez para la formulación, transmisión, registro y archivo de la declaración de mercancías, de la información relacionada con la misma y de los documentos que a ésta deban adjuntarse, así como para certificar el pago del adeudo, y su utilización producirá los mismos efectos jurídicos que produciría la entrega de esa misma información en soportes físicos."

Así como también en el Art. 8 Inc. 3°, cuando establece que *"la firma digital o electrónica, que para todos los efectos legales se constituye en el sustituto digital de la firma manuscrita...."*.

4.1.2 DIFERENCIAS

DEFINICIÓN

Aunque ambas legislaciones establecen un concepto de Firma Digital, las dos ofrecen definiciones diferentes, por ejemplo: la legislación española toma de objeto la Firma Electrónica, en su Art. 3 numeral 2 y 3 establece que:

Art. 3 numeral 2: "*La firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmado, que esta vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control".*

Art. 3 numeral 3: "*Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma".*

En la legislación salvadoreña no hacen ninguna distinción entre firma digital y firma electrónica.

Art. 8 Inc. 3°: *"...cada usuario autorizado, contará con una pareja de claves o llaves únicas y correspondientes entre sí, una pública y otra privada, de manera tal que ambas se correspondan de manera exclusiva y excluyente....La vinculación de ambas laves o clases constituye la firma digital o electrónica..."*.

AMBITO DE APLICACION

En la legislación española, la firma electrónica es utilizada en las transacciones que el usuario deba realizar con la Administración Pública, tal y como lo establece el Art. 4 numeral 1°: *"Esta ley se aplicara al uso de la firma electrónica en el seno de las Administraciones Públicas, sus organismos públicos y las entidades dependientes o vinculadas a las mismas y en las relaciones que mantengan aquéllas y éstos entre sí o con los particulares."*

En El Salvador, únicamente es utilizada la Firma Digital para realizar transacciones en el campo aduanal, específicamente en el sistema de Teledespacho, así como lo establece el Art. 6 Inc. 2°: *".....Teledespacho constituye el conjunto*

sistematizado de elementos tecnológicos de carácter informático y de comunicaciones que permitan, dentro de un marco de mutuas responsabilidades y mediante los procedimientos autorizados, el intercambio por vía electrónica de información de trascendencia tributaria entre la Dirección General y los usuarios y auxiliares del servicio aduanero, bancos y en general, los operadores e instituciones contraloras de comercio exterior."

SEGUROS DE AUTORIDADES DE CERTIFICACION

En la legislación española las Autoridades de Certificación están obligadas a constituir un seguro para afrontar daños y perjuicios que pueda ocasionar el uso de dichos certificados.

Art. 20 numeral 2°: "*Los prestadores de servicios de certificación que expidan certificados reconocidos deberán constituir un seguro de responsabilidad civil por importe de al menos 3,000,000 de euros para afrontar el riesgo de la responsabilidad por los daños y perjuicios que pueda ocasionar el uso de los certificados que expidan."*

En nuestra legislación no tenemos la cultura de reclamar por daños y perjuicios; usualmente encuentran la salida por la vía penal, y por lo tanto en la Ley de Simplificación Aduanera no encontramos nada que ampare económicamente a los usuarios.

4.1.3 VENTAJAS Y DESVENTAJAS

4.1.3.1 VENTAJAS

Podemos decir que una ventaja que la ofrece la legislación española es que equipara la firma digital con la firma manuscrita, esto quiere decir que le proporciona el mismo valor a los documentos firmados electrónicamente que los que se encuentran firmados en soporte papel.

Es también una ventaja el ámbito de aplicación que tiene la firma electrónica, ya que la legislación española permite su uso para la realización de actividades entre los entes de la Administración Pública y entre ésta y los usuarios, establece también la regulación del Documento Nacional de Identidad Electrónico, que es documento que acredita electrónicamente la identidad personal el titular y permite firmar electrónicamente un documento, esta figura del Documento Nacional de Identidad Electrónico, solo se presenta en países con una muy avanzada legislación sobre firma digital y comercio electrónico.

También otra ventaja, y una muy importante, es que la legislación española le otorga pleno valor probatorio a los documentos electrónicos y de esta manera hacen mas seguro para los usuarios su uso y menos problemático el proceso judicial en caso de controversias

4.1.3.2 DESVENTAJA

No existe una figura de una Autoridad de Registro, es decir un ente regulador de las Entidades de certificación, ya que todas trabajan en base a la libre competencia y en casos aislados delegan algunas de sus funciones al Ministerio de Ciencia y Tecnología.

4.2 EL SALVADOR Y COLOMBIA

La Ley 527/1999 de Colombia, del Comercio Electrónico y de las Firmas Digitales fue aprobada el 18 de Agosto de 1999. Esta ley reglamenta el acceso y uso de los mensajes de datos del comercio electrónico y de las firmas digitales, establece las entidades de certificación, da la misma fuerza y efectos jurídicos de la firma manuscrita a la firma digital al cumplir los requisitos establecidos en la misma.

4.2.1 SIMILITUDES

CONCEPTO

La Ley 527/1999 de Colombia, del Comercio Electrónico y de las Firmas Digitales, define en el Art. 2 inciso 4°, lo que debe entenderse por firma digital estableciendo que *"se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje, permite determinar que este valor se ha obtenido*

exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación."

En El Salvador, la Ley de Simplificación Aduanera, introduce a nuestra legislación, lo que debe entenderse por firma digital, ya que no existe una ley específica. Así tenemos que el Art. 8 inciso 4°, establece: *"Para la ejecución de las distintas actuaciones que conforman el sistema de teledespacho y para el intercambio de la información en general, cada usuario autorizado, contará con una pareja de claves o llaves únicas y correspondientes entre si, una pública y otra privada, de manera tal que ambas se correspondan de manera exclusiva y excluyente... La vinculación de ambas llaves o claves constituye la firma digital... que permite al receptor de un mensaje electrónico verificar con certeza la identidad proclamada por el transmisor, impidiendo a este ultimo desconocer en forma posterior la autoría del mensaje."*

VALOR PROBATORIO

La ley de Colombia sobre Comercio Electrónico y firmas digitales se refiere a la fuerza probatoria de los mensajes de datos en su Art. 10, en el cual establece *"los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del Capítulo VIII del Título XIII, Sección Tercera, Libro Segundo del Código de Procedimientos Civiles".*

Además en el inciso 2° del mismo artículo establece que *"no se le negará eficacia, validez o fuerza obligatoria y probatoria a la información contenida en forma de mensaje de datos"*.

La Ley de simplificación aduanera en el Art. 6, establece que *"los documentos contenidos en un soporte magnético, digital o electrónico producirá los mismos efectos jurídicos que los escritos en un soporte de papel".*

EQUIPARACIÓN DE LA FIRMA DIGITAL A LA FIRMA MANUSCRITA

En cuanto a la equiparación de la firma digital con la firma manuscrita, el Art. 7 de la Ley de Colombia del Comercio Electrónico, establece que *"cuando cualquier norma exija la presencia de una firma u otorgue consecuencias en ausencia de la misma, bastará con la presencia de un mensaje de datos firmado digitalmente con un método confiable que permita identificar al emisor y que indique la aprobación del contenido del mensaje, de esta forma se entiende satisfecho el requerimiento de la firma manuscrita"*.

CERTIFICADOS DIGITALES

Otra de las similitudes entre estas legislaciones es en cuanto a los certificados digitales; así tenemos que en el Art. 35 de la Ley de Colombia de Comercio Electrónico, establece que *"el certificado emitido por una entidad de certificación autorizada, además de estar firmado digitalmente, debe contener el nombre, dirección y domicilio*

del suscriptor, así como su identificación, su clave pública, número de serie del certificado y la fecha de emisión y expiración del mismo".

En la Ley de Simplificación Aduanera, en el art. 8-A literal d), establece como función de la entidad certificadora, *"....emitir certificados, los cuales son documentos electrónicos que, añadidos a la llave pública como datos e información características del firmante, acreditan o respaldan la vigencia del mismo"*.

4.2.2 DIFERENCIAS

ÁMBITO DE APLICACION

Una de las diferencias entre estas legislaciones es en cuanto al ámbito de aplicación de las mismas, así tenemos que el art. 1 de la Ley de Comercio Electrónico de Colombia, establece que *"será aplicable a todo tipo de información en forma de mensaje de datos, exceptuando las obligaciones contraídas por el Estado en virtud de convenios o tratados internacionales, y cuando la comercialización de un producto deba ser impresa debido al riesgo que implica su uso o consumo"*.

En tanto que en El Salvador, el uso de firma digital está destinado exclusivamente para el sistema de Teledespacho, el cual según el art.6 de la Ley de Simplificación Aduanera, *"constituye el conjunto sistematizado de elementos tecnológicos de carácter informático y de comunicaciones que permiten el intercambio*

por vía electrónica de información de trascendencia tributaria entre la Dirección General de la Renta de Aduanas y sus usuarios". Hasta la fecha, la entidad certificadora salvadoreña Certicamara, únicamente emite certificados digitales cerrados, es decir, que solo se utilizan con la Dirección General de la Renta de Aduanas, para el sistema de Teledespacho.

NATURALEZA DE LA ENTIDAD CERTIFICADORA

Otra diferencia es en cuanto a la naturaleza de la entidad certificadora; en el art. 29 de la Legislación Colombiana, establece que *"pueden ser entidades de certificación las personas jurídicas, tanto públicas como privadas de origen nacional o extranjero y las Cámaras de Comercio"*.

En El Salvador, debido al poco desarrollo de la firma digital, la Ley de Simplificación Aduanera, en el art. 8 establece que *"las entidades certificadoras deberán ser exclusivamente personas jurídicas"*. Hasta la fecha la única entidad autorizada es Certicamara, cuya naturaleza es privada.

AUTORIDAD DE REGISTRO

Otra de las diferencias con esta legislación se deriva de la falta de regulación de la firma digital en El Salvador, ya que en Colombia hay una ley específica que regula todos los aspectos relevantes de la misma; así tenemos que, en cuanto a la autoridad de registro, el art. 41 de la legislación colombiana, establece *"que la Superintendencia de*

Industria y Comercio ejercerá las facultades de autorizar a las entidades de certificación, velar por su funcionamiento, realizar auditorias, revocar o suspender la autorización y sancionar a las entidades certificadoras".

Mientras que en El Salvador, el art. 8 de la Ley de Simplificación Aduanera, establece que *"la autorización para operar, la fiscalización y la facultad sancionatoria relacionadas con las entidades certificadoras, será ejercida por el Ministerio de Hacienda, en tanto no se dicte una ley que regule de manera general todos los aspectos relacionados con el comercio electrónico, en cuyo caso, dicha potestad corresponderá a la autoridad acreditante o licenciante de entidades certificadoras que en la misma se establezcan"*.

ACUSE DE RECIBO

Finalmente, otra diferencia se refleja en cuanto al acuse de recibo, ya que en el art. 21 de la legislación colombiana establece que *"cuando el emisor reciba el acuse de recibo del destinatario se presume que éste último ha recibido el mensaje de datos enviado"*.

En El Salvador, el art. 9 de la Ley de Simplificación Aduanera, establece que *"los datos y registros recibidos y archivados en el sistema informático, constituyen plena prueba de que el usuario del servicio aduanero realizó los actos que le*

corresponden y que el contenido de esos actos y registros fue suministrado por éste, haciendo uso de su clave de acceso confidencial".

4.2.3 VENTAJAS Y DESVENTAJAS

4.2.3.1 VENTAJAS

La Ley 527/1999 de Colombia de Comercio Electrónico y Firmas Digitales da paso al advenimiento de las nuevas tecnologías que brinda el Internet, como lo es el manejo de documentos electrónicos y dejando en desuso a los documentos consignados en papel.

Permite distinguir dentro de los mensajes de datos, aquellos documentos electrónicos originales, es decir, que pueden reemplazar los escritos originales que suelen solicitarse en las relaciones entre particulares o frente al Estado, si cumplen las condiciones que trae la ley.

Reconoce el valor probatorio a los documentos electrónicos firmados digitalmente, y de esta forma garantiza la posibilidad de exigir el cumplimiento por la vía judicial, de un acuerdo electrónico.

Equipara el valor de una firma manuscrita con el de una firma digital.

Incorpora en su legislación el acuse de recibo, el cual es determinante para establecer el momento en que se ha consentido sobre la obligación contenida en un mensaje de datos firmado digitalmente.

4.2.3.2 DESVENTAJA

El uso de esta tecnología nueva, sigue siendo incierto ya que la mayoría de usuarios aún desconfía del sistema, por lo que la eficacia de los mismos tendrá que ser comprobada, lo cual retrasa su aplicación.

4.3 EL SALVADOR Y ARGENTINA

La ley de firma digital 25.506 de Argentina fue sancionada el 14 de noviembre del 2001 y promulgada de hecho el 11 de diciembre del 2001, dicha ley sigue el modelo de principios y reglas generales de la ley de la UNCITRAL.

4.3.1 SIMILITUDES

DEFINICIÓN

La ley de firma digital de argentina establece en su Art. 2 la definición, donde se entiende por firma digital *"el resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante encontrándose este bajo su absoluto control"*. En El Salvador la definición de firma digital no esta tan avanzada como en dicho país pero si plantea un definición en el

Art.8 de la Ley de Simplificación Aduanera en su inciso final manifestando que la firma *"es aquella que se utiliza para el intercambio de información donde cada usuario contara con una pareja de llaves o claves únicas que corresponden de manera exclusiva de manera que la vinculación de ambas llaves constituye la firma digital"*.

VALOR PROBATORIO DE LOS DOCUMENTOS FIRMADOS DIGITALMENTE

En este punto ambas leyes retoman el valor probatorio ya que la ley de Argentina en su Art. 11 expresa que *"los documentos electrónicos firmados digitalmente serán considerados originales y poseen como consecuencia de ello el valor probatorio como tales"*.

También en El Salvador manifiesta que los documentos contenidos en un soporte magnético, digital o electrónico producirán los mismos efectos jurídicos que los escritos en un soporte papel en su Art. 6 Inc. final.

EQUIPARACIÓN DE LA FIRMA MANUSCRITA CON LA FIRMA DIGITAL

Otra similitud de ambos países es la equiparación de la firma manuscrita con la firma digital, ya que en la legislación Argentina en su Art. 3 *"cuando una ley requiera una firma manuscrita esa exigencia también queda satisfecha para una firma digital"*, por lo tanto, cuando una ley establezca una obligación de firmar puede ser cualquiera de estas firmas.

En El Salvador, debido al limitado ámbito de aplicación de la firma digital, solo se refiere al intercambio de información del sistema de teledespacho, es decir que la firma digital constituye el sustituto digital de la firma manuscrita donde se podrá verificar con certeza la identidad del trasmisor.

ENTIDADES DE CERTIFICACIÓN

Para los efectos de garantizar la autenticidad, confidencialidad e integridad de toda la información y de impedir su posterior repudiación ambos países han tomado como base las entidades de certificación, tal es el caso que la legislación Argentina en su Art. l7 establece que *"se entiende por certificadoras a toda persona de existencia ideal o registro público de contrato u organismos público que expide certificados, presta otros servicios en relación con la firma digital, y cuenta con una licencia para ello"*.

En el país también existe una entidad certificadora y *"es una persona jurídica que esta capacitada tecnológicamente para prestar servicios de generación y certificación de firma digital"*, según Art. 8 Inc. 3°.

CERTIFICADOS DIGITALES

Una de las similitudes mas importantes de estos dos países son los certificados digitales; para Argentina en su art.13 expresa que *"se entenderá por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular"*; es así como en El Salvador en el art. 8-A literal d)

manifiesta que una de las funciones de las entidades certificadoras es *"la de expedir o emitir los certificados y estos son documentos electrónicos que añadidos a la llave pública acreditan la correspondencia de una llave con la persona que es titular de dicha llave"*.

4.3.2 DIFERENCIAS

ÁMBITO DE APLICACION

En Argentina el ámbito de aplicación de la firma digital se entiende para el sector privado y público, excluyendo aquellos actos jurídicos del derecho de familia, las disposiciones por causa de muerte, los actos personalísimos en general y aquellos actos que deban ser instrumentados bajo exigencias o formalidades incompatibles a la firma digital.

En cambio en El Salvador el ámbito de aplicación de la firma digital es reducido ya que solamente se da para la ejecución de las distintas actuaciones que conforman el sistema de teledespacho, entendiéndose éste como el conjunto sistematizado de elementos tecnológicos de carácter informático tributario entre la Dirección General de la Renta de Aduanas y los usuarios auxiliares del servicio aduanero y los operadores de las instituciones controladoras del comercio exterior, es decir que la firma digital por el momento en nuestro país, es de uso exclusivo para las aduanas.

ENTIDADES CERTIFICADORAS

Otra de las diferencias de estos países, se refiere a las entidades certificadoras, ya que en Argentina debido al nivel que presenta la firma digital existe una jerarquización de dichas entidades para una mejor apertura y control de la misma; ya que existe primero una comisión asesora para la infraestructura de la firma digital cuya función primordial es recomendar a las demás entidades, tales como a las autoridades de aplicación, es decir una jefatura del gabinete de Ministros y ésta a su vez, tendrá como función el de regular a la certificadora licenciante, quien es aquella que emite los certificados.

En El Salvador solo existe una entidad certificadora privada que es Certicamara y es ella la que regula e informa sobre todo lo relacionado con los certificados, ya que es la única que puede emitir dichos certificados.

CERTIFICADOS EXTRANJEROS

En la legislación argentina, como se dijo antes, por el nivel que tiene a lo relacionado a la firma digital, reconocen los certificados extranjeros así como lo establece el art. 16, siempre y cuando éstos cumplan con los mismos requisitos exigidos para la validez de los certificados nacionales.

En cambio en El Salvador, no existe ninguna disposición que regule si acepta un certificado extranjero y esto es debido a que solo existen certificados cerrados, es decir, para las aduanas en el sistema de teledespacho.

4.3.3 VENTAJAS Y DESVENTAJAS

4.3.3.1 VENTAJAS

En Argentina una de las ventajas que proporciona la Firma Digital, es que es un vehículo seguro para facilitar el Comercio Electrónico, ya que ayuda a la creación de nuevos mercados, donde genera redes productivas más ágiles entre diversas empresas, asegurando la información de los documentos informáticos.

Cuenta con una Ley de Firma Digital que permite que un documento firmado digitalmente tenga el mismo valor probatorio en un Tribunal que uno firmado con tinta; además de traer beneficios en cuanto a la productividad, eficacia y transparencia en todas las transacciones, ya que la firma digital garantiza la identidad de las partes que negocian sin conocerse, la integridad de los contenidos en sus envíos, así como también la aceptación de los compromisos adquiridos en un ambiente de confidencialidad.

El ámbito de aplicación de la firma digital, es otra ventaja, ya que puede ser aplicable tanto en el sector privado y público, es decir que el Estado cuenta con múltiples transacciones relacionadas al personal público y los particulares también puede realizar múltiples transacciones, evitando el traslado físico, ahorrando tiempo, agilizando todo tipo de procedimientos electrónicos.

Otra de las ventajas que presenta la firma digital en Argentina es que acepta certificados extranjeros facilitando el comercio electrónico internacional, reconociendo la validez de dicho certificados pero siempre reuniendo las condiciones que establece la ley.

4.3.3.2 DESVENTAJA

La desventaja que presenta Argentina en cuanto a la firma digital es que no existe una homogeneidad desde el punto de vista legislativo en relación a firma digital o electrónica y documento electrónico; es así que provoca una confusión no solo de términos sino también de las características que lo definen.

4.4 VENTAJAS Y DESVENTAJAS DEL USO DE LA FIRMA DIGITAL EN EL DESARROLLO DEL COMERCIO ELECTRONICO EN EL SALVADOR.

4.4.1 VENTAJAS

Hoy en día la firma digital trae consigo una modernización en las actividades cotidianas lo cual es un beneficio, dado el acelerado ritmo de vida que lleva la humanidad, por lo tanto se pueden plantear las siguientes ventajas:

- La firma digital permitirá realizar todo tipo de transacciones electrónicas con la certeza de quien es la persona con la cual se está interactuando, esto trae consigo

la posibilidad de omitir el requerimiento presencial para algunas actuaciones, ofreciendo al usuario una vida más cómoda, eficiente y productiva.

- El uso de la firma digital evitará el traslado físico para cualquier tipo de trámites evitando con esto al usuario pérdida de tiempo y ahorro en el costo del traslado, haciendo los procedimientos más rápidos y eficaces.

- Con la firma digital se hace posible hacer trámites públicos de todo índole a través de Internet, ya que muchos estados cuentan con páginas web en Internet, permitiendo al usuario hacer trámites desde su propia casa u oficina evitando lo molesto de realizarlo personalmente.

- Otra utilidad de la firma digital es que se ahorrará y reducirá en los papeles de los trámites, el llenado del formulario o se realizará a través de una computadora, haciendo más rápido, ágil y eficiente que si el formulario se llenara en papel. De esta manera no habrían errores en la digitación ya que ésta sería en forma automática sin intervención manual. Además no hay que preocuparse por robo o pérdida del formulario.

- El empleo de la firma digital tiende a aumentar la transparencia de los procesos de licitación del estado hechos por vía electrónica ya que esta ayuda a la creación de

nuevos mercados, genera redes productivas más ágiles e introduce mayor eficiencia en sector público y privado.

- Una aplicación mas de la firma digital es que reducirá el costo de los productos y servicios ya que se ahorrará en costos de transacciones y almacenamiento, pero en este caso es relativo porque dependerá de cada empresa si traduce esos menores costos a sus productos o lo utiliza para aumentar el margen de ganancias.

- Los bancos podrán tramitar créditos con la sola firma digital; ya no tendrán que ir mas al banco, se podrán hacer transacciones bancarias a través de la página web del banco en forma segura y rápida por la firma digital, estas transacciones van desde ser el saldo contable hasta transferencia de fondos.

- No será necesario ir de compras a los centros comerciales, ya que gracias a la firma digital se podrá comprar a través de Internet cómodamente desde su casa y en forma segura.

- Los pagos de luz, agua, teléfono y otros servicios se podrán cancelar en Internet desde cualquier lugar en forma rápida, cómoda y segura.

- La firma digital permitirá validar el uso de documentos tributarios como factura electrónica, boleta electrónica, notas de crédito, etc., esto generará un importante ahorro en los costos de operación, costos en papel, de almacenaje, entre otros.

- Permitirá conocer la fecha y hora exacta en la cual se generó el documento evitando fraudes o mal uso de los mismos, esto tiene gran repercusión en las transacciones entre distintos países con distintos honorarios.

- Seguramente el mayor beneficio será para el comercio electrónico. Se espera que con las garantías del sistema, las barreras impuestas por los empresarios empiecen a ceder.

4.4.2 DESVENTAJAS

- En El Salvador, la determinación de los medios idóneos para acreditar un hecho en juicio y la forma en que esta debe ser rendida, le corresponde señalarlo a la ley exclusivamente ya que rige el sistema de prueba tasada. Esta rigidez propia de este sistema de prueba, no admite el uso de las nuevas tecnologías y niegan la aceptación de documentos electrónicos como medios de prueba, lo cual no justifica la indefensión que acarrearía a quienes se desenvuelven en una sociedad tecnológica que contradictoriamente no le proporciona medios para acreditar sus pretensiones.

- El tipo de transacción a la que se le dá cobertura legal es limitado ya que se autoriza el uso de la Firma Digital para el sistema de Teledespacho, lo cual restringe la participación de las personas y el ámbito de aplicación, por lo tanto la aplicación de la firma digital no tienen fuerza jurídica para otros tipos de documentos que no sean aduanales.

- Y la más relevante es la inexistencia de una normativa específica que se encargue de regular todos los aspectos relacionados con el uso, eficacia, registro y validez de la firma digital como medio de seguridad al realizar transacciones en el comercio electrónico; aunque exista unas disposiciones aisladas en diferentes leyes nacionales que retoman únicamente ciertos aspectos y no de manera global.

CAPITULO V. CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- El uso de Internet y el Comercio Electrónico en El Salvador han tenido un crecimiento considerable en los últimos años, lo que abre las puertas a nuevas oportunidades para el desarrollo económico del comercio tanto a nivel local como internacional y contribuye a la creación de nuevas fuentes de empleo; lo anterior obliga a replantearnos cuestiones del comercio tradicional las cuales van desde la validez legal de las transacciones, contratos sin papel hasta la necesidad de acuerdos internacionales que armonicen las legislaciones sobre comercio electrónico.

- Para asegurar las transacciones del comercio electrónico se ha implementado el uso de la firma electrónica o digital la cual es un conjunto de datos electrónicos que identifican a una persona en concreto, suele unirse al documento que se envía por medio telemático, como si de la firma tradicional se tratara, de esta forma el receptor del mensaje está seguro de quien ha sido el emisor; este mecanismo de seguridad cumple con las características de integridad, autenticidad, no repudio y confidencialidad, con el fin de que exista una celebración válida de negocios jurídicos que impliquen la viabilidad de expresar la voluntad de una persona y con ello la posibilidad de celebrar contratos válidos y exigibles.

- La seguridad en las transacciones económicas es una preocupación para los responsables de los sistemas de información, es por eso que la Firma Digital es el sistema más seguro para enviar datos, con la certeza de que nadie mas que el receptor autorizado será capaz de leerlo, ya que hoy por hoy es el mejor método para garantizar la seguridad en las transmisiones de datos a través de la red porque aplica el máximo nivel en el encriptamiento de la información que protege.

- El fundamento de las firmas digitales es la criptografía, ya que es una ciencia que se ocupa de la transformación de mensajes en formas aparentemente ininteligibles para el lenguaje humano y posteriormente devolverlos a su forma original, lo cual permite proteger la integridad de los mensajes transformando los datos en signos ilegibles y solo los revela si se le aplica la clave para desencriptarlos.

- Las entidades de certificación son una pieza fundamental en el desarrollo del Comercio Electrónico, pues son los que brindan certeza sobre el autor y contenido de un mensaje de datos o permiten conocer a los emisores de una oferta y aceptación de actos jurídicos y las partes intervinientes en un contrato; por lo mismo de ellas depende el desarrollo de este tipo de canales de comunicación dentro de un marco de seguridad jurídica esencial para la proliferación del comercio por esta vía. Además permiten evitar que se cometan fraudes por

falsificación de identidad o que se caigan en errores contractuales por falta de personería jurídica.

- Las transacciones del comercio electrónico revisten seguridad y certeza, sin embargo, no están libres de enfrentarse a situaciones conflictivas debido a la dificultad de acordar transacciones o por el incumplimiento de alguna cláusula contractual; ante esta circunstancia se plantean la sustitución de la actuación judicial por formulas de solución extrajudicial, tales como la mediación, conciliación o arbitraje, mas acordes con lo característico que presenta la red y los conflictos derivados de su uso.

- Los mensajes y documentos electrónicos constituyen la forma en que los comerciantes y usuarios de los medios electrónicos realizan la mayoría de las transacciones comerciales, por lo tanto tendrán eficacia probatoria, si además de ser validos reúnen los requisitos de idoneidad y son conducentes para probar un hecho, además debe tener establecida su autenticidad.

- La sociedad salvadoreña que esta por ingresar a la cultura informática necesita de un soporte jurídico que despeje las inquietudes que plantea la realización de actividades a través de Internet, así como el uso de nuevos medios para dar

rapidez a las transacciones comerciales que permitirán a nuestro País aumentar su productividad, competitividad y así reducir tiempo y costo.

- El intento de regular el comercio electrónico y principalmente la firma digital queda limitado a establecer casos especiales que se adaptan a circunstancias específicas, tal es el caso de las aduanas, lo cual no es suficiente para proteger jurídicamente y poder determinar los mecanismos necesarios que permitan a lo usuarios de este sistema tener seguridad al utilizarlo.

5.2 RECOMENDACIONES

- El Estado salvadoreño es el que debe analizar y adoptar los mecanismos y sistemas que se están generando con la finalidad de brindar protección y garantía a las personas que interactúan dentro de los modernos medios de comunicación y contribuir al fortalecimiento de la educación, investigación y ampliación de los conocimientos tecnológicos relativos al uso de los medios informáticos y de esta manera hacerlo accesible a la población en general.

- Es necesario hacer un análisis exhaustivo, sistemático, serio y coherente de la actual legislación tanto sustantiva como procesal con la finalidad de concluir cual es el idóneo y cual debería ser derogado para establecer un nuevo cuerpo legal mas

valido, sólido y que brinde una mejor protección jurídica a las relaciones que se dan por medios electrónicos y a la vez establecer mecanismos procesales que permitan exigir el cumplimiento de obligaciones que se pactan por dichos medios.

- Es preciso la creación de entidades certificadoras abiertas que faciliten la aplicación del comercio electrónico en todos sus ámbitos, ya que al existir en nuestro medio una entidad certificadora cerrada limita el tipo de transacción a realizar y por ende el desarrollo del comercio electrónico en El Salvador.

- El anteproyecto de ley de comercio electrónico se centra en regular determinados puntos de manera muy amplia dejando mucha materia por regular; carece de un régimen sancionatorio, el procedimiento para producir prueba en juicio, entre otras cosas. Para evitar dicha situación se debería tomar el ejemplo de legislaciones extranjeras quienes cuentan con una ley exclusiva para comercio electrónico y otra para Firma Digital.

BIBLIOGRAFIA

LIBROS

BARCELÓ, ROSA JULIA Y VINJE, THOMAS. **"Hacia un marco Europeo sobre Firmas Digitales y Criptografía"** Revista de Derecho Mercantil N° 228, abril-junio 1998.

BCR y COEXPORT; **Secretos del comercio electrónico: Una guía para pequeños y medianos exportadores**, San Salvador, El Salvador, 2001.

CABANELLAS DE TORRES, GUILLERMO, **Diccionario Jurídico Elemental**, Editorial Heliasta S. R. L. Buenos Aires, 1994.

CARDOZA ISAZA, JORGE, **Pruebas Judiciales**. Librería Jurídica Welches, Bogotá Colombia, 1985.

CUBILLOS VELANDIA, RAMIRO Y OTRO, **Introducción jurídica al comercio electrónico**, Ediciones Jurídicas Gustavo Ibáñez, Bogotá (Colombia), 2002.

MARTÍNEZ NADAL, APOL-LONIA, **Comercio Electrónico, Firma Digital y Autoridades de Certificación**, Tercera Edición, Editorial Civitas, Madrid (España), 2001.

MARTÍNEZ NADAL, APOL-LONIA, **La Ley de Firma Electrónica**, Segunda Edición, Editorial Civitas, Madrid (España), 2001.

PERALES SANZ, JOSÉ LUIS, **La seguridad jurídica en las transacciones electrónicas**. Seminario organizado por el consejo general del notariado de la UIMP. Editorial Civitas, Madrid (España), 2002.

PALLARES EDUARDO, **Diccionario de Derecho Procesal Civil**, Séptima Edición, Editorial Porrua, S.A. México, 1973.

RIVAS HERNÁNDEZ, SALVADOR ANTONIO Y OTRO, **La Firma Electrónica**. Monografía. Universidad Francisco Gavídia, 2004

SARRA, ANDREA, **Comercio Electrónico y Derecho**, Editorial Astrea, Primera reimpresión, Ciudad de Buenos Aires, Argentina, 2001.

TESIS

ALFARO NAJARRO, RENE ADONAY Y OTROS, **Plan de implementación del comercio electrónico para la mediana empresa comercial Salvadoreña**, Universidad Tecnológica, Facultad de Ciencias Económicas, Licenciatura en Administración de Empresas, Noviembre 2001.

POLANCO VILLALOBOS, JOSÉ ANTONIO Y OTROS, **La regulación sobre el comercio Electrónico en el ordenamiento jurídico Salvadoreño**, Universidad José Simeón Cañas, Facultad de Ciencias del Hombre y la Naturaleza, Licenciatura en Ciencias Jurídicas, Noviembre 2001.

REVISTAS

HERRARTE, ANA, **Seminario de Mercadeo Interactivo**, El Salvador, Julio 2000.

PÁGINAS WEB

www.utem.sl/cyt/derecho/firma.html
Año de creación: 16 de octubre 2001
Tema buscado: La firma digital
Autor: Gustavo Sandoval
Lugar y fecha del articulo: Colombia, octubre 2001
Año de visita: 2005

www.monografias.com
Año de creación: 2003
Tema buscado: La firma digital
Autor: Lucas Morea
Lugar y fecha del articulo: Sinexi, Argentina, marzo 2004
Año de visita: 2005

www.vlex.com.
Año de creación: 2003
Tema buscado: La firma electrónica

Autor: Alex Networks S.L

Lugar y fecha del articulo: España, Barcelona, noviembre 2003

Año de visita: 2006 - 2005

www.tuguialegal.com/firma digital/1.htm

Año de creación: 2000

Tema buscado: La firma digital

Autor: José Antonio Hernández

Lugar y fecha del articulo: País Vasco, España, febrero 2001

Año de visita: 2005

www.iec.csic.es/criptonomicon/seguridad

Año de creación: 1997

Tema buscado: La seguridad en la firma digital

Autor: Gonzalo Álvarez Marañon

Lugar y fecha del articulo: España, abril 2000

Año de visita: 2005

www.espanol.groups.yahoo.com/groups/

Año de creación: 1998

Tema buscado: Comercio Electrónico

Autor: Benjamín García

Lugar y fecha del articulo: Caracas, Venezuela, febrero 2001

Año de visita: 2005

www.html.net/seguridad/varios/firma-certificado/

Año de creación: 2005

Tema buscado: Certificados Digitales

Autor: Andreas Astrup

Lugar y fecha del articulo: Joachim Cohn, Dinamarca, marzo 2005

Año de visita: 2006

www.ingenieroseninformatica.org/recursos/tutoriales/firmaelectronica/cap4.php

Año de creación: 2000

Tema buscado: La firma electrónica

Autor: Ingenieros en Informática

Lugar y fecha del articulo: España, junio 2004

Año de visita: 2005

www.internautas.org

Año de creación: 1998

Tema buscado: La firma electrónica

Autor: Asociación de Internautas

Lugar y fecha del articulo: Madrid, España, agosto 2003

Año de visita: 2005

www.scba.gov/fdweb.swf

Año de creación: 2002

Tema buscado: La firma digital y certificados digitales

Autor: Susana Margarita Trejo

Lugar y fecha del articulo: Colombia, julio 2002

Año de visita: 2005

www.cne.es/firmadigital/seguro/sisicne1/index1.asp

Año de creación: 1999

Tema buscado: Seguridad en la firma digital y certificados digitales

Autor: Comisión Nacional de Energía

Lugar y fecha del articulo: Alcalá, Madrid, España, enero 2000

Año de visita: 2005-2006

www.hfernandezdelpech.com.ar/leyes/trab/firma%20digital.deusto%202002.htlm

Año de creación: 2001

Tema buscado: La firma digital

Autor: Gustavo Fernández Mayorca

Lugar y fecha del articulo: Argentina, septiembre 2003

Año de visita: 2005

www.zonavirus.com/datos/articulos/44/firma_digital_certificados_digitales.asp

Año de creación: 2001

Tema buscado: La firma digital

Autor: Gustavo Fernández Mayorca

Lugar y fecha del articulo: Argentina, septiembre 2003

Año de visita: 2005

www.mailweb.udcap.mycontelect.html

Año de creación: 2001

Tema buscado: Contratación Electrónica

Autor: Carlos Ortiz

Lugar y fecha del articulo: México, julio 2002

Año de visita: 2005

www.htm/web.net/seguridad/varios/firma-jurídico.html

Año de creación: 2004

Tema buscado: Seguridad en la Firma electrónica

Autor: Joachim Cohn Jacobsen

Lugar y fecha del articulo: Dinamarca, mayo 2004

Año de visita: 2006

www.geocities.com/capitolgil/cenate8569/html

Año de creación: 2003

Tema buscado: La Firma electrónica

Autor: Yahoo Inc.

Lugar y fecha del articulo: California, Estados Unidos, octubre 2004

Año de visita: 2006

www.virusprot.com/art.36html/trabajofirmavenezuela#.asp

Año de creación: 2004

Tema buscado: La Firma digital

Autor: Arnoldo Moreno

Lugar y fecha del articulo: México, junio 2004

Año de visita: 2005

LEGISLACIÓN

Constitución de la República de El Salvador, aprobada por la Asamblea Constituyente del 15 de Diciembre de 1983, publicado en el Diario Oficial N° 234, Tomo N° 281, del 16 de Diciembre de 1983.

Código Civil, aprobado por la Cámara de Diputados, el día 12 de Febrero de 1858 y sancionado por el Poder Ejecutivo mediante decreto N° 17 del Ministerio General de fecha 13 de Febrero de 1858, declarado Ley de la Republica por Decreto del Poder Ejecutivo de fecha 23 de Agosto de 1859.

Ley de Bancos, aprobada por la Asamblea Legislativa, mediante Decreto Legislativo número 697, de fecha 2 de Septiembre de 1999, publicado en el Diario Oficial N° 181, Tomo N° 344, del 30 de Septiembre de 1999.

Ley de Anotaciones Electrónicas de Valores en Cuenta, aprobada por la Asamblea Legislativa, mediante Decreto Legislativo número 742, de fecha 21 de Febrero de 2002, publicado en el Diario Oficial N° 57, Tomo N° 354, del 22 de Marzo de 2002.

Ley del Mercado de Valores, aprobada por la Asamblea Legislativa, mediante Decreto Legislativo número 809, de fecha 16 de Febrero de 1994, publicado en el Diario Oficial N° 73, Tomo N° 323, del 21 de Abril de 1994.

Ley Orgánica de la Superintendencia de Valores, aprobada por la Asamblea Legislativa, mediante Decreto Legislativo número 806, de fecha 11 de Septiembre de 1996, publicado en el Diario Oficial N° 183, Tomo N° 333, del 4 de Octubre de 1996.

Ley de Mediación, Conciliación y Arbitraje, aprobada por la Asamblea Legislativa, mediante Decreto Legislativo número 914, de fecha 11 de Julio de 2002, publicado en el Diario Oficial N° 153, Tomo N° 356, del 21 de Agosto de 2002.

Ley de Simplificación Aduanera con sus Reformas, Decreto N° 523, 5 de Octubre de 2001, aprobada por la Asamblea Legislativa, mediante Decreto Legislativo número 529, de fecha 13 de Enero de 1999, publicado en el Diario Oficial N° 23, Tomo N° 342, del 3 de Febrero de 1999.

Anteproyecto de Ley de Comercio Electrónico y Firma Digital.

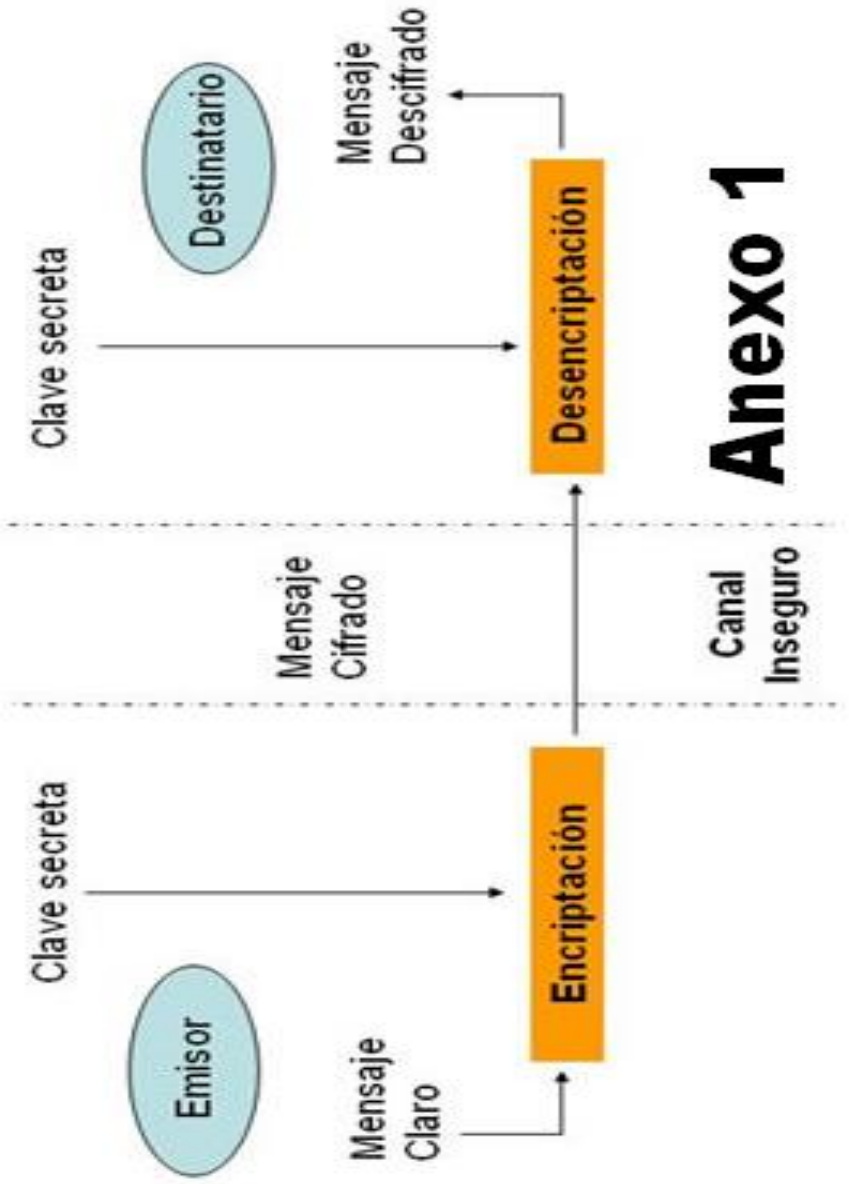
Ley de la UNCITRAL, texto adoptado por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional en su 29º periodo de sesiones, 28 de mayo a 14 de junio de 1996, Nueva York.

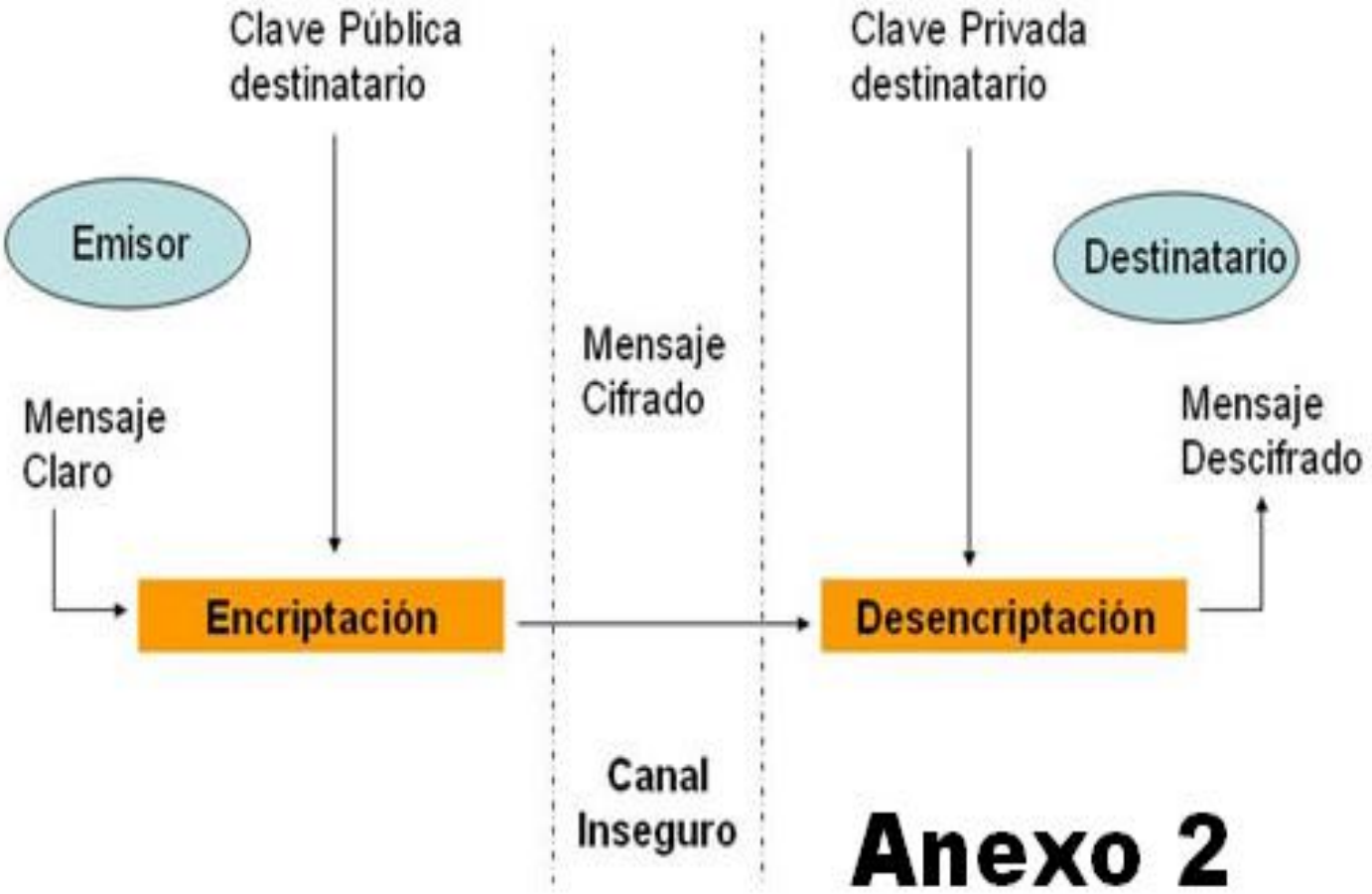
Ley 59/2003 de Firma Electrónica. España, aprobada por el Rey Juan Carlos I el 19 de Diciembre de 2003.

Ley 527/1999 de Colombia, del Comercio Electrónico y de las Firmas Digitales, aprobada el 18 de Agosto de 1999 y publicada en el Diario Oficial No. 43.673, de 21 de agosto de 1999.

Ley de Firma Digital 25.506 de Argentina, Sancionada el 14 de Noviembre de 2001, y Promulgada de Hecho el 11 de Diciembre de 2001.

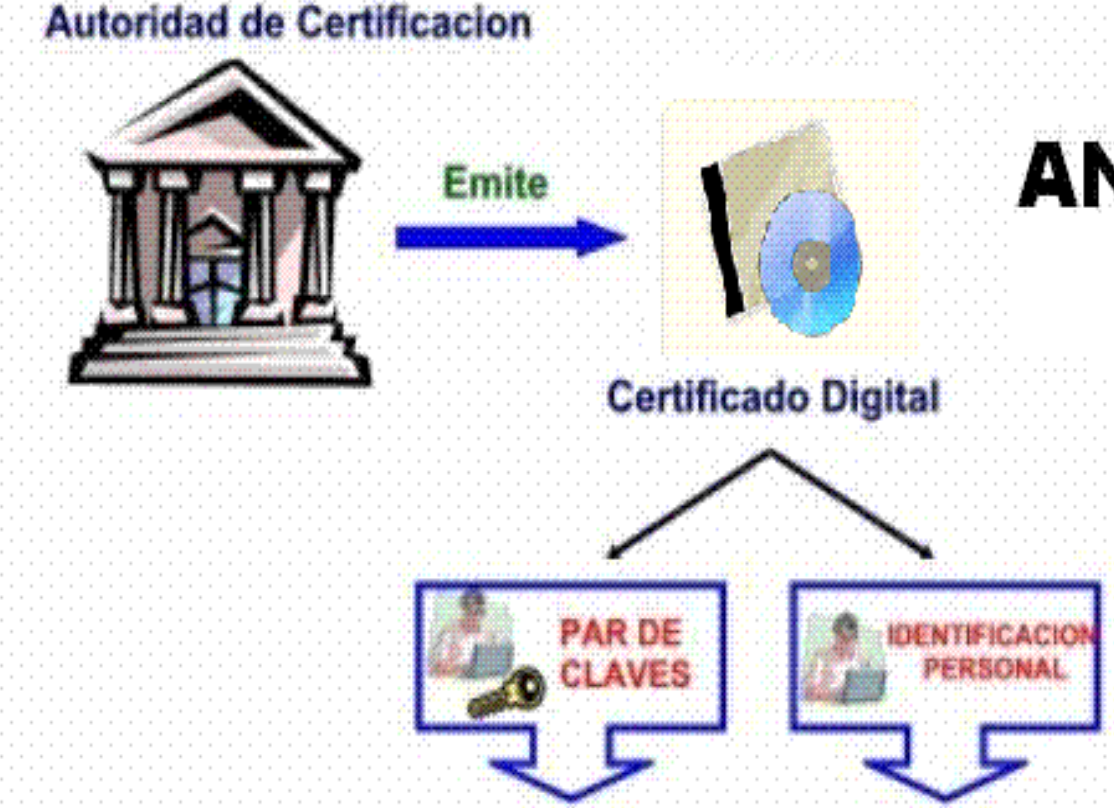
ANEXOS


Anexo 1
Emisor
Clave secreta
Mensaje Claro
Encriptación
Mensaje Cifrado
Canal Inseguro
Desencriptación
Clave secreta
Destinatario
Mensaje Descifrado


Clave Pública
destinatario
Clave Privada
destinatario
Emisor
Destinatario
Mensaje
Cifrado
Mensaje
Claro
Mensaje
Descifrado
Encriptación
Desencriptación
Canal
Inseguro

Anexo 2

ANEXO 3


Autoridad de Certificacion
Emite
Certificado Digital
PAR DE CLAVES
IDENTIFICACION PERSONAL