UNIVERSIDAD DE EL SALVADOR

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

ESCUELA DE CIENCIAS JURIDICAS

SEMINARIO DE GRADUACION EN CIENCIAS JURIDICAS AÑO 2007

PLAN DE ESTUDIO 1993

"LASEGURIDAD JURIDICA DE LOS CONTRATOS EN EL COMERCIO ELECTRONICO DE EL SALVADOR".

TRABAJO DE INVESTIGACION PARA OBTENER GRADO DE LICENCIADO EN CIENCIAS JURIDICAS

PRESENTAN:

AMAYA CORNEJO, JOSE HORACIO

SARAVIA ALFARO, SANDRA LISSETTE

DRA. DELMY RUTH ORTIZ SÁNCHEZ

DOCENTE DIRECTOR DE SEMINARIO

CIUDAD UNIVERSITARIA, SAN SALVADOR, MARZO DE 2009.

UNIVERSIDAD DE EL SALVADOR

INGENIERO RUFINO ANTONIO QUEZADA SANCHEZ
RECTOR

ARQUITECTO MIGUEL ANGEL PEREZ RAMOS
VICE-RECTOR ACADÉMICO

LICENCIADO DOUGLAS VLADIMIR ALFARO CHAVEZ
SECRETARIA GENERAL

DOCTOR MADECADEL PERLA JIMENEZ
FISCAL GENERAL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

DOCTOR JOSE HUMBERTO MORALES
DECANO

LICENCIADO OSCAR MAURICIO DUARTE GRANADOS
VICEDECANO

LICENCIADO FRANCISCO ALBERTO GRANADOS
SECRETARIO

LICENCIADA BERTA ALICIA HERNANDEZ AGUILA
COORDINADORA DE LA UNIDAD DE SEMINARIO DE GRADUACION

DRA. DELMY RUTH ORTIZ SÁNCHEZ
DOCENTE DIRECTOR DE SEMINARIO

DEDICATORIA

A DIOS: En primer momento por la vida, por hecho de darme valor y comprender mis debilidades y aceptarme tal como soy, agradecer por la inconformidad que deposito en mi ser y por omitir una multitud de faltas a un el hecho de dudar de su existencia en reiteradas ocasiones y culparlo de mis errores por todo eso y muchas cosas mas gracias.

A MIS PADRES: Por su ayuda según sus posibilidades por que son parte de mi existencia por el hecho de aceptarme mi forma de ser y mostrar paciencia gracias.

A MIS HERMANOS: Por ser fuente de inspiración**,** por su ayuda incondicional por la ternura demostrada en mis problemas, por sus palabras de aliento, ellos sin duda son la mayor parte de mi triunfo tenerlos como hermanos es para mi una de las pruebas que Dios existe, a mi hermanita que me quiere sin limite y con acogedora ternura, he visto un ángel, te he visto a ti hermanita.

A MI FAMILIA EN GERERAL: A mis queridísimos abuelos maternos y paternos, tíos y tías primos y primas gracias son parte importante de mi vida y de cualquier triunfo en mi vida.

A MIS AMIGOS: Son de lo mejor, son fuera de este mundo, su apoyo y amor ah tocado mi vida en muchas ocasiones por ustedes se que la vida es maravillosa, no puedo describir todo lo que siento lo resumiré en esto los amo.

A LA DRA .DELMY RUTH ORTIZ SANQUEZ: Sin duda una de las mejores personas que tengo el gusto de conocer, por su fina colaboración y su esfuerzo por contribuir al conocimiento tanto académico como de la vida profesional gracias.

JOSE HORACIO AMAYA CORNEJO

DEDICATORIA

A DIOS TODOPODEROSO: Le doy infinitas gracias porque me regalo la sabiduría para poder cumplir esta meta, me dio fuerzas en los momentos difíciles y me regalo la fortaleza para salir adelante, porque me acompaño en este largo camino para llagar al final del mismo con éxito, por todo eso y por muchas cosas más gracias.

A MIS PADRES: José Álvaro Saravia y a María del Carmen Alfaro de Saravia, por su gran apoyo y amor en esta etapa de mi vida, por que me han enseñado que sin esfuerzo no hay recompensa, y siempre estuvieron ahí en los momentos que mas los necesite dándome ánimos y siempre regalándome un consejo, y este logro se los dedico a ellos que son lo mas importante en mi vida.

A MIS HERMANOS*:* Alba del Carmen, Álvaro Ernesto, Martha Carolina y Patricia Marycel Saravia les doy las gracias por darme ánimos en los momentos difíciles, y por estar siempre ayudándome y animándome gracias con todo mi cariño. Y a mi hermana Marlyn Elizabeth Saravia que ya no esta conmigo pero se que desde el cielo me cuida y me bendice.

A MIS AMIGOS: Susana Esmeralda Castellanos, José Horacio Amaya Cornejo, y mis demás amigos a todos les doy las gracias por su amistad y paciencia, en momentos que mas los necesite.

A LA DRA. DELMY ORTIZ: Le Agradecemos por ser nuestra Directora de Seminario de Graduación que nos dirigió con paciencia, y por compartir con nosotros sus conocimientos, y regalarnos consejos que nos servirán en nuestra vida profesional y personal, y nos oriento para que pudiéramos terminar de una manera eficaz y oportuna, este Trabajo de Graduación

SANDRA LISSETTE SARAVIA

INDICE

INTRODUCCION.....¡

CAPITULO I

PLAN DE LA INVESTIGACIÓN

1.1. GENERALIDADES. 1

1.2. PLANTEAMIENTO DEL PROBLEMA DE INVESTIGACIÓN. 1

1.3 JUSTIFICACIÓN DEL PROBLEMA. 3

1.4. ENUNCIADO DEL PROBLEMA. 4

1.5.OBJETIVOS..... 5

1.5.1 Objetivos General. 5

1.5.2 Objetivos Específicos. 5

CAPITULO II

LA CONTRATACIÓN ELECTRÓNICA

2.1. GENERALIDADES 6

2.2 ANTECEDENTES Y SITUACIÓN ACTUAL. 7

2.2.1 Antecedentes Históricos del Contrato. 8

2.2.3 Historia de Internet. 9

2.2.4 Los Contratos y las Nuevas Tecnologías. 11

2.2.5 Importancia de La Tecnología. 12

2.2.6 Transacción Electrónica Segura. 14

2.2.7 La Informática como Soporte Contractual. 16

2.2.8 Soportes Adecuados para el Documento Electrónico. 16

2.2.9 Características de los Contratos Electrónicos. 19

2.2.10 Principios de La Contratación Electrónica. 21

2.2.10.1 Principio De Autonomía de la Voluntad. 22

2.2.10.2 Principio De Buena Fe. 22

2.2.10.3 Principio De Libertad de Forma. 23

2.2.10.4 Principio De Equivalencia funcional. 24

2.2.10.5 Principio De Neutralidad Tecnológica. 27
2.3 FASES DE LA CONTRATACIÓN ELECTRÓNICA. 28
2.3.1 La Generación. 28
2.3.2 La Fase del Perfeccionamiento del Contrato. 29
2.3.3 Oferta Electrónica. 30
2.3.4 Requisitos de La Oferta. 31
2.3.5 Oferta a través de Correo Electrónico. 34
2.3.6 Oferta Realizada a traves de Pagina web 35
2.3.7 Oferta Realizada a través de Correo Interactivo. 36
2.3.8 La Revocación de La Oferta Electrónica. 37
2.3.9 La Caducidad de La Oferta Electrónica. 40
2.3.10 Aceptación Electrónica. 41
2.4 FASE DE EJECUCIÓN O CONSUMACIÓN 45
2.5 CONTENIDO DEL CONTRATO. 46

CAPITULO III

ELEMENTOS DE LA RELACIÓN CONTRACTUAL ELECTRONICA

3.1 GENERALIDADES 53
3. 2 LIBERTAD CONTRACTUAL Y LIBERTAD DE CONTRATACIÓN. 54
3.2.1 Contratación Electrónica. 55
3.2.2 Identidad de las Partes. 56
3.2.3 Capacidad de las Partes. 56
3.2.3.1 Capacidad de las partes en la contratación electrónica. 58
3.4 REPRESENTACIÓN. 58
3.5 CONSENTIMIENTO. 59
3.6 LOS VICIOS DEL CONSENTIMIENTO. 60
3.6.1 Error en cuento a la Identidad de la Cosa. 60
3.6.2 Error en la Persona. 61
3.6.3 Error en el Nombre. 61
3.6.4 Error en el Titulo 61
3.6.5 Error en la Contratación Electrónica. 62
3.7 EL PERFECCIONAMIENTO DE LOS CONTRATOS POR MEDIOS ELECTRÓNICOS. 63

3.7.1 El perfeccionamiento del Consentimiento a través de Correo Electrónico. 66
3.7.2 El Perfeccionamiento del Consentimiento a través de Páginas Web. 70
3.7.3 El Perfeccionamiento del Consentimiento a través de Correo Interactivo. 71
3.8 LUGAR Y MOMENTO DE FORMACIÓN DEL CONTRATO. 71

CAPITULO IV

LA FIRMA ELECTRONICA EN EL SALVADOR

4.1 GENERALIDADES. 75
4.2 EL USO DE LA FIRMA ELECTRÓNICA EN LA ADMINISTRACIÓN PÚBLICA. 76
4.3 LEY DE SIMPLIFICACIÓN ADUANERA. 78
4.4 LEY GENERAL MARÍTIMO PORTUARIA. 80

CAPITULO V

LA FIRMA ELECTRONICA A NIVEL INTERNACIONAL Y EN EL DERECHO COMPARADO

5. LA FIRMA ELECTRÓNICA EN EL CONTORNO COMUNITARIO EUROPEO. 82
5.1 BREVE REFERENCIA SOBRE LA LEY MODELO DE LA COMISIÓN DE LAS NACIONES UNIDAS PARA EL DERECHO MERCANTIL INTERNACIONAL (CNUDMI) SOBRE LAS FIRMAS ELECTRONICAS..... 83
5.2 BREVE COMENTARIO SOBRE LA LEGISLACIÓN DE FIRMA ELECTRÓNICA EN ESTADOS UNIDOS DE NORTEAMERICA..... 84
5.3 FIRMA ELECTRÓNICA EN EL DERECHO COMPARADO, BREVE COMENTARIO DE ALGUNAS LEGISLACIONES QUE REGULAN EL USO Y LA APLICACIÓN DE LA FIRMA ELECTRÓNICA..... 85

CAPITULO VI

SEGURIDAD JURIDICA, FIRMA ELECTRONICA Y PRESTADORES DE SERVICIOS DE CERTIFICACIÓN

6. SEGURIDAD JURÍDICA. 92
6.1 LA CRIPTOGRAFÍA Y LA FIRMA ELECTRÓNICA. 95
6.1.1 La Criptografía. 96
6.1.2 Sistema de Clave Simétrica. 97

6.1.3 Ventajas y Desventajas del sistema simétrico. 99
6.1.4 Sistema Criptográfico Asimétrico. 100
6.1.5 Ventajas y Desventajas del Sistema asimétrico o de Clava Pública. 103
6.1.6 Combinación de los Sistemas de Clave asimétrica y de Clave asimétrica o Pública..... 104
6.1.7 Empleo de los algoritmos Hash. 107
6.1.8 Procedimiento utilizado para la aplicación de la Firma Digital. 108
6.2 CLASES DE FIRMAS. 110
6.2.1 Características de la Firma Electrónica o Digital.- 113
6.3 PRINCIPIOS DE LA FIRMA ELECTRÓNICA. 114
6.4 EL PAPEL QUE JUEGAN LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN EN EL PROCESO DE APLICACIÓN DE LA FIRMA ELECTRÓNICA. 114
6.5 GENERALIDADES DE LAS ENTIDADES DE CERTIFICACIÓN. 118
6.5.1 Componentes Técnicos. 119
6.5.2 Vigencia de los Certificados. 120
6.5.3 Definición de las entidades de certificación. 120
6.6 PROCEDIMIENTO PARA GENERAR UN CERTIFICADO DIGITAL 122
6.6.1 Contenido de los Certificados. 123
6.7 NATURALEZA JURÍDICA DE LAS ENTIDADES DE CERTIFICACIÓN. 124
6.8 FUNCIONES DE LAS ENTIDADES DE CERTIFICACIÓN. 124
6.9 CLASIFICACIÓN DE LOS CERTIFICADOS. 125
6.10 IMPORTANCIA DE LAS ENTIDADES DE CERTIFICACIÓN. 126
6.10.1 Certificados de Seguridad electrónica. 127
6.10.2 Certificados de Seguridad en comunicación. 127
6.10.3 Certificados de Seguridad entre las partes. 127
6.11 PRINCIPIOS GENERALES PARA LA PRESTACIÓN DE SERVICIOS DE CERTIFICACIÓN. 128
6.11.1 Régimen de Libre Competencia. 128
6.11.2 Sistema de acreditación de servicios de certificación. 128
6.11.3 Registro de Servicios de certificación. 128
6.12 OBLIGACIÓN DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN. 129
6.12.1 Obligaciones Generales. 129
6.12.2 Obligaciones Específicas. 129

6.13 REQUISITOS DE LAS ENTIDADES CERTIFICADORAS. 132
6.13.1 Requisito Temporal. 132
6.13.2 Requisitos Técnicos y de Personal. 132
6.13.3 Requisitos Economicos..... 132
6.13.4 Requisitos Informáticos y de Documentación. 132
6.14 RESPONSABILIDAD DE LAS ENTIDADES DE CERTIFICACIÓN. 133
6.14.1 Responsabilidad Civil. 133
6.14.2 Responsabilidad Civil por el Uso Indebido de Parte de Terceras Personas de los Certificados Reconocidos y Extendidos por las Entidades de certificaciòn..... 134

CAPITULO VII
CONCLUCIONES Y RECOMENDACIONES

7.1 CONCLUSIONES..... 136
7.2 RECOMENDACIONES 138

BIBLIOGRAFIA..... 140

ANEXOS

INTRODUCCIÓN

La sociedad se moderniza motivando cambios en la realidad mundial, debido a este acontecimiento, surgen incógnitas con respecto al hecho de cómo seguir la línea de la modernidad, es por ello que es de suma importancia, hacer investigaciones que vengan a enriquecer el ámbito intelectual, en este sentido es que surge la necesidad de investigar la realidad de los países llamados de primer mundo, para no quedar marginados y vivir de forma arcaica es por ello que es una motivación el desarrollar el tema La Seguridad jurídica de los Contratos en el Comercio Electrónico de Salvador .

La Globalización tecnológica incide en la evolución de las relaciones de la sociedad humana generando nuevas formas de relación jurídica a las que el Derecho debe dar respuesta, para no quedar relegado en los conceptos tradicionales y así adecuarse al desarrollo tecnológico de las modernas instituciones jurídicas.

En el presente trabajo se hace una breve introducción con respecto al ámbito de la historia esto con el fin de dar énfasis al desarrollo que es palpable debido a la creciente tecnología.

En este primer capítulo se determina el plan de la investigación estableciendo los parámetros que se seguirán a lo largo de la investigación, establecer la necesidad de investigar dicho tema y delimitarlo, el porqué de la investigación y que se pretende con el estudio de dicho tema.

En el capitulo dos se hace referencia a los hechos históricos que motivaron los contratos de forma general estableciendo el derecho canónico como fundamento, basada en la idea que el quebrantamiento de una promesa simple era moralmente reprochable, con ello se marca el comienzo de lo

concerniente a los contratos de forma general. También se mencionan los antecedentes modernos de la contratación electrónica como lo es el Internet y cual es la situación que se ve reflejada en la sociedad Salvadoreña, el ejercer el comercio por vía electrónica, el hecho de cómo las nuevas tecnologías ayudan a mejorar y facilitar los contratos además de mencionar cuales son los medios adecuados para almacenar información debido a sus características y su uso lo que se conoce como soportes informáticos.

Lo que se refiere al capítulo tres aquí se establece la diferencia entre libertad contractual y libertad de contratación además se hace referencia al hecho de los elementos constitutivos del contrato y por el hecho de ser entre ausentes el contrato electrónico es por presunción de aquí que todo contrato celebrado es obligatorio entre las partes, se establecen los vicios del consentimiento, el error es el predominante en las transacciones electrónicas, además, de donde se perfeccionan los contratos.

En el capitulo cuatro se establecen las generalidades de la firma electrónica en El Salvador y el uso que esta tiene en la administración pública (como ejemplo realizar la transmisión de datos de mercaderías en las aduanas). Por otro lado establece un marco legal en el cual se menciona la ley de simplificación aduanera como una normativa que aunque de forma escasa regula en cierta forma el ámbito electrónico en El Salvador, se otorga valides a las transacciones de datos por medios electrónicos y se dotan de plena validez, con la condición que estén certificados, ósea que en la institución encargada de dar confianza sobre lo establecido en un contrato se realiza en un día y hora especifico

En el capitulo cinco se hace una breve referencia a la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) relativa a la Firma Electrónica y su guía para la incorporación al derecho interno. Esta ley da parámetros a seguir para unificar la legislación sin

desmejoras o derogar los derechos de los consumidores refleja el principio de neutralidad respecto de los medios técnicos utilizados, el criterio de la no discriminación de todo equivalente funcional de los conceptos y prácticas que tradicionalmente funcionan sobre el soporte papel.

El fin de esta ley Modelo es ayudar a los estados a establecer un marco legislativo moderno, armonizado y equitativo para abordar de manera mas eficaz las cuestiones relativas a las firmas electrónicas, además ofrece un vinculo entre dicha fiabilidad técnica y la eficacia jurídica que cabe esperar de una determinada firma electrónica por esto y más esta ley puede ayudar a configurar practicas comerciales más armoniosas en el ciberespacio. También se hace una breve referencia a la legislación sancionada por la Unión Europea relativa a la Firma Electrónica esta lo que busca es armonizar las legislaciones de los países que conforman la unión europea en lo relativo al uso de la firma electrónica.

Al igual que muchos otros países que ya han incorporado a su normativa interna leyes especiales sobre firmas electrónicas, o han realizados reformas a las legislaciones ya existentes para armonizarlas con las nuevas tecnologías, se ha tomado en especial referencia al Real Decreto de España por el hecho que se comparte el mismo sistema Jurídico Romano-Germánico, y por ser uno de los países a nuestro parecer que mejor regula lo que refiere a la firma electrónica y lo concerniente a su método de empleo y detallar los requisitos y obligaciones de las entidades certificadoras, mencionando que debe contener como mínimo un certificado y las utilidades.

Y finalmente en el capítulo seis, se da una breve explicación de la importancia que tiene la seguridad jurídica en el desarrollo de la contratación electrónica, y se establecen las generalidades tanto de la criptografía, como las de la firma electrónica sus definiciones y clases además se detallan las características, principios y objetivos detallando sus aspectos técnicos como la definición de criptografía .en este se desarrollan las generalidades de las

entidades de certificación su concepto, características y su importancia, estableciendo la seguridad que brinda a la vinculación de una clave con su suscriptor además de las obligaciones que tiene como entidad de registro, como el de mantener actualizadas sus bases de datos para la consulta que se requiera de ella y los principios que rigen la prestaron de servicios de certificación.

CAPITULO I

PLAN DE LA INVESTIGACIÓN

SUMARIO: **1.1.**Generalidades. — **1.2.** Planteamiento del Problema de Investigación. — **1.3** Justificación del Problema. — **1.4.** Enunciado del Problema. — **1.5.** Objetivos. **1.5.1** Objetivo General. **1.5.2** Objetivos Específicos. —

1.1. GENERALIDADES.

Para simplificar el estudio que vamos a realizar hemos resumido en el siguiente capitulo de una forma muy breve la situación problemática que se busca desarrollar a lo largo del trabajo de investigación como es la *seguridad jurídica de los contratos en el Comercio Electrónicos de El Salvador.* Desarrollaremos la situación problemática, el porque de la investigación y cuales son los objetivos que se pretenden alcanzar con la investigación.

1.2. PLANTEAMIENTO DEL PROBLEMA DE INVESTIGACIÓN.

El Derecho Contractual se originó del derecho canónico mediante el cual se estableció el principio **"pacta sunt servando**", es decir, **"***que lo pactado obliga***"**, es con este hecho histórico que se declaran accionables todos los contratos. El fundamento de la doctrina canónica se basaba en la idea que el quebrantamiento de una promesa simple era moralmente reprochable.

En el Derecho Romano también se originó una obligación accionable, de ahí que los elementos esenciales de la doctrina canónica de los contratos fueron asumidos por el **"ius comune"**, o sea, **"**el derecho común**"**. Por su parte, el jusnaturalismo sostuvo que la creación de las obligaciones se encuentra en la libre voluntad de los contrayentes[1].

Conforme a la evolución histórica que han sufrido los contratos, y los avances tecnológicos que viene experimentando la sociedad tienen una

[1] HINESTROSA, FERNANDO, *El Contrato por Medios Electrónico***,** Homenaje a sus 40 años de Rectoría, Colombia, 1963 **–**2003**,** Pág. 66.

incidencia cada vez mas en la esfera del derecho, por la razón que la globalización tecnológica incide en la evolución de las relaciones de la sociedad humana y así generan nuevas formas de relación jurídica a las que el derecho debe dar respuesta; para no quedar relegado en los conceptos tradicionales y así adecuarse al desarrollo tecnológico de las modernas instituciones jurídicas como es el comercio electrónico.

La figura del contrato ha sido el instrumento básico en las relaciones humanas hasta la actualidad. El Código Civil salvadoreño en su Art. 1309 expone a las obligaciones como: "*Una convención en virtud de la cual una o más personas se obligan para con otras*". Es fundamental determinar el momento y la forma en que se perfecciona el consentimiento o cuando el contrato queda efectivamente celebra.

Por consiguiente, en el presente trabajo se establecerá donde y cuando se entiende establecida y aceptada la oferta que será el objeto del contrato. Para declarar la conformidad respecto a lo acordado, se requiere de elementos que brinden seguridad para dar confianza a las partes, por tal razón hay mecanismos que pueden brindar dicha seguridad jurídica como son la firma electrónica o digital y las entidades de certificación, estos elementos son los encargados de garantizar la legitimación de quien se comunica a través de la red y su adecuado conocimiento del alcance jurídico del contenido del documento firmado y emitido electrónicamente; estos permiten garantizar con alto grado de fiabilidad, el origen y integridad del mensaje. Estos son los que mejor satisfacen las exigencias de seguridad y confianza[2].

[2] MARTÍNEZ NADAL, APOL·LÒNIA, *Comercio Electrónico, Firma Digital y Autoridades de Certificación*, Editorial Civita, Madrid, 2001, Pág. 172.

Por lo general hay cierta resistencia en la realización de transacciones por medios electrónicos, por el hecho, que la normativa nacional resulta insuficiente para regular las relaciones jurídicas que se establecen en los contratos electrónicos, por la inseguridad que pueda haber en las nuevas formas de realizar negocios por medios digitales.

Mientras no exista normativa que garantice la seguridad en las transacciones por medios electrónicos existirá una problemática en el país, por el hecho, que el salvador se encontraría en una desventaja frente a las nuevas formas de realizar negocios a escala mundial, por no contar con los mecanismos adecuados, es decir, leyes apropiadas para garantizar esta novedosa herramienta de efectuar contrataciones electrónicas.

1.3. JUSTIFICACIÓN DEL PROBLEMA DE INVESTIGACIÓN

Después de plantear la situación problemática sobre la seguridad jurídica de los contratos en el comercio electrónico de El Salvador, se observa que en el país no hay investigaciones realizadas que aborden la problemática de la seguridad en la contratación electrónica.

Es por ello que en la indagación que se realizo se encontraron temas similares como lo son: 1) el análisis jurídico del comercio electrónico. 2) La necesidad de regulación jurídica en El Salvador, de los contratos electrónicos. 3) El comercio electrónico de El Salvador.

Es entonces la falta de investigación de un trabajo que desarrolle en si la seguridad de los contratos en el comercio electrónico de El Salvador, lo que lleva a determinar que la presente investigación vendrá a llenar un vació teórico que está experimentando la realidad jurídica de la nación por lo novedoso del tema.

El surgimiento de esta forma de contratación a través de medios electrónicos, permite establecer la agilidad y reducción de costos que estos contratos originan, de ahí la importancia de esta clase de negocios por medios electrónicos.

La presente investigación lo que busca es el desarrollo de una guía teórica que sirva para valorar los diferentes puntos de vista que sobre este tema se proporcionan, dando un enfoque con relación al entorno jurídico, en el país no hay una normativa que regula las transacciones electrónicas que se realizan dentro del comercio electrónico y que garantice la seguridad jurídica de esta forma de contratación y no se cuenta con un formato digital para la celebración de dichos actos jurídicos; en relación con otros países, El Salvador se encuentra en una gran desventaja en cuento a las negociaciones comerciales por medios electrónicos, en el presente trabajo se pretende dar un aporte al conocimiento jurídico teórico y hacer ver la necesidad de crear y adecuar la legislación para facilitar, el máximo desarrollo del comercio electrónico y garantizar la seguridad jurídica para la realización de contratos electrónicos.

1.4. ENUNCIADO DEL PROBLEMA

¿Cuál es la Seguridad Jurídica que ofrecen los contratos en el comercio electrónico de El Salvador y de que forma se perfecciona el consentimiento de las partes, así también, como se determinan los requisitos de formación y validez?

1.5. OBJETIVOS DE LA INVESTIGACIÓN

Con la aparición de Internet y el creciente fenómeno de la contratación por medios electrónicos, y por ser estas contrataciones transfronterizas estas generan desconfianza, consecuentemente se reclaman tanto soluciones jurídicas como técnicas para los nuevos retos que plantea la red y por lo tanto, se busca brindar seguridad, a través del medio técnico llamado firma electrónica y también por medio de una legislación adecuada que regule la primera, con estos se busca aportar seguridad y certeza a las contrataciones por medios electrónicos.

1.5.1 OBJETIVO GENERAL:

a. Investigar la seguridad jurídica que ofrecen los contratos en el comercio electrónico, su perfeccionamiento, los requisitos de formación, y la importancia de contar con una legislación adecuada que garantice la realización de dichos contratos.

1.5.2 OBJETIVOS ESPECIFICOS:

a. Verificar la seguridad jurídica que proporcionan estos contratos.

b. Indicar cuales son los requisitos de formación y validez de los contratos en el comercio electrónico.

c. Determinar cual es la importancia de contar con una legislación apropiada para regular esta forma de contratación.

d. Comparar la legislación nacional y internacional relacionada con la seguridad de los contratos en el comercio electrónico

CAPITULO II

LA CONTRATACIÓN ELECTRÓNICA

SUMARIO: 2.1.Generalidades 2.2 Antecedentes y Situación Actual. 2.2.1 Antecedentes Históricos del Contrato. 2.2.3 Historia de Internet. 2.2.4 Los Contratos y las Nuevas Tecnologías. 2.2.5 Importancia de La Tecnología. 2.2.6 Transacción Electrónica Segura. 2.2.7 La Informática como Soporte Contractual. 2.2.8 Soportes Adecuados para el Documento Electrónico. 2.2.9 Características de los Contratos Electrónicos. 2.2.10 Principios de La Contratación Electrónica. 2.2.10.1 Principio De Autonomía de la Voluntad. 2.2.10.2 Principio De Buena Fe. 2.2.10.3 Principio De Libertad de Forma. 2.2.10.4 Principio De Equivalencia Funcional. 2.2.10.5 Principio De Neutralidad Tecnológica. 2.3 Fases de La Contratación Electrónica. 2.3.1 La Generación. 2.3.2 La Fase del Perfeccionamiento del Contrato. 2.3.3. Oferta Electrónica. 2.3.4 Requisitos de La Oferta. 2.3.5 Oferta a través de Correo Electrónico .2 3.6 Oferta Realizada a través de Páginas webs. 2.3.7 Oferta Realizada a través de Correo Interactivo. 2.3.8 La Revocación de La Oferta Electrónica. 2.3.9 La Caducidad de La Oferta Electrónica. 2.3.10 Aceptación Electrónica. 2.4 Fase de Ejecución o Consumación 2.5 Contenido del Contrato.

2.1 GENERALIDADES

Como forma introductoria del presente capitulo se hará un breve comentario para cumplir dicho fin se comenzara por mencionar de donde proviene la contratación y su forma de evolución pasando por las diferentes etapas del Derecho Romano, para reflejar la idea, de cómo es que la realidad cambia y el derecho como parte de esta inevitablemente se ve en constante evolución, apareciendo así nuevas formas de comunicación por medios electrónicos a través de redes abriendo paso a otros datos de intercambio electrónico [3].

[3] http: //es ucla/personal history. Visitada el 5 de Agosto de 2008. Esta página establece la importancia que tiene la historia en relación directa con la sociedad y la realidad que cambia constantemente por ello se hace necesario establecer como es que es estos cambios se efectúan y la necesidad de ser parte de estos cambios para seguir el camino del cambio y desarrollo.

Como forma de antecedentes Históricos del Contrato el Derecho Romano tenemos el ***pacta sunt Servando,* el *nexun, y la sponcio*** que rompió los esquemas anteriores ya que con este se le dio la fuerza jurídica a los actos que realizaban las personas, luego avanzando un poco mas en la Historia se toma como otro antecedente del contrato electrónico el Internet como herramienta que agiliza el comercio es por ello que el contrato debe ir amoldándose a las nuevas tecnologías sin rechazar los cambios sino por el contrario acomodándose a estos de aquí que se reconoce la importancia de la tecnología para establecer nuevas formas de seguridad como lo es la firma Electrónica que es la que da protección a los mensajes de datos por medio de la encriptación.

La Trasmisión Electrónica Segura es un protocolo para que los pagos mediante tarjetas de crédito sean seguros y confidenciales[4].Los soportes y registros del documento electrónico se plasman con sistemas binarios es decir lenguaje maquina que representa las letras por medio de combinaciones de unos y ceros, así como el papel es un soporte para el documento escrito.

2.2 ANTECEDENTES Y SITUACIÓN ACTUAL

Se considerará necesario dar una breve Introducción con respecto al tema a tratar ya que éste por su carácter novedoso y dinámico necesita un desarrollo claro, es partiendo de esta idea que se debe dar un enfoque preciso sobre la contratación electrónica, es por ello que se dará un breve repaso a la historia de los contratos y su evolución dando énfasis al aspecto actual de esta problemática, partiendo de esta premisa se hará el siguiente esbozo.

---

[4] NAJARRO, KENELMA BERENICE *Comercio Electrónico y su Aplicación en la Trasformaciones Económicas y Tecnológicas de los Países en Desarrollo*. Universidad de El Salvador. Tesis -2002. Esta tesis plantea el hecho que la tecnología esta cambiando la realidad que nos rodea y además que el desarrollo en gran medida depende de la tecnificación de los países.

Como es sabido el derecho Romano es un antecedente histórico importante del Derecho y por tanto del contrato como una de las manifestaciones de éste, por tal motivo se remitirá a mencionar un poco sobre la evolución del Contrato en el Derecho Romano.

El crecimiento del comercio Electrónico es tan grande que nadie duda del profundo impacto económico y social que traerá todos los actores involucrados, desde Gobiernos, asociaciones Industriales y empresas individuales para aprovechar al máximo sus ventajas[5].

Por otra parte en cuanto al contrato Electrónico la redacción debe estar en términos jurídicos y técnicos debidamente precisados, citas de artículos inclusión de glosario y anexo para evitar los mal entendidos y de más claridad a la relación contractual.

2.2.1 ANTECEDENTES HISTÓRICOS DEL CONTRATO

Se establece como datos históricos que el Derecho Contractual pudo organizarse del ***Pacta Sunt Servando***, es decir que lo pactado obliga, es de este acontecimiento histórico que el derecho se consagra ya que surgen los comienzos de la obligación por medio del consentimiento[6]. Es decir ese acuerdo de voluntades tomadas entre dos o más personas que se ve concretizado por medio del contrato sus características y elementos, hechos que se estudiaran en su momento, por ahora es solo hacer mención de ellos, volviendo al tema de las obligaciones, estas fueron dinámicas no se quedaron solamente en un decir sino que se materializaba, por medio de diferentes medios como:

---

[5] VILLAR, JOSE MANUEL. "Derecho de Internet, Contratación Electrónica y Firma Digital" Capitulo I Una Aproximación a La Firma Electrónica, Editorial Aranzamendi, Madrid, 2001. Pág.167. Esta obra trata de que es lo que debemos de entender por firma Electrónica y cuales son los parámetros para considerar un contrato Electrónico.

[6] PETIT, EUGENE. Derecho Romano, Editorial Porrua, Tercera Edición, México, 1997, Pág.320. Esta obra trata de la importancia que tiene el derecho en la sociedad y explica los cambios que este ha sufrido en el

El *Nexum*, forma antigua de obligarse, la causa era el préstamo de dinero solemnidad requerida, declaración del acreedor, ésta contenía una damnatío, ésta era una condena y consistía en comprometer al obligado si no pagaba se sometía al ***manus injecto*** especie de toma de cuerpo del acreedor hacia su deudor, esto causó muchos abusos se podía incluso encadenar y tratar como esclavo para pagarse[7]. Fue por ese motivo que ya no se aplicó dando cabida a otras formas de obligación:

La ***Sponcio*** dio fuerza jurídica a los actos de las personas, consistía en una pregunta del acreedor seguida de la respuesta de su deudor con el verbo ***Pondere*** que no se sabe con certeza cual es su significado pero evidentemente evolucionó, en su forma de hacer valer la obligación que contenía el acuerdo.

2.2.3 HISTORIA DE INTERNET

El Internet es un antecedente debido al hecho que es a través de ésta que ha adquirido mayor relevancia la temática de la contratación electrónica, ya que es a través de Internet que es posible que dichos contratos tengan la posibilidad de realizarse en pocos minutos a grandes distancias hecho que evidentemente agiliza el comercio electrónico[8].

Se vio como necesario el hecho de una comunicación que fuera de forma global y en minutos es por ello que en el presente trabajo se remita a mencionar al señor J.C.R. Licklider como pionero de la red mundial como consta en el

---

devenir del tiempo, el derecho Romano es muy importante pues de este provienen en su mayoría las instituciones jurídicas.

[7] Vid. PETIT EUGENE. Derecho Romano…, Cit., Pág. 320. Esta obra trata de la importancia que tiene el Derecho Romano para el contrato actual pues es este de donde proviene y para saber sus bases es necesario consultar dicha fuente de información, para saber sobre los orígenes de las obligaciones se parte del Derecho Romano pues es este el que tiene en sus orígenes una explicación de por que es importante el obligarse

[8] http:www.ik.es.ucla/personal History. Visitada el 5 de Agosto de 2008.

documento de Enero 1960, Man-Computer Simbiosis (Simbiosis Hombre-Computadora)[9].

Licklider fue nombrado Jefe de DARPA (Departamento de Defensa de los Estados Unidos), en Octubre de 1962 esto dio paso a estudios sobre redes para comunicación de aquí que se desarrolla un poco más la tecnología abriendo paso a datos de intercambio[10].

En 1972 a través de las investigaciones se sostuvieron discusiones en línea, teniendo de este modo acceso a base de datos remotos intercambiando archivos y enviando y recibiendo correos electrónicos, esto permitió la creación de tecnología Internet/Web que fue fundamental para redes de computadoras y usuarios.

Las redes basadas de ARPANET eran pagadas por el gobierno y se restringían, no tenían usos comerciales se usaban para investigación, su conexión se tenía con sitios militares y universidades, se veía como algo netamente de datos sobre estudios y no se mirará el comercio como algo realmente relevante para establecerse en la red.

En la actualidad debido al avance que tiene la tecnología es preciso indagar sobre la realidad mundial para no quedarse atrás de aquí que el desarrollo de la sociedad exige modernidad en cuanto a la utilización de nuevas formas de hacer negocios.

[9] http:www.ik.es.ucla/personal History. Visitada el 5 de Agosto de 2008

[10] http:www.ik.es.ucla/personal History. Visitada el 5 de Agosto de 2008. Se desarrolla lo que es la historia del Internet y su forma de evolución de aquí la importancia de la consulta realizada para establecer el hecho de cómo es que los cambios tecnológicos afectan todo el ámbito de la realidad y no solo una parte de esta

2.2.4 LOS CONTRATOS Y LAS NUEVAS TECNOLOGÍAS

Como forma introductoria de esta parte se comenzará por definir que es un contrato de aquí que se cita a Alessandri y Somarriva definiéndolo como*: El acuerdo de voluntades de dos o más personas destinado a crear obligaciones*[11]*.* Ramón Meza Barros, por su parte, lo define como *La convención generadora de obligaciones*[12]*.*

Se debe entender que los contratos son numerosos y tienen características y elementos que se desarrollarán en el transcurso de este trabajo por el momento solo se hará un breve comentario, con respecto a la definición del contrato.

En un primer momento se comenta el hecho de establecer un acuerdo de voluntades que se concretiza en el consentimiento de aquí que para crear obligaciones se debe estar de acuerdo con lo que se plantea ya que si no es así el contrato no se concretiza por ser la voluntad un elemento indispensable ya que al ser obligado o forzado de alguna forma una parte contratante se tomará como que nunca se dio dicho contrato.

Otro dato importante es que menciona dos o más personas, sin definir la clase de éstas como es sabido existen naturales y jurídicas. Por el momento de no establecer, a qué tipo se refiere se entiende que son de las dos clases, claro está que un ente ficticio no piensa, ni puede materializar algo, puesto que él mismo no está materializado, entonces se entiende que será por medio de la

---

puesto que es un acontecimiento en cascada si existe un cambio este exige otro y así es como la sociedad se encuentra inmersa en la realidad y su necesidad de cambio.

[11] RODRÍGUEZ ALESSANDRI, ARTURO; UNDURRAGA SOMARRIBA, MANUEL, *Curso de Derecho Civil Fuente de las Obligaciones*. Redactado por Antonio, Vodanovic H; Tomo IV; Editorial Nascimento; Chile; 1976, Pág. 9. Esta obra menciona que debemos entender por contrato es por ello que es importante tomarlo como una guía, puesto que la contratación electrónica solo posee pequeños cambios como lo es el medio empleado para realizar la formación del consentimiento debido a que es a través de el mensaje electrónico de datos.

[12] MESA BARROS, RAMÓN; *Manual de Derecho Civil; de las Fuentes de las Obligaciones*, Tomo Quinta Edición; Editorial Jurídica de Chile; 1976, Pág. 9.

representación de una persona natural, definición que se establece en el artículo 52 del Código Civil[13], solamente se menciona en este momento para relacionarlo con el aspecto jurídico de lo que son las personas debido a la importancia que reviste cada aspecto se desarrollará a continuación lo concerniente a lo tecnológico.

2.2.5. IMPORTANCIA DE LA TECNOLOGÍA

La tecnología por su importancia ha modificado el mundo dado las modernas técnicas informáticas que permiten la utilización de un gran número de controles, como, por ejemplo, las tarjetas magnéticas, los códigos secretos, o el número de identificación personal (NIP), la identificación por medio del iris y los vasos capilares de la retina del ojo, la decodificación de la voz y la identificación de huellas dactilares[14].

Si bien es cierto que estas tecnologías no están para el uso común, son formas de seguridad al igual que la firma electrónica que es aquella que brinda protección a un mensaje de datos puesto que los codifica y descodifica.

Es por ello que también las tecnologías no aplicadas plenamente deben ser comprendidas por las normas en la medida y extensión en la cual se hace la aprobación de la ley correspondiente a la tecnología que tiene pleno uso de esta forma dando así vigencia al principio de la neutralidad tecnológica, por estos motivos se establece como una interpretación legal.

---

[13] Código Civil Salvadoreño Editorial Jurídica Salvadoreña Republica de El Salvador Año 2007. Art. 52. Se explica en este articulo en sentido amplio el concepto de persona estableciendo que existen de dos tipos una natural y otra jurídica esta ultima es aquel ente ficticio capas de adquirir derechos y contraer obligaciones que tiene su representante que es aquel que materializa las acciones que ejecute La Empresa.

[14] http/www.derecho.org. Visitada el 25 de Agosto de 2008. Aquí se encuentra mucha información con respecto ha información jurídica valiosa se recomienda analizarla en diferentes aspectos como un claro ejemplo la contratación en su forma amplia.

El hacer énfasis en que se estará sujeto a la situación en concreto de modo que la legislación como su interpretación busquen estar en consonancia con las nuevas tecnologías.

Estableciendo la palabra nuevas tecnologías debe entenderse que éste incluye los medios electrónicos para captar, procesar, almacenar, transmitir y comunicar información[15].

Se entenderá por captación el recibir información por los diferentes medios que la tecnología ofrezca, es evidente que ésta dinámica ha aumentado la productividad y ha mejorado los sectores económicos y otros gracias a muchos factores como por ejemplo las comunicaciones rápidas y baratas, de aquí que las empresas pequeñas aprovechan este recurso para poder tener más acercamiento a la población en general y de ésta manera ser más competitivo en el mercado y buscar un desarrollo equitativo[16], esto se ve reflejado en el hecho que en las épocas antiguas eran pocas las empresas que aglomeraban el comercio y en la actualidad existen más del doble de las empresas que dominaban el mercado, tan importante ha sido el desarrollo de la tecnología que países enteros han comenzado en el proceso del desarrollo todo gracias a el acoplamiento efectivo que tienen con los cambios tecnológicos.

Lastimosamente la desigualdad en cuanto a la obtención de la tecnología y el manejo de ésta afecta en gran manera a los países menos desarrollados es evidente que si la educación básica es poca en un país aún menos será la tecnificada por el hecho de ser más compleja.

---

[15] Vid. NAJARRO, KENELMA BERENICE, *Comercio Electrónico y su implicación en las transformaciones.., Cit*., Pág. 17. esta tesis desarrolla el hecho de la importancia que posee La Contratación Electrónica por sus características dada la agilidad que se posee con esta en el Comercio Electrónico además de mencionar que la tecnificación produce profundos cambios en la sociedad y la economía.

[16] Vid. NAJARRO, KENELMA BERENICE, *Comercio Electrónico y su implicación en las transformaciones*..., Cit., Pág.17.

Otro hecho muy importante es que cuando sale un producto de alta tecnología su precio en ese momento tiende a ser elevado y por regla general solo se vuelve un poco común en países que no son catalogados como pobres, es decir los de primer mundo y ésta tecnología en países subdesarrollados solo la obtienen personas privilegiadas.

2.2.6 TRANSACCIÓN ELECTRÓNICA SEGURA.

SET es un protocolo de transmisión de datos en Internet diseñado para que los pagos mediante tarjeta de crédito sean seguros y confidenciales[17].

El estándar de SET especifica el formato de los mensajes que se intercambian entre el vendedor, el comprador y los otros participantes (bancos, agencias de autorización, etc.).

La seguridad y privacidad se logra mediante el encriptamiento de los mensajes, y mediante la autenticación de todos los participantes[18]. La seguridad de los datos en un mensaje está protegido por tecnología en el sentido que mientras más difícil sea el desarrollo de encriptación mayor seguridad para su contenido, como se logra apreciar a simple vista los cambios de la sociedad influyen de manera decisiva en las formas de hacer negocios y tratos de diferente índole, la comunicación es sumamente importante en épocas antiguas para llevar un mensaje de un extremo del país a otro se verificaba en días debido a que dichos mensajes eran enviados por escrito en correos que tardaban mucho hoy en día, aún niños se comunican en segundos, se puede apreciar que ésta es una de las mayores ventajas de el desarrollo que la sociedad experimenta entre otras que se establecerán en su momento.

---

[17] Vid. NAJARRO, KENELMA, BERENICE. *Comercio Electrónico y su implicación en las Trasformaciones*...., Cit., Pág. 68. Se Desarrolla la importancia que representa lo Electrónico en el Ámbito Social

[18] Vid. NAJARRO, KENELMA, BERENICE. *Comercio Electrónico y su implicación en las Trasformaciones*…., cit., Pág.69. Se comenta en esta parte la seguridad que se necesita para dar confianza a la contratación Electrónica para que el comercio sea mayor ya que ha mayor confianza mayor aceptación y por ende mas comercio.

Debido a la creciente tecnología y en especial del Internet se han creado las empresas virtuales, que son aquellas que están en un sitio electrónico el cual es su único medio de difusión de sus negocios. Las ventajas principales de utilizar la red son:

1. El alcance mundial a bajo costo.
2. No existen fronteras geográficas.
3. Se otorga valor probatorio a los Documentos Electrónicos[19].

Los cambios que se sufren en virtud del desarrollo son muchos, no solo la informática sino todo aspecto de la realidad, debido a que en la sociedad todo está conectado, como se aprecia al cambiar el comercio en su forma material a virtual en el sentido de transacciones que tengan que ver con información de mensajes de datos, claro está que la entrega de una mercancía en sentido material deberá hacerse en sentido tangible, se menciona que el Internet, no posee limitaciones geográficas, la red no posee fronteras por el simple hecho que no se detiene, es dinámico y no posee limitaciones en el sentido geográfico, así como se puede platicar con alguien de México, se puede también con otra persona que viva en Italia sin ningún problema, por el simple hecho que la red no se detiene, es dinámica y no posee limitaciones en el sentido geográfico, la limitante, tiempo, espacio no existe, es por ello la importancia de la tecnología, por tanta relevancia es necesario también dar su aporte a esta tecnología, es por ello que a ese apartado se le dedicarán las líneas siguientes.

[19] GALAN CORTEZ, JEANNIE ELIZABETH, *La firma Digital como medio de Seguridad y consentimiento en las transacciones del comercio Electrónico*. Universidad de El Salvador. Tesis 2006, Pág. 118 y siguiente. Esta tesis establece las ventajas que se dan en el comercio Electrónico y por ende al contrato Electrónico como producto del desarrollo.

2.2.7 LA INFORMÁTICA COMO SOPORTE CONTRACTUAL

Los soportes y registros del documento electrónico se plasman con sistemas binarios, en soportes magnéticos, ópticos etc., y requieren para su reproducción de un software y un hardware específico compatible con el sistema informático donde se crearon y para su trasmisión redes de comunicación digital de distinta topología[20]*.*

El registro y almacenamiento de documentos jurídicos multimedia, deben ser registrados en memorias digitales produciéndose de esa manera una desmaterialización del documento, sin que ello quiera decir que todos los soportes sobre los que opera la contratación electrónica sean inestables o volátiles.

En los planteamientos anteriores se plantea que los soportes electrónicos no están registrados en papel sino en sistemas binarios, la computadora no conoce letras sino la representación de estas y se plasman a través de su lectura electromagnética por medio de lente óptico u otras similares formas conocidas de almacenamiento, disco duro, memorias, disquetes, etc.

2.2.8 SOPORTES ADECUADOS PARA EL DOCUMENTO ELECTRÓNICO

El soporte óptico, *es un soporte no degradable, con gran capacidad de almacenamiento y fiabilidades encuentran dentro de este tipo los siguientes CD, DVD, CD-R y otros ,en estos sistemas la grabación y lectura del documento se efectúa por medio de un micro rayo láser digitalmente es decir ,una vez convertida la señal análoga ,se graba codificada en binario ,en formas de surcos con zonas de bajo relieve o lisas la información se leída por la incidencia de un*

[20] GAITÁN CORTES, CARLOS ERNESTO, GUZMÁN, MARTA, RIVAS, VICENTE *Relaciones Contractuales en Internet y su Desprotección por la falta de Legislación de Comercio Electrónico*. Universidad de El Salvador 2003, Pág. 164. Se plantea en esta tesis la falta de protección que tiene las relaciones contractuales en cuanto a una Ley General aplicable a todo tipo de transacciones en el ámbito del comercio Electrónico.

láser cuya luz reflejada produce dos tipos de intensidad según el relieve de la pista , que una vez procesada reproduce la información análoga contenida en ella[21]*.*

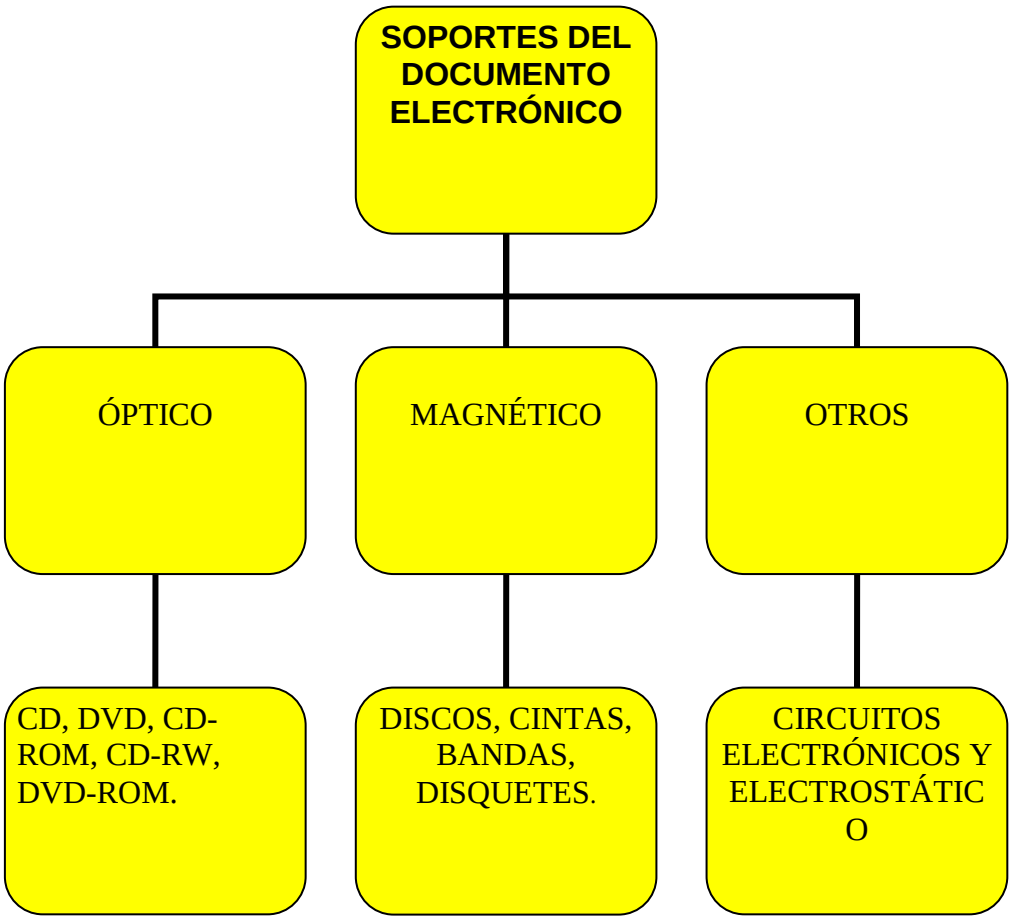
"*Los soportes tienen gran capacidad de almacenamiento y esto es sumamente útil en un CD se puede guardar mucha información que seria difícil traerla consigo con la facilidad que se hace por este medio y no se desmejora o degrada con ello se quiere decir que tiene ventajas sobre el soporte en papel puesto que este si se desmejora y degrada ensuciándose o maltratándose perdiendo su presentación decorosa*". En estos soportes la información se procesa y reproduce el contenido y esta es la interpretación de los códigos convertida en la información que se requiere se planteo ya que la computadora no sabe de letras sino de códigos que representan letras a través de diferentes combinaciones que al interpretarse son plasmadas en el contenido.

Combina ambas características, su durabilidad, capacidad de almacenamiento y velocidad de lectura la capacidad de grabación es mayor. No es sensible a campos de agresiones. Lo más aconsejable para la grabación del contrato electrónico serán: una memoria estable, imborrable y que reproduzca fielmente la voluntad de los contratantes con métodos y sistemas estándar, se ajustan a estos requisitos EL COMPACT DISC, CD ROM, DVD, que grabados inutilizan la parte del soporte no usada y en la usada no puede regrabarse, lo que unido a elementos de software y hardware de autenticidad, autoría pueden proporcionar documentos fiables.

La capacidad de almacenamiento es algo que se explico en su momento, se señalo que consistía en la gran capacidad de tener mucha información que pueda cargarse sin los inconvenientes que se tienen al tener esa misma información de manera tradicional o escrita por ello se pasara a dar una breve

[21] Vid GAITÁN CORTES, CARLOS ERNESTO, GUZMÁN, MARTA, RIVAS, VICENTE, *Relaciones Contractuales en Internet y su Desprotección por la falta… Cit.,* Pág. 165. Explica esta parte que debe

explicación sobre la velocidad de al lectura ,en líneas anteriores también se estableció que la computadora no entiende el lenguaje humano sino que este sabe de combinaciones que a través de codificar y descodificar se representa *lenguaje binario,* la velocidad que establece esta forma de lectura computacional de representación es muy alta tanto así que pareciera que la escritura con la representación son simultáneos pero esto es a nuestra vista debido a la gran velocidad que tiene.



entenderse como soporte dando algunos ejemplos y mencionando algunas de sus ventajas.

2.2.9 CARACTERÍSTICAS DE CONTRATOS ELECTRÓNICOS

Por ser el contrato electrónico un nuevo medio para emitir declaraciones de voluntad tienen estas singularidades que lo caracterizan entre las cuales podemos mencionar:

1) Se realiza entre ausentes, es decir no existe presencia física o corpórea, por el hecho que las partes no están frente a frente no pueden apreciarse el uno al otro a través de sus sentidos en ese momento solo son representaciones de voluntades que en base al principio de buena fe se establece que son capaces de ejercer derechos y contraer obligaciones pues así es establecido por ley con el propósito de que los contratos no padezcan de incertidumbre jurídica.

2) El consentimiento es expresado por medio Electrónico dado la naturaleza de la transacción. Como elemento esencial del contrato no debe faltar por ser un requisito indispensable el sentir de los contratantes al mencionar que se hace por medios electrónicos se debe entender que es debido a la creciente tecnología.

El consentimiento expresado por medios electrónicos partiendo del principio de no discriminación se determina que la tecnología es un instrumento que sirve para plasmar el consentimiento de diferentes formas, como es el hecho que el manifestar la voluntad se realiza incluso por medio de un Click o aceptando lo establecido en las indicaciones de una determinada forma de propuesta en el ámbito de la electrónica, dando vida por así decirlo al acto unilateral de aceptación que vinculados entre si forman el sentir de los contratantes como elemento esencial del contrato [22].

[22] Vid. De manera general, NAJARRO KENELMA, BERENICE, *Comercio Electrónico y su Implicación en las trasformaciones*…, Pág. 72 y siguientes.

3) Ofrece alcance mundial a bajo costo no existen fronteras geográficas para este tipo de transacciones. Se logra un alcance mundial gracias a la tecnología que puede lograr una gran velocidad en la información producida para ser enviada no tiene limites en cuanto la burocracia terrestre esta viaja en un espacio diferente este es el virtual.

Las antiguas fronteras económicas levantadas en torno de los países por gobiernos intervencionistas y proteccionistas han cedido y están dando paso de manera creciente y acelerada a nuevos contratos de poder en el sector privado.

Las tecnologías de información, tienen el potencial de acelerar el crecimiento económico de los países por su capacidad para mejorar la calidad de los servicios existentes y crear nuevos servicios y elevar la productividad.

4) Se realiza en tiempo real. Es decir en mismo instante de la contratación no se tiene que esperar a que pasen días para recibir una respuesta si no que se recibe en el preciso momento en el cual se hace una pregunta determinada.

Los contratantes están frente ha acuerdos de intercambio .Es interactivo es decir en el momento preciso que se ejecuta la acción que se esta requiriendo al mencionar en tiempo real en este apartado es importante mencionar que el tiempo es un acontecimiento que pasa inevitablemente a pesar de no establecerse la misma hora si será en el mismo momento que se esta realizando la comunicación.

Es importante tener en cuenta entonces mencionar la hora que se recibe y se manda un mensaje para hacer referencia a la respuesta de

esa interrogante, es casi instantáneo, no debe esperarse días para recibir un resultado[23].

2.2.10 PRINCIPIOS DE LA CONTRATACIÓN ELECTRÓNICA

En este aparto es importante tener en cuenta que dentro de la legislación salvadoreña no contamos con una ley especifica que regule acerca del comercio electrónico. No así en otros países como el caso de Colombia que cuenta con un régimen jurídico de comercio electrónico y por medio de este incorporan a su derecho interno principios generales aplicables al comercio electrónico y a las relaciones contractuales por medios electrónicos que creemos pertinente tomar en cuenta.

También tomaremos como referencia para este apartado la ley de servicio de la sociedad de la información de España que da una serie de criterios que podemos calificar como principios básicos de la contratación electrónica.

Por lo que, se hará un estudio de algunos principios que son rectores en estas legislaciones que regulan tanto el comercio electrónico como las relaciones contractuales por medios electrónicos. Para el desarrollo de esta clase de negocio jurídico tomaremos como base los principios de: Autonomía de la voluntad, buena fe, Libertad de forma, Equivalencia funcional, y Principio de neutralidad tecnológica[24].

---

[23] Vid NAJARRO QUENELMA, BERENICE, *Comercio Electrónico y su implicación en las trasformaciones*…, Pág.18 y siguientes.

[24] REYES VILLAMIZAR, FRANCISCO; *Algunas Consideraciones sobre el Régimen Jurídico del Comercio Electrónico en Colombia,* en foro de justicia, Cámara de Comercio de Medellín para Antioquia, 2001, Pág.158.

2.2.10.1 PRINCIPIO DE AUTONOMÍA DE LA VOLUNTA

Este es una de las piedras angulares del derecho de contratación, por lo tanto este principio se puede definir diciendo que "*es la libertad que tienen las particulares para contratar y determinar el contenido del contrato"*, por lo tanto, lo que se concibe de esta definición es que ninguna persona puede quedar vinculada a una obligación en la que no ha consentido y equivalentemente toda obligación consentida por una persona debe producir efectos. Este principio se encuentra consagrado en la legislación Salvadoreña en el Art. 1416 del Código Civil[25].

La Autonomía de la Voluntad es la razón de ser de la contratación electrónica por que las partes vinculadas consienten en quedar sujetas a obligaciones utilizando soportes tecnológicos para la formación y validez de dicho contrato.

2.2.10.2 PRINCIPIO DE BUENA FE

Este principio resulta importante por el hecho de tratarse de transacciones donde la manifestación de la voluntad se realiza por redes informáticas o telemáticas, donde las partes no están presentes (y por la clara discreción que se tiene sobre la seguridad y lo complejo que pueden resultar las transacciones electrónicas).

La buena fe básicamente se puede decir que es la lealtad, probidad y la confianza que puede tener un individuo que una obligación nacida de una contratación electrónica surtirá efectos en un caso concreto.

Este principio de buena fe debe preceder todas las etapas de un contrato no importa que el medio utilizado sea el digital o tradicional los

[25] Art. 1416 C.C. Salvadoreño, se encuentra el principio de autonomía de la voluntad, textualmente expresa "*Todo contrato legalmente celebrado, es obligatorio para los contratantes, y solo cesan sus efectos entre las partes por el consentimiento mutuo de éstas o por causas legales".*

individuos deberán adoptar este principio independientemente el medio utilizado para la formación y validez de un contrato.

2.2.10.3 PRINCIPIO DE LIBERTAD DE FORMA

Lo que se busca con este principio es que no haya ningún obstáculo jurídico para que quienes quieran obligarse puedan relacionarse jurídicamente y celebrar un contrato, empleando cualquier medio o forma[26].

Lo anterior tiene su sustento doctrinario en jurisprudencia emanada de la sala de lo constitucional de la Corte suprema de justicia de El salvador en una sentencia sobre contenido y alcance de la libre contratación; según esta sentencia uno de los aspectos que ofrece contratación es "*el derecho a determinar el contenido del contrato, es decir la forma y modo en que quedan consignados los derechos y las obligaciones de las partes*"[27]. De acuerdo a lo anterior se puede interpretar que el régimen jurídico salvadoreño no pone ningún obstáculo a este nuevo medio de contratación porque en nuestra constitución esta consagrado el derecho a la libre contratación por lo tanto el régimen jurídico no debe ser obstáculo para celebrar contratos por vía electrónica, ni prive a estos de efectos y validez jurídica.

---

[26] Vid. HINESTROSA, FERNANDO, *El Contrato por medios*…., Cit., Pág. 156. En la medida que el principio de libertad de forma rige los contratos, y se admite la eficacia obligatoria de las declaraciones emitidas por medios de comunicación producto de las nuevas tecnologías, cabe afirmar que la validez y fuerza obligatoria de un contrato no resulta en principio afectada por que las declaraciones de voluntad negóciales hayan sido emitidas por medios de datos comunicados entre terminales de ordenador, bien sea a través de servicios y aplicaciones de Internet, o bien por otras vías.

[27] Constitución de la República de El Salvador con Jurisprudencia, Editorial Fespad. Quinta Edición, Año 2000, art.23 Sentencia 13-VIII-2002, Inc. 15-, considerando VI 3. sobre el contenido y los alcances de la libre contratación, la sala de lo constitucional ha señalado que los aspectos que ofrece el derecho a la libre contratación son. (i) el derecho a decidir si quiere o no contratar, esto es, el derecho a decidir la celebración o no de un contrato; (ii) el derecho a elegir con quien quiere contratar; y (iii) el derecho a la libertad de forma, ahora este libertad puede estar limitada por razones de interés publico y de distintos modos. Así, el estado puede eventualmente alterar *ex post iapso* los efectos de los contratos celebrados con anterioridad al pronunciamiento de una norma.

Lo que debe hacer es adecuar los conceptos tradicionales a esta nueva forma de contratación. Por lo tanto no importa la forma en que ellos se hayan celebrado, pero que en ellos siempre concurran las condiciones esenciales para su validez. Es decir los contratos existen desde que contienen todos los elementos básicos para ser considerados como tal. Siendo la forma nada más una manera de acreditar su existencia frente a terceros.

2.2.10.4 PRINCIPIO DE EQUIVALENCIA FUNCIONAL

Este principio se refiere a la equiparación del documento electrónico con el documento en soporte papel, la Ley modelo sobre comercio electrónico aprobada por las Naciones Unidas para el derecho Mercantil internacional, que ahora en adelante conoceremos como UNCITRAL enuncia en su art. 5. El principio de equivalencia funcional, bajo el encabezado *Reconocimiento jurídico de los mensajes de datos,* en los siguientes términos: "*Que no se negara de efectos jurídicos, validez o alcance probatorio por la razón de que la información este en forma de mensaje de datos*"[28].

De acuerdo al artículo mencionado el mensaje de datos se identifica con la noción de documento electrónico, al tratarse de información que se transmite y se genera por medios electrónicos o informáticos. El principio de equivalencia funcional se refiere a que el contenido de un documento electrónico tenga la misma eficacia y validez que el contenido de un documento en soporte papel, es decir que el documento electrónico por medio de un mensaje de datos desempeñe la

[28] CUBILLOS VELANDIA, RAMIRO, RINCÓN CARDENAS, ERICK. *Introducción Jurídica al Comercio Electrónico,* Gustavo Ibáñez, Colombia, 2002, Pág.176. La conceptualización de la noción de mensaje de datos la encontramos en el Art.1 a) de la Ley Modelo UNCITRAL que indica: "*por mensaje de datos se entenderá la información generada, enviada, recibida, archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el telegrama, el telex o telefax".*

misma función jurídica que desempeña la documentación habitual[29], en lo anterior también podemos ver reflejado el principio de no-discriminación el cual se refiere a que el régimen jurídico aplicable a al proceso de contratación convencional, no ponga barreras a la utilización de mensajes de datos para la declaración de voluntad por el simple hecho que esta sea emitida por medios electrónicos.

La ley modelo sobre comercio electrónico UNCITRAL aborda cinco problemas de equivalencia funcional entre los cuales tenemos: El documento escrito, la firma electrónica, originales y copias, el problema de la prueba, y la conservación de los mensajes de datos.

Con respecto al problema de que el documento debe constar por escrito el articulo 6.1 de la referida ley, establece que "*si la ley requiere que la información conste por escrito, este requisito quedara satisfecho con un mensaje de datos, si la información que este contiene es accesible para su ulterior consulta*", de acuerdo a está idea cuando dicho articulo expresa que el mensaje de datos debe ser accesible sugiere que la información debe ser legible e interpretable y que debe conservarse en programa informatico para ser legible, ahora bien cuando el articulo en mención utiliza la expresión ulterior consulta esta, ahora bien cuando dicho articulo utiliza la expresión ulterior consulta esta sugiriendo que la información sea conservada y pueda reproducirse, o sea, pueda ser consultada con posterioridad [30].

---

[29] Vid. HINESTROSA, FERNANDO. *El Contrato por medios electrónicos***,** Homenaje por sus 40 años de Rectoría 1963-2003, Agustín Madrid Parra..... [y otros], Pag.154.

[30] Vid. CUBILLOS VELANDIA, RAMIRO, RINCÓN CARDENAS, ERICK. *Introducción Jurídica al Comercio Electrónico...,* Cit., Pág. 178. lo importante a la hora de equiparar los efectos jurídicos de un documento en soporte papel a un documento electrónico, es la posibilidad de recuperación del mensaje en el sentido que su contenido sea accesible posteriormente y reconocido por las partes o por terceras personas.

En el caso de la firma electrónica y su equiparación con la firma manuscrita, el medio técnico de firma electrónica debe asegurar la procedencia y el contenido de la manifestación de voluntad negóciales a través de la red. Por consiguiente el documento electrónico y la firma electrónica emitida por un mensaje de datos deben de cumplir la misma función jurídica que cumplen la documentación tradicional y la firma autógrafa. Es importante decir que esto lo ampliaremos en un capitulo aparte, en este apartado se trae a mención por que tienen una relación intrínseca con el principio de equivalencia funcional[31].

El mensaje de datos es la prueba de la existencia de la voluntad de las partes de quedar obligadas, porque este es como un documento que puede ser legible y por tal razón este puede ser presentado ante tribunales como cualquier medio de prueba. Y con respecto a la validez de los [32]documentos electrónicos originales es trascendente, que se

[31] MARTINEZ NADAL, APOL·LÓNIA *Comercio Electrónico, Firma Digital y Autoridades …., Cit.,* Pág.199. la firma electrónica, y, en concreto la firma digital consigue iguales, si no superiores efectos, que los de la firma manuscrita pues puede proporcionar integridad, autenticidad, y, en definitiva, no rechazo en origen. Por ello, el Real decreto-ley 14/1999, siguiendo la directiva comunitaria, y al igual que algunas de las iniciativas legislativas existentes sobre firma digital, realizan un reconocimiento de los efectos de la misma equiparándola, con mas o menos exigencias, a la firma manuscrita. En concreto, el articulo 3.1, párrafo primero, basado en el articulo 5 de la directiva, establece que "*La firma electrónica...tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como pruebe en juicio, valorándose esto según los criterios de apreciación establecidos en normas procésales".* Es, en suma, la regla del equivalente funcional entre firma electrónica y firma manuscrita.

[32] Guía para la incorporación al Derecho Interno de la Ley Modelo de la CNUDMI (Comisión de las Naciones Unidas para el Derecho Mercantil Internacional) sobre Comercio Electrónico. *Artículo 8. — Original* Si por "original" *se entiende el soporte en el que por primera vez se consigna la información*, por tanto, sería imposible hablar de mensajes de datos "originales", pues el destinatario de un mensaje de datos recibiría siempre una copia del mismo. No obstante, el artículo 8 habría de verse en otro contexto. La noción de "original" en el artículo 8 es útil, pues en la práctica muchas controversias se refieren a la cuestión de la originalidad de los documentos y en el comercio electrónico el requisito de la presentación de originales es uno de los obstáculos principales que la Ley Modelo trata de suprimir. Aunque en algunas jurisdicciones pueden superponerse los conceptos de "escrito", "original" y "firma", la Ley Modelo los trata como conceptos separados y distintos. El artículo 8 también es útil para aclarar los conceptos de "escrito" y "original", dada particularmente su importancia a efectos probatorios. El artículo 8 es pertinente para los documentos de titularidad y los títulos negociables, para los que la especificidad de un original es particularmente importante. Sin embargo, conviene tener presente que la finalidad de la Ley Modelo no es sólo su aplicación a los títulos de propiedad y títulos negociables ni a sectores del derecho en los que haya requisitos especiales con respecto a la inscripción o legalización de "escritos", como las cuestiones familiares o la venta de bienes inmuebles. Como ejemplos de

conserve la integridad de la información es decir que el mensaje recibido pertenece al enviado y no ha sido modificado.

Este principio tiene como base determinar las funciones y propósitos exigidos tradicionalmente para el documento en papel y la firma manuscrita y como pueden ser equiparadas estas tanto por el documento electrónico y la firma electrónica

.

2.2.10.5 PRINCIPIO DE NEUTRALIDAD TECNOLÓGICA

Este principio es importante por la razón que tanto las telecomunicaciones y las tecnologías de la información se caracterizan por su gran dinamismo, por lo tanto, se encuentran en permanentes cambios tecnológicos, y de acuerdo a esto las leyes sobre Comercio Electrónico deben definir criterios muy flexibles, para ir adaptándose a los avances tecnológicos, que sean validos también para tecnologías que se utilizan escasamente o que están en fase de desarrollo experimental[33]. Por la razón, que si la ley privilegia a una sola clase de tecnologías y con

---

documentos que tal vez requieran un "original", cabe mencionar documentos comerciales tales como certificados de peso, certificados agrícolas, certificados de calidad o cantidad, informes de inspección, certificados de seguro u otros. Esos documentos no son negociables y no se utilizan para transferir derechos o la titularidad, pero es esencial que sean transmitidos sin alteraciones, en su forma "original", para que las demás partes en el comercio internacional puedan tener confianza en su contenido. Cuando se trata de documentos escritos, los documentos de esa índole generalmente se aceptan únicamente si constituyen el "original", a fin de reducir las posibilidades de que hayan sido alterados, cosa que sería difícil detectar en copias. Existen diversos procedimientos técnicos para certificar el contenido de un mensaje de datos a fin de confirmar su carácter de "original". Sin este equivalente funcional del carácter de original, se interpondrían obstáculos a la compraventa de mercaderías mediante la transmisión electrónica de datos si se exigiese a los iniciadores de los documentos correspondientes que retransmitiesen el mensaje de datos cada vez que se vendiesen las mercancías o se obligara a las partes a utilizar documentos escritos para complementar la operación efectuada por comercio electrónico.

[33] MATEU DE ROS, RAFAEL, CENDOYA MENDEZ DE VIGO, JUAN MANUEL, *Derecho de Internet. Contratación Electrónica y Firma digital,* Tercera Edición, Editorial Aranzadi, Madrid, 2001, Pág. 90. La ley del servicio de la sociedad de la información en lo que se refiere sobre los contratos electrónicos no preconiza ni determina la validez o la preferencia de una solución tecnológica concreta ni en lo que se refiere a la emisión o prestación del consentimiento, ni a la identidad y autenticidad de las partes contratantes, ni a la seguridad de las comunicaciones a través de las cuales se perfecciona y ejecuta el contrato, criterios de identidad y no repudio de origen ni destino, ni tampoco por ultimo, en lo relativo a la prueba de los contratos electrónicos.

el constante dinamismo con el que estas evolucionan; estas leyes en poco tiempo resultaran obsoletas[34].

Este principio lo retoma la Ley modelo sobre la firma electrónica que aprobó la comisión de las naciones Unidas para el Derecho Mercantil Internacional (CNUDMI), encontramos este principio en su art.3, bajo el titulo *igualdad de tratamiento de las tecnologías para la firma*, a lo que se refiere es que ningún método de firma electrónica puede ser objeto de discriminación debe darse a todas las tecnologías la misma oportunidad.

2.3. FASES DE LA CONTRATACIÓN ELECTRONICA

En términos generales dentro de la formación de los contratos tradicionalmente se han distinguido tres fases:

2.3.1 LA GENERACION.

La cual comprende el desarrollo de las negociaciones, la preparación o gestión del contrato, o también se puede entender como el proceso interno de formación del contrato del que surge el consentimiento contractual[35].

Esta fase se puede concebir como aquella donde el oferente envía la oferta por cualquier medio de comunicación al consumidor, en nuestro caso concreto seria por la red abierta de Internet, en esta oferta

---

[34] Vid. MATEU DE ROS, RAFAEL, CENDOYA MENDEZ DE VIGO, JUAN MANUEL, *Derecho de Internet. Contratación Electrónica y Firma digital,* 3 Edición, Editorial Aranzadi, Madrid, 2001, Pág. 91. La evolución de las técnicas de la comunicación a distancia, de las comunicaciones comerciales electrónicas, de los mecanismos de accesibilidad de la red, almacenamiento y reproducción de contratos celebrados por vía electrónica, así como las firmas digitales, claves criptográficas de autenticación y sistemas de seguridad informática en general, dejaría obsoletas en poco tiempo las normas jurídicas que pretendieran elevar determinada solución tecnológica a la categoría formal de obligatoria o exclusiva. Las leyes sobre Comercio Electrónico deben, por tanto, definir criterios muy generales.

[35] ALTERINI, ATILIO ANÍBAL, DE LOS MOZOS, JOSÉ LUIS, *Contratación contemporánea*, Editorial Temis, Bogotá-Colombia, 2000, Pág. 150. Este autor distingue tres fases en la vida de un contrato: a) Generación (negociación, tratos Preliminares); b) Perfección (Formación y nacimiento); c) Consumación (Cumplimiento, extinción).

electrónica debe de estar detallada toda la información necesaria sobre el producto ofrecido y que cumpla con todos los requisitos necesarios para dar vida al contrato que se formara[36].

2.3.2. LA FASE DE PERFECCION DEL CONTRATO

Esta segunda fase que comprende la manifestación de las voluntades de las partes que formaran el contrato, o sea, cuando dos declaraciones unilaterales de voluntades se coinciden para consentir y dan nacimiento a un contrato a la vida jurídica, esas declaraciones de voluntad unilaterales la conforman la oferta y la aceptación.

Es necesario tener en cuenta la clasificación legal y tradicional de los contratos, en el artículo 1314 del Código Civil Salvadoreño que nos presenta una definición legal de los contratos que los clasifica en contratos reales, consensúales y solemnes[37].

En lo que respecta a esto, los contratos realizados por Internet son contratos consensúales, es decir, se perfeccionan por el mero consentimiento de los sujetos que intervienen en la relación contractual[38], también es importante señalar que nos encontramos frente a contratos en los cuales las partes no se encuentran presentes y que estos se

---

[36] Vid. MATEU DE ROS, RAFAEL, CENDOYA MENDEZ DE VIGO, JUAN MANUEL, *Derecho de Internet. Contratación Electrónica y Firma digital ..., cit.*, Pág.287. Se entiende, como un conjunto de hechos y actos jurídicos, simultáneos o sucesivos, ordenados a la manifestación del consentimiento con la que el contrato se perfecciona.

[37] Vid. Art.1314 C.C. Salvadoreño Textualmente expresa " *el contrato es real cuando, para que sea perfecto, es necesaria la tradición de la cosa a que se refiere; Es solemne cuando esta sujeto a la observancia de ciertas solemnidades especiales, de manera que sin ellas no produce ningún efecto civil; y es consensual, cuando se perfecciona con el solo consentimiento".*

[38] GRANILLO DE TOBAR, ANA YESSENIA, *La Firma Electrónica, su uso en el ámbito de la Contratación Electrónica y su Aplicación por las Administraciones Publicas, Trabajo de Tesina, San Salvador, 2004*, Pág. 136. En la generalidad de contratos realizados a través de Internet se refieren a venta de bienes o prestación de servicios, estos se perfeccionan con el solo consentimiento sin necesidad de mas requisitos, empero, no obsta para que cualquier otro tipo de contrato se lleve a cabo a través de Internet.

perfeccionan por el concurso de la oferta y aceptación sobre la cosa y la causa que han de constituir el contrato[39].

Para hacer un poco más fácil la comprensión de lo anteriormente expuesto se hará referencia a la oferta ya la aceptación[40] pero no a las tradicionalmente conocidas sino a las realizadas por medios electrónicos, es decir, a la [41]oferta electrónica y a la aceptación electrónica.

2.3.3. OFERTA ELECTRÓNICA

Debemos recordar que la oferta es: "*la manifestación unilateral de voluntad en la cual se propone la celebración de un contrato a una o más personas determinadas"*. En lo que respecta a la oferta nos interesa aquella que se realiza por medios electrónicos, la llamada oferta electrónica y se puede entender a esta como: "*la declaración unilateral de voluntad que una persona realiza por medios electrónicos, en la cual propone a otra persona o personas determinadas la celebración de un contrato que se perfeccionara con la aceptación de esta".*

---

[39] OSPINA FERNADEZ, GUILLERMO, OSPINA ACOSTA, EDUARDO, *Teoría General del Contrato y del Negocio Jurídico,* 6ª Edición, Editorial Temis, Bogotá, 2000, Pág. 146. *La propuesta y su aceptación.* Es necesario que uno de los interesados le proponga a otro u otros la celebración de la convención y que este o estos, a su turno manifiesten que están de acuerdo con tal propuesta y que adhieran a ella. Así, el encuentro y la unificación de la propuesta y su aceptación es lo que genera el consentimiento.

[40] Vid. CUBILLOS VELANDIA, RAMIRO, RINCÓN CARDENAS, ERICK. *Introducción Jurídica al Comercio Electrónico...,* Cit., Pág. 155. Es necesario analizar con profundidad estos dos conceptos, ya que sobre estos descansa la formación y perfeccionamiento del consentimiento en materia de contratación electrónica y por lo tanto la contratación a través de la red Internet.

[41] http.//www.teleley.com/articulos/art_patroni.pdf. Visitada el 13 de octubre de 2008. Las ofertas electrónicas son aquellas realizadas: vía E-mail o correo electrónico: se envían a ordenadores determinados. Vía on-line, en redes de comunicación como Internet: se encuentran en modo permanente en las redes y a las que se tienen acceso navegando por diferentes páginas, pero estás no llegan a los ordenadores de cada persona individualmente (dirigido), sino que se accede a ellas en presencia de una oferta indeterminada, pues se desconoce la persona a la cual se dirige. Por otro lado, en toda relación contractual de tipo electrónico, está como elemento indispensable, la aceptación electrónica, entiéndase por está la declaración unilateral y el desarrollo de voluntad que una persona realiza a través de medios de comunicación y/o informáticos, manifestando su conformidad a una propuesta recibida por ella, y está tiene que darse mientras la oferta este vigente, mientras no se produzca la retracción o caducidad de la misma.

2.3.4. REQUISITOS DE LA OFERTA

Es importante saber que la diferencia de la oferta habitual con relación a la oferta electrónica es el medio empleado por el cual se hacen la una y la otra. Por tanto la oferta electrónica debe de cumplir con los siguientes requisitos

a) La Intención del Oferente de Obligarse Contractualmente

En atención al primer requisito este se refiere a la voluntad de quien propone la oferta a quedar vinculado contractualmente al momento que esta sea aceptada, este requisito es adoptado por la convención de las Naciones Unidas sobre el Contrato de Compraventa Internacional de Mercaderías[42].

No obstante, se puede decir, que no toda declaración de voluntad constituye una oferta como por ejemplo la simple publicidad de un producto un servicio web se califica como una simple invitación a negociar, que es la típica publicidad y como tal no es vinculante y no esta dirigida a persona determinada, si no que es hecha al publico en general la cual se conoce como policitación. Esta "*invitación a ofrecer*" es especialmente importante en la Contratación Electrónica, puesto que en la red se presenta como un atractivo lugar para fijar publicidad, bien a través de catálogos en tiendas virtuales (como por ej. www.elcorteingles.es) o a través de links que llevan a otras páginas que ofrecen bienes de consumo.

Lo anterior lo encontramos regulado en la convención de las Naciones Unidas sobre el Contratos de Compraventa Internacional de Mercaderías en su art.14.2, donde expresa: "*Toda propuesta no dirigida a*

[42] Convención de las Naciones Unidas sobre los Contratos de Compraventa Internacional de mercaderías adopta e3ste requisito: Parte II Formación del contrato, Art. 14.1 " *la propuesta de celebrar un contrato dirigida a una o varias personas determinadas constituirá oferta es suficientemente precisa e indica la intención del oferente de quedar obligado en caso de aceptación. Una propuesta es suficientemente precisa si indica las mercaderías y, expresa o tácitamente, señala la cantidad y el precio o prevé un medio para determinarlo".*

una o varias personas determinadas será considerada como una simple invitación a hacer oferta, a menos que la persona que haga la propuesta indique claramente lo contrario".

La policitación[43] se pueda clasificar en policitación simple y policitación compromisoria, de acuerdo a la primera esta se refiere a la invitación al publico en general de formular oferta respecto del negocio que se trate. La policitación compromisoria, esta se refiere a que el policitante se obligue de antemano a aceptar la oferta que reúna las condiciones señaladas.

Sé esta ante una autentica oferta contractual cuando en dichas comunicaciones estén presentes todos los elementos del contrato, determinando con claridad el objeto del mismo y este dirigida a una o varias personas determinadas, de modo que solo se precise la aceptación de la contraparte

b) La Oferta debe ser Completa

El segundo requisito, se refiere a que la oferta debe contar con toda la información necesaria, el carácter completo de la oferta significa que la

[43] Vid. OSPINA FERNADEZ, GUILLERMO, OSPINA ACOSTA, EDUARDO, *Teoría General del Contrato y del Negocio Jurídico...,* Cit. Pág.156. se considera que la policitación, salvo caso de que implique claro compromiso de parte del proponente, es una simple invitación general para que cualquier interesado formule una oferta ya concreta, estos autores estiman que esta opinión es la que consulta mejor la practica comercial, por ejemplo, quien distribuye catálogos de precios, o exhibe mercancías en una vitrina, o inserta en la prensa aviso de su intención de vender un objeto determinado, apenas si pretende comunicar su propósito de entrar en *negociaciones concretas* con la persona o personas interesadas en el anuncio o aviso, y solo al iniciarse estas negociaciones se presentaría la oportunidad de entrar a decidir si cada una de las partes abriga ya el animo de obligarse (*animus obligandi),* que es el determinante de la eficacia de los actos jurídicos. Otra cosa completamente distinta sucede cuando la policitación u oferta al publico o a persona indeterminada, implica claramente que quien la hace si tiene ya ese animo de obligarse o comprometerse a favor de la persona o personas que se coloquen concretamente en la situación de hecho prevista en ella, como cuando se promete una recompensa a quien entregue un objeto perdido o un premio a quien gane un concurso artística. La reglamentación legal de la policitación debe de prescindir de todo casuismo y consagrar simplemente el principio que esta no es obligatoria, al menos que le policitante al hacerla claramente manifieste su voluntad de comprometerse a favor de quien la acepte.

misma debe de contener todos los elementos del contrato, o sea, aquellos elementos sin que este no puede existir o degenera en otro distinto[44].

Así la contraparte, solo tenga que aceptar dicha oferta sin que esta pueda generar la más mínima incertidumbre desconfianza al destinatario, como por ejemplo en el caso de las ventas en Internet específicamente en una página web estas deberían cumplir ciertos requisitos como condición de validez. Entre estos se pueden mencionar: La identidad del proveedor; las características del producto; el precio; gastos de transporte; forma de pago; y plazo de ejecución del pedido entre otros. Esto reviste una importancia mayor con relación al destinatario de la oferta porque este se limitaría hacer "clic" sobre el icono de acepto destinado en la pagina web, para realizar su declaración de voluntad al respecto de la propuesta hecha[45].

c-) La Determinación del Destinatario.

El ultimo requisito sin que este sea menos importante que los dos anteriores, y este es la determinación de la persona del destinatario, se refiere a que una oferta debe ir dirigida a una persona determinada, por tanto si esta dirigida a persona determinada e individualizada estamos

---

[44] UREBA, ALBERTO ALONSO, VIERA GONZALEZ, ARÍSTIDES JORGE, "*Formación y perfección de los contratos a distancia celebrados por Internet",* en AA VV Derecho de Internet, La ley de Servicios de la Sociedad de la Información y de Comercio Electrónico, Coordinado por MATEUS DE ROS, RAFAEL, 3 Edición, Editorial Aranzadi, Madrid, 2001, Pág. 295. Este requisito del carácter completo de la oferta se empieza a sustituir por el mas flexibles de la "*suficiente precisión de la oferta",* tomado del articulo14.1 de la CNUCCIM (Convención de las Naciones Unidas Sobre Contratos de Compraventa Mercantil Internacional) que, además, fija como criterio de interpretación para determinar la existencia de una oferta suficientemente precisa el hecho que indique "*las mercancías y expresa o, tácitamente señala la cantidad y el precio o prevea un medio para determinarlos".* Para la doctrina que comenta este precepto se abre ahora tres posibilidades distintas de constituir de forma licita una oferta contractual. La primera seria mediante una determinación expresa de las mercaderias, de su cantidad y su precio; la segunda posibilidad a la que se alude seria aquella en que la mercancía se encuentra determinada expresamente, pero la cantidad y el precio lo esta tácitamente y la tercera posibilidad que se deriva de aquel precepto de la CNUCCIM es la que la oferta aparezca indeterminada tanto en cantidad de mercaderias, como el precio de las mismas pero estableciendo, en cambio criterios para su determinación.

[45] Vid. CUBILLOS VELANDIA, RAMIRO, RINCÓN CÁRDENAS, ERICK. *Introducción Jurídica al Comercio Electrónico*..., Cit., Pág. 155.

frente a una verdadera oferta, por el contrario como lo dijimos anteriormente si nos encontramos frente a una propuesta hecha a personas indeterminadas, estamos frente a una simple invitación a negociar.

Por lo tanto, es necesario decir que la realidad contractual en Internet no se puede dar una sola respuesta en un espacio como Internet se deben de considerar los diferentes canales por los cuales las partes pueden exteriorizar su voluntad, también es importante estipular la vía ha utilizar para realizar la oferta, y en cuanto a estas pueden ser hechas tanto a personas determinadas o indeterminadas y el caso concreto nos referimos a la oferta electrónica realizada por medio de Internet, y estas pueden ser realizadas por: el correo electrónico, la pagina web y el correo interactivo[46].

De acuerdo a lo anterior se desarrollara de manera muy breve la oferta electrónica realizada por los diferentes medios antes mencionados.

2.3.5. OFERTA A TRAVÉS DE CORREO ELECTRÓNICO

El correo electrónico como medio de comunicación, es un medio perfectamente apropiado, para enviar ofertas y recibir aceptaciones, por lo tanto, para realizar contratos en Internet, sin embargo es un medio de comunicación en el cual entre la emisión y recepción del mensaje existe diferencia temporal, por lo que no estamos frente a una comunicación en tiempo real entre las partes, de tal manera que su función es de igual

[46]Vid. CUBILLOS VELANDIA, RAMIRO, RINCÓN CÁRDENAS, ERICK. *Introducción Jurídica al Comercio electrónico*..., Cit., Pág. 164. El principal problema que se enfrenta con las ofertas, incluidas en las pagina web o transmitidas por correo electrónico, se centra en un lado en la dificultad de localizar el lugar de producción de la oferta y del otro, en el hecho de la determinación de la naturaleza jurídica del mensaje, contenidos en estos instrumentos, si realmente deben considerarse como verdaderas ofertas que obliguen al oferente o si por el contrario deben ser consideradas como simples mensajes publicitarios constitutivos de una simple invitación a ofertar.

naturaleza al correo tradicional[47] y su aplicación no discrepa mucho en cuanto a la oferta, aceptación y consentimiento.

Se está frente a un supuesto de contratación entre ausentes, por la razón, que las partes en la contratación electrónica, no hay una verdadera interacción entre ambas partes, si no que los mensajes se depositan en el servidor y se abren cuando se vacía su cuenta de correo, o sea, todavía se tiene que contar con que se abran y lean, lo mismo que con la correspondencia convencional. Por lo que se aplicaran las reglas de la contratación entre ausentes, con referencia a esto en la legislación salvadoreña se aplica el sistema de recepción para el perfeccionamiento de los contratos entre ausente, al cual nos referiremos mas adelante.

En este aspecto la oferta electrónica que se realiza por medio de correo electrónico esta dirigida a persona determinada y conocida, pero distante en cuanto a espacio físico se refiere

2.3.6. OFERTA REALIZADA A TRAVÉS DE PÁGINA WEB

Otro medio de comunicación por el cual también se realizan ofertas son las paginas web, se encontró una clasificación de paginas web donde se habla de paginas web pasivas y activas[48], en la primera se realizan propuestas o anuncios publicitarios, en las cuales se realizan ofertas al publico en general, por tanto están dirigidas a personas

[47] Vid. GRANILLO DE TOBAR, ANA YESSENIA, *La Firma Electrónica, su uso en el ámbito de la Contratación Electrónica...,* Cit., Pág. 139. El análisis de las oferta por medio de correo convencional, puede estudiarse a través de la tesis que buscan regular el perfeccionamiento del consentimiento, sistema este que ha sido adoptado dentro de la legislación interna de cada país en particular y para el caso concreto se suele considerarse como en consentimiento entre personas ausentes.

[48] Vid. GRANILLO DE TOBAR, ANA YESSENIA, *La Firma Electrónica, su uso en el ámbito de la Contratación Electrónica...,* Cit., Pág. 140. se debe de considerar que hacer una publicación en una página web en Internet no constituye una oferta, sobre todo si tomamos en cuenta que muchos de los contenidos de las páginas web son de interés cultural, informativo, recreativo entre otros. Y otras finalidades que nunca podrían llegar a ser constitutivas de una oferta. Sin embargo las páginas web pueden ser clasificadas como activas y pasivas.

indeterminadas, de tal manera que son una simple invitación a negociar, de acuerdo al negocio que se trate.

En cambio se considera que en la página activa hay una verdadera propuesta contractual de la cual se deriva una verdadera oferta que puede ser vinculante, por la razón, que se puede dar el caso que tanto una persona física o jurídica posean un listado de direcciones de personas con quienes han tenido trato previo real o virtual, y que están en espera de que el destinatario entre en contacto con ellos para realizar un nuevo acuerdo contractual, de tal manera que, la oferta así realizada se considera una verdadera oferta dirigida a una persona determinada[49].

2.3.7. OFERTA REALIZADA A TRAVÉS DE CORREO INTERACTIVO

Otro sistema comunicación que ofrece Internet es el denominado "*Cha*t". El cual hace referencia a una forma de comunicación interactiva o en tiempo real en formato de texto. Diferente tratamiento se le debe dar a la oferta realizada por medio de correo interactivo "*Chat",* en el cual la comunicación es en tiempo real entre oferente y destinatario pero no hay presencia física entre ellos.

Este tipo de comunicación permite a dos o más personas al mismo tiempo, ubicadas en diferentes lugares, entrar en conversaciones para negociar y celebrar un contrato, de acuerdo a este sistema de comunicación la voluntad de uno o del otro es conocida inmediatamente, es decir no hay un lapso de tiempo que medie entre el conocimiento del

[49] Vid. GRANILLO DE TOBAR, ANA YESSENIA, *La Firma Electrónica, su uso en el ámbito de la Contratación Electrónica...,* Cit., Pág. 141. La oferta a través de la pagina web pasiva, se considera como una invitación a ofertar, ya que su método nos permite demostrar que la misiva esta dirigida a una persona indeterminada, conclusión a la que se llega al determinar que no se trata de una oferta formal, por ende, esta forma de oferta ha sido conocida en la doctrina con el nombre de Policitación simple, que es la invitación a personas determinadas a formular ofertas respecto del negocio de que se trata; y la pagina web activa en cambio, es considerada como una verdadera oferta dirigida a persona determinada.

oferente de la aceptación del destinatario[50]. Esta nueva forma de comunicación se considera un contrato entre presentes, la oferta que se realiza por este medio se considera una oferta proyectada a persona determinada, por lo tanto, la oferta puede ser vinculante.

2.3.8. LA REVOCACIÓN DE LA OFERTA ELECTRÓNICA

La revocación de la oferta[51] se refiere a la voluntad que tiene el oferente en dejar sin eficacia y validez la oferta propuesta, esto puede hacerse durante el tiempo en que la oferta este vigente o mientras no haya respuesta del destinatario que puede ser de aceptación o rechazo

[50] Vid. HINESTROSA, FERNANDO, *El Contrato por medios electrónicos*…**,** Cit., Pág. 282. La dificultad de encuadrar las herramientas tecnológicas en los conceptos casuistas de la normatividad, la correspondencia se relaciona exclusivamente con el documento escrito en soporte físico, que requería transporte por los medios tradicionales y se vinculaba directamente con la distancia entre las partes, el teléfono era el único medio existente para lograr comunicación en tiempo real, pero el *"chat"* cumple la doble función y permite comunicaciones con estas características entre ausentes, pero mediante el uso de medios escritos, con lo que cumple exactamente la misma finalidad que la comunicación telefónica con el uso de una herramienta distinta. Se acoge por tanto el criterio de comunicación ininterrumpida, conforme al cual, existirá un contrato entre presentes, según esta regla, en aquellos supuestos en que las partes, para realizar el intercambio oferta-aceptación, emplean un instrumento de transmisión que les permite una comunicación sin espacios temporales, características plenamente cubiertas por un medio como el descrito.

[51] Htt://www.protegedatos.com/web/lssice/contratos.html#arriba visitada el 20 de octubre de 2008. Para que el contrato se considere perfecto es menester que la aceptación se manifieste a quien ha formulado la oferta y que no altere los términos en que ha sido formulada. Asimismo, es necesario que la aceptación tenga lugar antes de que la oferta se extinga o sea revocada. En el primer caso, la oferta estaría sometida a un término, vencido éste la oferta se extinguiría, en el segundo caso, es una facultad del oferente revocar la oferta hasta tanto el contrato no se considere perfecto. En relación con la revocabilidad de la Oferta, cabe distinguir dos supuestos: Que el oferente puede revocar la oferta antes de la aceptación, y aun después de ella antes de su recepción, y Que el oferente esté obligado, independientemente de que el destinatario haya aceptado, a no revocar la oferta durante un cierto plazo**.** El primer supuesto determina la perfección del contrato, puesto que las teorías que explican la perfección del Contrato se basan en los sistemas de la expedición o de la recepción de la aceptación. El segundo supuesto, se refiere a la revocabilidad de la oferta, como un elemento intrínseco a ella, independiente de la existencia o no de aceptación. Para este último supuesto, dos son los sistemas: a. Los que establecen que el oferente no podrá revocar la oferta hasta que el destinatario la haya rechazado o haya dejado transcurrir sin aceptarla el tiempo suficiente para considerar razonable la revocación, como el Código Civil Alemán (δ δ 145-149); y b. Los que consideran que la oferta es revocable mientras el contrato no se haya perfeccionado (Sistema del Derecho Francés y de todos los Códigos de tradición Latina). En el Código Civil Italiano, este sistema tiene un matiz, puesto que si el aceptante ha emprendido de buena fe la ejecución del contrato antes de haber tenido conocimiento de la revocación, el proponente ha de indemnizarle los gastos y las pérdidas sufridas por la iniciada ejecución (art. 1328). En el Derecho Francés este principio también se mitiga, pues se considera que el plazo debe darse por admitido cuando resulte impuesto por los usos, como sucede en materia comercial. En cualquiera de los dos sistemas, en todo caso en que el oferente se obligue a mantener la oferta por un tiempo determinado, la revocación carece de efecto durante ese plazo.

de la oferta. La revocación de la oferta se refiere a la declaración de voluntad del oferente de hacerle saber al destinatario que no quiere continuar con la propuesta realizada y por lo tanto, no desea contraer obligaciones[52]. Es importante tener en cuenta, que la oferta puede ser revocada mientras no haya aceptación por que se considera que si no ha habido aceptación, no se ha perfeccionado el contrato, por tanto este todavía no existe y por ende no se ha contraído obligación alguna, por tal razón puede retractarse el oferente de la propuesta realizada.

En el ámbito de los Contratos Electrónicos cuando se está en presencia de una oferta por ejemplo de un catalogo de ventas en una página web, y se pulsa para aceptar la oferta, en ese momento el contrato se ha perfeccionado, por tanto la posibilidad de revocar la oferta se convierte en nula. Por el contrario si se trata del envío de una oferta, la revocación de la misma habrá de enviarse antes de que llegue a

[52] Vid. OSPINA FERNADEZ, GUILLERMO, OSPINA ACOSTA, EDUARDO, *Teoría General del Contrato y del Negocio Jurídico...,* Cit. Pág. 149. al respecto de la teoría de la no obligatoriedad de la oferta, esta es parte de la doctrina clásica francesa, fundada en un principio racionalista que enuncia diciendo " *nadie adquiere ni pierde un derecho sin su voluntad",* esta teoría niega eficacia jurídica a todos los actos unilaterales y e especialmente los excluye del catalogo de las fuentes de las obligaciones, por tal razón, la esencia de esta teoría clásica francesa consiste en negar categóricamente la obligatoriedad de la oferta, por tanto le reconoce la facultad de arrepentir se al oferente, pero introducen a esto una posición muy peculiar y contradictoria a la esencia de dicha teoría. Por otra parte se encuentra *la teoría de la obligatoriedad de la oferta*, esta sustentada por la doctrina alemana, y es la que ha logrado imponerse en la mayoría de legislaciones de derecho privado el principio racionalista que enuncia la teoría de la no obligatoriedad de la oferta a quedado superado por el pensamiento contemporáneo el cual se que la voluntad privada queda reducida a su voluntad subordinación a las normas e instituciones jurídicas, en lo referente a la oferta existen razones muy poderosas para justificar su inclusión en la lista de los actos unipersonales obligatorios, la imperatividad coercitiva del orden jurídico, mediante el cual se impone el respeto del integres general, como también el de los legítimos intereses ajenos, s por tanto se debe exigir que quien interviene en una convención llamase oferente o aceptante obre a sabiendas que dicho negocio no tiene por objeto exclusivo procurarle a el su personal satisfacción. Si no que afecta también, de manera muy importante a las demás personas que intervienen en su celebración. En conclusión la teoría de la obligatoriedad de la oferta por cualquier lado que se mire, se impone racional y jurídicamente de esta teoría se derivan las siguientes consecuencias: 1)si la oferta es obligatoria, el proponente no puede retractarse de ella, antes del vencimiento del termino de su duración señalado por el o por la ley; 2) La oferta no caduca por la muerte o incapacidad del oferente sobrevenida estas durante el termino, en caso de muerte la obligación se transmite a sus herederos; y, 3) Si la oferta es aceptada oportunamente dentro del termino de su duración, el contrato propuesto queda formado y produce la plenitud de sus efectos propios. Esta teoría de la obligatoriedad de la oferta es que recoge el Código de Comercio en el Art.969 Inciso primero Código de Comercio Salvadoreño "Si un comerciante se ha obligado a mantener en firme una oferta por tiempo determinado, no podrá revocarla".

conocimiento del destinatario y sea aceptada, lo que puede resultar imposible dada la velocidad con que los mensajes viajan a través de la red

En la legislación salvadoreña la revocación de la oferta se encuentra sujeta al plazo, esto lo encontramos regulado en el Art.969 del Código de Comercio, expresa "*que si un comerciante se ha obligado a mantener firme una oferta por tiempo determinado, no podrá revocarla"*, por ende, este articulo tiende a confundir dos situaciones diferentes la revocación de la oferta y el vencimiento de la oferta, por el hecho que si no hubiera plazo el oferente podría revocar la oferta cuando el quisiera, pero si hay un plazo el oferente debe de esperar el vencimiento del plazo para poder revocar la oferta, pero anteriormente mencionamos que puede haber revocación mientras la oferta este vigente, por tanto si esta ya venció la revocación ya no tiene razón de ser, por que el oferente no puede quedar Obligado por una propuesta la cual venció su plazo de vigencia y la cual ya no tiene validez.

El oferente puede revocar la oferta[53] cuando él así lo quisiera, mientras no concurra una condición dentro de la misma oferta que se lo impida. Cosa que no puede suponerse con el mero establecimiento del plazo. Al respecto la revocación se puede realizar por cualquier medio de comunicación como la Internet, en consecuencia la oferta quedara sin eficacia cuando la revocación llegue a conocimiento del destinatario.

---

[53] Vid. GRANILLO DE TOBAR, ANA YESSENIA, *La Firma Electrónica, su uso en el ámbito de la Contratación Electrónica...,* Cit., Pág. 144. Lo difícil de determinar no es derecho a revocar, sino el momento en el cual quedara sin efecto la oferta, lo cual depende de los medios por los cuales se dará a conocer la revocación, medios que pueden ser muy variados y pueden tratarse desde los convencionales como el correo, el teléfono, el fax, etc, hasta otros mas modernos como el correo electrónico o *e-mail,* el chat la videoconferencia, etc.

2.3.9. *LA CADUCIDAD DE LA OFERTA ELECTRÓNICA*

La caducidad de la oferta se da en los casos en que esta no es considerara irrevocables, según el Art.969 del Código de Comercio salvadoreño expresa que la *"muerte o incapacidad superveniente no privan la eficacia a la oferta hecha por este, es decir, que estas causas que provocan la caducidad no afectan a la oferta hecha por los comerciantes mientras no venza el plazo establecido",* es decir, que estas causas que provocan la caducidad no afectan a la oferta hecha por el comerciante, mientras no venza el plazo establecido, y aun cuando no se haya fijado plazo este se entenderá de acuerdo a los usos de los negocios o por la naturaleza del asunto.

Al respecto del articulo anterior, sobre las causas de caducidad se entiende que la oferta caduca con la muerte o incapacidad sobreviviente del oferente en este caso se refiere a las personas naturales, en el caso de muerte del oferente se extingue las obligaciones, en la circunstancia que estas solo pueden ser cumplidas exclusivamente por el oferente o deudor en su caso, es decir, es de las llamadas obligaciones ***intuito personae***[54]*,* o viceversa, puede ser que las obligaciones sean de aquellas que se transmiten a sus herederos, en tal caso los sucesores del deudor pueden cumplir con la obligación contraída por este. Y al respecto por incapacidad sobrevenida del oferente o deudor dicha obligación, o dicho de otra forma, la oferta no caduca si no que esta debe mantenerse firme y ser cumplida por quien lo represente legalmente[55].

---

[54] Vid. CUBILLOS VELANDIA, RAMIRO, RINCÓN CÁRDENAS, ERICK. *Introducción Jurídica al Comercio Electrónico....,* Cit. Pág. 169. obligaciones *Intuito personae* son aquellas que se celebran en consideración a las cualidades o aptitudes propias de una persona, por ende, el único que puede cumplir con las mismas, es el deudor y nadie mas puede hacerlo en su nombre.

[55] Vid. GRANILLO DE TOBAR, ANA YESSENIA, *La Firma Electrónica, su uso en el ámbito de la Contratación Electrónica...,* Cit., Pág. 145. Y a que el Internet es solo un medio de comunicación entre el oferente y el destinatario, por tanto, podría tratarse de una obligación general en la que la condición de la persona no es determinante para el contrato, en tal caso sus sucesores pueden mantener la oferta y llevar a cabo contrato en caso de aceptación por el destinatario, pero sise tratara de una obligación *intuito personae,* la oferta no podrá ser mantenida por sus sucesores y

Al respecto, esto en principio no se aplica a las personas jurídicas, pero tomando en cuanta que la mayoría de ofertas electrónicas en Internet son hechas por personas jurídicas que participan en la contratación electrónica, con respecto a lo anterior, la única manera que una oferta realizada por una persona jurídica pueda caducar, es cuando esta es disuelta, es por que la disolución de la persona jurídica es el fin de esta, o sea, equivale a la muerte de la persona natural.

2.3.10. ACEPTACIÓN ELECTRÓNICA

El autor Diez-Picazo en su libro "*Fundamentos del Derecho Civil Patrimonial"*, define a la aceptación como: "*aquella declaración o acto del destinatario de una oferta que manifiesta el asentimiento o conformidad con esta",* es decir, es la declaración unilateral de voluntad por una persona o personas de adherirse a la propuesta efectuada. De acuerdo a lo anterior podemos decir que la aceptación electrónica "*es la declaración unilateral de voluntad que emite el aceptante por cualquier medio electrónico declarando su conformidad a una propuesta realizada".*

Lo importante de la aceptación es el asentimiento del aceptante con la oferta realizada que lleva adherida la voluntad de este de quedar vinculado contractualmente.

La aceptación[56] al igual que la oferta debe de cumplir con ciertos requisitos que son necesarios para la formación del consentimiento, los cuales son:

---

la obligación tampoco se vera cumplida, es en este caso ultimo en el que la caducidad de la oferta se habría producido, esta es la tesis adoptada por nuestra legislación.

[56] http://www.monografias.com. Visitada el día 13 de septiembre. En la cual aparece un texto denominado contratos electrónicos se refiere a que la aceptación necesariamente debe realizarse mediante algún medio electrónico, solo así estaremos en presencia de un contrato electrónico, por lo que resulta indispensable que la aceptación reúna ciertos requisitos para su validez: debe ser congruente con la oferta; ser oportuna, es decir a tiempo, debiendo ser recibida por el oferente durante el tiempo de vigencia de la oferta; dirigida al oferente (recepticia), o sea a quien ha formulado la propuesta y en el caso de ser electrónica siguiendo todo procedimiento establecidos

1. La aceptación debe realizarse mientras la oferta se encuentre vigente;

2. La aceptación debe ser oportuna;

3. La aceptación debe ser pura y simple.

De acuerdo, al primer requisito es importante tener en cuenta que el vencimiento esta implícito en toda oferta por que no existen ofertas eternas, aunque pudiera ser que nos encontremos frente a una de estas, que no diga nada sobre el plazo de la misma, en este caso se entiende que esta pierde vigencia con el transcurso del tiempo, que se deduce, como suficiente de acuerdo con los usos de los negocios y con la naturaleza del asunto.

También es importante tener en cuenta que el plazo de vigencia de la oferta en la legislación salvadoreña es predominantemente convencional; el Código de Comercio Establece que el plazo debe ser determinado por las partes o por un juez y si no se estipula el plazo se considera que la oferta estará vigente por tiempo indefinido, pero además la oferta puede estar vigente mientras no se produzcan dos hechos jurídicos los cuales son:

1. La Retractación;

2. La Caducidad.

Hicimos referencia anteriormente, a la retractación que esta es cuando el oferente puede dejar sin efecto la oferta mientras esta no haya sido aceptada. Recordemos que hablamos de aceptación electrónica, por lo tanto, vamos a referirnos a la forma en que se da la retracción por medió de correo electrónico y por página web.

---

sobre el uso de firmas y certificados digitales. Al igual que la oferta la aceptación debe contener la intención de contratar, de dar lugar con ella a la formación del contrato.

La forma en que se puede dar la retracción[57] por pagina web, para esto, tenemos que tomar en cuenta primeramente que la pagina web esta en constante actualización por lo tanto la oferta no tiene un plazo muy extenso de existencia y porque cuando las personas acceden a la respectiva pagina, compra en el mismo instante que accede a ella, por lo mismo es muy difícil que se pueda dar una retracción.

La retracción podría darse cuando una persona accede a una pagina web y observa una oferta que le interesa pero no realiza el negocio en el instante, decide pensarlo mejor y posteriormente accede de nuevo a la pagina y se encuentra que la pagina web ya se actualizo por lo tanto la oferta ya no tiene las mismas condiciones que tenia anteriormente o ya no se encuentra, es decir, que en lapso de tiempo en que el interesado decide pensarlo y de nuevo accede a la pagina web dentro de ese lapso de tiempo, se puede dar que el oferente se retracto de su oferta original y la saco de la pagina web y en lugar de la oferta anterior se encuentra una nueva oferta haya cambiado en cuanto a condiciones, por lo tanto, no podrá manifestar aceptación de una oferta anterior por la razón que esta ya no se encuentra vigente.

En cuanto al correo electrónico se le aplicaran las reglas tradicionales de la revocación de la cual nos referimos anteriormente.

Con respecto a la caducidad de la misma manera es aplicaran las reglas a las que nos referimos anteriormente, solo diremos que la caducidad es la perdida de vigencia de la oferta por muerte o incapacidad legal de una persona. Y que no se le debe dar el mismo tratamiento

[57] Vid. CUBILLOS VELANDIA, RAMIRO, RINCÓN CÁRDENAS, ERICK. *Introducción Jurídica al Comercio Electrónico....,* Cit. Pág. 164. La oferta debe de contener un plazo de duración. Es importante que los oferentes establezcan el periodo de validez de la oferta 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.

cuando estas ofertas son hechas por personas naturales y por personas jurídicas sin embargo las posibilidades deben ser contempladas.

Con respecto al segundo requisito, como se señaló anteriormente que el plazo en la legislación salvadoreña es predominantemente convencional, es decir este es pactado por las partes, por tanto la aceptación cumple con este requisito de oportunidad, cuando esta es manifestada o concedida dentro del plazo convenido, por lo tanto, se entiende que la aceptación es oportuna cuando esta se emite dentro del plazo en que la oferta esta vigente.

Sin embargo podemos encontrarnos en la situación que no se encuentre determinado el plazo de la oferta, entonces hasta cuando se puede considerar valida la oferta, como en el caso de las páginas web, con relación a esto algunos autores consideran que el plazo de la oferta puede estar ligado a las constantes actualizaciones de las páginas web, por lo que, no se pude emitirse aceptación de una oferta que ya no se encuentre vigente[58].

El ultimo requisito se refiere a que la aceptación debe ser pura y simple, esto como consecuencia que la oferta fue realizada de la misma manera, es decir que la aceptación hecha de manera pura y simple sin ninguna modificación seria el reflejo de la oferta realizada de igual forma, esto en doctrina es conocido como la ***teoría del espejo***[59]. Pero si al

---

[58] Vid. CUBILLOS VELANDIA, RAMIRO, RINCÓN CÁRDENAS, Erick. *introducción Jurídica al Comercio Electrónico....,* Cit. Pág. 167. El problema en Internet con la validez de la oferta esta directamente relacionado con la actualización constante de las paginas web donde se pueden añadir o suprimir elementos que el comprados pudo haber considerado esenciales en el momento de manifestar su aceptación y que luego no se encuentran vigentes en el momento de la ejecución del contrato. En razón de ello hay quienes recomiendan vincular el plazo de validez de la oferta hasta el momento que la web permanezca sin modificar de manera que no se podrán cursar pedidos que se acojan a condiciones de ofertas anteriores.

[59] Vid. CUBILLOS VELANDIA, RAMIRO, RINCÓN CÁRDENAS, ERICK. *introducción Jurídica al Comercio Electrónico....,* Cit. Pág. 163. Si la aceptación viene pura y simple se produce un reflejo de la oferta. Por el contrario, si ella se modifica, no existe tal reflejo. Sin embargo, sucede con

contrario en la aceptación emitida se introducen cambios que signifiquen una alteración sustancial en el contrato, no se daría el reflejo de la oferta, sino que estaríamos frente a una contraoferta.

Con respecto a lo anterior, si la oferta se presenta redactada de una forma tal en que los términos de la misma se encuentren claros, y en ese caso el destinatario no tenga opción mas que aceptarla, es en este caso cuando se ve manifestada la teoría del espejo, esto por el hecho que frente a una oferta puna y simple, paralelamente debe de existir una aceptación emitida de igual forma.

2.4. FASE DE EJECUCIÓN O CONSUMACIÓN

Es en esta fase cuando se ejecutan las obligaciones surgidas del contrato, dentro de esta fase es importante tener en cuanta aquella clasificación de los contratos que los separa en: contratos de ejecución instantánea y contratos de ejecución sucesiva, llamada también de tracto sucesivo; de acuerdo al primero es aquel en que *las prestaciones resultantes son de tal naturaleza que pueden ser cumplidas en un solo acto* instantáneamente*;* por el contrario si son los contratos llamados de tracto sucesivo, el *cumplimiento del contrato supone la ejecución de prestaciones sucesivas durante un periodo de tiempo mas o menos largo.* Esta división hace referencia a la forma como se cumplirán las obligaciones en esta fase[60].

Dentro del comercio electrónico hay una clasificación que lo divide en comercio electrónico directo y comercio electrónico indirecto; en el

---

alguna frecuencia que en las negociaciones tanto nacionales como internacionales, se introducen algunos cambios de menor envergadura a las ofertas que se emiten, pero que en ningún caso alteran los elementos esenciales en ella. Un Ejemplo lo constituye el que se modifique el lugar de la recepción de un producto, siendo diferente al ofertado, siempre que no signifique una alteración sustancial que altere la esencia del contrato, caso en el cual, en estricto sentido, según esta teoría no es habría formado el consentimiento.

[60] Vid. OSPINA FERNADEZ, GUILLERMO, OSPINA ACOSTA, EDUARDO, *Teoría General del Contrato y del Negocio Jurídico...,* Cit. Pág. 73. Algunos han pretendido descubrir una tercera categoría intermedia, la de los *contratos de cumplimiento escalonado,* que no son ni de ejecución instantánea ni de ejecución sucesiva.

caso específico de las ventas a distancia y de acuerdo a dicha división hay dos formas diferentes de ejecución del contrato. Cuando estamos frente a un contrato de comercio electrónico directo en el cual la perfección y ejecución se producen por medios electrónicos, porque el objeto de dichos contratos son servicios y productos digitalizados, o sea, inmateriales, es decir, aquellos bienes que son susceptibles de reducirse a un juego de números binarios, como por ejemplo programas informáticos, revistas electrónicas entre otros.

Por el contrario cuando se trata de contratos del comercio electrónico indirecto o mixto, el cual se perfecciona por algún medio de comunicación electrónico o informático, pero la ejecución se llevaría acabo a través de canales de distribución tradicional, por que estamos frente a bienes materiales y por tanto, en este caso nos remitiríamos a las reglas de distribución y entrega que se encuentran en el Código de Comercio.

2.5 CONTENIDO DEL CONTRATO

Al respecto lo que debemos de entender como contenido del contrato: "*es la composición misma del contrato, su sustancia más intima entrañable*"[61]. De acuerdo a la estructura jurídica de los contratos, el contrato electrónico es interactivo y dinámico y es un contrato a distancia, y por tanto, esta nueva forma de contratación altera la estructura del contrato.

Los contratos electrónicos, son contratos que lo único que los hace diferente son el medio por el cual se formaron y que por su forma traen consigo nuevos usos y dificultades, por lo que es necesario una preparación cuidadosa de las cláusulas que van a contener estos

---

[61] DIEZ PICAZO, LUÍS; "*Fundamentos del Derecho Civil Patrimonial",* Quinta Edición, Editorial Civita, Madrid-España, 1996, Pág. 353.

contratos; para que las individuos tengan un acceso claro, comprensible e inequívoco de las condiciones del mismo.

Es posible que una de las partes no haya intervenido en la formación del contenido contractual, Esta modalidad contractual tiene algunas características que lo distinguen de los cánones tradicionales de contratación, entre ellas esta en que son contratos consensuales y se someten a condiciones generales y de formación virtual.

Así ocurre en los contratos de adhesión, que serán la mayoría de los celebrados a través de Internet. La despersonalización en el consentimiento es creciente y también la preponderancia del contrato de adhesión en este medio, pero no por ello el contrato deja de serlo y de producir efectos, en estos contratos no hay la misma libertad en este caso para una parte que para la otra, pero no por ello el consentimiento deja de existir.

El contrato debe reunir para su existencia los elementos esenciales del contrato, lo que también es plenamente aplicable al contrato electrónico, celebrado entre las partes a través de medios o procedimientos informáticos como es el caso de los contratos celebrados en Internet.

De acuerdo a lo antes expresado se considera que los contratos realizados por medios electrónicos en específico los contratos realizados por Internet son contratos de adhesión o de condiciones generales[62], por

[62] http://www.monografias.com. Visitada el 22 de octubre de 2009. El punto de partida no puede ser otro que fijar en definitiva interpretar el alcance de la expresión "contratos de adhesión" y si la misma tiene un significado distinto del de las "*Condiciones generales de la Contratación*", y en su caso las posibles relaciones entre ambas expresiones. Las dudas acerca de tal alcance se plantean al examinar el conjunto de los temas de estas Jornadas, ya que no obstante su denominación general: "*Contratos de Adhesión y derecho de los Consumidores*", la enumeración particularizada de los temas concretos de las diversas sesiones contempla de forma casi exclusiva la problemática de "*las condiciones generales*"; de manera que la referencia a "*los contratos de adhesión*" sólo reaparece precisamente con ocasión del examen de la interpretación. Suele citarse como autor de la expresión "*contratos de adhesión*" al jurista Saleilles, y la misma ha sido

lo tanto estos contratos deben de cumplir o incluir dentro de su contenido las siguientes cláusulas[63]:

a. Cláusulas de privacidad: Con esta cláusula se busca proteger y garantizar la confidencialidad de la información suministrada por el usuario y garantizar que ha esta información se le dé un uso adecuado por parte de quien ofrece el servicio.

b. Cláusulas de protección a la propiedad Intelectual[64]: este tipo de cláusulas es importante para restringir los derechos de autor y

---

aceptada de forma unánime tanto por la doctrina como por jurisprudencia y si bien pueden separarse conceptualmente las ideas de "*condiciones generales" y de "contratos de adhesión*", lo cierto es que en la práctica se emplean de forma indiscriminada una u otra expresión.
Con la frase "condiciones generales" se hace referencia al momento de formulación del contenido del contrato, al modo en que los términos de este han quedado fijados. Mientras que con la expresión "*contratos de adhesión*" se hace referencia a la imposición del contenido de dicho contrato a una de las partes del mismo; se trata de dos aspectos de un mismo fenómeno complejo, que acredita la interrelación de ambos significados lo que ha permitido afirmar que "*los contratos de adhesión"* no son más que contratos celebrados en base a previas "*condiciones generales*". La cualidad específica de los "contratos de adhesión" bajo condiciones generales viene referida a la predeterminación de su contenido por la voluntad de una de las partes del contrato que se impone a la otra parte del mismo, sin que esta tenga posibilidades de alterar o influir en los términos de tal contenido. A tal rasgo característico se añade otro no menos significativo: se trata de contratos ideados en contemplación de determinadas esferas del tráfico jurídico y para una pluralidad más o menos extensa de situaciones contractuales que se reiteran de forma semejante ante idénticas necesidades humanas. O en otros términos se trata de contratos en los que se fija su contenido no en relación a las conveniencias individualizadas del sujeto que se adhiere a los términos del contrato, sino que tal sujeto se limita a aceptar un contenido que ha sido predeterminado por referencia a unas necesidades medias objetivamente tomadas en consideración por la parte proponente del contrato; las consideraciones individuales de la parte débil del contrato sólo de modo excepcional son asumidas en el contrato y además mediante *"condiciones particulares*", establecidas como excepción a los términos generales del contrato. Una última característica de los "*contratos de adhesión bajo condiciones generales"* es la de contemplar intereses generales o colectivos en los que es posible observar la confluencia de los intereses particulares de las partes del contrato, con intereses generales de la colectividad que explican la intervención estatal no sólo en el control del contenido de dichos contratos, sino también estableciendo sistema de autodefensa de la parte más débil del contrato que se engloba bajo la figura del "consumidor", mediante el cual se busca incrementar la protección del particular que se adhiere al contrato permitiendo que sus intereses sean asumidos por entes colegiados que agrupan a personas afectadas por idénticos intereses.

[63] Vid. GAITÁN CORTEZ, CARLOS ERNESTO, GUZMÁN LÓPEZ, MARTHA MARÍA., *Relaciones contractuales en Internet y su desprotección por la falta de...*, Cit., Pág.71 y siguientes.

[64] http://www.resa.es Visitada el 24 de octubre de 2008. En este sitio web se establecen las condiciones generales para poder contratar con dicha pagina en cumplimiento de lo previsto en la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, se informa que el titular del sitio web **www.resa.es** es **RESIDENCIAS DE ESTUDIANTES, S.A.** (en adelante, **RESA**) con domicilio en C/ Roger de Llúria nº118, 1º, 08037

propiedad industrial de cada una de las partes que intervinieron en el contrato, es decir, este tipo de cláusulas busca establecer el alcance del derecho que van a tener las partes respecto al contrato que se trate en específico a los de tipo de derecho de autor, propiedad intelectual y propiedad industrial. También se busca establecer que las partes no infrinjan la legislación internacional, ni vulneré el derecho de alguna de las partes vinculadas a la relación contractual.

c. Cláusulas compromisorias: Esta es aquella cláusula en la cual se establece en el cuerpo del contrato que en caso de que se presente un conflicto durante la ejecución del mismo, tal divergencia será resuelta a través de un arbitro, es decir de un tercero el cual será el encargado de dirimir el conflicto[65]. Dentro de esta cláusula se

---

Barcelona, España, con C.I.F. número A-60.109.188, inscrita en el Registro Mercantil de Barcelona, Tomo 24.281, Folio 95, Hoja núm. B-67.261, Inscripción 1ª. El siguiente texto regula la utilización del *Sitio Web* titularidad de **RESIDENCIAS DE ESTUDIANTES (RESA)** por parte de los usuarios de Internet. El presente *Aviso Legal* tiene por objeto establecer las condiciones que regulan el acceso y uso general de este *Sitio Web* para todos lo usuarios, de manera que el acceso y uso del mismo, implica necesariamente la sumisión y aceptación de las presentes condiciones generales, así como, en caso de contratación de un servicio de reserva alojamiento, las Condiciones Generales que caracterizan dicha contratación (en adelante Cláusulas Generales) **Propiedad industrial e Intelectual.** Todos los contenidos de esta página *Web*, entendiendo por estos, los textos, fotografías, imágenes, y otros contenidos audiovisuales, así como el diseño gráfico, y en general sus contenidos, son propiedad intelectual de **RESA** o en su caso, de terceros si los hubiese. De la misma manera, las marcas o signos distintivos son titularidad exclusiva de **RESA** o de terceros, en cuyo caso se expresará de forma específica. El *Usuario* deberá respetar en todo momento los derechos de propiedad intelectual e industrial sobre la página *Web*, titularidad de **RESA.** Queda estrictamente prohibido reproducir, copiar, comunicar públicamente, distribuir, transformar o modificar los elementos de la página *Web* con fines comerciales o vulnerar cualquier otro derecho susceptible de protección por la Ley de Propiedad Intelectual o industrial, a menos que se cuente con la autorización del titular de los correspondientes derechos o ello resulte legalmente permitido. **RESA** autoriza a los *Usuarios* a utilizar, imprimir y descargar los contenidos insertados en el *Sitio Web* y que considere necesarios, exclusivamente para su uso personal, privado y no lucrativo, siempre que no sea utilizado con la finalidad de desarrollar actividades de carácter comercial o profesional, así como su distribución, modificación, alteración o descompilación. La infracción de cualquiera de los citados derechos puede constituir una vulneración de las presentes disposiciones, así como un delito castigado de acuerdo con los artículos 270 y siguientes del Código Penal o cualquier otra disposición general que se dicte al efecto.

[65] Vid. CUBILLOS VELANDIA, RAMIRO, RINCÓN CÁRDENAS, ERICK., *introducción Jurídica al Comercio Electrónico....,* Cit. Pág. 198. La situación actual y en general el nuevo enfoque desarrollado por la tendencia internacional sobre el empleo de los Métodos Alternativos para la Solución de conflictos (MASC), ha generado que se llegue al empleo de las cláusulas

establecerá el lugar donde se realizara el arbitraje, el idioma que se utilizara para el procedimiento arbitral y se establecerá la legislación por la cual se resolverá.

d. Cláusulas de Limitación de Responsabilidad: Este tipo de cláusulas puede en cierta medida convertirse en un medio para desarrollar cláusulas abusivas en la medida que una de las partes en caso concreto el prestador de servicio se encuentre en una posición de superioridad con respecto a la otra parte. Sin embargo es importante establecer este tipo de cláusulas dentro del contenido del contrato en aras de evitar que se vaya extender la responsabilidad de cada una de las partes, mas haya de lo que estas esperan y sean aptas de efectuar.

e. Cláusulas de legislación aplicables[66]: De igual manera es transcendental que se incluya dentro del contenido de estos contratos una cláusula de sumisión, esto es referente a que legislación será aplicable en caso de conflicto, por la razón que las transacciones en Internet son transfronterizas y no se cuenta con una legislación uniforme entre los países que se encuentran conectados a Internet es decir que realizan comercio electrónico,

---

Multifuncionales, con lo que se busca complementar la noción y aplicación de la Cláusula compromisoria. En tal sentido el uso de la mediación y la conciliación, a nivel internacional como un mecanismo apto para la solución de conflictos como un paso previo al proceso de resolución, ayuda en gran medida por su rentabilidad económica y las consecuencias positivas que genera, de allí deriva la necesidad de implementar este tipo de cláusulas en las cuales se prevé primero una etapa de conciliación y mediación y posteriormente en caso de no lograrse el acuerdo, acudir al arbitraje.

[66] Vid. GAITÁN CORTEZ, CARLOS ERNESTO, GUZMÁN LÓPEZ, MARTHA MARÍA., *Relaciones contractuales en Internet y su desprotección por la falta .....,* Cit., Pág. 73. La proliferación de transacciones comerciales a través de Internet a ocasionado la aparición de las siguientes propuestas para la determinación de la legislación aplicable en los casos que no exista sumisión expresa:**1.** Aplicar los convenios internacionales; **2**. Aplicar la legislación del país de origen del vendedor; **3**. Aplicar la legislación del país de origen del comprador; **4**. Crear normas específicas para Internet; y **5**. Aplicar de forma estricta el sistema de direcciones IP (protocolo de Internet) en este último caso la ley aplicable debería ser la del país donde se halle el servidor del que partió la oferta, hecho determinable para la dirección IP del vendedor.

determinando cual va ser la legislación aplicable y el medio por el cual se va resolver el conflicto.

Las normas existentes del derecho internacional reconocen, en su mayoría, la autonomía de la voluntad de las partes como criterio referente de aplicación. Así lo establece el **Convenio sobre la Ley Aplicable a las Obligaciones Contractuales** que abrió a la firma en Roma el 19 de junio de 1980 en el marco de la Unión Europea, cuando dispone en su Art.3 "*que las partes de un contrato podan designar la ley aplicable a la totalidad o solamente a una parte del contrato, así como el tribunal competente en caso de litigio. De común acuerdo, podrán cambiar la ley aplicable en caso que lo deseen"*[67].

Sin embargo por la creciente prolirefación de las transacciones a través de la red Internet y que las relaciones contractuales son transfronterizas y no se cuenta con una normativa uniforme que regule las transacciones que realizan todos los países conectados a Internet, hay cierta inseguridad de los usuarios si dentro del contenido del contrato no se especifica la legislación aplicable en el caso que contrate con una empresa extranjera, porque no se puede saber a priori cual será la ley aplicable al contrato ni los tribunales que serán competentes, y dependerá de lo que dispongan las normas de derecho internacional privado y los Tratados internacionales suscritos sobre la materia.

F. Cláusulas de representación: estas cláusulas se refieren al conocimiento de la información que da la pagina web acerca del

---

[67] http:// www.alviolor.com**.** Visitada el 1 de noviembre de 2008. Dentro de esta página se encuentran las presentes Condiciones Generales de contratación y se dispone que se sujetan a la legislación española. Para cualquier controversia o discrepancia que surja de la interpretación y/o cumplimiento de esta Licencia de Uso, las Partes de someten a los Juzgados y Tribunales del domicilio del Cliente, salvo que **(i)** el domicilio del Cliente esté fuera de España y/o **(ii)** el Cliente fuera una empresa no considerada consumidor en los términos de la legislación vigente, en cuyo

prestador de servicio y acerca del usuario, dicha información funciona como una garantía para el usuario que se esta contratando con una empresa confiable y segura, es decir, "*en esta cláusula se deben de incluir los datos completos como el nombre de la empresa, su dirección, y la forma por la cual puede contactarlos, país donde tiene sedes, así como la certificación de que se trata de una pagina web real y segura.* Dentro de este tipo de cláusulas se establece las condiciones que una persona debe reunir para que el contrato sea valido.

caso, las Partes, con renuncia expresa a su propio fuero, si lo tuvieran, se sujetan a los Juzgados y Tribunales de Barcelona (España).

CAPITULO III

ELEMENTOS DE LA RELACIÓN CONTRACTUAL ELECTRONICA

SUMARIO: 3.1.Generalidades 3.2 Libertad Contractual y Libertad de Contratación. 3.2.1 Contratación Electrónica. 3.2.2 Identidad de las Partes. 3.2.3 Capacidad de las Partes. 3.2.3.1 Capacidad de las Partes en la Contratación Electrónica. 3.3 Representación. 3.3.1 Consentimiento. 3.3.2 Los Vicios del Consentimiento. 3.3.3 Error en cuento a la Identidad de la Cosa. 3.3.4 Error en la Persona. 3.3.5 Error en el Nombre. 3.3.6 Error en el Titulo. 3.3.7 La Generación. 3.3.8 Error en la Contratación Electrónica. 3.4. El Perfeccionamiento de los Contratos por medios Electrónicos. 3.4.1 El Perfeccionamiento del Consentimiento a través de Correo Electrónico. 3.4.2 El Perfeccionamiento del Consentimiento a través de Páginas web. 3.4.3 El Perfeccionamiento del Consentimiento a través de Correo Interactivo. 3.5. Lugar y Momento de Formación del Contrato.

3.1. GENERALIDADES.

La Contratación Clásica es el medio a través del cual se da la comunicación entre las partes. En la Contratación Clásica el contacto entre los contratantes es directo; es así que las partes físicamente se ponen de acuerdo sobre los elementos del contrato, como por ejemplo, sobre el bien, el precio y forma de perfección del contrato. En materia contractual, nuestro sistema jurídico se centra sobre la base de la Autonomía de la Voluntad, 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. Los particulares ejercen esta autonomía a través de dos principios constitucionalmente amparados: **Libertad de Contratar y Libertad Contractual** los que desarrollaremos a continuación.

3.2 LIBERTAD DE CONTRATACION Y LIBERTAD CONTRACTUAL.

La materia contractual está basada en la libertad y la autonomía de la voluntad, respectivamente garantizada en los artículos 2 y 8 de la Constitución de la República de El 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.

La autonomía privada se ejerce a través de dos principios: Libertad Contractual y Libertad de Contratar.

Artículo 2 de la Republica de El Salvador establece que: toda persona tiene derecho a la vida, a la integridad física y moral, la libertad, a la seguridad (…)[68].

Artículo 8 de la Republica de El Salvador menciona que: Nadie esta obligado a hacer lo que la ley no manda ni privarse de lo que ella no prohíbe[69].

Artículo 23 de la Constitución de la Republica de El Salvador establece que: Se garantiza la libertad de contratar conforme a las leyes. 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 arbitrariamente (…)[70].

---

[68] Constitución de la República de El Salvador Editorial Fespad. Quinta Edición, Año 2000. Art. 2

[69] Constitución de la República de El Salvador…, Cit., Art. 8

[70] Constitución de la República de El Salvador…, Cit., Art. 23. En estos artículos se establece respectivamente el derecho a la libertad en su sentido amplio y de contratación con el principio de legalidad.

Artículo 1309 Código Civil Salvadoreño menciona que: Contrato es una convención en virtud de la cual una o mas personas se obligan para con otra u otras, o recíprocamente, a dar, hacer o no hacer alguna cosa[71].

3.2.1. CONTRATACION ELECTRONICA.

Existen formas diversas de definir la contratación electrónica, y autores que la definen de diferente manera entre ellas las siguientes:

"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"[72].

"Todo contrato celebrado sin la presencia física simultanea de las partes, prestando estas 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"[73].

Las normas vigentes no contemplan estas nuevas realidades, de aquí la necesidad de una ley especial que regule el comercio electrónico

---

[71] Código civil salvadoreño. Editorial jurídica Salvadoreña República de El Salvador Año 2007 Art. 1309. Los sujetos de derecho pueden 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, celebrando cualquier contrato se debe establecer el contenido, aunque no se encuentre regulado con nuestra legislación siempre que cumpla con los requisitos de ley. El articulo 1309 código civil menciona "Contrato es una convención… es importante hacer notar que nuestro legislador erróneamente establece esta afirmación puesto que una convención crea, modifica y extingue obligaciones mientras que el contrato solo crea obligaciones.

[72] PATRONI, VIZQUERRE, URSULA. "Contratación Electrónica y acuse de recibido". www.mailweb.mycontelect.html Visitada el 25 de octubre de 2008.

[73] DAVARA, RODRIGUEZ, MIGUEL ANGEL." Manual de Derecho Informático". Ediciones Aranzandi. España. 1997. Pág. 165 La contratación y el comercio electrónico, tratan de una nueva forma de expresión de la voluntad derivada de los avances tecnológicos que hoy en día facilitan la transmisión electrónica de mensajes de datos, agilizando las transacciones comerciales, 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.

en El Salvador, para dar mayor seguridad y despejar dudas sobre la temática.

3.2.2 IDENTIDAD DE LAS PARTES.

IDENTIDAD DIGITAL.

La cedula de identidad y el pasaporte son imprescindible para desempeñarnos en la sociedad global de nuestro tiempo. Sin ellos no se puede demostrar la identidad de ninguna persona. Es por eso, que se necesita un documento de identidad que se denomina Certificado de Identidad Personal (CDI), para demostrar la identidad.

Las funciones de las entidades certificadoras según el Art. 8-A de la ley de Simplificación Aduanera.

- *Ejercer la potestad Jurídica de otorgar fe pública en el marco del intercambio electrónico de datos respecto de la pertenencia de las firmas digitales a personas naturales o jurídicas y de los términos en que se ha generado y transmitido un mensaje de datos[74].*

3.2.3. CAPACIDAD.

La capacidad es la aptitud de una persona para adquirir derechos y poderlos ejercer por sí misma[75].

---

[74] La Ley de simplificación Aduanera, Decreto Nº 529, D O. Nº 23, tomo 342, del 3 de febrero /1999.Esta ley tiene como objetivo la facilitación del intercambio de información automático establece que los registros en soporte electrónico tendrán la calidad de plena prueba también establece que la información que se establezca de esa forma no podrá ser negada o repudiada posteriormente.

[75] Vid. RODRÍGUEZ, ARTURO ALESSANDRI Y UNDURRAGA MANUEL SOMARRIVA, “Curso de Derecho Civil fuente de las Obligaciones” Redactado por Antonio Vodanovic H; tomo IV Editorial Nascimento; Chile; 1976, Pág. 176.

El artículo 1316 del código civil salvadoreño menciona: la capacidad legal de una persona consiste en poderse obligar por sí misma, y sin el ministerio o la autorización de otra[76].

Capacidad legal quiere decir que es dada por ley, cabe la pregunta, entonces si la ley puede quitar esa capacidad y si lo hace cuales serán las circunstancias que motivan estos acontecimientos legales.

El artículo 1317 del Código Civil Salvadoreño menciona: toda persona es legalmente capaz, excepto aquellas que la ley declara incapaces[77].

Cuáles son esas excepciones al leer el artículo 1318 del Código Civil establece: son absolutamente incapaces los dementes, los impúberes y los sordos que no puedan darse a entender de manera indudable[78].

---

[76] Vid. Código Civil Salvadoreño…, Cit., Art. 1316. La capacidad puede ser de goce y de ejercicio, la capacidad de goce es la aptitud de una persona para adquirir derechos, para ser titular de ellos, para ser sujeto de derecho y la capacidad de ejercicio es la aptitud legal de una persona para poder ejercer personalmente, por si misma los derechos que le competen; en este punto se entiende que la capacidad de ejercicio es entonces aquella aptitud para ejecutar actos jurídicos validos

[77] Vid. Código Civil Salvadoreño…, Cit., Art. 1317

[78] Código Civil Salvadoreño…, Cit., Art. 1318.La incapacidad no se presumen debe existir en un texto expreso pero para establecer este punto se debe entender que se entiende por persona según la doctrina se define como todo ente susceptible de ser sujeto de derechos y obligaciones, también se define la persona jurídica diciendo que es "*una persona ficticia, capaz de ejercer derechos y contraer obligaciones civiles, y de ser representada judicial y extrajudicialmente*". La incapacidad proviene del hecho de no ser sujetos en conceptos de ley, las incapacidades de goce son excepcionales y especiales por ejemplo el muerto civil se le prive del derecho de propiedad, otros derechos que no sean de propiedad pueden ser adquiridos por el muerto civil, por otro lado, la persona que adolece de incapacidad de ejercicio puede ser titular de derechos, incorporarlos a su patrimonio, existen clases de incapacidad de ejercicio como lo es la absoluta, relativa y especial además de estas hay otras particulares que consisten en la prohibición que la ley ha impuesto a ciertas personas para ejecutar ciertos actos. Para mayor ilustración consultar a Rodríguez, Arturo Alessandri y Undurraga Marvel Somarriva "Curso de Derecho Civil" tomo IV fuentes de las obligaciones Pág. 177 a la 189.

El artículo 52 del Código Civil establece: Las personas son naturales o jurídica, son especie humana, cualquiera que sea su edad, sexo, estirpe o condición.

Son personas jurídicas las personas ficticias capaces de ejercer derechos y contraer obligaciones y ser representadas judicial o extrajudicialmente[79].

3.2.3.1 CAPACIDAD DE LAS PARTES EN LA CONTRATACIÓN ELECTRÓNICA

Base el principio de buena fe articulo 1417 Código Civil Salvadoreño, y la firma electrónica como medio para identificar con quien se está contratando, partiendo de la idea que la clave debe ser únicamente conocida por la persona registrada como dueño y ésta responderá de el uso que de la firma se haga ya que el está obligado a guardar la clave simbolizada en la firma[80].

3.4 LA REPRESENTACIÓN

Se entiende celebrado por la persona titular de las claves, aunque no sea esta la que ha hecho cierta operación pero se establece que tiene la autorización y consentimiento del titular, que le transfiere sus claves, éste proceder es ilícito en principio puesto que la clave es personal e intransferible y permita la comisión de hechos fraudulentos. Esto puede ser previsto entregando claves al representante que identifiquen que es una representación autorizada y distinta de la del representado, operación que debe estar a cargo de las entidades certificadoras

---

[79] Código Civil Salvadoreño…, Cit., Art. 79.

[80] GALÁN CORTEZ, JEANNIE ELIZABETH *La firma digital como medio de seguridad y consentimiento de las*…, Cit., Pág.55. Esta tesis da un leve planteamiento sobre el hecho de establecer la seguridad por medio de la tecnología, imagen, voz sin descartar otras en El Salvador por la poca_tecnología que se tiene es una actividad muy difícil que debe ser cambiado tecnificando a las personas y traer mas muy mejor tecnología.

El contrato celebrado a nombre de otro por quien no tenga su autorización o representación legal será nulo, a no ser que lo ratifique la persona a cuyo nombre se otorgue antes de ser revocado por la parte contratante.

Inexistencia del contrato si hubiera fallecido o incapacidad sobre venida de cualquiera de los contratantes sin haber sido ratificado.

Validez del contrato, si es ratificado por la persona en cuyo nombre se actuó prestando consentimiento a posterior, y con efectos desde el día de su celebración[81].

3.5. CONSENTIMIENTO

El consentimiento. Es el acuerdo de voluntades de dos o más personas con un objeto lícito. El consentimiento debe reunir algunos Requisitos como que la voluntad sea seria, es decir, emitida con el propósito de crear un vínculo jurídico. Que se exteriorice, que se dé a conocer externamente[82].

El consentimiento como elemento esencial del contrato se desglosa en varios supuestos a cumplir como lo es, un acuerdo de voluntades, se debe entender entonces que la manifestación unilateral conocido como voluntad se debe poner en un mismo sentido que sería el acuerdo, se establece además la realización por dos o más personas que es la regla

---

[81] Vid. GAITÁN CORTEZ, CARLOS ERNESTO, GUZMÁN LÓPEZ MARTHA MARÍA. "*Relaciones contractuales en Internet y su desprotección por la falta…., Cit.,* Pág. 130 y 131.

[82] Vid. RODRÍGUEZ, ARTURO ALESSANDRI; UNDURRAGA, MANUEL SOMARRIVA "*Curso de Derecho Civil fuente de*…., Cit., Pág. 76 a la 80. Esta obra establece los elementos constitutivos del contrato y como el de mayor importancia el consentimiento manifestado a través de la voluntad que se define como "*La facultad que tiene un individuo de actuar en sentido determinado, es importante establecer cómo se forma el consentimiento para este efecto se menciona que es a través de la oferta y aceptación como la propuesta por la cual una persona propone a otra la celebración de un contrato sobre bases determinadas. Requisitos de la oferta, debe producirse con la intención de producir un vinculo jurídico, que dicha intención se exteriorice a quien va dirigida diga "si", dicha oferta debe ser voluntaria por tanto emitida libremente"*

general, y uno debe cumplir con ser un objeto licito es decir que no esté prohibido por la ley.

3.6 VICIOS DEL CONSENTIMIENTO

Son aquellos acontecimientos que como su nombre lo indica impiden que el consentimiento se perfección, puesto que el sentir de los contratantes sobre un punto especifico no llega a concretizarse.

Como ejemplo, un contratante piensa vender un carro y el otro comprar una casa este hecho impide la perfección del consentimiento. Existe error en cuanto a la identidad de la cosa esto invalida el consentimiento.

Para establecer este tema se debe hacer mención a la tradición y a este efecto se dirá que: *la tradición es un modo de adquirir el dominio de las cosas y consiste en la entrega que el dueño hace de ellas a otro, habiendo por una parte facultad e intención de transferir el dominio y por otra la capacidad e intención de adquirirlo. Articulo 651 Inc. 1º Código Civil Salvadoreño*[83]*.*

3.6.1 EL ERROR EN CUANTO A LA IDENTIDAD DE LA COSA

Produce invalidez, la tradición no vale conforme a los artículos 1324 y 657 Código Civil Salvadoreño y es causal de nulidad absoluta, a esta clase de error se le denomina error esencial. Como ejemplo se establece que al comprar un televisor yo doy mi consentimiento identificando el objeto si me dieran una vaca pues el consentimiento no se

[83] BARRIERE, JORGE ALBERTO, *Guía para el estudio de Derecho…, Cit…,* Pág. 42 Establece los requisitos que debe cumplir la tradición el elemento personal, cual es la presencia del tradente y adquirente Art. 652 Inc. 1º Código Civil Salvadoreño, consentimiento del tradente y del adquirente, existencia de un titulo traslaticio de dominio, entrega de la cosa y establece que el tradente debe reunir algunas exigencias como son ser dueño de la cosa entregada y tener facultad para transferir dominio, con respecto al consentimiento vaciado es en realidad, consentimiento, aunque dado en condiciones irregulares; la persona que bajo error, dolo o fuerza, consiente, ha expresado su voluntad, que no es libre, pero en todo caso es voluntad.

perfecciona por el hecho que no existe realmente un acuerdo de voluntades con respecto a la identidad de la cosa querida y la otorgada.

3.6.2 ERROR EN LA PERSONA

No vale la tradición si existe error en cuanto a la persona a quien se le hace la entrega, es decir debe existir de parte de la persona que recibe voluntad e intención de adquirir[84] .

3.6.3 ERROR EN EL NOMBRE

Si se yerra en el nombre solo la tradición vale, porque las personas tradente y adquirente han manifestado su voluntad e intención.

Las personas físicas, son las mismas por consiguiente la equivocación en el nombre no invalida la tradición articulo 657 inciso ultimo Código Civil Salvadoreño.

3.6.4 ERROR EN EL TITULO

Falso conocimiento que las partes tienen en cuanto a la causa por el cual se pasa a ser dueño es decir sobre el titulo.

Falta concurrencia de voluntades no hay acuerdo mutuo en cuanto a la causa de adquisición por tanto no hay tradición, aunque ambos títulos invocados sean traslaticios de dominio. (Articulo 658 Código Civil Salvadoreño[85].

---

[84] Vid BARRIERE, JORGE ALBERTO "Guía para el estudio de Derecho…., Cit., Pág. 44. El error en sentido general se le define como el concepto equivocado de la ley, de una persona o cosa; es el falso concepto de la realidad; consiste en creer lo falso como verdadero y lo verdadero como falso, existe error de hecho y de Derecho. De Hecho: falso concepto de una persona, cosa es suceso. De Derecho: concepto falso o ignorancia que se tiene de la ley. "Nadie puede alegar ignorancia de ley" es por ello que el error sobre un punto de derecho no vicia el consentimiento. Existe excepción a esta regla general cuando no se alegue para el lucro o deshacer la obligación si no para evitar un daño mayor lo que los Romanos decían "olamno vitando, lucro captado… para evitar un perjuicio

[85] Vid BARRIERE, JORGE ALBERTO *"Guía para el estudio de Derecho*…., Cit., Pág. 45. Según la doctrina el error obstáculo, es el que impide la existencia del consentimiento, es decir el error en

3.6.5 ERROR EN LA CONTRATACION ELECTRONICA

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

Errores que pueden ocurrir en la contratación electrónica:

- Pérdida o demora: cuando el documento ha sido enviado y no fue recibido por la otra parte, debido a contrario o demora en la recepción.

- 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.

- Imposibilidad de comunicación: protocolo no adecuados o sistemas incompatibles

- Contradeclaración: documentos electrónicos con fechas posteriores al contrato.

- Contradeclaraciones: documentos electrónicos con fecha posterior al contrato.

---

el titulo, Juan entiende comprar y Pedro arrendar; error en la identidad de la cosa como que “A” entiende comprar el caballo x pero “B” entiende vender el caballo “y” en estos casos evidentemente no existe consentimiento debido a que las voluntades de las partes no han concurrido sobre el objeto materia de la declaración de voluntad o del acto o contrato, es decir no existe acuerdo en cuanto a el objeto o intención de contratación, trae consigo el desacuerdo de los contratantes autores del contrato.“Para mayor ilustración consultar, Rodríguez, Arturo Alessandri”. “Curso *de Derecho Civil fuente de las obligaciones”* Pág. 120 a la 134.

Importe es hacer mención que la clase de error que aquí se da es en cuanto a la identidad puesto que se menciona que al pedir un objeto determinado ese objeto será el que se tiene que recibir y no otro puesto que si ocurre de esta manera no existe el acuerdo de voluntad lo que la doctrina conoce como error obstáculo puesto que sirve de atraso para que se perfeccione el contrato claro si es subsanado tal error porque de no serlo pues no existiría un verdadero acuerdo de voluntades.

Es ese hecho el que determina si el contrato se perfecciona o no puesto que el consentimiento es un elemento esencial del contrato no se puede hablar de contrato sin el elemento del consentimiento.

3.7 EL PERFECCIONAMIENTO DEL CONTRATO POR MEDIOS ELECTRÓNICOS.

De manera muy general diremos que el consentimiento[86] es la manifestación de voluntad de las partes para la celebración de un contrato y esta determinado por el acuerdo de dos o más declaraciones de voluntad las cuales pueden ser manifestadas a través de diversos medios de comunicación. En este sentido, el consentimiento que se presta en los contratos celebrados por medio de Internet no difiere del que se debe proporcionar en otro tipo de ámbitos fuera de la contratación electrónica. Por tanto, lo que habrá que analizar serán las formas o mecanismos

[86] htt://www.comunidadene.com/docu/contratos.pdf. Visitada el 13 de octubre de 2008. Como todo contrato el "*contrato electrónico*" toma forma a partir del consentimiento y la ausencia de fronteras obliga a analizar el lugar de celebración que a su vez determinara la ley aplicable y la jurisdicción competente en caso de conflicto. La convención de Viena de 1998 sobre compraventa internacional de mercaderias establece que el contrato se perfecciona cuando llega al oferente la notificación de la aceptación. En los contratos electrónicos, la comisión de las Naciones Unidas para el Derecho Mercantil Internacional, el la ley Modelo para el Comercio Electrónico y el derecho comparado, en general, aceptan pacíficamente que el contrato queda perfeccionado en el momento que la aceptación ingresa al sistema informatico del oferente. No es necesario que el oferente tenga conocimiento de la aceptación. Basta que ingrese en su esfera de control. Se establece además, la obligación a cargo del oferente de emitir "acuse de recibo" de la aceptación para dar seguridad a las transacciones comerciales.

técnicos a través de los cuales se puede prestar el consentimiento en Internet.

El perfeccionamiento del consentimiento, igual que cualquier otro contrato se manifiesta mediante el concurso de la oferta y la aceptación sobre, la cosa y la causa que han de constituir el contrato. Recordemos además, que la mayoría de contratos que se realizan en Internet son contratos consensuales, es decir, que se perfeccionan con el mero consentimiento sin necesidad de más requisitos.

Debe advertirse por otra parte, que se esta frente a un supuesto de contratación entre personas ausentes, es decir, donde estas se encuentran separadas físicamente, por tal razón se debe de determinar en que momento se considera perfeccionado el consentimiento, y por ende perfeccionado el contrato. Por contrato a distancia se entiende aquellos en que la oferta, la negociación y la celebración se efectúan a distancia, sin la presencia física simultánea de los contratantes[87].

De acuerdo a lo anterior, haremos una distinción que resulta importante para nuestro estudio, y es aquella que clasifica los contratos entre personas ausentes o distantes y contratos entre personas presentes, esto en virtud del espacio temporal jurídicamente relevante que media entre la aceptación y su conocimiento por parte del oferente. Respecto del momento de la perfección de los contratos celebrados por medios electrónicos, se debe de considerar que Internet ofrece distintos

---

[87] Vid. htt://www.comunidadene.com/docu/contratos.pdf. Visitada el 13 de octubre de octubre de 2008. El contrato necesita de la manifestación inequívoca de la voluntad de las partes que conformarán el acto jurídico. Así, cuando las partes contratantes expresan su voluntad en el momento que se forma el contrato, se denomina *entre presentes*. Cuando la manifestación de la voluntad se da en momentos diferentes, se denomina *entre ausentes*. La distinción es importante para poder determinar con exactitud el momento en que el contrato entra en la vida jurídica de los contratantes. El contrato entre presentes entrará en vigencia en el momento de la manifestación simultánea de la voluntad, mientras que el contrato entre ausentes solamente hasta que el último contratante haya dado su manifestación.

servicios por los cuales las personas pueden entrar en comunicación, entre los servicios que ofrece Internet tenemos[88]: el correo electrónico, correo interactivo conocido también como "*chat", y las páginas "*web".

Sobre este ultimo aspecto, debemos decir, que no se puede dar un mismo tratamiento ni tampoco se les debe de encasillar en una misma categoría, a las diversas formas de comunicación que ofrece Internet, o sea, distinguiremos entre los contratos perfeccionados por medio de correo electrónico y los que se perfeccionan por "*chat"* o página "*web".* Por ende, se desarrollará de una forma breve la perfección de los contratos a través de los distintos medios antes mencionados.

3.7.1. PERFECCIONAMIENTO DEL CONSENTIMIENTO A TRAVÉS DE CORREO ELECTRÓNICO

Como expresamos anteriormente la diferencia entre personas distantes y personas presentes, es el espacio de tiempo que media entre la aceptación y su conocimiento por parte del oferente, esto de acuerdo, al medio de comunicación utilizado para emitir la aceptación. Cuando

---

88 htt://www.scielo.cl/scielo.php?pid=so718001200500020009&script=sci_arttex#nota18. Visitada el 16 de octubre de 2008, el primer problema, el referido a los conceptos de tiempo y espacio en Internet, el que como decimos responde muchas veces a cánones diversos de los hasta ahora conocidos. Piénsese en la comunicación por correo electrónico que, en principio es asimilable a la comunicación por carta tradicional, sin embargo, el correo electrónico puede llegar en cuestión de segundos a los rincones más lejanos y apartados del mundo, lo que traerá como consecuencia, según veremos, que muchas de las aprehensiones de los legisladores de los siglos pasados relativas a la demora en la recepción de las comunicaciones, en el caso de correo electrónico no se justifiquen. Tal prevención, efectuada para la comunicación vía correo electrónico, puede hacerse extensiva en general a la mayoría de los medios de comunicación pertenecientes a las nuevas tecnologías, resultando que la frecuentemente presumida falta de continuidad en los procesos de comunicación a distancia no se da en el caso de la formación del consentimiento electrónico. Todos los aspectos señalados han llevado a más de algún a autor a sostener, con buena dosis de razón, la insuficiencia de los conceptos clásicos para explicar adecuadamente las hipótesis de contratación electrónica, en el sentido que en tal modalidad contractual carece de sentido, bajo algunos respectos, el calificar un determinado negocio como celebrado entre ausentes o entre presentes. En todo caso, teniendo en cuenta las características generales de simultaneidad y rapidez en los procesos comunicacionales mediante nuevas tecnologías si de clasificarlos se trata, una parte importante de la doctrina parece considerar que estaríamos en presencia, según los cánones tradicionales, de una especie de contratación entre presentes, ello para los efectos previstos en las leyes respecto a la perfección del negocio jurídico. Lo anterior, como regla general que admite excepciones en atención a las diversas características de los diferentes medios pertenecientes a las tecnologías de la información.

pasa un lapso de tiempo que puede llegar hacer jurídicamente importante y dentro del cual se debe de señalar el momento en que se entenderá perfeccionado el contrato. Esto es lo que sucede con la clásica contratación por correspondencia, y de acuerdo a esto, podemos decir que la perfección del contrato por medio de correo electrónico se asemeja a la perfección del contrato por correspondencia convencional[89].

Al respecto cuando utilizamos el correo electrónico para emitir la aceptación, no podemos decir que esta ha sido conocida inmediatamente por la otra parte o oferente, aunque esta sea emitida por medio de ordenadores y redes capaces de transmitir declaraciones de voluntad a una velocidad cada vez mas rápida, por el hecho, que debemos recordar que los mensajes se depositan en el servidos y todavía se debe de contar con que estos se abran y lean cuando se vacíe la cuenta de correo. De igual manera sucede en el correo convencional y como este es un supuesto de contrato entre personas ausentes o distantes, por tanto el contrato celebrado por medio de correo electrónico es también un supuesto de contrato entre personas distantes por lo cual se le aplicara para determinar el perfeccionamiento las reglas de la contratación entre ausente.

Partiendo de que nos encontramos ante un contrato entre personas ausentes o distantes, el problema a resolver es el momento en que este se entiende perfeccionado, por lo cual haremos referencia a los

---

[89] Vid. htt://www.scielo.cl/scielo.php?pid=so718001200500020000 9&script=sci_arttex#nota18. Visitada el 16 de octubre de 2008, el correo electrónico, por el contrario, es considerado, por regla general, una especie de contratación entre ausentes, por tratarse de un proceso de comunicación sucesivo o interrumpido ya que según es públicamente conocido pueden transcurrir horas o días hasta que el mensaje de correo electrónico sea leído por su destinatario. Lo paradójico es que, si se aplica la teoría de la recepción y la normas que hasta el momento han sido elaboradas especialmente para la contratación electrónica, el perfeccionamiento del negocio se producirá, por regla general, en forma prácticamente instantánea, ya que lo que se exigirá no es que el destinatario haya leído el correo sino que éste haya llegado a su órbita de conocimiento, lo que sucederá en el instante en que mensaje haya ingresado en la cuenta de correo electrónico que el destinatario mantiene en un determinado servidor, con independencia del momento en que decida recuperar y tomar conocimiento del mensaje.

distintos sistemas[90] que existen al respecto los cuales pueden ser resumidos de la siguiente manera:

1. **SISTEMA DE LA DECLARACIÓN O APROBACIÓN***:* considera que para que el contrato quede perfeccionado basta simplemente que el destinatario de la oferta manifieste su voluntad de aceptarla, bien sea expresamente, bien mediante hechos inequívocos. Este sistema sitúa el momento de la perfección del contrato en el primer estado de la aceptación, en aquel en el que el destinatario de la oferta declara su aceptación, no importa si el oferente conoce o no la aceptación el contrato queda perfeccionado.

2. **SISTEMA DE LA EXPEDICIÓN***:* Este sistema no admite que el destinatario de la oferta se limite a declarar se voluntad de aceptarla, si no que le impone la obligación de enviar una respuesta al proponente. Porque mientras la declaración de voluntad del aceptante se encuentre dentro del ámbito propio de este, esta debe ser considerada ineficaz para determinar la existencia de un contrato; por que el acto de expedición de la aceptación es el que señala el momento de la formación del consentimiento.

3. **EL SISTEMA DE RECEPCIÓN**[91]*:* Consiste en exigir que la contestación de la oferta llegue al domicilio del proponente, con la

---

[90] Vid. De manera general, OSPINA FERNADEZ, GUILLERMO, OSPINA ACOSTA, EDUARDO, *Teoría General del Contrato y del Negocio Jurídico,* 6ª Edición, Editorial Temis, Bogotá, 2000, Pág. 167 y siguientes. Vid. Diez Picazo, Luís, *Fundamentos del Derecho Civil Patrimonial",* Quinta Edición, Editorial Civita, Madrid-España, 1996, Pág. 357 y siguientes. Vid. UREBA, ALBERTO ALONSO, VIERA GONZALEZ, ARÍSTIDES JORGE, *Formación y perfección de los contratos a distancia celebrados por Internet,* en AA VV Derecho de Internet, La ley de Servicios de la Sociedad de la Información y de Comercio Electrónico, Coordinado por MATEUS DE ROS, RAFAEL, 3 Edición, Editorial Aranzadi, Madrid, 2001, Pág.346 y siguientes.

[91] *Convención de Viena sobre la compraventa internacional de mercaderías* en su artículo 18.2 de la Convención señala: "la aceptación de la oferta surtirá efecto en el momento en que la aceptación

posibilidad de conocerla, aunque este por cualquier causa no se imponga de su contenido, por ejemplo, en el caso de la correo convencional el contrato quedaría perfeccionado de acuerdo a este sistema, en el momento que la aceptación llegue al domicilio del proponente, a un cuando sea otra persona quien reciba la carta de aceptación de la oferta.

4. **SISTEMA DE INFORMACIÓN***:* este se refiere a al conocimiento que el proponente debe tener de la aceptación de su oferta, mientras esta información no se realice, no hay consentimiento, dicho de otra manera, el contrato queda perfeccionado cuando el oferente toma conocimiento efectivo de la aceptación.

Cada uno de estos sistemas es recogido por diversas legislaciones, en el caso de El Salvador nuestro ordenamiento jurídico positivo adopta el sistema de recepción que ofrece más ventajas desde el punto de vista lógico y de la seguridad jurídica, en el supuesto de los contratos entre ausentes[92], el Art.966 del Código de Comercio señala que *"el contrato*

---

de asentimiento llegue al oferente". Este precepto contiene un pronunciamiento a favor de la "teoría de la recepción".

[92]Vid. htt://www.scielo.cl/scielo.php?pid=so718001200500020009&script=sci_arttex#nota18 Visitada el 16 de octubre de 2008, Encontrándonos abocados al estudio de los problemas que genera la determinación de la perfección del contrato electrónico cuando éste se desarrolla entre ausentes, cabe preguntarse si constituyen realmente los supuestos negóciales electrónicos una modalidad de contratación entre ausentes. Al parecer francamente mayoritaria, es la normativa y doctrina que entienden los supuestos de contratación electrónica como una clase de contratación a distancia o sin presencia física de las partes, ello debido principalmente a que en un comienzo las nuevas tecnologías fueron desarrolladas casi exclusivamente como medios de comunicación a distancia -función hoy evidentemente sobrepasada-, sin embargo, en la actualidad comienza a dudarse que tal modalidad contractual constituya realmente un proceso formativo a distancia o entre ausentes, al menos de acuerdo a los criterios tradicionales que se han utilizado para dar tal calificación a los contratos. Al respecto es necesario abordar dos cuestiones principales. Por una parte preguntarse si es posible que el negocio jurídico electrónico se celebre entre presentes -ya hemos dicho que en un principio sólo estaba considerado como una hipótesis negocial a distancia- y, por la otra, esclarecer si la formación del consentimiento electrónico entre personas distantes físicamente puede ser explicado de acuerdo a las reglas clásicas que gobiernan la formación del consentimiento entre ausentes. Respecto al primer punto, ya hemos expresado nuestra opinión en el artículo Nº 2 de la presente serie en el sentido de que si bien es cierto que la contratación electrónica se originó como un fenómeno comunicacional entre personas distantes físicamente, en la actualidad, debido principalmente a los avances experimentados en los últimos años en

queda perfeccionado desde el momento que el oferente recibe la aceptación de la propuesta que él realizo".

Por todo lo anteriormente expuesto, se entenderá que la perfección del consentimiento por medio de correo electrónico, es equivalente a la perfección del consentimiento por correo convencional, por tanto se le aplicaran las reglas del sistema de recepción el cual postula que el contrato queda concluido, desde el momento que el documento que contiene la aceptación hecha por el destinatario de la oferta llega a poder del oferente, no siendo necesario que el oferente se entere de su contenido, pues basta que llegue fehacientemente la aceptación al ámbito de acción o esfera jurídica del oferente, y de a cuerdo a lo anterior se entenderá perfeccionado el consentimiento.

---

aspectos tales como suscripción, archivo y prueba del documento electrónico, es posible anticipar que el formato electrónico será preferido por una proporción de los suscriptores de documentos de naturaleza negocial que se encuentran en el mismo lugar de suscripción, ello debido principalmente al hecho de que se transita decididamente desde el documento en soporte papel al documento en soporte electrónico. El segundo aspecto importante en el análisis de la cuestión, se refiere a la determinación de si el proceso de formación del consentimiento electrónico entre personas ausentes obedece a los criterios usados por el legislador -al establecer normas especiales para el perfeccionamiento de negocios jurídicos entre personas no presentes- en la teoría general de obligaciones y contratos. Para ello será necesario determinar, en primer lugar, cuál ha sido, el criterio utilizado por el legislador en la distinción entre contratos entre presentes y ausentes. Un dato de la jurisprudencia española servirá para ilustrar esta cuestión. Nos referimos a la sentencia del Tribunal Supremo español, de 5 de enero de 1948, que señaló que el acuerdo alcanzado durante una conversación telefónica daba lugar al perfeccionamiento del contrato, lo mismo que se hubiera concertado entre presentes. Validando el criterio jurisprudencial señalado la doctrina es pacífica en el sentido de considerar a la contratación telefónica como una especie de contratación entre presentes. Igual criterio es seguido en los países del *"common law",* y específicamente en Estados Unidos e Inglaterra, países en los que los contratantes que se comunican por teléfono son considerados *"presentes".* La doctrina estima, asimismo, que la *ratio legis* del razonamiento que considera la comunicación telefónica como una especie negocial entre presentes se encuentra en la circunstancia de que en tal medio de comunicación existe un proceso interrumpido. En el sentido indicado se sostiene que: *"El problema no se plantea si, no obstante el distanciamiento o la lejanía, existe entre las partes un proceso de comunicación interrumpido",* continúa, *"Lo mismo puede decirse cuando se produzca un interrumpido proceso de comunicación por télex, si ambas partes se encuentran simultáneamente en cada uno de los extremos de la comunicación".*En atención al mismo criterio, la doctrina no duda en calificar como una especie de contratación entre ausentes aquella que se produce mediante carta o correspondencia telegráfica, ya que entre las diversas comunicaciones, entre aceptante y oferente, media interrupción o un espacio de tiempo jurídicamente relevante. Por su parte, en el ámbito normativo español, parece prevalecer la idea de que la contratación electrónica es una especie de contratación a distancia

3.7.2. PERFECCIONAMIENTO DEL CONSENTIMIENTO A TRAVÉS DE LA PÁGINA WEB

En las páginas web en la practica existen dos maneras distintas de comunicar las diferentes declaraciones de voluntad negóciales, primeramente en una pagina web podemos encontrar que esta contiene toda la información y condiciones de la oferta contractual, pero para emitir la declaración se predispone el intercambio de correo electrónico, se considera a esta pagina web como equivalente al catalogo de las ventas a distancia, por tal razón estaríamos frente a un supuesto de contrato entre personas ausentes o distantes, es decir, se le aplicarían las reglas de sistema de recepción que comentamos en el apartado anterior.

En cambio cuando el contrato se formaliza chicleando la palabra "*acepto"* o "*estoy de acuerdo*" u otra equivalente que se encuentre dentro de dicha pagina, y es de los contratos en que se establece comunicación entre la persona del aceptante y un ordenador o un dispositivo automático, en este caso se considera que hay consentimiento desde el momento que se manifiesta la aceptación, por tanto, estaríamos frente a los denominados contratos entre personas presentes, por el hecho que se considera que entre los dos ordenadores se establece una comunicación interactiva en tiempo real, en el sentido que cada una de las partes conoce inmediatamente la declaración de voluntad de la otra parte[93].

[93]Vid.htt://www.scielo.cl/scielo.php?pid=so71800120050200009&script=sciarttex#nota18. visitada el 16 de octubre de 2008. En relación con la formación del consentimiento electrónico vía página Web, no es posible dar una respuesta unitaria a la cuestión relativa a si se trata de una especie de contratación entre presentes o no, sino que será necesario realizar la distinción entre páginas Webs interactivas u *on line* o pasivas u *off line,* de tal suerte que, por regla general, en los casos en que la Web cuente con un sistema electrónico de comunicación bidireccional en línea, esto es, se trate de una Web interactiva, deberemos considerar tal proceso negocial dentro de la categoría *entre presentes* y, en caso contrario, como una especie negocial entre ausentes.

3.7.3. PERFECCIÓN DEL CONSENTIMIENTO A TRAVÉS DE CORREO INTERACTIVO

Este medio de comunicación también es denominado "Chat"[94], el cual opera como una comunicación en tiempo real, entre dos o mas personas que se encuentran en diferentes lugares, pero el consentimiento se considera que se emite instantáneamente, por tanto, se estará frente a un contrato entre personas presentes, por la razón que no media espacio temporal entre la oferta y la aceptación.

Finalmente, el perfeccionamiento del consentimiento dependerá del medio utilizado para emitir la aceptación y se aplicara las reglas dependiendo el caso concreto si se trata de contratos entre personas ausentes o por el contrario si se trata de contrato entre personas presentes para la formación consentimiento.

3.8 LUGAR Y MOMENTO DE FORMACIÓN DEL CONTRATO

Uno de los problemas más relevante que encontramos dentro de la contratación por medios electrónicos celebrada a través del medio de comunicación Internet es la cuestión de la internacionalidad de dichos contratos, de tal manera que el lugar de celebración de los contratos es importante al momento de determinar la jurisdicción competente y la ley aplicable al mismo. Esta materia relativa al momento y lugar del perfeccionamiento[95] del contrato ha adquirido un nuevo interés pues se ha

---

[94] Vid. htt://www.comunidadene.com/docu/contratos.pdf Visitada el 13 de octubre de 2008. El Chat, por su parte, aún cuando no significa una mejora en comparación con la comunicación telefónica tradicional, es un proceso comunicacional en tiempo real, esto es, exige la presencia de las partes al mismo tiempo en ambos extremos de la línea de comunicación establecida, recibiéndose las respuestas a las interrogantes planteadas por las partes en cuestión de segundos en el otro extremo de la línea de comunicación. Es por eso, que consideramos conforma también un proceso fluido de comunicación en el que las partes pueden conocer, en cuestión de segundos, la aceptación a una oferta contractual determinada.

[95] http://civil.udg.es/normacivil/estatal/CC/4T2.htm. Visitada el 18 de octubre de 2008. En el ámbito de la contratación Internacional, la Convención de Viena sobre compraventa Internacional de mercaderías prescribe en su artículo 18.2, Que la aceptación de la oferta surtirá efecto en el momento en que la indicación de asentimiento llegue al oferente. La aceptación no surtirá efecto si

constatado que las nuevas tecnologías de la información han alterado algunos de los elementos usados tradicionalmente para el análisis del proceso de formación del contrato, tal es el caso de la nueva dimensión que han adquirido en Internet nociones tan importantes como las de tiempo y espacio, aspectos que necesariamente han llevado a la revisión de las soluciones que hasta antes de la aparición de las nuevas tecnologías se daban por satisfactorias.

Al respecto, el lugar de celebración del contrato se entiende que es donde se hizo la oferta, o en defecto, si las partes pactan al respecto será el lugar donde estas se sometan.

En cuanto a la formación del contrato esta determinada el lugar y momento que nace el contrato a la vida jurídica, por tanto, debemos reiterar que el momento de la formación del contrato se da cuando el oferente recibe la aceptación de la oferta realizada a la otra parte.

Con relación a lo anterior el momento de la formación[96] del contrato es cuando el mensaje de datos del aceptante llega al oferente. El domicilio

---

la indicación de asentimiento no llega al oferente dentro del plazo que éste haya fijado o si no se ha fijado plazo, dentro de un plazo razonable, habida cuenta de las circunstancias de la transacción y, en particular, de la rapidez de los medios de comunicación empleados por el oferente. Como puede apreciarse el artículo 18.2 de la Convención de Viena ha optado por el criterio vinculado a la *recepción* de la aceptación por parte del oferente para la determinación del momento de perfección del contrato. El criterio seguido por la Convención de Viena sobre compraventa Internacional corresponde a la tendencia "*de los modelos de contrato de intercambio electrónico, tanto europeos como norteamericanos"*, circunstancia que queda confirmada en el artículo 2:205 de los Principios del Derecho Europeo de Contratos, en el que bajo el epígrafe de: "*Time of Conclusion of the Contract",* se señala en su apartado 1º que, si una aceptación ha sido enviada por el destinatario de la oferta se concluye el contrato cuando la aceptación llega al oferente. En una línea similar, en los principios de Unidroit se dispone en su artículo 1.9 que: *"la comunicación surtirá efectos cuando llegue a la persona a quien va dirigida" y, "se considerará que una comunicación llega a la persona cuando le es comunicada oralmente o entregada en su establecimiento o en su dirección postal",* acogiéndose, por tanto, también el criterio conceptual izado como teoría de la recepción.

96 Http//www.teleley.com/articulos/art_patroni.pdf. Visitada el 13 de octubre de 2008. En la actualidad el consentimiento puede emitirse por vía electrónica. Al emitir el consentimiento la información transita desde la computadora del cliente, pasa por varios servidores hasta llegar al

del oferente constituye entonces el punto de conexión para determinar cual es el lugar de celebración del contrato. El numeral 4) del Art.15 de la de la Ley Modelo que efectuara la Comisión de Trabajo de las Naciones Unidas para el Derecho Mercantil Internacional relativa al Comercio Electrónico (UNCITRAL). Establece que el mensaje de datos del oferente se considera emitido en el lugar donde tiene su establecimiento principal, aunque haya sido emitido en otro, al igual que del aceptante, por lo que el lugar de celebración del contrato sería aquel en el que le oferente tiene su establecimiento y si tiene mas de uno, en el domicilio que guarda una relación mas estrecha con la operación realizada o, de no haberlas, el de la residencia habitual del oferente, independientemente el lugar donde se ubiquen los sistemas de información en que efectivamente se hubieran emitido los mensajes de datos conteniendo la oferta y aceptación.

Al respecto se aplica el criterio de buena fe, ya que se debe evitar que la posibilidad real de emitir mensajes desde cualquier punto del planeta pueda incidir en la determinación de la legislación aplicable y la jurisdicción competente en caso de conflicto. Esto se aplica para contratos

---

interesado. Muchos autores se preguntan cuál es el momento de la aceptación, cuando llegó al servidor o cuando lo abrió la empresa. Este es un tema delicado, teniendo dos puntos de vista, uno del que envía la información y otro del que la recibe. El oferente que envía la información entiende aceptada la oferta desde el mismo momento que la envía no sintiéndose responsable si los servidores presentan algún tipo de dificultad. El otro punto de vista es de quién recibe la información quién no sabrá la decisión de la otra parte hasta tanto no reciba la información en su empresa, la pregunta es: ¿Quién pone el servicio a favor del cliente? Por ejemplo Cubatur, Agencia de Viajes receptiva, tiene un sitio web (www.cubatur.cu), con los paquetes turísticos que este ofrece; el cliente solicita y paga el servicio que escogió pero si la información no es recibida Cubatur deberá reclamar con quien tiene el contrato de servidor por no haber recibido la información. Desde mi punto de vista el momento y el lugar del consentimiento es desde que arriba a la empresa ya que será el momento en que sabrá si la oferta fue aceptada o no. La diferencia que presentan estos medios con el correo ordinario es la rapidez con que llega la información y en la forma que se ofrece el servicio, en los correos ordinarios que se utilizan para realizar contratos a distancia, la mensajería atraviesa por varias zonas postales y no es hasta que llega al destinatario no se hace efectiva la relación jurídica. Los aspectos, que hoy se cuestiona la doctrina tienen lugar precisamente porque no se encuentran definido con claridad en las diferentes legislaciones. Teniendo en cuenta que la utilización del comercio electrónico involucra a varios países sería prudente establecer normas de carácter internacional que estandaricen los aspectos polémicos y que pudieran variar en las diferentes legislaciones nacionales. La contratación tradicional siempre engendra algo de duda, sobre todo el muy analizado concepto de la buena fe en las relaciones comerciales, pero se han confeccionado normas que contrarrestan estas dudas, como es precisamente la ley de protección al consumidor. Considero que esta misma seguridad debe

entre empresas, en el caso que sea un contrato con consumidor en los cuales por regla general se establece como lugar de la formación del contrato el domicilio del consumidor.

Finalmente el contrato se entenderá perfeccionado en el momento en que el oferente tome conocimiento de la aceptación de su oferta, esto de acuerdo al sistema de recepción que establece en el Art.966 el Código de Comercio, pero de acuerdo a este sistema no es necesario que el oferente tenga un conocimiento real, si no que la aceptación se encuentre dentro de su orbita de conocimiento. El lugar de celebración del contrato será donde se hizo la oferta, o de consentir las partes lo contrario, en el lugar donde estas se sujeten, por tanto, este 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 costumbres del cada lugar

---

trasladarse a la contratación electrónica que permite mejores ventajas, teniendo en cuenta la necesidad de proteger al sujeto económico más débil de la relación contractual.

CAPITULO IV

LA FIRMA ELECTRONICA EN EL SALVADOR

SUMARIO: 4.1 Generalidades. 4.2 El Uso de la Firma Electrónica en la Administración Pública. 4.3 Ley de Simplificación Aduanera. 4.4 Ley General Marítimo Portuaria.

4.1 GENERALIDADES.

La seguridad se ha transformado en un elemento esencial en el terreno de las comunicaciones electrónicas. El comercio electrónico, el desarrollo empresarial, la Administración publica, y las comunicaciones de datos requieren de una respuesta técnica segura como la firma electrónica/ digital. En El salvador la firma electrónica va adquiriendo una presencia cada vez mayor en las transacciones en general, así como, también en la administración pública.

Actualmente en el salvador la regulación sobre la firma electrónica y su aplicación en las transacciones en general es insuficiente y escasa, aunque existe un anteproyecto de ley sobre comercio electrónico, dicho anteproyecto de ley busca ser el marco regulatorio para las transacciones realizadas a través de Internet con el fin de proteger a todas las personas que realizan sus operaciones en la web.

Como manifestamos anteriormente en el salvador no contamos con una ley especial que regule la contratación electrónica la cual aporte la confianza necesaria para que las transacciones electrónicas sean fáciles y seguras para los que realizan operaciones en la web, tengan la seguridad o confiabilidad necesaria que si se suscita un problema con trascendencia jurídica, esta contiene las pautas para solucionarlo.

El único marco legal que hace referencia sobre la contratación electrónica es el Tratado de Libre Comercio (TLC), entre Centroamérica,

Republica Dominicana y Los Estados Unidos de América. Que es ley secundaria de El Salvador[97].

En este tratado las partes se comprometieron a compartir información y experiencia sobre la firma electrónica. Republica Dominicana y Los Estados Unidos de América cuentan con leyes especiales sobre firma electrónica con lo que dejan a El Salvador en una desventaja con relación a esta materia.

4.2 EL USO DE LA FIRMA ELECTRÓNICA EN LA ADMINISTRACIÓN PÚBLICA.

La utilización de las nuevas tecnologías en el estado salvadoreño es escasa, aunque la mayoría de carteras de estado cuenta con su propio sitio web, sus paginas, mas que todo, cuentan con información general de sus actividades; a la fecha las únicas implementaciones de gobierno electrónico son la declaración de los impuestos sobre la renta que el Ministerio de Hacienda implemento desde el dos mil cuatro, con lo que facilita a todos los contribuyentes a presentar sus declaraciones mediante la pagina web de dicha identidad, y reciente se ha implementado el pago de los impuestos por vía electrónica..

El Ministerio de Hacienda, es la entidad que ha innovado en la utilización y regulación de la firma electrónica a través de la Ley de Simplificación Aduanera, que es empleada en el intercambio de información, particularmente en la declaración de mercancías, el pago de impuestos aduanales mediante el sistema de teledespacho. Este sistema

[97] Vid. GRANILLO DE TOBAR, ANA YESSENIA, *La Firma Electrónica, su uso en el ámbito de la Contratación Electrónica...,* Cit., Pág. 25. Las partes reconocieron en el Capitulo catorce, denominado “comercio electrónico”, que este ultimo genera crecimiento económico y oportunidad, por tal razón, las partes se han comprometido a no gravar con impuestos internos, directa o indirectamente los productos digitales por transmisión electrónica. Para alcanzar los objetivos propuestos en el TLC, las partes además se comprometieron a trabajar en conjunto con la finalidad de superar obstáculos compartir información en áreas básicas del comercio electrónico, incluyendo la firma electrónica.

aporta ventajas a los importadores nacionales. Agilizando en gran medida el procesamiento de información para la importación de mercadería; los importadores nacionales son los primeros en utilizar la firma electrónica con la que aseguran la autenticidad de la información transmitida a la dirección de aduanas[98].

También el Centro Nacional de Registro de El Salvador y el Colegio de registradores de España firmaron un acuerdo de asistencia técnica con el objetivo de implementar en el salvador el uso de la firma electrónica; con el que se espera conceder seguridad jurídica a las transacciones[99].

Es posible que en un futuro próximo la firma electrónica pueda ser utilizada o implementada por toda la administración, y así poder aprovechar todos los benefició que de esta se derivan.

Finalmente es verdad que no contamos, en El Salvador con una ley que regule la firma electrónica de forma general, sin embargo si se cuenta con decretos que prevén el uso de la firma electrónica. A continuación nombraremos algunos de estos decretos.

---

[98] Vid. GRANILLO DE TOBAR, ANA YESSENIA, *La Firma Electrónica, su uso en el ámbito de la Contratación Electrónica...,* Cit., Pág. 28. La Ley de Simplificación Aduanera es la primera regulación que se ha creado acerca del empleo de la firma electrónica en el salvador, la cual ha sentado las bases del sistema criptográfico empleado, el régimen de las Entidades de Certificación, los efectos del Documento Electrónico, entre otros.

[99] Vid. GRANILLO DE TOBAR, ANA YESSENIA, *La Firma Electrónica, su uso en el ámbito de la Contratación Electrónica...,* Cit., Pág. 29. La autorización para ejercer la Función Notarial, al menos por el momento, no incluye la funciones de certificación de Firmas Digitales, como consecuencia lógica de la ausencia de regulación de dicho tema, esto no obsta para que el legislador salvadoreño puede contemplar la posibilidad de conceder la función de certificación de firmas digitales a los notarios, mas aun si tomas en cuenta que el impulso así los nuevos tipos de contratación vienen representados por el TLC antes señalado y por la intención del registro salvadoreño de hacer uso de la firma electrónica.

4.3 LEY DE SIMPLIFICACIÓN ADUANERA (DECRETO LEGISLATIVO Nº 529, PUBLICADO EN EL DIARIO OFICIAL Nº23, TOMO 342, DE 3 DE FEBRERO DE 1999.)

La finalidad de la Ley, es de adecuar los servicios aduaneros a los estándares mundiales de calidad y eficiencia en términos de facilitación del comercio internacional, control de recaudación fiscal y protección de la sociedad, así como también, la implementación de un marco legal moderno que permita las nuevas modalidades de despacho y la adopción de mecanismos de simplificación, facilitación y control de las operaciones aduaneras que otorguen ventajas competitivas a los productores nacionales[100].

La Ley de Simplificación Aduanera regula la utilización de la firma electrónica. Sin embargo, el terreno de aplicación de esta es limitado exclusivamente al división de aduanas sea esta terrestre, marítima o aérea. Los transportistas o los agentes de transporte están obligados a proporcionar a la aduana, mediante transmisión electrónica, la información contenida en el manifiesto general de carga[101].

El Sistema de Teledespacho consiste en el flujo o transferencia de datos en forma electrónica, el cual debe estar estructurado por procedimientos que aseguren la autenticidad, confidencialidad, integridad y no repudiación de la información transmitida[102].

---

[100] Ley de Simplificación Aduanera, Republica de El Salvador, Decreto Legislativo Nº 529, del 13 de enero de 1999, Publicado en el Diario Oficial Nº23, Tomo 342, del 3 de Febrero de 1999.

[101] Vid. Art.2 de la Ley de Simplificación Aduanera.

[102] htt://www.diescoean.com.sv. Visitada el 22 de noviembre de 2008. Para el sistema de TELEDESPACHO POR INTERNET, se ha implementado el uso de la Firma Electrónica Y Certificados Digitales con el objetivo de asegurar las transacciones electrónicas de dicho proyecto. Estos mecanismos de seguridad nos permiten asegurar 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 con las siguientes características de seguridad: No repudio, autenticación e integridad del emisor del mensaje. Esto le da la certeza al receptor de que quien firma y envía, es quien dice ser, por lo tanto no se puede hacer a nombre de un tercero. Adicionalmente este mensaje firmado se codifica (cifra) para que viaje por Internet en un lenguaje en que solo las partes involucradas podrán entenderlo.

Así como también, constituye el "*conjunto sistemático de elementos tecnológicos de carácter informático y de comunicación 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 controladoras del comercio exterior*"[103]; es decir, regula a todos los intervinientes que participan en el intercambio de información electrónica.

Encontramos una definición legal de firma electrónica en el Art.8 Inc.3 "*una pareja de llaves o llaves únicas y correspondientes entre si, una publica y una privada, de manera tal que ambas se correspondan de manera exclusiva y excluyente. La vinculación de ambas llaves o clases constituye la Firma Digital o Electrónica, que para todos los efectos legales se constituye en el sustituto digital de la firma manuscrita*"[104]; La cual otorga seguridad al intercambio electrónico de datos.

La ley también hace referencia a las Entidades de certificación o certificadoras llamadas en adelante entidades de certificación. Establece que ha efectos de garantizar la autenticidad, confidencialidad e integridad

---

[103] Vid. htt://www.diescoean.com.sv. Visitada el 22 de noviembre, Desde Octubre de 2002, con el objetivo de facilitar al Usuario de TELEDESPACHO (trámites electrónicos de importación) el poder realizar una Orden de Pago de los impuestos de Importación desde su oficina, y así evitar tener que enviar a alguien a certificar cheques para poder retirar la mercadería en las diferentes aduanas del país, el Ministerio de Hacienda tuvo a bien contratar los servicios de consultoría GS1 El Salvador , para el desarrollo de una Plataforma de Pago Electrónico de Impuestos, en adelante TELEPAGO. Desde Febrero de 2003, TELEPAGO cuenta con la participación de 7 Bancos: BANCO CUSCATLÁN ahora del grupo Citibank, BANCO SALVADOREÑO ahora HSBS, BANCO AMERICANO, CITIBANK, BANCO DE COMERCIO (BanCo), ahora scotiabank, Banco Agrícola y Banco Promérica.

[104] Vid. Art.8 Inc.3 de la Ley de Simplificación Aduanera. Cit., en este articulo se ve reflejado el principio de equivalencia funcional, en el sentido en que equiparar a la firma electrónica o digital con la firma manuscrita, otorgándole a la primera los mismos efectos legales, validez y eficacia que la segunda.

de la información e impedir su ulterior rechazo, se establece el sistema de certificación.

La ley faculta para que personas jurídicas puedan ofrecer los servicios de certificación de dicha información; pero se requiere que estas estén capacitadas tecnológicamente para prestar servició de generación y certificación de firmas, y además deben cumplir con todos los requisitos legales y reglamentarios para poder operar y una vez autorizadas para iniciar sus operaciones estas entidades están dotadas de la potestad de otorgar fe publica con respecto a que en una fecha y hora determinada, personas especificas realizaron una transmisión electrónica de datos en determinados términos, y es el Ministerio de Hacienda el ente licitante de entidades de certificación y entre sus facultades se encuentra la de autorizar para operar, la fiscalización y facultades sancionatorias relaciones con las entidades certificadoras, en tanto no se dicte una Ley que regule de manera general todos los aspectos relacionados con el comercio electrónico será el Ministerio de Hacienda quien ejerza esas potestades entre otras.

4.4 LEY GENERAL MARÍTIMO PORTUARIA DECRETO LEGISLATIVO Nº: 994 DE 19 DE SEPTIEMBRE DE 2002, PUBLICADA EN EL DIARIO OFICIAL Nº 182 TOMO 357 DE 1 OCTUBRE DE 2002.

Esta ley también otorga soporte legal al uso de la firma electrónica en la en la actividad portuario marítima. La Ley General Marítimo Portuaria en su capitulo x bajo el titulo denominado "*Régimen de Responsabilidad de los Armadores"* confiere a los armadores responsabilidades entre las que se encuentra el emitir al momento de recibir la mercancías la documentación necesaria por escrito en donde se identifiquen las mercancías recibidas y acuse recibo de su recepción. Se establece que para la emisión del documento podrá utilizarse cualquier

medio por el quede constancia de la información que contenga la información emitida.

Y si el usuario y el armador o transportador acordado comunicarse electrónicamente, dichos documentos podrán ser sustituidos por un mensaje de intercambio electrónico de datos, de igual forma establece que la firma, podrá ser manuscrita o bien estampada mediante facsímiles o autenticada por un código electrónico[105].

[105] Art. 90 de la Ley General Marítimo Portuaria de El Salvador, Intercambio electrónico de datos, para la emisión de los documentos a que es 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 sustituido por un mensaje de intercambio electrónico de datos. La firma podrá ser manuscrita, o bien estampada mediante facsímile o autenticada por un código electrónico.

CAPITULO V

LA FIRMA ELECTRONICA A NIVEL INTERNACIONAL Y EN EL DERECHO COMPARADO

SUMARIO: 5.La firma Electrónica en el contorno comunitario Europeo. 5.1 Breve referencia sobre la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho mercantil Internacional (CNUDMI) sobre las Firmas Electrónicas (2001). 5.2 Breve comentario sobre la Legislación de firma electrónica en Estados Unidos de Norteamérica**.** 5.3 Firma Electrónica en el Derecho Comparado, breve comentario de algunas legislaciones que regulan el uso y la aplicación de la Firma Electrónica.

5. LA FIRMA ELECTRÓNICA EN EL CONTORNO COMUNITARIO EUROPEO

La directiva 1999/93 del Parlamento Europeo [106] y del Consejo de 13 de diciembre de 1999 con la que se establece un marco jurídico comunitario sobre la firma electrónica por medio de la cual se establecen lineamientos generales y comunes para todos los países miembros, el objetivo principal de esta legislación es armonizar todas las leyes referentes a la firma electrónica.

Esta ley establece los criterios para el reconocimiento de la firma electrónica cuya principal disposición es que se reconozca la firma electrónica avanzada en un certificado reconocido equivale a una firma manuscrita y por tal razón debe ser admisible como prueba

[106] http://www.delitosinformaticos.com/firmaelectronica/analisis2.shtml. Visitada el 13 de diciembre sobre firma electrónica a nivel mundial visitada el 15 de diciembre de 2008.

Así mismo, La unión europea emitió en junio la llamada directiva 2000/31/CE del Parlamento Europeo y del Consejo de 2000 Relativa a Determinados Aspectos Jurídicos de los Servicios de la Sociedad de la Información, en particular el Comercio Electrónico en el mercado interior. El fin principal de este cuerpo normativo es garantizar una integración jurídica comunitaria cada vez más estrecha con el objeto de abrir espacio autentico sin fronteras interiores entre los Estados y los puebles europeos para eliminar las barreras que los dividen y así asegurar el progreso económico y social.

5.1 BREVE REFERENCIA SOBRE LA LEY MODELO DE LA COMISIÓN DE LAS NACIONES UNIDAS PARA EL DERECHO MERCANTIL INTERNACIONAL (CNUDMI) SOBRE LAS FIRMAS ELECTRÓNICAS (2001)

En 1997 a iniciativa de UNCITRAL se aprobó la Ley Modelo de comercio electrónico el 16 de diciembre de 1996 esta ley fue la consecuencia del creciente empleo de medios modernos de comunicación para la realización de las operaciones comerciales internacionales cuando estas comunicaciones tuvieran cierta relevancia Jurídica en forma de mensajes de datos, sin soporte papel podrían verse estos obstaculizados por algunos impedimentos legales al empleo de mensaje de datos, o por la incertidumbre que estos pudieran generar sobre la validez Jurídica de esos mensajes. Esta ha servido de base al desarrollo normativo en este ámbito[107].

De igual manera la asamblea de la ONU, decretó la ley modelo sobre firma electrónica el 24 de marzo de 2002, la cual se hace

[107] http://www.delitosinformaticos.com/firmaelectronica/analisis2.shtml. Visitada el 13 de diciembre. Los avances de la legislación *Considerando que la elaboración de legislación modelo que facilite la utilización de las firmas electrónicas de forma que sea aceptable para Estados con distintos ordenamientos jurídicos, sociales y económicos podría contribuir al fomento de relaciones económicas armoniosas en el plano internacional,*

acompañar de una guía para la incorporación al derecho interno, la ley modelo es la base para equilibrar las legislaciones a nivel internacional, aunque esta no es obligatoria para los estados. Los objetivos de la Ley Modelo, entre los que figuran el de permitir o facilitar el empleo de firmas electrónicas y el de conceder igualdad de trato a los usuarios de documentación consignada sobre papel y a los de información consignada en soporte informático, son fundamentales para promover la economía y la eficiencia del comercio internacional

5.2 BREVE COMENTARIO SOBRE LA LEGISLACIÓN DE FIRMA ELECTRÓNICA EN ESTADOS UNIDOS DE NORTEAMÉRICA.

la primera ley en materia de firma digital que fue aprobada en el mendo es la llamada "*Utah Digital Signature Act"* publicada en mayo de 1995. Este estado fue el primero en legislar el uso comercial de la firma digital, regulando el uso de la criptografía asimétrica, además esta ley tiene como finalidad facilitar la realización de transacciones por medio de mensajes electrónicos firmados electrónicamente.

Siendo esta ley una empuje, posteriormente se emite en Estados Unidos la Ley Federal sobre Firmas Electrónicas denominada "*Electronic Signatures in Global and National Commerce Act*"; conocida también como: *E-sign A ct.* Esta fue aprobada el 30 de junio de 2000, y entro en vigencia el 1 de octubre de 2000.

Esta ley otorga a la firma y al documento electrónico un valor legal equivalente al de la firma autógrafa y al documento en papel, así mismo, reviste de validez a todos los actos y transacciones que se realizan por medios electrónicos, es decir ninguna ley, reglamento o norma podrá negarle valor legal por el simple hecho que su firma esta en forma electrónico.

5.3 FIRMA ELECTRÓNICA EN EL DERECHO COMPARADO, BREVE COMENTARIO DE ALGUNAS LEGISLACIONES QUE REGULAN EL USO Y APLICACIÒN DE LA FIRMA ELECTRONICA.

Actualmente la mayoría de países de Europa cuentan con una legislación aprobada en materia de firma electrónica entre los que podemos enunciar se encuentra: Italia, España, Alemania, Portugal, Francia, Suecia, Dinamarca entre otros. Al respecto haremos referencia a algunas legislaciones de Europa que regulan la firma electrónica.

En el caso de **España** la Ley 30/1992 de 26 de noviembre de 1992 del Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo común sentó las primeras bases para facilitar el uso de las nuevas tecnologías en las relaciones entre los ciudadanos y la administración.

Pero con la aprobación de la Ley 66/1997 de 30 de diciembre, con esta aparece el primer indicio de lo que podría ser el despliegue de una infraestructura de clave pública, esta Ley atribuye a la Fabrica Nacional de Monedas y Timbres-Real llamada también casa de la moneda, como el ente encargado de prestar servicios de certificación[108].

Finalmente se llega a la aprobación del Real Decreto-Ley 14/1999 sobre Firma Electrónica de 17 de septiembre de 1999. Con esta normativa da inicio el Estado Español a leyes relativas a la firma electrónica consciente de la necesidad de aprobar un marco jurídico básico regulador de los aspectos más urgentes de la materia, España promulgo tres meses antes el Decreto Ley 14/1999 sobre Firma Electrónica con lo que se anticipó a Directiva Europea que regularía sobre la firma electrónica para todos los partes de la Unión Europea.

---

[108] http://www.delitosinformaticos.com/firmaelectronica/analisis2.shtml Avances de la legislación sobre firma electrónica a nivel mundial. Visitada el 25 de diciembre de 2008.

Esta Ley fue aprobada con el fin de fomentar el rápido uso de las nuevas tecnologías de seguridad de las comunicaciones electrónicas, con lo que se esperaba acelerar el crecimiento económico, pero más que todo se buscaba crear un marco normativo que aportara confianza en las transacciones electrónicas realizadas en redes abiertas como el Internet. Por su parte también se regula el uso de la firma electrónica, se reconoce su eficacia jurídica y se regula prestación al público de los servicios de certificación.

Sin embargo la anterior Ley fue reemplazada por el Real Decreto Ley 59/2003 relativo a la firma electrónica el cual fue aprobado el 19 de diciembre de 2003, de firma electrónica con la que se sustituye la anterior Ley 14/1999 relativa al mismo tema, en esta nueva legislación encontramos nuevos conceptos, evolución en algunos ya existentes, además trae dos novedades importantes dos figuras que no regula la anterior ley.

Una de las novedades de la nueva ley española es la creación del DNI electrónico (Documento Nacional de Identidad Electrónico) por medio del cual, se busca que todos los ciudadanos puedan emitir firmas electrónicas certificadas por el estado. Con lo cual, el ciudadano podrá realizar tramites administrativos, transacciones electrónicas y tramites en la banca on-line.

Así mismo otra novedad es la regulación de los certificados de personas jurídicas, en todo caso los certificados electrónicos a personas jurídicas no alteran la legislación civil o mercantil en cuento a la figura del representante, esto se ve como un gran paso para la seguridad jurídica entre empresas.

Por su parte **Italia** fue el primer país de Europa que dicto una regulación sobre firma electrónica y lo hizo con el "*Regolamento contenenete modalite di aplicazione del articolo 15"*; de la ley de 15 de

marzo de 1997, numero 59, esta disposición se refiere a la creación de un reglamento sobre acto, documento y contrato en forma electrónica esta reglamento de aplicación regula el concepto de firma electrónica, la que esta formada por un par de claves asimétricas, también regula el uso de los certificados y establece la validez y eficacia de los documentos electrónicos

Este reglamento no regula a los prestadores de servicios de certificación solo los definir como sujetos públicos y privados, que son los encargados de certificar y guardar las claves públicas entre otras atribuciones.

En el caso de **Alemania** se promulgo la Ley sobre Firmas Digitales el 13 de junio de 1997, esta ley posee un cuerpo breve y conciso de 16 artículos el objetivo de esta ley es la creación de las condiciones generales para el uso seguro de la firma digital, sin embargo esta ley fue sustituida por la ley de 16 de mayo de 2001, con esta nueva ley se adecua a los parámetros establecidos por la Comunidad Europea con lo que se busca que los estados miembros establezcan normativas sobre firma electrónica que sean uniforme entre ellos para que no hayan barreras dentro del mercado común llamado ahora mercado interior.

Latinoamérica por su parte no se queda atrás, países como Colombia, Perú, Venezuela, Argentina, México, Guatemala entre otros. Cuentan ya con una legislación que regula la aplicación de la firma electrónica algunos han dictado leyes especiales y otros solo han realizado reformas a la normativa existente. Al respecto haremos referencia a alguna de las legislaciones que regulan la firma electrónica.

Perú [109] por su parte, aprobó el decreto legislativo numero 681 del 14 de octubre de 1991, el cual fue sustituido posteriormente por la ley

[109] http://www.comunidad.derecho.org. Visitada ele 29 de diciembre de 2008.

numero 26612 de 21 de mayo de 1996, con estas normativas se cimentaron las bases de la contratación electrónica, así también permiten el uso de los documentos electrónicos con pleno valor probatorio.

Más tarde se aprobó la Ley número 27269 del 26 de mayo de 2000, denominada Ley de Firmas y Certificados Digitales con esta ley Perú dio un paso importante en la regulación de las medidas técnicas de seguridad. Posteriormente se aprobó la Ley 27291 del 24 de junio de 2000, con dicha ley se modifican algunos artículos del Código Civil de Perú, con lo que se regula el uso de los medios electrónicos para la utilización de los medios electrónicos para la comunicación de la voluntad y el uso de la firma electrónica.

En el caso de **Venezuela** se promulgo la Ley Sobre Mensajes de Datos y Firmas Electrónicas de Venezuela fue publicada en la Gaceta Oficial de la República Bolivariana de Venezuela Nº 37.148 de fecha 28 de Febrero de 2001 quedando identificada como Decreto Ley Nº 1204.con la que se establece la necesidad de otorgar validez y reconocer certeza jurídica al mensaje de datos, a la firma electrónica y a toda información inteligible en formato electrónico, independientemente de su soporte material que pueda ser atribuida a personas naturales o jurídicas, públicas o privadas, así como regular todo lo relativo a los Proveedores de Servicios de Certificación y los Certificados Electrónicos.

El marco normativo de la República **Argentina**[110] en materia de Firma Digital está constituido por la Ley numero 25506 14 de diciembre de 2001 denominada ley sobre firma digital, el Decreto Nº 2628 de 20 de diciembre de 2002, el Decreto numero 724 que modifica al anterior de 13 de junio de 2006 y un conjunto de normas complementarias que fijan o modifican competencias y establecen procedimientos.

[110] http://www.comunidad.derecho.org. Visitada el 29 de diciembre de 2008.

Para la legislación argentina los términos "Firma Digital" y "Firma Electrónica" no poseen el mismo significado. La diferencia radica en el valor probatorio atribuido a cada uno de ellos, dado que en el caso de la "Firma Digital" existe una presunción "*iuris tantum*" en su favor; esto significa que si un *documento firmado digitalmente* es verificado correctamente, se presume *salvo prueba en contrario* que proviene del suscriptor del certificado asociado y que no fue modificado. Por el contrario, en el caso de la *firma electrónica*, en caso de ser desconocida la firma por su titular corresponde a quien la invoca acreditar su validez.

La legislación argentina emplea el término "Firma Digital" en equivalencia al término "Firma Electrónica Avanzada" o "Firma Electrónica Reconocida" utilizado por la Comunidad Europea o "Firma Electrónica" utilizado en otros países como Brasil o Chile.

En **Colombia** se emitió la ley 527 de 1.999, llamada Ley de Comercio Electrónico, el objetivo central de la ley es otorgar pleno valor probatorio a los mensajes de datos, como denomina la ley a la información digital. Hoy en día no se le pueden negar efectos jurídicos, validez o fuerza obligatoria a información alguna por el solo hecho de estar en forma de mensajes de datos. La información que se encuentra almacenada en un formato digital tiene el mismo valor jurídico que la información que se consigna en hojas de papel o en cualquier otro soporte escrito

Esta ley en la parte general hace definiciones de conceptos básicos usados en la ley, dentro de los que cabe destacar los de mensaje de datos, comercio electrónico, firma digital, y entidad de certificación. La ley 527 se aplica de manera general a todo tipo de relaciones jurídicas, y no sólo a relaciones jurídicas comerciales. Por ejemplo, se aplica a las relaciones jurídicas entre los particulares y el Estado, incluyendo los trámites administrativos ante autoridades públicas.

Con el fin de reglamentar el funcionamiento de las entidades de certificación digital a que se refirió la ley 527 de 1999, el Gobierno Nacional expidió el Decreto numero 1747 de 11 de septiembre de 2000, este distingue entre Entidades de Certificación Cerradas y Entidades de Certificación Abiertas: Los certificados digitales que expiden las primeras deben ser gratuitos y sólo pueden ser usados para las comunicaciones entre el suscriptor y la entidad de certificación. Por el contrario, los certificados digitales de las entidades de certificación abierta se pueden utilizar para cualquier tipo de comunicación, independientemente de su remitente o destinatario.

En el caso de **México** el 29 mayo de 2000 se publicaron reformas al código de comercio, a la ley federal de protección al consumidor y al código civil federal con dichas reformas se proyectaba establecer un marco jurídico cuyo principal objetivo era otorgar seguridad en las transacciones comerciales realizadas por medios electrónicos o digitales, posteriormente el 29 de agosto de 2003 entro en vigencia un decreto que consiste en reformas y adiciones al código de comercio modificándose el titulo segundo denominado ”comercio electrónico”, el capitulo primero denominado “de los mensajes de datos”, capitulo segundo titulado “de las firmas electrónicas” y un capitulo tercero titulado “de los prestadores de los servicios de certificación. Con el objetivo de crear un marco jurídico cada vez más apropiado para la segura aplicación de la firma electrónica.

En el caso de Centroamérica Uno de los avances más importantes para la región es la ley emitida en el congreso de **Guatemala** sobre la aprobación del uso de la firma electrónica algo que no tenía validez como en otros países. La ley entrara en vigor en el mes de octubre de 2008 y permitirá a personas individuales, empresas y/o organizaciones adquirir su firma electrónica sin ningún problema, recordemos que la firma

electrónica se obtiene de datos del individuo y/o datos de la empresa para generar mediante un algoritmo un resultado encriptado. Por el momento solo la sección de Coordinación de Desarrollo del Comercio Electrónico de la Cámara de Comercio de Guatemala (CCG) esta emitiendo dichos datos digitales**.**

Con lo que se fortalecen las comunicaciones digitales en Guatemala. Por su parte, Costa Rica no se queda atrás el 30 de agosto de 2005 se emitió la ley de Certificados, Firmas Digitales y Documentos Electrónicos el objetivo de estas leyes es un mejor control y seguridad para las transacciones y gestiones en Internet, con la aprobación de estas leyes en territorio Centroamericano se da un paso bastante interesante para encaminar a todos los países de la región en la brecha digital[111].

[111] Vid. http://www.delitosinformaticos.com/firmaelectronica/analisis2.shtml. Visitada el 13 de diciembre de 2008.

CAPITULO VI

SEGURIDAD JURIDICA, FIRMA ELECTRONICA Y PRESTADORES DE SERVICIOS DE CERTIFICACIÓN

SUMARIO: 6. Seguridad jurídica. 6.1 La Criptografía y la Firma Electrónica. 6.1.1 La Criptografía. 6.1.2 Sistema de Clave Simétrica 6.1.3 Ventajas y Desventajas del sistema Simétrico. 6.1.4 Sistema Criptográfico Asimétrico. 6.1.5 Ventajas y Desventajas del Sistema Asimétrico o de Clava Publica.- 6.1.6 Combinación de los Sistemas de Clave simétrica y de Clave Asimétrica o Publica.- 6.1.7 Empleo de los Algoritmos Hash.- 6.1.8 Procedimiento Utilizado para la Aplicación de la Firma Digital.- 6.2. Clases de Firmas.- 6.2.1. Características de la Firma Electrónica o Digital.- 6.3. Principios de la Firma Electrónica.- 6.4. El Papel que Juegan los Prestadores de Servicios de Certificación en el Proceso de Aplicación de la Firma Electrónica.- 6.5. Generalidades de las Entidades de Certificación.- 6.5.1 Componentes Técnicos.- 6.5.2 Vigencia de los Certificados.- 6.5.3 Definición de las Entidades de Certificación.- 6.6 Procedimiento para Generar un Certificado Digital.- 6.6.1. Contenido de los Certificados.- 6.7 Naturaleza Jurídica de las Entidades de Certificación.- 6.8 Funciones de las Entidades de Certificación.- 6.9 Clasificación de los Certificados.- 6.10 Importancia de las Entidades de Certificación. 6.10.1 Certificados de Seguridad Electrónica; 6.10.2 Certificados de Seguridad en Comunicación; 6.10.3 Certificados de Información entre las partes.- 6.11 Principios Generales para la Prestación de Servicios de Certificación. 6.11.1 Régimen de Libre Competencia; 6.11.2 Sistema de Acreditación de Servicios de Certificación; 6.11.3 Registro de Servicios de Certificación.- 6.12 Obligación de los Prestadores de Servicios de Certificación. 6.12.1 Obligaciones Generales; 6.12.2 Obligaciones Especificas.- 6.13 Requisitos de las Entidades Certificadoras. 6.13.1 Requisito Temporal; 6.13.2 Requisitos Técnicos y de Personal; 6.13.3 Requisitos Económicos; 6.13.4 Requisitos Informáticos y de Documentación.- 6.14 Responsabilidad de las Entidades de Certificación. 6.14.1 Responsabilidad Civil; 6.14.2 Responsabilidad Civil por el uso Indebido de parte de Terceras Personas de las entidades de Certificación.

6. LA SEGURIDAD JURIDICA

La seguridad es el valor que fundamenta la construcción de las "*Reglas de Juego",* es decir, reglas claras, dentro del estado constitucional. El ordenamiento jurídico salvadoreño no recoge una definición determinada del concepto seguridad jurídica[112].

---

[112] Guillermo Cabanellas, *en su Diccionario Enciclopédico de Derecho Usua*l, tomo VII, Pág. 312. dice: Seguridad Jurídica.: La estabilidad de las instituciones y la vigencia auténtica de la ley, con el respeto de los derechos proclamados y su amparo eficaz, ante desconocimientos o trasgresiones, por la acción establecedora de la justicia en los supuestos negativos, dentro de un cuadro que tiene por engarce al Estado de Derecho.

Por ende diremos que la seguridad jurídica es el conjunto de todas las reglas jurídicas que el Estado asegure a las partes que entran en una relación jurídica contractual[113], en lo relativo a la creación del contrato, la validación del contrato, la validez del contenido contractual, la confidencialidad y la posibilidad de prueba de dicho contrato.

Al respecto la seguridad jurídica en el Derecho Civil, es decir, en las relaciones contractuales convencionales guarda estrecha relación con la cuestión de saber si el contrato da fe realmente entre las partes en el sentido jurídico.

El Derecho Civil da respuesta a los elementos del sistema de seguridad jurídica que rigen la creación del contrato y su contenido. Por medio de un conjunto de elementos que garantizan dicha seguridad. Como por ejemplo uno de los elementos de la seguridad jurídica es el de la forma, las partes para escapar de la sanción de nulidad deben de respetar una forma determinada (como por ejemplo la compraventa de un bien inmueble debe recogerse en escritura publica ante notario).Otro elemento para garantizar la seguridad en el mundo del papel es el sistema de registro, las partes cumplen estos requisitos en las relaciones contractuales convencionales para dar certeza y garantizar la seguridad en el mundo del papel.

---

[113] Armando Arias, presidente de la Cámara Americana de Comercio de El Salvador, explicó las condiciones mínimas que el país debe ofrecer a los inversionistas extranjeros para lograr que El Salvador tenga un desarrollo social y económico. *"Que prevalezcan las reglas y leyes claras", dijo Arias al comenzar a desglosar algunos de los aspectos evaluados por los inversionistas para decidir llegar a El Salvador o cualquier otro país. "Le tememos a reglas y normas no consensuadas y analizadas*", agregó en el punto de la **seguridad jurídica**, una de las características que más pesan al momento de que un inversionista decida donde quedarse. Arias subrayó la agilidad en procesos. Y la seguridad jurídica que las leyes de cada país puedan ofrecer a los empresarios y consumidores este en el plano del comercio tradicional, ya no digamos en el comercio electrónico donde las transacciones son transfronterizas y por redes abiertas.

En este sentido y como nuestro estudio esta dirigido a la seguridad jurídica de la contratación electrónica, entorno a esa idea desarrollaremos el siguiente apartado.

En la actualidad Internet es un sistema de información transfronterizo en el que se comercializa a escala mundial, y por lo tanto, estas comunicaciones y transacciones comerciales pueden realizar tanto en el sector público, privado y en el ámbito nacional e internacional.

Por otra parte, con el auge de la denominada revolución tecnológica, todavía se refleja una considerable sensación de inseguridad en las transacciones electrónicas por partes de las personas. En definitiva agilizar y facilitar la expansión del comercio electrónico y por ende de las transacciones por medios electrónicos sin garantizar la seguridad no favorece su desarrollo.

Desde un punto de vista jurídico la contratación electrónica, es un contrato a distancia que tiene notas peculiares, como que la información circula por canales abiertos en donde todos pueden tener acceso a ella, por esa razón, es importante adoptar medidas de seguridad que garanticen la confidencialidad y la identidad de quien emite el mensaje, además la contratación electrónica es sin presencia personal y sobre condiciones generales a efecto se requieren medidas normativas que aseguren una debida formación en la voluntad contractual.

Es importante tener en cuenta que la seguridad es uno de los valores más deseados y es importante que en las redes abiertas y fundamentalmente internet puedan alcanzar ese grado de certeza y confianza para crear una atmosfera segura con la cual se posibilite el aumento de las transacciones electrónicas pero esto no puede ser posible si el derecho no regula las transacciones realizadas por redes abiertas, lo

cual es fundamental para generar la seguridad jurídica necesaria que posibilite la realización de negocios por este medio. Por ello es imprescindible la búsqueda de la seguridad desde un doble punto de vista tanto técnico, como jurídico.

Finalmente para que haya seguridad jurídica, es necesario contar con un cuerpo normativo que regule los medios técnicos (como la firma electrónica) creados para garantizar y dar seguridad al tráfico comercial. Además, la seguridad jurídica como uno de los fines del derecho también es uno de los objetivos esenciales del derecho informático

6.1 LA CRIPTOGRAFIA Y LA FIRMA ELECTRONICA.

La criptografía es el elemento sustancial para que la implementación de la firma electrónica produzca la seguridad necesaria para garantizar las transacciones electrónicas, al respecto, en este apartado estudiaremos los elementos de la criptografía que son utilizados para la creación de la firma electrónica y se abordaran los sistemas mas utilizados para el uso de la misma.

Es elemental comprender en qué consiste la firma electrónica aunque para ello se deba hacer un estudio meramente técnico y no jurídico, trataremos de explicar de una manera sencilla el proceso de la firma electrónica y de todos los elementos anexos a los técnicas criptográficas. Es decir, toda una serie de medidas complementarias que son básicas para que el proceso en su conjunto se verdaderamente operativo.

En definitiva se debe destacar la importancia de las entidades de certificación como tercera parte de confianza las cuales actúan para asegurar el proceso de envió y la recepción del mensaje de datos a través de Internet cuando estos están firmados electrónicamente.

6.1.1 LA CRIPTOGRAFÍA.

La criptografía[114] es la ciencia que estudia los procedimientos que hacen opacos o ininteligibles los mensajes para aquellas personas que no conocen las claves utilizadas. "*La criptografía utiliza generalmente un algoritmo matemático para cifrar datos para hacerlos ininteligibles para aquellas persona que no conozca el procedimiento, ni la clave criptográfica necesaria para descifrar los datos cifrados".*

Actualmente la criptografía es utilizada para realizar el proceso de encriptación y descriptación de la firma digital. Utilizando un algoritmo matemático para cifrar la información y trasformar un texto claro en uno ininteligible, de acuerdo, aun procedimiento y utilizando una clave determinada para descifrar, pretendiendo que solo quien conoce dicha clave pueda acceder a la información original; evitando así que personas ajenas conozcan la información[115].

---

[114] Vid. MARTÍNEZ NADAL, APOL·LÒNIA, *Comercio Electrónico, Firma Digital Y Autoridades de Certificación....,* *Cit.,* Pág. 45. La Criptografía es la ciencia que se ocupa de transformar mensajes aparentemente ininteligibles y devolverlos a su forma original. L a criptografía se ha usado durante siglos y ha sido especialmente útil durante las guerras. El uso de la criptografía moderna basada en medios informaticos, comenzó durante la segunda guerra mundial. Y el desarrollo del comercio electrónico ha provocado actualmente la difusión del uso de técnicas criptográficas para fines no bélicos ni militares. Criptografía es la ciencia de la seguridad de la información aunque muchas veces ha sido descrita como el arte o la ciencia de la escritura secreta. La criptografía es la ciencia de usar las matemáticas para encriptar y desencriptar datos. Una vez que la información ha sido encriptada, puede ser almacenada en un medio inseguro o enviada a través de una red insegura (como Internet) y aún así permanecer secreta. Luego, los datos pueden desencriptarse a su formato original. Por medio de ella se puede almacenar o transmitir información en una forma tal que permite ser revelada únicamente a aquellos que deben verla. La palabra viene del griego kryptos, que significa "oculto". La criptografía está relacionada con el criptoanálisis, que es la práctica de violar los intentos de esconde información y es parte de la criptología, donde se incluye la criptografía y el criptoanálisis. El origen de la criptografía data de el año 2000 AC., con los egipcios y sus jeroglíficos. Los jeroglíficos estaban compuestos de pictogramas complejos, donde sólo el significado completo podría ser interpretado por algunos. El primer indicio de criptografía moderna fue usado por Julio César (100 AC. a 44 AC.), quien no confiaba en sus mensajeros cuando se comunicaba con los gobernadores y oficiales. Por esta razón, creó un sistema en donde los caracteres eran reemplazados por el tercer carácter siguiente del alfabeto romano. No solo los romanos, sino los árabes y los vikingos hicieron uso de sistemas de cifrado. Gabriel de Lavinde hizo de la criptografía una ciencia más formal cuando publicó su primer manual sobre Criptología en 1379. Samuel Morse. El Código Morse, desarrollado en 1832, aunque no es propiamente un código como los otros, es una forma de cifrar las letras del alfabeto dentro de sonidos largos y cortos.

[115] VILLAR, JOSE MANUEL, "*Una Aproximación a la Firma Electrónica", en AA VVV* Derecho de Internet, Contratación Electrónica y Firma Digital, Coordinado por Mateus de Ros, Rafael y Cendoya Méndez de Vigo Juan Manuel, Editorial Aranzandi, Navarra, Madrid, 2000, Pág. 170. La

Los sistemas criptográficos aplicados a la firma electrónica y digital son: Sistema de clave simétrica, sistema de clave asimétrica y por ultimo una combinación de ambos sistemas llamado Sistema criptográfico mixto o combinado.

6.1.2 SISTEMA DE CLAVE SIMÉTRICA[116].

Este sistema es llamado así por que las partes que intervienen en el mensaje tanto emisor y receptor utilizan la misma clave para cifrar coma la descifrar el mensaje enviado[117], es decir, utilizan una clave común anteriormente conocida por ambos.

Las principales desventajas del sistema simétrico son la distribución de las claves, el peligro de que muchas personas deban conocer una misma clave y la dificultad de almacenar y proteger muchas claves diferentes.

Esta clave se debe intercambiar entre los equipos por medio de un canal seguro en el caso de internet no es un canal seguro de comunicación por tanto este sistema no es apropiado para soportar fiemas electrónicas.

---

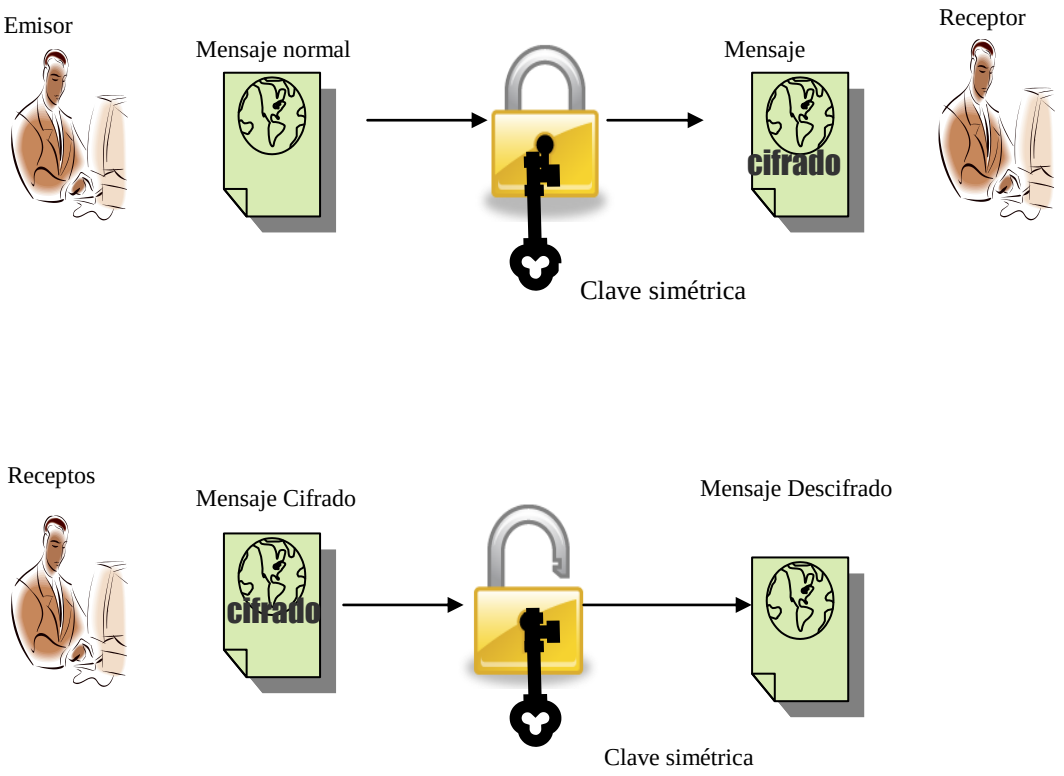
firma digital basada en el uso de claves asimétricas o criptografía de clave pública es la que mejor satisface las exigencias de seguridad y confianza que requieren las comunicaciones electrónicas.

[116] Vid. NASH, A. DUANE, W. JOSEPH, C. BRINK, D., "*PKI Infraestructura de Claves Publicas...,* Cit., Pág. 24 y siguiente, los algoritmos mas comunes en la criptografía simétrica son. Los algoritmos simétricos usados con mayor frecuencia son: DES, 3DES, RC2, AES (denominado también Rijndael). estos algoritmos permiten tener diferentes niveles se seguridad por que unos son más fuertes que otros y ofrecen mayor resistencia a ataques de fuerza bruta, el algoritmo Rijndael es el más aceptado y recomendado en este momento por que permite utilizar claves mas grandes y complejas y se recomienda para encriptar información sensible, este es mas complejo y flexible que DES.

[117]Vid. NASH, A. DUANE, W. JOSEPH, C. BRINK, D., "*PKI Infraestructura de Claves Publicas...,* Cit., Pág. 23. En ocasiones, las personas las personas se refieren a la clave simétrica como la "*Clave Secreta",* por el hecho que la clave debe permanecer en secreto para que terceras personas no autorizadas no puedan acceder a ella; pero no debemos de referirnos a la clave simétrica como clave secreta, porque puede resultar muy confuso, debido a que la clave privada en criptografía asimétrica también debe de mantenerse en secreto.

[118]El proceso de aplicación del sistema simétrico es muy sencillo y opera de la siguiente manera: A (emisor) tomo un mensaje en texto claro al cual le aplica la clave simétrica, y como resultado se obtiene un mensaje cifrado, el cual enviara a través de Internet a B (receptor), y cuando este lo reciba le aplicara la misma clave simétrica (de la cual tenia conocimiento previo) para descifrarlo y de esa forma obtener el texto original. Como anticipamos el procedimiento del sistema simétrico es bastante sencillo. Lo cual veremos en el siguiente grafico.

Aplicación del Sistema Simétrico Grafico Nº.1.



[118] Vid. NASH, A. DUANE, W. JOSEPH, C. BRINK, D., "*PKI Infraestructura de Claves Publicas...*, Cit., Pág. 22. Las claves simétricas no son nada más que un número aleatorio de la longitud correcta; si el algoritmo simétrico tiene un cifrado simétrico de 40 bits, la clave simétrica tendrá 40bits de longitud. Si el algoritmo simétrico tiene un cifrado simétrico de 128 bits, la clave simétrica tendrá 128 bits de longitud.

6.1.3 VENTAJAS Y DESVENTAJAS DEL SISTEMA SIMÉTRICO.

El sistema asimétrico tiene las siguientes ventajas:

1-) Confiere confidencialidad, ya que tan las dos partes que comparten y conocen la clave simétrica pueden encriptar y desencriptar la información contenida en el mensaje[119].

2-) El cifrado simétrico es rápido en aplicarse sobre la información, de manera que el cifrado de grandes cantidades de datos puede realizarse a un ritmo veloz.

3-) En los algoritmos criptográficos simétricos se utiliza la misma clave para cifrar y descifrar.

4-) El texto cifrado como consecuencia de un cifrado simétrico es compacta, es decir, no expande el texto cifrado.

El sistema asimétrico tiene las siguientes desventajas:

1-) como la aplicación del sistema de clave simétrica será utilizado para enviar información a través de Internet, es poco probable que las dos personas tengan conocimiento previo de la clave, es preciso que la clave sea enviada junto con el mensaje. Y como consecuencia esta sujeta a ser interceptada y vulnerada. Porque la seguridad de dicho sistema radica en mantener la clave en secreto.

2-) El sistema de criptografía simétrico requiere una administración compleja de claves[120]. Por la razón, que es necesario la creación de

---

[119] Vid. MARTÍNEZ NADAL, APOL·LÒNIA, *Comercio Electrónico, Firma Digital Y Autoridades de Certificación...., Cit.,* Pág. 46. Puede ser útil y adecuada para dar confidencialidad (por que solo las dos partes que comparten la clave simétrica pueden descifrar el mensaje), pero como veremos no es firma porque no soluciona la cuestión del no rechazo de origen.

diferentes claves de acuerdo al numero de mensajes que se quieran cifrar.

3-) Este sistema no puede ser utilizado para la aplicación de las firmas digitales[121], ya que no confiere seguridad alguna.

6.1.4 SISTEMA DE CRIPTOGRAFÍA ASIMÉTRICA.

Conocido también como sistema de clave pública este sistema esta basado en el uso de un par de claves asociadas. Una clave privada[122] conocida solo por el titular del mensaje y una clave publica que conocen o pueden ser conocida por todas las personas; ambas claves están matemáticamente relacionadas entre si y por tratarse de dos claves distintas es imposible que quien conozca la clave publica, pueda derivar de ella la clave privada, de ahí deriva la seguridad del sistema de clave publica[123].

---

[120] Vid. NASH, A. DUANE, W. JOSEPH, C. BRINK, D., "*PKI Infraestructura de Claves Publicas...,* Cit., Pág. 27. La cantidad de claves es proporcionalmente el cuadrado de la cantidad de los participantes, y cada una de estas claves se utiliza una vez; de algún modo se transfiere a la otra persona y no se vuelve a utilizar.

[121] Vid. NASH, A. DUANE, W. JOSEPH, C. BRINK, D., "*PKI Infraestructura de Claves Publicas...,* Cit., Pág. 27. Otro punto importante sobre loas algoritmos simétricos son las firmas digitales, como una técnica criptográfica para relacionar información con una persona. Si se necesita contar con una firma digita en algún documento, se necesita que sea algo único asociado solo con la persona que firma. Si dos personas tienen la misma clave simétrica tanto para cifrar como para descifrar, cualquiera que sea el cálculo matemático que haga una de ellas, también lo puede hacer la otra. Por esta razón es que las claves no se eligen para las firmas digitales.

[122] Vid. MARTÍNEZ NADAL, APOL·LÒNIA, *Comercio Electrónico, Firma Digital Y Autoridades de Certificación...., Cit.,* Pág. 47. En los años setenta se produce un gran avance en la criptografía moderna, con el desarrollo de un sistema alternativo a la criptografía simétrica tradicional: los criptosistemas de clave asimétrica o publica, basados en el uso de un par de claves asociadas: una clave privada, 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, y se podrá acceder a ella mediante un numero de identificación personal, o, en la situación ideal, mediante un dispositivo de creación biométrica, por ejemplo, a través del reconocimiento de una huelle digital) y una clave publica relacionada matemáticamente con ella, y que puede ser accesible para cualquiera(e incluso debe serlo a través por ejemplo, de directorios públicos de fácil acceso).

[123] Vid. MARTÍNEZ NADAL, APOL·LÒNIA, *Comercio Electrónico, Firma Digital Y Autoridades de Certificación...., Cit.,* Pág. 47. Generalmente la criptografía de clave publica se basa en el empleo de funciones algorítmicas para generar el par de claves, distintas pero matemáticamente relacionadas entre si(grandes números producidos utilizando una serie de formulas matemáticas aplicadas a números primos); en la actualidad se están utilizando o desarrollando otras técnicas

Lo interesante de este sistema Criptográfico asimétrico[124] es que una clave no puede descifrar, lo que cifra, es decir, si se codifico un mensaje con la clave privada para descodificarlo necesariamente se debe utilizar la clave publica y viceversa, por tanto, no se puede averiguar una clave a partir de la otra[125].

---

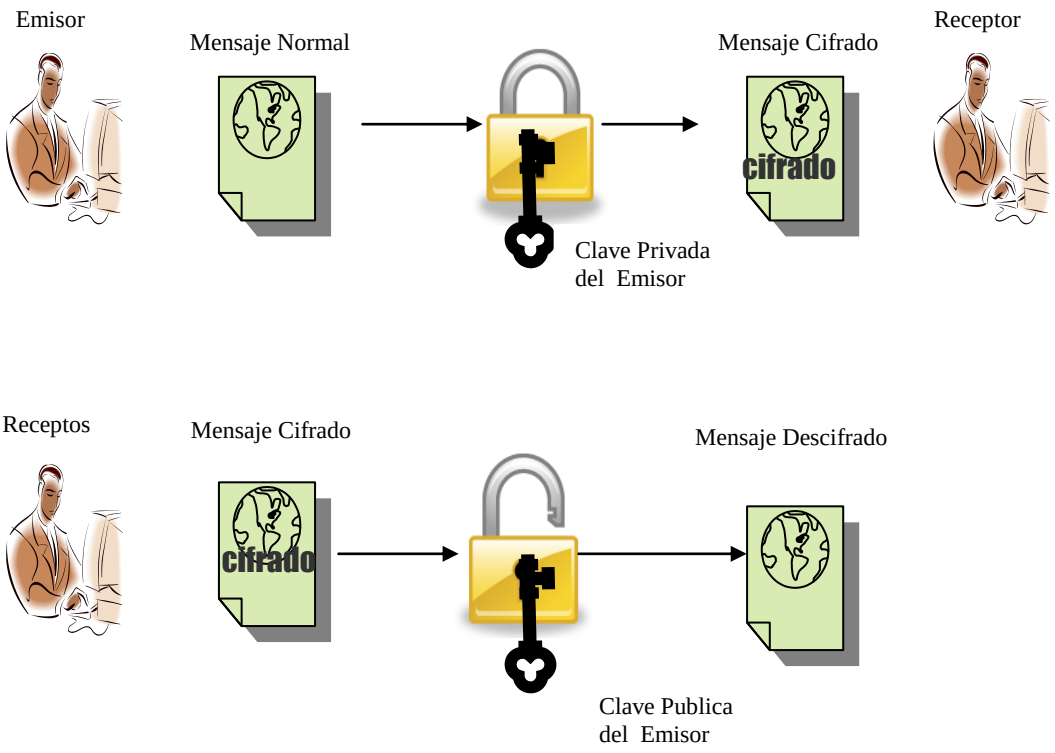
matemáticas, como los criptosistemas de curvas elípticas, que se suelen describir cono sistemas que ofrecen un alto grado de seguridad mediante el empleo de longitudes de clave significativamente reducidas.

[124] Vid. NASH, A. DUANE, W. JOSEPH, C. BRINK, D., "*PKI Infraestructura de Claves Publicas...,* Cit., Pág. 29. Existen pocos algoritmos Criptográficos Asimétricos y, por lo general, se basan en matemáticas mucho más complejas y obtusas. Whitfield Diffie y Martín Hellman fueron los primeros de introducir el concepto de criptografía asimétrica a mediados de los 1970, el algoritmo criptográfico de Diffie-Hellman se desarrollan para manejar los problemas sobre la distribución segura de claves de cifrado simétrico. El algoritmo Diffie-Hellman se base en matemáticas de algoritmos discretos, es un algoritmo de uso común. El algoritmo RSA es el algoritmo Criptográfico mas exitoso de la clave publica / privada fue inventado en el MIT por *Riverst, Shamir y Adleman* las siglas del criptosistema corresponden a las iniciales de sus autores.

[125] Vid. MARTÍNEZ NADAL, APOL·LÒNIA, *Comercio Electrónico, Firma Digital Y Autoridades de Certificación...., Cit.,* Pág. 48. La criptografía asimétrica proporciona confidencialidad, es decir, enviar mensajes secretos a través de canales inseguros, como Internet, sin necesidad de comunicación previa de una clave secreta compartida. Y, precisamente, esta confidencialidad que la criptografía puede proporcionar a planteado, y sigue planteando, problemas, pues entra en conflicto con el interés publico de poder intervenir determinadas comunicaciones en determinadas situaciones, posibilidad que no existiría, en principio, si no se tuviera acceso a la clave privada. De ahí las restricciones comerciales a la venta y exportación de productos criptográficos, y las diversas iniciativas existentes en distintos países tendentes conseguir que las autoridades publicas puedan intervenir también comunicaciones electrónicas cifradas, iniciativas basadas en la exigencia de deposito de las claves privadas. El algoritmo RSA es el más usado en Internet dado a que es parte de los navegadores como Netscape e Internet Explorer, así como de muchos otros productos. Los problemas de autenticación y protección de la información en grandes redes de comunicación fueron analizados en 1976, en el plano teórico, por Whitfield Diffie y Martin Hellman, en un trabajo en el que explicaron sus conceptos respecto del intercambio de mensajes sin necesidad de intercambiarse claves secretas. La idea fructificó en 1977 con la creación del Sistema Criptográfico de Clave Pública RSA, por parte de Ronald Rivest, Adi Shamir y Len Adleman, por aquel entonces profesores del Instituto de Tecnología de Massachusetts (M.I.T.).
En lugar de emplear una sola clave para encriptar y desencriptar datos, el sistema RSA emplea un par combinado de claves que desarrolla una transformación en un solo sentido. Cada clave es la función inversa de la otra, es decir, lo que una hace, sólo la otra puede deshacerlo. La Clave Pública en el sistema RSA es publicada por su propietario, en tanto que la Clave Privada es mantenida en secreto. Para enviar un mensaje privado, el emisor lo encripta con la Clave Pública del receptor deseado. Una vez que ha sido encriptado, el mensaje sólo puede ser descifrado con la Clave Privada del receptor. Inversamente, el usuario puede encriptar datos utilizando su Clave Privada. Es decir, las claves del sistema RSA pueden ser empleadas en cualquier dirección. Esto sienta las bases para la firma digital. Si un usuario puede desencriptar un mensaje con la Clave Pública de otro usuario, éste debe, necesariamente, haber utilizado su Clave Privada para encriptarlo originariamente. Desde el momento que solamente el propietario puede utilizar su propia Clave Privada, el mensaje encriptadose transforma en una especie de firma digital, un documento que nadie más ha podido crear.

La aplicación del sistema asimétrico es mucho mas complejo, que el sistema anterior y su procedimiento se desarrollaría de la siguiente manera: A (emisor) toma el mensaje en texto normal y claro, y procede a cifrarlo con su clave privada, inmediatamente el mensaje así cifrado lo envía a través de Internet a B (receptor) y este al recibir el mensaje le aplica la clave publica de A(emisor) que obtuvo a través de un directorio publico, y al aplicarle la clave publica, obtiene el mensaje en texto original y claro. Y viceversa, B (receptor) toma un mensaje normal y claro y lo cifrara aplicándole la clave publica de A (emisor), y el mensaje así cifrado lo envía a través de Internet a A (emisor) y este al recibirlo le aplica su clave privada y así obtener el mensaje original y claro. Procedimiento que veremos en el grafico numero 2.

Grafico Nº. 2 Aplicación del Sistema Asimétrico o de Clave Pública.



6.1.5 VENTAJAS Y DESVENTAJAS DEL SISTEMA ASIMÉTRICO O DE CLAVE PÚBLICA.

El sistema asimétrico tiene las siguientes ventajas:

1-) En el Sistema de Clave asimétrica no se necesita intercambiar previamente la clave, por la razón, que los algoritmos asimétricos requieren dos claves; una para codificar y la otra para descodificar.

2-) La criptografía asimétrica no requiere una administración compleja de claves, ya que la misma clave puede ser utilizada para enviar diferentes mensajes.

3-) Con este sistema de clave asimétrica, no es necesario enviar la clave a través de Internet, y por tanto, no se tiene el peligro que esta sea interceptada por personas no autorizadas.

4-) Este sistema de clave asimétrica puede ser utilizado para soportar firmas digitales; porque proporciona confidencialidad, autenticidad, integridad y no rechazo de origen.

El sistema asimétrico tiene las siguientes desventajas:

1-) El cifrado asimétrico es comparativamente lento, es decir, si se quisiera cifrar poca información no habría problema, la dificultad seria si se quisiera cifrar un mensaje bastante extenso[126].

2-) El cifrado asimétrico expande el texto cifrado, y por tanto, el tamaño del texto cifrado es mayor que el texto claro original.

---

[126] Vid. NASH, A. DUANE, W. JOSEPH, C. BRINK, D., "*PKI Infraestructura de Claves Publicas...,* Cit., Pág. 34. Los algoritmos asimétricos son comparativamente lentos, pueden ser diez a cien veces más lentos que un algoritmo simétrico con una fortaleza comparable.

6.1.6 COMBINACIÓN DE LOS SISTEMAS DE CLAVE SIMÉTRICA Y DE CLAVE ASIMÉTRICA O PÚBLICA.

Ahora que ya conocemos el proceso que se utiliza tanto en el sistema simétrico, como en el sistema asimétrico para cifrar y descifrar, podemos observar una situación curiosa, en cada parte donde un algoritmo simétrico es débil, en esa parte el algoritmo asimétrico es fuerte y viceversa, afortunadamente exista una manera de combinar ambos métodos, donde se puedan utilizar las fortalezas de cada uno, sin heredar sus debilidades[127].

Antes de continuar es importante subrayar, que este nuevo sistema al que se le denomina mixto, por ser una combinación de los dos sistemas anteriores, su método es más complejo, por que su procedimiento es gran medida el que se utiliza para la firma digital. A continuación desarrollaremos el proceso de la siguiente forma:

Primera fase: A (emisor) toma un mensaje en texto claro y lo cifra, utilizando para ello una clave simétrica aleatoria, con ello se consigue la aplicación de un sistema seguro, rápido y compacto.

Segundo fase: es aquí donde entra a funcional el sistema de clave publica, conseguimos la clave publica del receptor en el directorio y la utilizamos para cifrar solamente la clave simétrica aleatoria, el resultado de lo anterior seria una clave simétrica aleatoria, cifrada con una clave

---

[127] Vid. NASH, A. DUANE, W. JOSEPH, C. BRINK, D., "*PKI Infraestructura de Claves Publicas...,* Cit., Pág. 36. Con la combinación de la criptografía simétrica y asimétrica, usted pue3de estar muy cerca de una solución ideal que tenga las siguientes propiedades: La solución debe ser segura; el cifrado debe ser rápido; el texto cifrado debe ser compacto; la solución debe servir en escala de grandes poblaciones; la solución no debe ser vulnera a la interceptación de claves; la solución no debe requerir una relación previa entre las partes; la solución debe soportar firmas digitales y aceptación. La combinación de la criptografía simétrica y asimétrica satisface cada uno de estos requerimientos. Con el cifrado simétrico puede lograr velocidad y texto compacto, y con la criptografía de clave publica / privada puede lograr escalabilidad, mayor facilidad de administración de clave, resistencia a la intercepción y firma digital y aceptación.

publica asimétrica, es decir, una clave cifrada con otra clave, a este proceso se le denomina *operación de la clave empaquetada.*

Tercer fase: aquí es donde se une la clave empaquetada al texto cifrado, a esta combinación se le conoce como *Sobre Digital;* y se envía al receptor a través de Internet, con este proceso evitamos que una tercera persona que intercepte el sobre digital, pueda descifrar la clave empaquetada y poder descifrar el texto, alterarlo o cambiarlo por otro. El proceso hasta aquí lo podemos ver en el grafico número 3.

Cuarta fase: Comienza la etapa de la Verificación de la Firma Digital y esta etapa comienza con la recepción del sobre digital, el cual debe ser descompuesto en dos partes: el texto cifrado y la clave empaquetada, se iniciara descifrando la clave empaquetada con la clave privada de B (receptor) obteniendo la clave simétrica con la que se cifro el mensaje original.

Quinta fase: se utiliza la clave simétrica para descifrar el texto cifrado y así obtener el mensaje original en texto claro y normal[128]. Veamos el proceso de verificación en el siguiente grafico número 4.

[128] Vid. NASH, A. DUANE, W. JOSEPH, C. BRINK, D., "*PKI Infraestructura de Claves Publicas...,* Cit., Pág. 38. El proceso que se acaba de describir (con algunas variaciones) es el fundamento para la mayoría de soluciones de cifrado moderno, que van desde el correo electrónico cifrado, pasando por las sesiones cifradas en la web, hasta las redes privadas virtuales cifradas. Hemos tenido éxito en lograr los beneficios de la criptografía simétrica (Seguridad, velocidad, texto compacto) con los beneficios de la criptografía asimétrica (Seguridad, escalabilidad, sin relaciones previas). Actualmente la criptografía asimétrica es muy usada, sus dos principales aplicaciones son el intercambio de claves privadas y la firma digital, una firma digital se puede definir como una cadena de caracteres que se agrega a un archivo digital que hace el mismo papel que la firma convencional que se escribe en un documento de papel ordinario. Los fundamentos de la criptografía asimétrica pertenecen a la teoría de números.

Grafico Nº 3. Cifrado con la combinación.

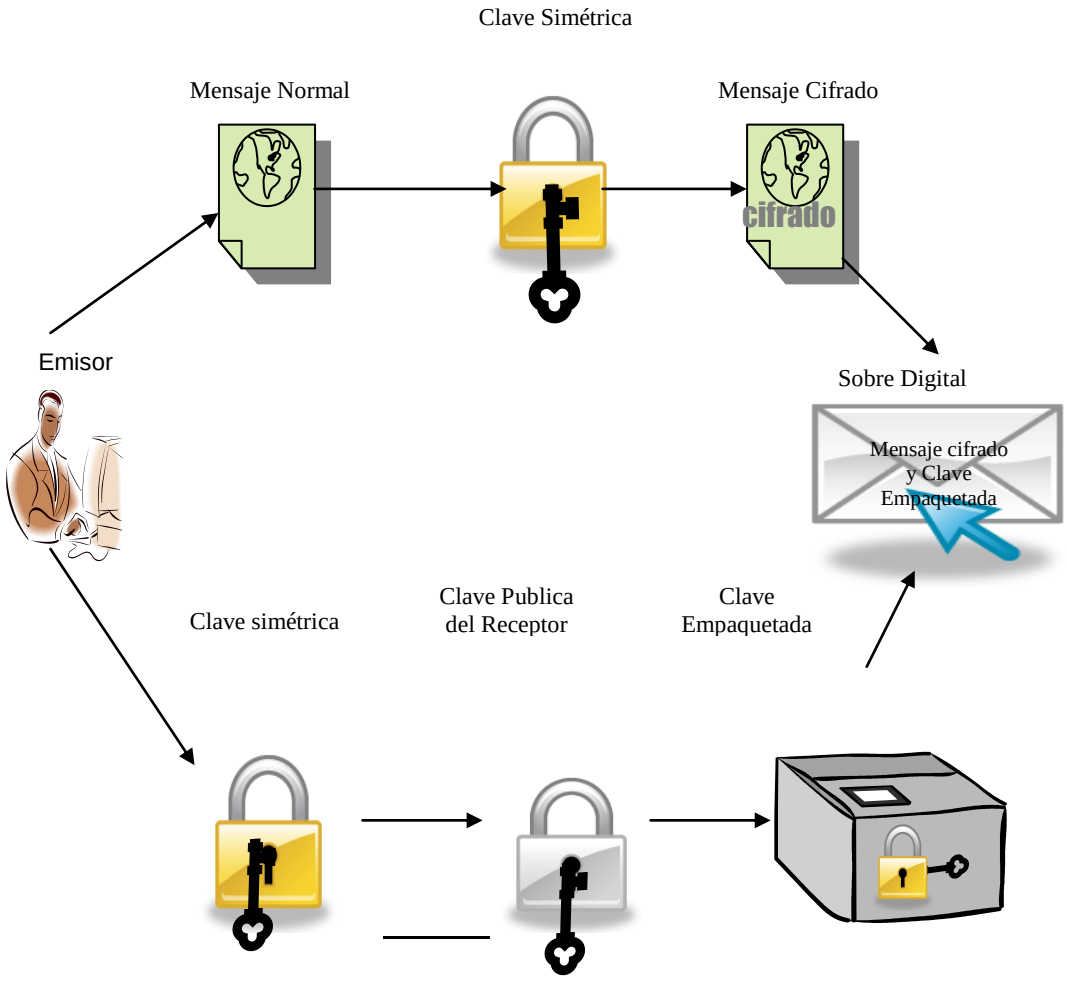
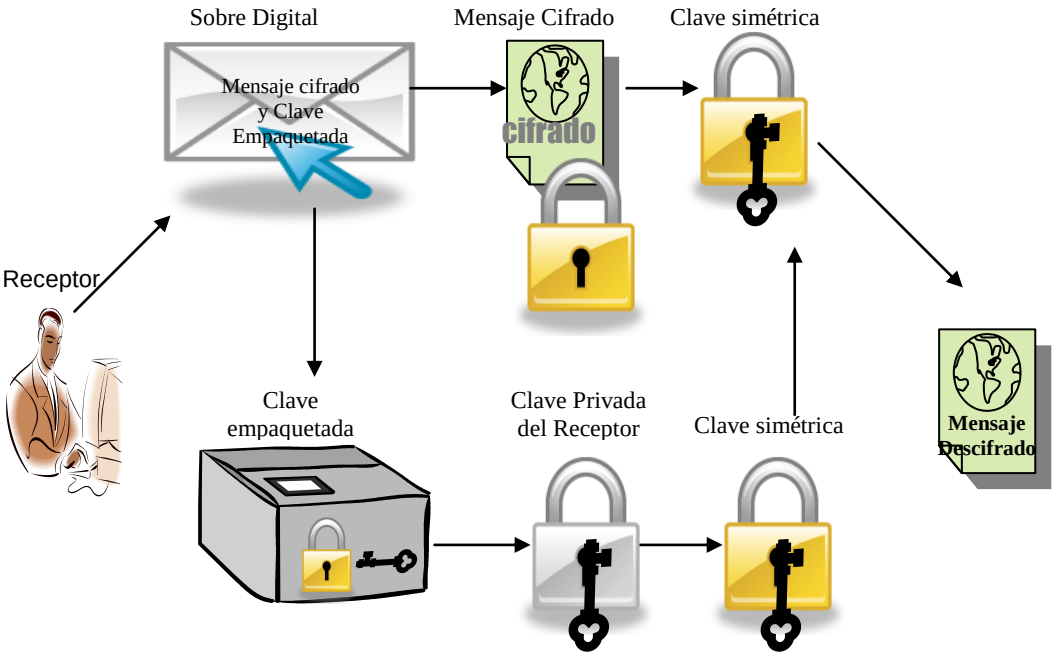


Grafico Nº 4. Descifrado con la Combinación.



Sin embargo ha este procedimiento falta añadirle un elemento más que seria: La función *hash*.

6.1.7 Empleo de los Algoritmos *hash*

Es una herramienta fundamental en la criptografía, la función hash, es usada principalmente para resolver el problema de la integridad de los mensajes, así como la autenticidad de mensajes y de su origen. Una función hash es también ampliamente usada para la firma digital, ya que los documentos a firmar son en general demasiado grandes, la función hash les asocia una cadena de longitud de 160 bits que los hace más manejable para el propósito de la firma digital.

Los algoritmos *hash* transforman una secuencia de bits en otra menor, es decir, este algoritmo efectúa un cálculo matemático sobre los datos que constituyen el documento y da como resultado un numero único

denominado MAC (*Messeges Authentication Code*), la función hash se caracteriza por su irreversibilidad, es decir, no se puede construir el texto a firmar dada la función hash y estos se aplican tanto para la creación, como para la verificación de la Firma Digital. Los algoritmos *hash* o algoritmos de resumen proporcionan al destinatario seguridad en la integridad de la información recibida[129].

Este algoritmo *hash* se aplica sobre un mensaje inicial, obteniendo así un resumen del mismo denominado *Reseñe del Mensaje o Huella Digital[130];* es decir, el resultado del *hash* es un valor mucho más pequeño que los datos originales.

6.1.8 PROCEDIMIENTO UTILIZADO PARA LA APLICACIÓN DE LA FIRMA DIGITAL.

Ahora que conocemos en que consisten los algoritmos *hash;* veamos como es su empleo dentro del procedimiento de la Firma Digital. A continuación nos referiremos al proceso de la firma digital.

Primera fase: A (emisor) selecciona un algoritmo *hash* apropiado, y a través de este algoritmo procesa el mensaje en texto normal y claro y

---

[129] Vid. NASH, A. DUANE, W. JOSEPH, C. BRINK, D., "*PKI Infraestructura de Claves Publicas...,* Cit., Pág. 41. Todos los algoritmos hash que se utilizan en criptografía están diseñados con algunas propiedades especiales: Usted no puede poner a funcionar el hash hacia atrás y recuperar algo del texto, es decir, un mensaje resumido no puede desresumirse; la reseña resultante no dirá nada sobre el texto claro inicial; Desde un punto de vista computacional, no es factible crear / descubrir texto claro que verifique un valor especifico. Esto evita que un pirata informatico trate de sustituir un documento sin que se presenten fallas en la correspondencia de la reseña.

[130] Vid. GRANILLO DE TOBAR, ANA YESSENIA, *La Firma Electrónica, su uso en el ámbito de la Contratación Electrónica...,* Cit., Pág. 78. Los hash pueden operar de dos formas: MDC (Modification Detection Codes) o MAC (Massages Authentication Codes). Los primeros sirven para detectar modificaciones en la información enviada, de tal forma que se aplica el algoritmo al mensaje y se envía adjunto con mismo mensaje, como prueba de la integridad y cuando el receptor recibe el mensaje, aplica el hash al mismo y si el resultado coincide con el hash enviado adjunto, entonces habríamos concluido que el mensaje se ha transmitido sin alteración. En cambio en el MAC, sirve también para autenticar el origen de los mensajes, para esto se adjunta al mensaje una clave simétrica y se aplica el hash al conjunto, cuando llega a su destino, el receptor comprueba la integridad del mensaje completo y posteriormente se utiliza la clave adjunta para comprobar su origen.

como resultado de ese proceso obtiene una reseña o resumen del mensaje original, y inmediatamente este resumen es cifrado con la clave privada de A (emisor).

Segunda fase: El resumen cifrado se hace acompañar del mensaje en texto claro, también se incluye un bloque de información que contiene la identificación del algoritmo *hash* que fue utilizado para crear el resumen original, y se remite a B (receptor) por medio de Internet.

Tercera fase: nuevamente llamaremos a esta paso Verificación de la Firma Digital, es acá donde B(receptor) recibe la reseña cifrada y el mensaje en texto normal y claro, además de otra información; para realizar la verificación de la firma digital B(receptor) deberá realizar dos operaciones: la primera B (receptor) tomara el mensaje en texto claro que le fue enviado junto a la reseña y lo procesara a través del mismo algoritmo *hash* obteniendo así una nueva reseña o resumen del mensaje enviado.

Cuarta fase: B (receptor) conseguirá la clave publica de A (emisor) en un directorio público de claves públicas[131], con la que descifrará la reseña y obtendrá una reseña descifrada. a continuación B(receptor) compara si la reseña original que le fue enviada, y la reseña que obtuvo de la aplicación de su propio procedimiento y si ambas reseñas concuerdan, B(receptor) tendrá la seguridad que el mensaje no fue modificado, ni alterado durante su recorrido por Internet, pero si por el contrario el mensaje hubiere sido alterado, los resúmenes no se

[131] Vid. NASH, A. DUANE, W. JOSEPH, C. BRINK, D., "*PKI Infraestructura de Claves Publicas...,* Cit., Pág. 46. La clave publica no esta realmente en directorio. La clave publica esta almacenada realmente en un certificado digital y, por lo general, una copia de el esta almacenada en un directorio de la autoridad de confianza que expide el certificado.

corresponderían, es decir, dos textos iguales originan huellas digitales iguales y dos textos diferentes originan huellas digitales diferentes[132].

A continuación veremos un ejemplo de un mensaje encriptado:

¡EYEARECAAYFAjzLHrAACgkQUWg/+OKRH9/
+UQCg15imVd8y+ZwG3P/uL04YFj0AnAoNNusq
wWUuhxKYWxw0tiPjF1=ueZj

Es así como luce un mensaje encriptado es ininteligible y solo quien conoce el proceso y quien conoce la clave podrá obtener un mensaje legible después de descifrarlo.

6.2 CLASES DE FIRMAS.

Quizá la primera cuestión que se debe tratar dentro de este apartado es que se entiende por firma en términos tradicionales, "*.es aquella expresión del nombre o apellido del suscriptor o de algunos de los elementos que los integren o de un signo o símbolo utilizados como medio de identificación personal"*[133]*.* Los cuales son plasmados en un documento mediante, el cual, el suscriptor adquiere todos los derechos y las obligaciones que de el deriven. La función de las firmas manuscritas[134] es identificar a una persona y vincular a esa persona con el contenido del documento.

---

[132] Vid. NASH, A. DUANE, W. JOSEPH, C. BRINK, D., "*PKI Infraestructura de Claves Publicas...,* Cit., Pág. 43. Se debe recordar que si cambia un solo bits del texto claro, la reseña del algoritmo hash será diferente. Esta capacidad de los *haches* para detectar el mas pequeño de los cambios en el texto claro es lo que les da su utilidad para verificar la *integridad del mensaje.*

[133] Vid. CUBILLOS VELANDIA, RAMIRO, RINCÓN CÁRDENAS, ERICK., *introducción Jurídica al Comercio Electrónico....,* Cit. Pág. 207. La firma electrónica y la firma digital, non son firma en los términos convencionales, es decir que no es un signo o marquilla que se coloca sobre un objeto material.

[134] CASTELLANOS DE UBAO, LEOPOLDO GONZALES-ECHENIQUE, "*La Firma Electrónica" en AA VVV* Derecho de Internet, Contratación Electrónica y Firma Digital, Coordinado por Mateus de Ros, Rafael y Cendoya Méndez de Vigo Juan Manuel, Editorial Aranzadi, Navarra, 2000, Pág. 611.

El propósito de las diversas técnicas que se encuentran disponibles en el mercado, es ofrecer medios técnicos que cumplan con algunas o todas las funciones que cumple la firma manuscrita se puedan cumplir en un entorno técnico, estas técnicas se denominan, en general, "*Firmas Electrónicas".*

La Ley Modelo de Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) para la Firma Electrónica, en su Art.2, define lo que se entiende por firma electrónica "*se entenderán 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 contenida en el mensaje de datos".* La firma electrónica seria una variedad de métodos o símbolos basados en un medio electrónico.

Es decir, es un concepto amplio y general que puede abarcar tanto técnicas simples como por ejemplo la firma manual digitalizada, hasta técnicas muy complejas como las utilizadas para la aplicación de la firma digital la cual es una especie del genero firma electrónica[135].

La firma digital se puede definir como "*La transformación de un mensaje utilizando una función hash, y un criptosistema asimétrico y simétrico de forma que una persona que tenga el mensaje inicial y la clave*

La firma Manuscrita ha de constatarse en un papel físico y que, por tanto, tiene una clara configuración material o física.

[135] http://www.firmadigital.com. Visitada el 14 de octubre de 2008. Una firma electrónica es un conjunto de caracteres que acompaña a un documento o fichero, acreditado quien es su autor (autenticación) y que no ha existido ninguna manipulación posterior de los datos (integridad). Para firmar un documento digital, su autor utiliza su propia clave secreta (Sistema criptográfico asimétrico), a la que solo el tiene acceso, lo que impide que pueda después negar su autoría (no revocación o no repudio). De esta forma el autor queda vinculado al documento de la firma. La validez de dicha firma podrá ser comprobada por cualquier persona que disponga de la clave pública del autor.

publica del firmante pueda determinar de forma segura la autenticidad y la integridad del documento"[136].

También existen otros tipos de firma, que merecen ser mencionados como la firma electrónica avanzada y la firma electrónica reconocida, términos añadidos al texto del Real-Decreto ley sobre la firma electrónica 59/2003 de España. Comenzaremos por definir la firma electrónica avanzada como "*aquella firma que esta vinculada al firmante de manera única, permitiendo su identificación creada por medios que el firmante mantenga bajo su exclusivo control, estando vinculada a los datos a que se refiere de modo que cualquier cambio ulterior de los mismos sea detectable".*

Para que una firma electrónica, pueda ser considerada como una firma electrónica avanzada debe de cumplir con los requisitos que se derivan de su definición.

En último lugar, definiremos que es una firma electrónica reconocida tal como lo establece la ley de firma electrónica de España y es aquella "*basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.*

Este tipo de firma para ser considerada como tal, debe ser una firma electrónica avanzada y que este amparada en un certificado reconocido y haya sido creada mediante un dispositivo seguro de creación de firma.

---

[136] Vid. MARTÍNEZ NADAL, APOL·LÒNIA, *Comercio Electrónico, Firma Digital Y Autoridades de Certificación...., cit.,* Pág. 50. Las firmas digitales, que proporcionan autenticidad, integridad y no rechazo en origen, y que puedan resultar tanto o más útiles, validas y eficaces en el comercio y en los procedimientos legales como la firma escrita sobre papel.

6.2.1 CARACTERÍSTICAS DE LA FIRMA ELECTRÓNICA.

De lo anterior podemos concluir que no existe un concepto único sobre firma electrónica, al contrario son variadas las definiciones utilizadas por la doctrina y por las legislaciones que regulan la firma electrónica, es por eso, que es fundamental tomar en cuenta las características que se derivan de la aplicación de la firma electrónica y de acuerdo al número de particulares propias que reúna cada definición; determinaremos a que tipo de firma nos estamos refiriendo, nos limitaremos a resaltar las siguientes características:

1. se trata de un conjunto de datos electrónicos, consignados en forma electrónica.

2. que proporcione seguridad que el mensaje no ha sido alterado o modificado durante su viaje por Internet, con lo que se asegura la integridad del mismo.

3. Que por medio de ella se pueda identificar al autor del mensaje.

4. Que haya sido creada bajo medios que el firmante pueda tener bajo su exclusivo control.

5. Que haya una vinculación entre la creación de cada firma electrónica y los datos a los que se refiere.

6. que esta sea creada mediante un dispositivo seguro de creación de firmas.

7. que este basada en un certificado reconocido.

6.3 PRINCIPIOS DE LA FIRMA ELECTRÓNICA.

Uno de los principios de la firma electrónica, es la **neutralidad tecnológica**, el cual tiene su origen en la ley modelo de la comisión de las Naciones Unidas sobre comercio electrónico(UNCITRAL), este principio hace referencia a la aptitud de las nuevas normas que regulan el comercio electrónico para que abarquen la tecnología existente en el momento que se formulan, y también incorporen a las tecnologías futuras, para evitar que esas disposiciones se sometan en el futuro nuevamente a modificaciones, y con eso garantizar la vigencia de las normas.

Otro de los principios de la firma electrónica es el **Principio de compatibilidad Internacional,** este se refiere a que debe de existir una relación en todas las legislaciones ya que se trata de una sola tecnología, y por tanto, no puede ser regulada de manera diferente sino con muchas coincidencias sin llegar hacer idénticas.

Finalmente tenemos el **Principio de Equivalencia Funcional**, con el que se busca que la firma electrónica cumpla las mismas funciones jurídicas, que cumple la firma autógrafa, es decir, que se busca que la primera equipare las funciones de la ultima. Este principio también implica aplicar a las mensajes de datos electrónicos un principio de no discriminación respecto a las declaraciones de voluntad por el hecho que estas son emitidas por medios tecnológicos.

6.4 EL PAPEL QUE JUEGAN LAS ENTIDADES DE CERTIFICACIÓN EN EL PROCESO DE APLICACIÓN DE LA FIRMA ELECTRÓNICA.

Mientras que la firma autógrafa va ligada indisolublemente a la persona del firmante, esto no-pasa con la firma electrónica que es una pura secuencia de datos electrónicos, es de ahí, donde surge la necesidad de vincular a los operadores con sus claves, a fin de garantizar que una clave publica pertenece a una persona en particular, es aquí

donde entran a funcionar las entidades de certificación que emiten un documento llamado certificado, y nosotros estudiaremos el denominado certificado digital que es utilizado en el proceso de aplicación de la firma digital.

Para entender mejor cual es la participación de las entidades de certificación en la implementación de la firma electrónica[137], a continuación desarrollaremos el proceso de esta que explicamos anteriormente agregando la participación de las entidades de certificación. Pero primero veremos como se puede obtener un certificado[138].

En este caso A (emisor) se dirige al proveedor de servicios de certificación y le comunica cual es su clave publica. El proveedor después de comprobar la identidad de A (emisor) y la correspondencia de sus claves, cifra con su clave privada (clave del proveedor) la clave publica de A (emisor) y su nombre, denominando a este documento certificado de clave publica o simplemente certificado. Ahora que A (emisor) cuenta con su certificado, cada vez que opere enviara junto con el mensaje firmado

---

[137] Iniciativa GLIN AMERICAS Banco Interamericano de Desarrollo, Documento Conceptual para la Legislación en Era de la Información, "*firma digital y contratos electrónicos",* 2005, Pág. 18. La infraestructura de clave publica (*Publica Key Infraestructura* sus siglas en ingles PKI) es la combinación de productos de hardware y software, políticas y procedimientos para proveer un nivel adecuado de seguridad en transacciones electrónicas a través de redes publicas, como la Internet. La infraestructura de clave publica se basa en identificaciones digitales, también conocidas como "certificados digitales" los cuales actúan como pasaportes electrónicos vinculados a un usuario de firma digital con su clave publica. Debido a la característica impersonal involucrada en este tipo de tecnología-sin intercambio de documentos- es que se hace necesario contar con medios que garanticen una efectiva identificación y autenticación de los usuarios participantes con el fin de poder lograr el no repudio de las operaciones realizadas. Así mismo, en todo momento debe poder ser garantizada la confidencialidad e integridad de las transacciones que viajan por la red.

[138] Vid. NASH, A. DUANE, W. JOSEPH, C. BRINK, D., "*PKI Infraestructura de Claves Publicas...,* Cit., Pág. 44. Un certificado digital simplemente es un documento que dice "*Garantizo que esta clave Publica particular esta asociada con este usuario en particular; confié en m*i". En su forma más simple eso es todo a lo que se refieren los certificados digitales. Presentan en lista quien es el propietario de la clave pública y contiene una copia de la clave pública de ese usuario. Entonces una autoridad de confianza firma la certificación. Por "firma la certificación" quiero decir el proceso de firma digital que acabamos de tratar. Se crea un *hash* para todo el certificado y ese *hash* queda codificado utilizando la clave privada de la autoridad de confianza. Para verificar la validez de un certificado digital, todo lo que usted necesita hacer es usar la clave pública de la autoridad de confianza para validar la firma del certificado.

con su clave privada dicho certificado. A continuación veremos dicho proceso:

Primera fase: A (emisor) selecciona un algoritmo *hash* apropiado, y a través de este algoritmo procesa el mensaje en texto normal y como resultado de ese proceso obtiene una reseña o resumen del mensaje original, y inmediatamente este resumen es cifrado con la clave privada de A (emisor).

Segunda fase: El resumen cifrado se hace acompañar del mensaje en texto claro, también se incluye un bloque de información que contiene la identificación del algoritmo *hash* que fue utilizado para crear el resumen original, y además se añade el certificado digital el cual acredita la vinculación de esa clave publica a A (emisor), y se remite a B (receptor) por medio de Internet.

Tercera fase: nuevamente llamaremos a esta paso Verificación de la Firma Digital, el primer paso es separar los tres componentes: la reseña cifrada y el mensaje en texto normal y claro, además de otra información, y la copia del certificado digital(los certificados digitales contienen cierta información como el nombre, la dirección, entre otros datos personales y una copia de la clave publica del usuario, además también contienen fecha de validez del certificado y la firma digital de la autoridad de certificación).

Cuarta fase: en esta etapa B (receptor) verificara si la firma del certificado digital es valida, utilizando la clave publica de la autoridad de certificación lo descifrara, con lo que obtendremos la clave publica vinculada A (emisor) y verificaremos la fecha de validez del certificado, inmediatamente B receptor descifrara el mensaje cifrado que le fue enviado con la clave publica de A (emisor) con lo que obtendrá el

resumen descifrado. Con este proceso se establece la autoría del mensaje[139].

Quinta fase: para realizar la verificación de la firma digital B (receptor) deberá realizar dos operaciones: la primera B (receptor) tomara el mensaje en texto claro que le fue enviado junto a la reseña y lo procesara a través del mismo algoritmo *hash* obteniendo así una nueva reseña o resumen del mensaje enviado.

Sexta fase: en esta etapa B (receptor) compara si la reseña original que le fue enviada, y la reseña que obtuvo de la aplicación de su propio procedimiento concuerdan, y si ambas reseñas coinciden B (receptor) tendrá la seguridad que el mensaje no fue modificado, ni alterado durante su recorrido por Internet, pero si por el contrario el mensaje hubiere sido alterado, los resúmenes no se corresponderían. En esta etapa se determina la integridad del documento enviado.

Con el uso de los certificados en el proceso de aplicación de la firma electrónica, podemos tener la seguridad que dicho mensaje fue enviado por el titular de la clave pública que se encuentra en el certificado. Con lo que se determina la autoría de dicho mensaje. Pero necesitamos otro elemento para que el sistema que estructura la firma electrónica sea realmente operacional, es necesario fijar la hora en que se originan y que pueda quedar fijada tanto en los mensajes como en los certificados el

---

[139] Vid. NASH, A. DUANE, W. JOSEPH, C. BRINK, D., "*PKI Infraestructura de Claves Publicas...,* Cit., Pág. 45. La identidad de confianza creara un certificado con su propia información de identidad, lo mismo que la clave publica de dicha autoridad, y la firmara. Esto se conoce como *certificado autofirmado.* El software debe manejar estos certificados de máximo nivel con sumo cuidado, ya que se basan en la confianza que existe para todos los certificados firmados por esa autoridad. El software que usted usa ya conoce los certificados autofirmados de muchas de estas autoridades de confianza. Si usted considera las configuraciones de seguridad de su navegador web, descubrirá una larga lista de las autoridades competentes que ya conoce el navegador.

momento temporal en que se producen, los informáticos denominan a este elemento como *sellos temporales*[140].

La hora en que se originan los mensajes debe ser incorporada a este antes de ser procesado el mensaje por el algoritmo *hash* y obtener el resumen; con lo que no puede ser modificada y si lo fuera al momento de realizar la verificación de la firma los resúmenes no coincidirían, pero se precisa encomendar la fijación de la hora a un tercero que cuente con un reloj exacto o confiable, función que seria asumida por las entidades de certificación[141].

En conclusión podemos observar que la criptografía contribuye en gran medida a la seguridad, en las transacciones realizadas a través de Internet; pero la criptografía es solo una parte de esa tan anhelada seguridad, por lo tanto, se debe de contar con una tercera parte de confianza como son las entidades de certificación las cuales deberán actuar para asegurar el vinculo entre la clave publica y el titular de la clave privada emitiendo para ello certificados digitales

6.5 GENERALIDADES DE LAS ENTIDADES DE CERTIFICACIÓN.

Sus orígenes se establecen junto a la firma electrónica, algunos autores señalan que su función es iniciado en tiempos de Roma con la

---

[140] Vid. VILLAR, JOSE MANUEL, "*Una Aproximación a la Firma Electrónica", en AA VVV* Derecho de Internet, Contratación Electrónica y Firma Digital..., Cit., Pág. 186. El sistema precisa como es obvio que los sellos temporales no puedan ser manipulados por las partes y ello lleva a la necesidad de encomendar su fijación en los mensajes a terceros.

[141] Vid. GRANILLO DE TOBAR, ANA YESSENIA, *La Firma Electrónica, su uso en el ámbito de la Contratación Electrónica...,* Cit., Pág. 86. La hora de envió de mensaje es de suma importancia jurídica, para efectos de determinar el momento de formación del consentimiento y el momento de perfeccionamiento del contrato, si se trata de aquellos consensuales. Además la hora juega un papel decisivo si se trata de ofertas presentadas durante un tiempo determinado, debido a que si la aceptación llegara después de vencido el termino, no se habría formado el contrato. Igual situación sucedería si se tratara de la celebración del contrato por medio de mandatarios, en el que el mandato se encuentra próximo a caducar, ya que si la aceptación llegara después de la caducidad del mismo, el contrato se habría celebrado pero seria imponible al mandante.

figura de los tabeliones a pesar que estos no tenían funciones públicas, y carecían de fe pública, pero ellos estaban inspeccionados por el estado y tenían ante autoridades y tribunales fuerza legal, es por ello que son considerados como antecedentes de los notarios.

Importante es hacer notar que al considerarse la figura del tabelión como comparación a la función del notario las entidades de certificación tienen fe pública, realmente esto no es así, pues se establece que estas normas no modifican las funciones otorgadas a los funcionarios autorizados para dar fe pública esto en países como España.

En El Salvador se menciona según la ley de simplificación aduanera que las entidades de certificación tienen fe pública en cuanto a la fecha y hora específica que personas individualizadas realizan transmisión de datos, de la pertenencia de las firmas y los términos en los cuales se generó la firma digital[142].

6.5.1 COMPONENTES TÉCNICOS

Los componentes técnicos revelan con certeza firmas digitales falsificadas y datos manipulados y suministran contra no autorizado de claves privadas de firma .Se necesitan componentes técnicos que permiten la identificación de los datos que la firma digital se aplica. Comprueba la integridad de los datos a los que se asocia la firma digital y comprueba la identidad del propietario de la clave de firma utilizada.

---

[142] VID. GRANILLO DE TOBAR, ANA YESSENIA. *La firma electrónica, su uso en el ámbito de la contratación electrónica y su aplicación por las administraciones públicas*, trabajo de tesina, San Salvador, 2004, Pág.93. Básicamente esta tesina plantea la idea del surgimiento de las certificaciones desde un punto de vista remoto y otro actual por ello debe entenderse que el primero es como el surgimiento general y el segundo un acontecer específico generado por la tecnología, de aquí que se afirma que la certificación se da al mismo tiempo que la firma electrónica.

Los componentes técnicos, serán adecuadamente comprobados según los estándares de ingeniería y deberán ser confirmados por un organismo reconocido por la autoridad competente

6.5.2 Vigencia de los Certificados

Artículo 9 Real Decreto ley 14/1999, De 17 de Septiembre, sobre firma electrónica. Los certificados de firma electrónica quedarán sin efecto, si concurre alguna de las siguientes circunstancias:

a) *Expiración del período de validez del certificado tratándose de certificados reconocidos, éste no podrá ser superior a cuatro años, contados desde la fecha que se hayan expedido.*

b) *Revocación por el signatario, por la persona física o jurídica representada por éste o por un tercero autorizado.*

c) *Pérdida o inutilización por daños del soporte del certificado.*

d) *Resolución jurídica o administrativa que lo ordene, etc* [143].

6.5.3 DEFINICIÓN DE ENTIDADES DE CERTIFICACIÓN

Definición Legal que se deriva del Artículo 8 de la ley de Simplificación Aduanera. *"Son aquellas entidades que su objetivo es establecer sistemas de certificación de la información transmitida por medios electrónicos a efecto de garantizar la autenticidad e integridad de la información transmitida"*[144]

---

[143] *Firma Electrónica y Comercio Electrónico, Cuadernos de Derecho y Comercio Monográfico 1999, Corredores de Comercio*, Madrid 2000. Editorial Dykinson, S. l. Pág. 153.

[144] Vid *Ley de simplificación Aduanera…Artículo 8.* En esta ley se establece de forma breve la regulación de lo que son las transacciones electrónicas dándole plena validez, además establece las obligaciones de las entidades certificadoras.

- **ENTIDADES DE CERTIFICACIÓN:**

  Son aquellas que se encargan 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[145]*.*

- **AUTORIDADES CERTIFICADORAS***: Son las entidades que dan testimonio de la pertenencia o atribución de una determinada firma digital a un usuario*[146]*.*

- **ENTIDADES CERTIFICADORAS***: Son la parte fiable que acredita la ligazón entre una determinada clave y el usuario propietario de la misma y actúan como una especie de notario electrónico que garantiza la veracidad de la información puesta en la red.*

- **AUTORIDAD CERTIFICADORA O ENTIDAD DE CERTIFICACIÓN**: Son terceros de confianza para las partes que intervienen alrededor de una firma electrónica.

Son las entidades que emiten certificados electrónicos basados en los estándares técnicos establecidos, permitiendo conocer a quien se realiza la oferta y al destinatario de la oferta al manifestar su aceptación.

Ley de Comercio Electrónico de Colombia. Ley 527 de 1999 Art. 2.

---

[145] Vid *GALAN CORTES, JEANNIE ELIZABETH, "La firma digital como medio de seguridad y consentimiento en las transacciones…, Cit., Pág. 153*. En esta tesis se establece el hecho que en El Salvador las Entidades Certificadoras operan bajo la autorización del Ministerio de Hacienda, mientras no se dicte un lay especial al respecto.

[146] *ALCANTARA QUINTANILLA, MILTON LEONIDAS, "Análisis Jurídico del Comercio Electrónico".* Universidad Francisco Gaviria, Tesis 2003. Pág.19 y siguientes. Se entiende por autoridad Certificadora, la entidad que da testimonio de la pertenencia o atribución de una firma digital determinada a un usuario o certificador de nivel jerárquico inferior.

Letra d) Entidad de Certificación: “Es aquella persona que autorizada conforme a la presente ley está facultada para emitir certificados en relación con los servicios de registro y estampado cronológico de transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales [147].

6.6 PROCEDIMIENTO PARA GENERAR UN CERTIFICADO DIGITAL

Se debe presentar una solicitud en soporte material manifestando el deseo de que se emita un certificado ante la entidad certificadora. Además que se registre de forma pública.

Existen criterios en relación a la forma de inscribirse algunos autores mencionan que es necesario que se haga en soporte material dicha solicitud, la razón que se argumenta es que la entidad certificadora tiene que ser garante de la correspondencia entre el par de claves generadas y el titular o propietario de las mismas y esto por la necesidad de autenticar al suscriptor, con el propósito de asegurarse que se trata de la persona quien dice ser. Estos autores señalan que no es recomendable que se utilice el registro on line a través de Internet, por la dificultad que se presenta al llevar a cabo la autenticación del suscriptor.

Presentada la solicitud la entidad certificadora admitirá la misma y procederá a la autenticación en esta etapa se toman los métodos tradicionales de comprobación.

---

[147] AGUILAR MORAN, RAUL ARMANDO. HERNANDEZ NUÑEZ, EVELYN YESENIA. “*El Comercio Electrónico en El Salvador*”. Universidad de El Salvador. Tesis Año 2002. Pág. 57. Se establece en esta tesis la importancia que posee las entidades certificadoras para brindar seguridad a la contratación electrónica por el hecho de que dichas entidades establecen la identidad de los contratantes esto posee una íntima relación con la prueba ya que se menciona que no se podrá negar el hecho realizado por ello, los entes certificadores deben poseer las medidas técnicas necesarias para cumplir con su función la cual es brindar seguridad.

Otros autores mencionan que es válido la suscripción on line es decir sin presencia física y documentación de forma material pero se advierte que deberá garantizarse por algún medio idóneo de prueba de que se es quién se dice ser[148].

6.6.1 EL CONTENIDO DE LOS CERTIFICADOS

En forma general debe contener lo siguiente.

1) *El identificador de la Autoridad de Certificación que expide el certificado.*

2) *El nombre del titular o su seudónimo inequívoco con su rol único tributario.*

3) *Un dispositivo de verificación de firma, que corresponda a un dispositivo de creación de firma bajo el control del titular.*

4) *El período de validez del certificado.*

5) *Los límites de uso del certificado, si procede*[149]*.*

---

[148]Vid. Vid. MARTÍNEZ NADAL, APOL·LÒNIA, *Comercio Electrónico, Firma Digital Y Autoridades de Certificación...., Cit.,* Pág. 178. Para determinar la autenticidad del suscriptor esta se puede realizar por medio de la presentación de un documento de identidad, cotejo de firmas, huellas digitales entre otros. No se recomienda que se utilice el registro on-line a través de internet, por la dificultad que se presenta al llevar a cabo la autenticación del suscriptor.

[149] *La firma Electrónica y su Certificación, bases jurídicas de la Tecnología Informática y el Comercio Electrónico* .Editorial Portobelo – 1ª Edición, Marzo del 20004, Pág. 46. El contenido del certificado dependerá del tipo de certificado, de la política de certificación del prestador, de ciertas normas estandarizadas estos registros de la identificación del titular son independientes del nivel de seguridad de la identidad desde un correo hasta la firma avanzada. Una entidad certificadora en el sentido de esta ley es una persona física jurídica que certifique la asignación de claves públicas de firma a personas físicas para lo cual dispone de una licencia. Un certificado digital autenticado mediante una firma digital de la asignación de una clave pública de firma pública a una persona física u otros certificados digitales.

El contenido de los certificados es unánime por estar en un estándar a nivel internacional, estando en aplicación el modelo X509 de la ITU (Internacional Telecomunications Union).

6.7 NATURALEZA JURIDICA DE LAS ENTIDADES DE CERTIFICACIÓN

Debido a que las actividades de esta forma de certificación está orientada al beneficio público es que se somete a los principios del derecho público. En cuanto a la definición de su naturaleza se considera que puede ser pública o privada:

PÚBLICA: *Porque beneficia a la comunidad con su funcionamiento y por ser un esfuerzo estatal para la incorporación de Tecnología.*

PRIVADA: *Debido a que las corrientes económicas de globalización buscan un régimen de competencia, en la cual la calidad de sus servicios determinará su lucratividad*[150]*.*

6.8 FUNCIONES PRINCIPALES DE LAS ENTIDADES DE CERTIFICACIÓN.

Las funciones giran en torno al certificado y la firma electrónica es por ello que se hace necesario establecer que se entiende por certificado digital para tal efecto se define como: "*El documento electrónico generado y firmado digitalmente por una entidad de certificación, la cual vincula un par de claves con una persona determinada confirmando su identidad".*

Otra de las funciones aparte de emitirlos es cancelar los certificados digitales dejándolos sin efecto ya sea por el vencimiento del

[150] Vid AGUILAR MORAN, RAÚL ARMANDO. HERNÁNDEZ NÚÑEZ, EVELYN YESENIA. "El Comercio electrónico…, Cit., Pág. 59 y 60. En esta tesis se plantea el hecho de la importancia que tienen las funciones de las entidades de certificación como lo es el hecho de brindar seguridad.

plazo para el cual fue otorgado, o por revocatoria de la entidad certificante y cesación de las funciones de la entidad certificadora.

6.9 CLASIFICACIÓN DE LAS ENTIDADES DE CERTIFICACIÓN

Atendiendo al contenido del certificado, pueden clasificarse en:

- **CERTIFICADOS DE IDENTIFICACIÓN**: son aquellos que identifican la entidad o persona, que expide la clave pública del suscriptor, entidades de certificación.

- **CERTIFICADOS DE AUTORIZACIÓN***, estos son los que otorgan un bloque de información adicional acerca de la identidad del suscriptor*[151]*.*

- **CERTIFICADOS DE AUTENTIFICACIÓN**, son aquellos que dan fe de hechos adicionales excepcionales del suscriptor estos son enumeraos y puestos por la petición de el mismo.

- **CERTIFICADOS DE FECHA Y HORA**, este es aquel que deja constancia de la fecha y la hora en la cual se envía el instrumento electrónico[152]

En razón a si cumplen o no con los requisitos por el legislador pueden ser: Reconocidos y No reconocidos.

---

[151] Vid. GRANILLO DE TOBAR, ANA YESSENIA.*"La firma electrónica, su uso en el ámbito de la contratación electrónica y su aplicación*…., Cit., Pág. 117 Se concretiza la clasificación de los certificados digitales según el contenido que poseen estableciendo el hecho de encaminar a identificar algunas características según sea el tipo de certificado y la intención para la cual fue creado.

[152] Vid. GRANILLO DE TOBAR, ANA YESSENIA."*La firma electrónica, su uso en el ámbito de la contratación electrónica y su aplicación*…., Cit., Pág. 118. En este apartado se definen diferentes certificados estableciendo la clasificación de los requisitos que se piden por el legislador y su cumplimiento.

- **CERTIFICADOS RECONOCIDOS**, según este tipo de certificados deben de cumplir con los rigorismos legislativos necesarios por cada país.

- **CERTIFICADOS NO RECONOCIDOS**. Aquellos que no llegan a cumplir los requisitos de rigor pero que le son exigidos ciertos elementos para su concretización.

6.10 IMPORTANCIA DE LAS ENTIDADES DE CERTIFICACIÓN

La importancia está en la función de vincular la identidad de un signatario con un dispositivo de firma, es en si una cédula de identidad digital. Se establece un nivel de seguridad de identidad. Por ello ningún certificado puede ser indefinido debido a que la identidad debe actualizarse cada cierto período, para preservar la seguridad.

Dan fe pública a grandes rasgos menciona el Artículo 8 de la ley de simplificación aduanera que las entidades de certificación podrán otorgar fe pública con respecto a que en una fecha y hora específica, personas individualizadas realizaron términos. Dicha información no puede ser negada a repudiada con posterioridad.

La importancia de las entidades de certificación también se desarrolla en lo que es la validez que tiene la contratación y los mensajes de datos por medios electrónicos a tal efecto el artículo 7 de la ley de simplificación aduanera establece *“El uso de medios informáticos y de la vía electrónica para el intercambio de información, 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"[153]*.*

6.10.1 CERTIFICADOS DE SEGURIDAD ELECTRÓNICO.

Implica no repudio y seguridad de la identidad y de la integridad del documento, es decir, que el documento firmado es el original y que nadie ha modificado su contenido después de su firma.

6.10.2 CERTIFICADOS DE SEGURIDAD EN LA COMUNICACIÓN.

Sirve para codificar una comunicación entre dos personas, haciendo que toda la información transmitida sea confidencial. Con ello se garantiza que cualquier documento enviado por una persona a otra estará cerrado y sólo podrá ser abierto por su legítimo destinatario[154].

6.10.3 CERTIFICADOS DE SEGURIDAD ENTRE LAS PARTES

Se da el caso que no estamos seguros que el receptor sea realmente quien dice ser, y por lo tanto el emisor puede tener dudas acerca de si enviar una información o no, la autoridad de certificación es la parte de confianza ella tiene un papel importante puesto que certifica a este como un autentico receptor.

---

[153] La firma electrónica y su Certificación, Bases Jurídicas de la Tecnología Informática y el comercio Electrónico. Editorial Portobelo, 1ª Edición Año 2004, Pág.45. Esta tesis el hecho de la importancia de los certificados reconociendo el hecho de su seguridad a través de la tecnología que está en la norma y por tanto es de carácter legal teniendo la potestad de hacerse valer como prueba en juicio.

[154] La Firma Electrónica y los Servicios de Certificación Hispadata Solutions. Los dispositivos de almacenamiento de diversos datos relativos al propietario de los mismos que permiten identificarlo en la red, garantizando la emisión de datos, como su recepción y la integridad de la información transmitida, es lo que se conoce como certificados electrónicos.

6.11 PRINCIPIOS GENERALES PARA LA PRESTACIÓN DE SERVICIOS DE CERTIFICACIÓN.

6.11.1 RÉGIMEN DE LIBRE COMPETENCIA.

Este principio se ve reflejado en la prestación de servicio de certificación sin que el ejercicio de esta actividad quede reservado a determinadas autoridades, sin necesidad de autorización previa o una inscripción registral.

6.11.2 SISTEMAS DE ACREDITACIÓN DE PRESTADORES DE SERVICIOS DE CERTIFICACIÓN.

La acreditación voluntaria, conforme al Artículo 2, Apartado II) del Real Decreto ley 14/1999, es un permiso, licencia o autorización que conlleva una serie de derechos y una serie de obligaciones para el prestador que voluntariamente la solicita y la obtiene, efectos positivos la presunción con la que se ven favorecidas aquellas firmas electrónicas avanzadas basadas en un certificado reconocido por certificadora acreditada[155].

6.11.3 REGISTRO DE PRESTADORES DE SERVICIOS DE CERTIFICACIÓN.

El incumplimiento de la inscripción general tiene escasa consecuencias y no impide el ejercicio de la actividad de certificación, esto debido a que no debe en ningún caso constituir un obstáculo al principio de libre competencia.

---

[155] MARTINEZ NADAL, APOLONIA, “La Firma Electrónica como Equivalente funcional, Espejismo o Realidad”. Universidad de las Islas Balcares, Pág. 191 y 192. Se dispone en este libro el hecho de la importancia de mantener como mercado un régimen de competencia en el cual la prestación del servicio sea primordial en los aspectos técnicos y económicos de seguridad para lograr crear confianza en los usuarios de firmas electrónicas.

6.12 OBLIGACIONES DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN.

6.12.1 OBLIGACIONES GENERALES

A) Comprobar la identidad y demás datos personales del solicitante.

B) Facilitar al signatario el dispositivo de creación y verificación de firma.

C) No almacenar ni copiar los datos de creación de firma del solicitante.

D) Antes de la emisión del certificado, deberán informar al solicitante sobre el precio, condiciones de uso y limitaciones del certificado.

E) Mantener un registro público de los certificados emitidos.

6.12.2 OBLIGACIONES ESPECÍFICAS

F) Indicar la fecha y hora de la expedición y/o revocación del certificado.

G) Demostrar fehacientemente la fiabilidad de servicios.

H) Garantizar rapidez y seguridad en la prestación de sus servicios.

I) Contar con empleados cualificados para los servicios ofertados[156].

[156] La Firma Electrónica y los Servicios de Certificación. Hispadata Solutions. Las obligaciones citadas tienen como principales objetivos proporcionar seguridad y confianza en la prestación de servicios y garantizar la calidad de los mismos, es por ello que identifican y corroboran los datos de los solicitantes, ya que ellos luego de tenerlos en sus datos darán fe que lo que se estableció es así, como queda escrito, porque ya hay una comprobación de esos datos, además de facilitar los dispositivos de creación de firma para fomentar y establecer la cercanía necesaria entre entidad certificadora y usuario, por ello es necesario que comuniquen hasta donde será su obligación como limitante de los certificados que sean emitidos.

Comprobar la Identidad y además datos personales del solicitante. *Para la comprobación de la identidad es necesario un documento que se denomina Certificado de Identidad Personal.*

Los Certificados de Identidad son los expedidos por las Autoridades de Certificación, para obtener el certificado de usuario de E-mail o de servicios se necesita como mínimo:

a) *Nombre y Apellido*
b) *Dirección de E-mail*
c) *País de Origen*
d) *Código Postal*
e) *Fecha de Nacimiento* [157].

Estas certificaciones de identidad establecen un sin número de beneficios como por ejemplo, pueden ser utilizadas, para validar operaciones y pagos y protegiendo y personalizando los contenidos electrónicos.

Poner a disposición del solicitante los sistemas de creación y verificación de la firma electrónica**.** Forma Física, se entiende aquella que llega de forma material hasta el usuario es necesario entonces tener locales con el propósito de brindar este servicio, se debe tener en cuenta que es seguro por el hecho de la garantía de resguardo de los datos personales del solicitante.

Solicitud on-line que por razones de tiempo y dinero se concibe para muchos empresarios y otros usuarios con la forma más práctica.

---

[157] Vid. NAJARRO, KENELMAN, BERENICE. *Comercio Electrónico y su Implicación en las Transformaciones…, Cit.,* Pág. 61 y 62. Se establece en esta tesis la importancia de la contratación electrónica y su implicación en el desarrollo económico y además hace mención de la seguridad que debe contener los mensajes de datos para establecer las obligaciones respectivas derivadas de la contracción por medios electrónicos.

Al solicitante del certificado se le informará sobre el costo económico que tendrá dicho certificado y las limitantes de su uso, estableciendo que documentos podrán encriptarse con respecto a los derechos del consumidor.

Se debe informar sobre las obligaciones del firmante, los mecanismos para garantizar la fiabilidad de la firma electrónica de un documento a lo largo del tiempo y condiciones precisas de utilización del certificado.

Declaración de prácticas de certificación, consiste en un documento por medio del cual el prestador de servicios detallará el marco legal que le rige las obligaciones a que se compromete y de los procedimientos especiales con los registros públicos correspondientes[158]*.*

Crear y conservar actualizado el registro de certificado. Los certificados tienen características de ser públicos es por ello que debe hacerse constar en los certificados emitidos a favor del suscriptor la fecha de caducidad y vigencia así como mantenerlo actualizado con el fin que las consultas realizadas sean eficaces y asegurar la integridad y protección de estos.

Regular la cesación de sus funciones de forma especial. Obligación de la autoridad certificadora de informar al usuario acerca del régimen aplicable en caso de que la entidad de certificación llegara a cesar por causas diferentes en sus funciones, que pueden hacer los usuarios en estos casos trasladarse a otra entidad de certificación o dejar sin efecto tales certificados debiendo comunicarlo a la autoridad competente[159].

---

[158] Vid. GRANILLO DE TOBAR, ANA YESSENIA."*La firma electrónica, su uso en el ámbito de la contratación electrónica y su aplicación*…., Cit., Pág.120. En este apartado se establece la diligencia del solicitante observando los alcances del certificado en relación directa a las condiciones que se derivan de la utilización.

[159] Vid. GRANILLO DE TOBAR, ANA YESSENIA."*La firma electrónica, su uso en el ámbito de la contratación electrónica y su aplicación*…., Cit., Pág.121. En este apartado se plantea el hecho de la actualización como una forma de dar confianza a las partes contratantes que los negocios que se

6.13 REQUISITO DE LAS ENTIDADES CERTIFICADORAS

6.13.1 REQUISITO TEMPORAL

Se debe indicar la fecha y la hora que se expide o se deja sin efecto un certificado. Importante también es hacer notar la hora en la cual es firmado de forma electrónica el mensaje.

6.13.2 REQUISITOS TÉCNICOS Y DE PERSONAL

Por el hecho de rapidez y seguridad en la prestación del servicio, el personal calificado para mantener seguridad que la tecnología que se utiliza es fiable y garantizan la seguridad técnica en los procesos de certificación, además se deben tomar medidas para la falsificación de los certificados.

6.13.3 REQUISITOS ECONÓMICOS

Se debe mantener recursos financieros suficientes con el fin de proteger a terceros que se relacionen al menos un 4 por 100 de la suma de los importes límite de las transacciones en que se puedan emplear el conjunto de los certificados que emita cada prestador de servicio.

6.13.4 REQUISITOS INFORMATIVOS Y DE DOCUMENTACIÓN

Se exige el registro de toda la información y documentación relativa a un certificado reconocido durante un período adecuado (quince años), con la finalidad de utilización como medio de prueba de la certificación[160].

---

realizen sean estables, con ello se hace referencia al hecho que la no actualizar los datos personales de una de las partes contratantes, se pensaría que con las condiciones que se contrata no han variado por el hecho que no esta reflejado en el registro de las entidades certificadoras.

[160] Vid MARTINEZ NADAL, APOL-LONIA. *La firma electrónica como equivalente…., Cit*., Pág. 194. Se denota en este libro la importancia que tienen los componentes técnicos y económicos para brindar seguridad a las partes que intervengan en las diferentes actividades electrónicas.

6.14 RESPONSABILIDADES DE LAS ENTIDADES DE CERTIFICACIÓN

6.14.1 RESPONSABILIDAD CIVIL

Por Incumplimiento de sus Obligaciones previamente Establecidas en la Ley. Con respecto a este punto la doctrina menciona que deben producirse daños y perjuicios a cualquiera de las personas involucradas por incumplimiento de obligaciones, por parte de las entidades de certificación es por ello que corresponderá a ella la obligación de demostrar que actuó con la debida diligencia.

Causas en las cuales el prestador de servicios no será responsable de daños y perjuicios.

a) No proporcionar al prestador de servicios de certificación información veraz y completa.

b) Negligencia en la conservación de sus datos de creación de firma.

c) Utilizar los datos de creación de firma cuando haya expirado el período de validez del certificado electrónico.

d) No utilizarlo conforme a las condiciones establecidas y comunicadas al firmante por el prestador de servicios de certificación[161].

[161] Vid GRANILLO DE TOBAR, ANA YESSENIA .*La firma electrónica, su uso en el ámbito de la contratación electrónica…., Cit.,* Pág. 126. Se menciona en esta parte que las obligaciones deben estar previamente establecidas en la ley, con ello se debe entender que difícilmente se podrá alegar algo que no esté contemplado en la ley.

6.14.2 RESPONSABILIDAD CIVIL POR EL USO INDEBIDO DE PARTE DE TERCERAS PERSONAS DE LOS CERTIFICADOS RECONOCIDOS Y EXTENDIDOS POR LAS ENTIDADES DE CERTIFICACIÓN.

El destinatario de los documentos firmados de forma electrónica deben de actuar diligentemente, ejemplo de esto sería que pudiendo consultar la vigencia del certificado en el registro público de certificados no lo hace.

En todo caso la responsabilidad civil deberá caer en la entidad certificadora la cual deberá satisfacer inicialmente con el capital mínimo que exige la ley.

El certificado al ser remitido al usuario debe consignarse los alcances del certificado y sus limitaciones y la fecha de vencimiento.

Es lógico considerar que al mencionar el alcance del certificado la entidad certificadora ha prevenido de forma tácita hasta donde puede utilizarse dicho certificado y además se establece el vencimiento para que el usuario no pueda alegar ignorancia con respecto a la vigencia y por ende validez de sus negocios con aspecto a la utilización de la tecnología depositada en el certificado para asegurar la utilización de una firma electrónica. [162]Es importante hacer mención que la Ley de simplificación Aduanera equipara los escritos en soporte papel con los documentos con los contenidos en un soporte magnético, digital o Electrónico.

La referida ley menciona que Teledespacho es un conjunto sistematizado de elementos tecnológicos de carácter informativo y de comunicaciones que permiten ,dentro de un marco de mutuas

[162] Vid. GRANILLO DE TOBAR, ANA YESSENIA."*La firma electrónica, su uso en el ámbito de la contratación electrónica y su aplicación* …., Cit., Pág. 127. Se establece de forma lógica el alcance de los certificados de forma clara y precisa para el buen manejo de estos y así evitar inconvenientes en el futuro.

responsabilidades y procedimientos autorizados ,el intercambio de información ,por vía electrónica esa información será de carácter tributaria entre la dirección general los usuarios[163].

Además La Ley de Simplificación Aduanera establece que el uso de medios informáticos y de la vía electrónica para el intercambio de información, gozara de plena validez y los efectos jurídicos será la misma que la producida en soportes físicos, establece además que en caso de disconformidad de datos de un mismo documento registrados en bancos o usuarios y los registrados por aduana se tomaran como correcto los datos sobre los cuales la entidad certificadora hubiere otorgado fe publica.

En esta Ley (LSA) se establecen los requisitos de las entidades certificadoras como capacidad tecnológica y cumplir con los requisitos legales, además menciona que la vinculación de llaves o claves, publica y privada constituye la firma digital o electrónica, también señala que los suscriptores tendrá la obligación de guardar secretos acerca de las llaves privadas que se les haya sido asignadas.

[163] Ley de Simplificación Aduanera…, Cit., Articulo 6. párrafo segundo. Importante es hacer notar que se establece el intercambio de información de carácter tributario con valides para su no repudio esto con el fin de brindar seguridad Jurídica por medio de la tecnología y brindar confianza en aquellas personas que hagan uso de estos métodos además de dar agilidad y evitar de esta forma los atrasos que se pueden dar por el hecho de verificar todo en forma material.

CAPITULO VII

CONCLUCIONE Y RECOMENDACIONES

SUMARIO: 7.1 Conclusiones.- 7.2 Recomendaciones

7.1 CONCLUCIONES

PRIMERA: El Salvador no se cuentan con soluciones técnicas que respalden el contenido de los mensajes realizados por medios electrónicos de forma adecuada.

SEGUNDA: La contratación electrónica no posee, el desarrollo que debería tener por el hecho de la dinámica mundial, ya que a nivel internacional se exigen estándares de calidad es por este motivo que El Salvador debe modernizarse aprobando una ley que dinamice el comercio por medios electrónicos

TERCERA: No existen soportes adecuados para el comercio electrónico que aseguren el funcionamiento de las tecnologías empleadas.

CUARTA: Se establece como uno de los principios de la contratación electrónica la neutralidad tecnológica que consiste en no discriminar el uso de las diferentes tecnologías incluso aquellas que no existen con el propósito de dar de forma amplia cobertura a todas las tecnologías existentes y no existentes.

QUINTA: En muchos Estados se regula a nivel nacional el funcionamiento de las redes en sus sistemas jurídicos, con lo que se está en un riesgo grande en cuanto que cada uno de estos Estados puede quedar aislado por la incompatibilidad tecnológica que no les permita integrarse y la

normativa puede resultar insuficiente para resolver las particularidades que las redes presentan.

SEXTA: La firma electrónica y los demás elementos que hacen que esta sea operativa representan solo una porción de la certeza en las transacciones electrónicas, pero esta representa tan solo una seguridad técnica, y para que sea fiable es necesario que la firma electrónica tenga un fundamento legal.

SEPTIMA: En definitiva la firma electrónica es importante como medio de acreditación de la identidad e integridad del autor, tanto del contenido cuanto del documento electrónico. Cuyo uso se irá incrementando en la medida en que los países regulen homogéneamente su utilización.

OCTAVA: Es importante reconocer que en El Salvador el uso de la firma electrónica solo seda en la administración pública, como por ejemplo en el caso del ministerio de Hacienda con la trasmisión de datos de mercaderías en las aduanas por medio del teledespacho.

7.2 RECOMENDACIONES

PRIMERA: Crear soluciones técnicas, como el hecho de establecer software y hardware propicios que respalden lo contenido en un mensaje electrónico de forma adecuada en El Salvador ,para que las partes contratantes emisor y receptor puedan establecer sus relaciones comerciales con toda confianza.

SEGUNDA: Incentivar el desarrollo de la contratación electrónica en El Salvador, para generar mayor competitividad en el área internacional adecuándose a los estándares mundiales.

TERCERA: Se recomienda dar soportes técnicos adecuados para establecer el comercio electrónico por ejemplo, el mantenimiento de computadoras tanto en el software como en el hardware, con periodos constantes de revisión para asegurar el funcionamiento en las tecnologías empleadas.

CUARTA: Se recomienda que no exista discriminación en cuanto al método utilizado para implementar tecnología en la contratación electrónica podrán hacerse por medios biométricos, tarjetas inteligentes y otras.

QUINTA: Se recomienda sancionar normas uniformes tanto a nivel centroamericano como internacional que establezcan criterios mínimos comunes que puedan ser adoptados por todos los Estados para que no hayan barreras entre las naciones y permitir un desarrollo uniforme en los mercados, para que estas normas sean capaces de mantener una adaptabilidad permanente a los nuevos desafíos que aparezcan por la constante evolución tecnológica.

SEXTA: Es transcendental crear una política de seguridad tecnológica y jurídica en el campo de la contratación por medios electrónicos en el país, para poder aprovechar las ventajas que estas puedan traer tanto como a la administración pública como ,a los empresarios y consumidores ,porque con estas políticas se estaría brindando en el caso de Administración Pública mayor agilidad en los tramites con sus administrados; los empresarios que cada día necesitan de soportes electrónicos para poder competir en el mercado que cada día se vuelve más exigente ,y les pueda permitir a los empresarios nacionales desarrollar su actividad de una manera igualitaria a sus competidores, y no solo en el ámbito nacional si no que a nivel internacional. Y a los consumidores les permitiría la oportunidad de acceder de una manera más cómoda a los diferentes productos y servicios que ofrece el mercado.

SEPTIMA: Es conveniente que nuestra legislación le de valor a la firma electrónica como un método seguro y fiable con lo que se le dará validez jurídica a los acuerdos en los que esta se ha utilizado, por si surgiera un conflicto entre las partes de la contratación electrónica estas tendrían la posibilidad de ejecutar las demandas ante los tribunales competentes.

OCTAVA: Es esencial que en El Salvador exista una ley especial que regule el comercio electrónico, firma electrónica y las contrataciones por medios electrónicos para permitir un desarrollo del mercado Salvadoreño tanto a nivel regional como internacional y no quedar relegados de las modernas formas de hacer negocios y en desventaja con países como: Guatemala, Costa Rica, México, Panamá, Colombio, Argentina entre otros.

BIBLIOGRAFIA

LIBROS

ALTERINI, ATILIO ANÍBAL, DE LOS MOZOS, JOSÉ LUIS, *Contratación contemporánea*, Editorial Temis, Bogotá-Colombia, 2000.

ÁLVAREZ CIENFUEGOS, JOSÉ MARÍA, "La Firma Electrónica Y el Comercio Electrónico en España", Comentarios a la legislación Vigente, Editorial Aranzadi, S.A, Navarra, España, 2000.

CASTELLANOS DE UBAO, LEOPOLDO GONZALES-ECHENIQUE, "*La Firma Electrónica" en AA VVV* Derecho de Internet, Contratación Electrónica y Firma Digital, Coordinado por Mateus de Ros, Rafael y Cendoya Méndez de Vigo Juan Manuel, Editorial Aranzadi, Navarra, 2000.

CUBILLOS VELANDIA, RAMIRO, RINCÓN CARDENAS, ERICK. *Introducción Jurídica al Comercio Electrónico,* Gustavo Ibáñez, Colombia, 2002.

DAVARA, RODRIGUEZ, MIGUEL ANGEL. "*Manual de Derecho Informático*". Ediciones Aranzandi. España.1997.

DIEZ PICAZO, LUÍS, "*Fundamentos del Derecho Civil Patrimonial",* Quinta Edición, Editorial Civita, Madrid-España, 1996.

HINESTROSA, FERNANDO, **"***El Contrato por Medios Electrónico"***,** Homenaje a sus 40 años de Rectoría, Colombia, 1963 **–**2003**.**

MARTÍNEZ NADAL, APOL·LÒNIA, "*Comercio Electrónico, Firma Digital Y Autoridades de Certificación",* Editorial Civita, Madrid, 2001.

MATEU DE ROS, RAFAEL, CENDOYA MENDEZ DE VIGO, JUAN MANUEL, "*Derecho de Internet. Contratación Electrónica y Firma digital",* 3 Edición, Editorial Aranzadi, Madrid, 2001

MESA BARROS, RAMÓN, *Manual de Derecho Civil; de las fuentes de las Obligaciones*, Tomo Quinta Edición; Editorial Jurídica de Chile; 1976.

NASH, A. DUANE, W. JOSEPH, C. BRINK, D., "*PKI Infraestructura de Claves Publicas*", Osborne MacGraw-Hill, Bogotá, 2002.

OSPINA FERNADEZ, GUILLERMO, OSPINA ACOSTA, EDUARDO, *Teoría General del Contrato y del Negocio Jurídico,* 6ª Edición, Editorial Temis, Bogotá, 2000.

PETIT, EUGENE, *"Derecho Romano*" Editorial Porrua, Tercera Edición, México, 1997.

REYES VILLAMIZAR, FRANCISCO; *Algunas Consideraciones sobre el Régimen Jurídico del Comercio Electrónico en Colombia,* en foro de justicia, Cámara de comercio de Medellín para Antioquia, 2001

RODRÍGUEZ ALESSANDRI, ARTURO; UNDURRAGA SOMARRIBA, MANUEL, *Curso de Derecho Civil fuente de las obligaciones*. Redactado por Antonio, Vodanovic H; Tomo IV; Editorial Nascimento; Chile; 1976.

UREBA, ALBERTO ALONSO, VIERA GONZALEZ, ARÍSTIDES JORGE, *Formación y perfección de los contratos a distancia celebrados por Internet,* en AA VV Derecho de Internet, La ley de Servicios de la Sociedad de la Información y de comercio electrónico, Coordinado por Mateus de Ros, Rafael, 3 Edición, Editorial Aranzadi, Madrid, 2001.

VILLAR, JOSE MANUEL." Una aproximación a La Firma Electrónica"" en AA VV Derecho de Internet, Contratación Electrónica y Firma Digital , coordinado por Matéu de Ros, R. y Cendoya Méndez de Vigo, J.M., Editorial. Aranzadi, Navarra, Madrid, 2000.

TESIS

AGUILAR MORAN, RAUL ARMANDO. HERNANDEZ NUÑEZ, EVELYN YESENIA. "El Comercio Electrónico en El Salvador". Universidad de El Salvador. Tesis Año 2002.

ALCANTARA QUINTANILLA, MILTON LEONIDAS, "Análisis Jurídico del Comercio Electrónico". Universidad Francisco Gaviria, Tesis 2003.

GAITÁN CORTES, CARLOS ERNESTO, GUZMÁN, MARTA, RIVAS, VICENTE *Relaciones Contractuales en Internet y su Desprotección por la falta de Legislación de Comercio Electrónico*. Universidad de El Salvador 2003.

GALAN CORTEZ, JEANNIE ELIZABETH, *La firma Digital como medio de Seguridad y consentimiento en las transacciones del comercio Electrónico*. Universidad de El Salvador. Tesis 2006.

GRANILLO DE TOBAR, ANA YESSENIA, *La Firma Electrónica, su uso en el ámbito de la Contratación Electrónica y su Aplicación por las Administraciones Publicas, Trabajo de Tesina, San Salvador, 2004*.

NAJARRO, KENELMA BERENICE *Comercio Electrónico y su aplicación en las trasformaciones Económicas y tecnológicas de los países en desarrollo*. Universidad de El Salvador. Tesis -2002.

SITIOS WEB

http: //es ucla/personal history. Visitada el 5 de Agosto de 2008.

http/www.derecho.org. Visitada el 25 de Agosto de 2008.
http://www.monografias.com visitada el día 13 de septiembre de 2008.

htt://www.comunidadene.com/docu/contratos.pdf visitada el 13 de octubre de 2008.

htt.//www.teleley.com/articulos/art_patroni.pdf visitada el 13 de octubre de 2008.

http://www.firmadigital.com visitada el 14 de octubre de 2008.

htt://www.scielo.cl/scielo.php?pid=so718001200500020009&script=sci_arttex#nota18 visitada el 16 de octubre de 2008.

http://civil.udg.es/normacivil/estatal/CC/4T2.htm visitada el 18 de octubre de 2008.

Htt://www.protegedatos.com/web/lssice/contratos.html#arriba visitada el 20 de octubre de 2008.

http://www.resa.es visitada el 24 de octubre de 2008.

http**://** www.alviolor.com visitada el 1 de noviembre de 2008.

htt://www.diescoean.com.sv. Visitada el 22 de noviembre de 2008.

http://www.delitosinformaticos.com/firmaelectronica/analisis2.shtml visitada el 13 de diciembre de 2008.

.http://www.comunidad.derecho.org. Visitada el 29 de diciembre de 2008.

LEGISLACIONES

Constitución de la República de El Salvador con Jurisprudencia, Decreto Legislativo Nº.154, del 2 de Octubre del 2003, Publicado en el Diario Oficial Nº 191, Tomo 361, del 15 de Octubre de 2003.

Convención de las Naciones Unidas sobre los Contratos de Compraventa Internacional de mercaderías, Ratificada el 18 de Noviembre de 1999, Publicado en el Diario Oficial Nº 239, Tomo 345, del 22 de diciembre de 1999.

Código Civil Salvadoreño, Decreto Legislativo Nº.512, del 11 de noviembre de 2004, Publicado en el Diario Oficial Nº 276, Tomo 365, del 17 de diciembre de 2004.

Ley General Marítimo Portuaria Decreto Legislativo Nº: 994 de 19 de septiembre de 2002, Publicada en el Diario Oficial Nº 182 Tomo 357 de 1 octubre de 2002.

Ley de Simplificación Aduanera, Decreto Nº 529, D O. Nº 23, tomo 342, del 3 de febrero /1999.

Guía para la incorporación al Derecho Interno de la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI9 para las Firmas Electrónicas (2001).

Directiva 2000/31/CE, del Parlamento Europeo y del Consejo de 8 de junio, relativa a determinados aspectos de los servicios de la sociedad de la información, en particular, el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico)

Real –Decreto ley 14/1999 Sobre la Firma Electrónica de 13 de Septiembre de 1999.(derogado)

Real Decreto Ley 59/2003 sobre la Firma Electrónica de fecha 19 de Diciembre del año 2003.

OTROS DOCUMENTOS

Guía sobre la firma Electrónica y Entidades de Certificación, bases jurídicas de la Tecnología Informática y el Comercio Electrónico .Editorial Portobelo, 1ª Edición, Marzo del 20004.

Guía para el estudio de Derecho Civil II Bienes, febrero 2003. Iniciativa GLIN AMERICAS Banco Interamericano de Desarrollo, Documento Conceptual para la Legislación en Era de la Información, "*firma digital y contratos electrónicos",* 2005

ANEXOS

GLOSARIO

Autoridad Certificante: Organización o entidad de confianza encargada de emitir, registrar y publicar certificados. Además verifica la identidad del solicitante del certificado y publica las listas de revocación de certificados. También son las encargadas de mantener los registros de claves públicas directamente en línea (on line).

Certificado digital: Registros electrónicos que atestiguan fehacientemente que determinada clave pública pertenece a una persona o entidad, permite realizar un conjunto de acciones de manera segura y con validez legal.

Cifrado de claves pública y privada: Es una forma asimétrica de cifrado basado en un par de claves, pública y privada, generadas criptográficamente. Los datos cifrados con una clave privada pueden descifrarse únicamente con la clave pública correspondiente y viceversa.

Clave: Valor utilizado en combinación con un algoritmo para encriptar o desencriptar información. Los algoritmos de cifrado simétricos utilizan la misma clave para cifrar y descifrar mientras que los algoritmos asimétricos utilizan un par de claves: pública y privada.

Clave privada y clave pública: Mitad del secreto de un par de claves: pública y privada. Se utilizan para firmar digitalmente un mensaje o descifrarlo.

Código Hash: Utiliza una función matemática consistente en crear una representación numérica para todo el certificado, de tal forma que éste pasa a ser representado por un valor numérico o cadena de datos.

Firma digital: Herramienta tecnológica que se incluye o transmite con un mensaje y se utiliza para identificar y autentificar al emisor y a la información del mensaje y así garantizar su validez, integridad e invariabilidad de los datos durante el tránsito.

Firma electrónica: Conjunto de datos electrónicos adjuntados o asociados a un mensaje y utilizados como medio para identificar al autor con relación al mismo e indicar que lo aprueba.

Firma electrónica avanzada: Denominación equivalente a la “firma digital” utilizada por algunas legislaciones, como es el caso de España, la Unión Europea, Brasil y Chile.

Infraestructura de Clave Pública: Conocida mundialmente con las siglas PKI por su denominación en inglés Public Key Infraestructure, es al conjunto de leyes, normativa legal complementaria, obligaciones legales, hardware, software, bases de datos, redes, estándares tecnológicos y procedimientos de seguridad que permiten que distintas entidades (individuos u organizaciones) se identifiquen entre sí de manera segura al realizar transacciones en redes.

Par de claves: Formado por una clave pública y otra privada pertenecientes a una entidad y utilizadas para cifrar y descifrar datos.

Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la Guía para su incorporación al derecho interno 2001

NACIONES UNIDAS
Nueva York, 2002

Resolución aprobada por la Asamblea General [sobre la base del informe de la Sexta Comisión (A/56/588)] 56/80 Ley Modelo sobre las Firmas Electrónicas de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional

La Asamblea General, Recordando su resolución 2205 (XXI), de 17 de diciembre de 1966, por la que estableció la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional con el mandato de fomentar la armonización y la unificación progresivas del derecho mercantil internacional y de tener presente, a ese respecto, el interés de todos los pueblos, en particular el de los países en desarrollo, en el progreso amplio del comercio internacional,

Observando que un número creciente de transacciones comerciales internacionales se realizan por el medio de comunicación habitualmente conocido como comercio electrónico, en el que se usan métodos de comunicación, almacenamiento y autenticación de la información sustitutivos de los que utilizan papel,

Recordando la recomendación relativa al valor jurídico de los registros computadorizados aprobada por la Comisión en su 18.° período de sesiones, celebrado en 1985, y el apartado b) del párrafo 5 de la resolución 40/71 de la Asamblea General, de 11 de diciembre de 1985, en la que la Asamblea pidió a los gobiernos y a las organizaciones internacionales que, cuando así convenga, adopten medidas acordes con las recomendaciones de la Comisión 1 a fin de garantizar la seguridad jurídica en el contexto de la utilización más amplia posible del procesamiento automático de datos en el comercio internacional,

Recordando también que la **Ley Modelo sobre Comercio Electrónico** fue aprobada por la Comisión en su 29.° período de sesiones, celebrado en 19962, y complementada por un nuevo artículo 5 bis, aprobado por la Comisión en su 31.° período de sesiones, celebrado en 19983, y recordando el párrafo 2 de la resolución 51/162 de la Asamblea General, de 16 de diciembre de 1996, en la que la Asamblea recomendaba que todos los Estados consideraran de manera favorable la Ley Modelo cuando promulgaran o revisaran sus leyes, habida cuenta

de la necesidad de que el derecho aplicable a los métodos de comunicación y almacenamiento de información sustitutivos de los que utilizan papel sea uniforme, convencida de que la **Ley Modelo sobre Comercio Electrónico** es de considerable utilidad para los Estados al posibilitar o facilitar la utilización del comercio electrónico, como demuestra la incorporación de esta Ley Modelo al derecho interno de un cierto número de países y su reconocimiento universal como referencia esencial en lo relativo a la legislación sobre el comercio electrónico,

Consciente de la gran utilidad de las nuevas tecnologías de identificación personal utilizadas en el comercio electrónico, generalmente conocidas como firmas electrónicas,

Deseosa de desarrollar los principios fundamentales enunciados en el artículo 7 de la **Ley Modelo sobre Comercio Electrónico** con respecto al cumplimiento de la función de la firma en las operaciones de comercio electrónico, con miras a fomentar la confianza en las firmas electrónicas para que surtan efectos jurídicos cuando sean el equivalente funcional de las firmas manuales,

Convencida de que la armonización tecnológicamente neutral de ciertas normas relativas al reconocimiento jurídico de las firmas electrónicas y el establecimiento de un método para evaluar de un modo tecnológicamente neutral la fiabilidad práctica y la idoneidad comercial de las técnicas de firma electrónica darán una mayor certidumbre jurídica al comercio electrónico,

Estimando que la Ley Modelo sobre las Firmas Electrónicas constituirá un útil complemento de la Ley Modelo sobre Comercio Electrónico y ayudará en gran medida a los Estados a formular legislación que regule la utilización de técnicas modernas de autenticación y a mejorar la legislación ya existente,

Considerando que la elaboración de legislación modelo que facilite la utilización de las firmas electrónicas de forma que sea aceptable para Estados con distintos ordenamientos jurídicos, sociales y económicos podría contribuir al fomento de relaciones económicas armoniosas en el plano internacional,

1. Expresa su gratitud a la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional por haber completado y aprobado la Ley Modelo sobre las Firmas Electrónicas que figura en el anexo a la presente resolución y por haber preparado la Guía para la incorporación de la Ley Modelo al derecho interno;

2. Recomienda que todos los Estados consideren de manera favorable la Ley Modelo sobre las Firmas Electrónicas, junto con la **Ley Modelo sobre Comercio Electrónico** aprobada en 1996 y complementada en 1998, cuando promulguen o revisen sus leyes, habida cuenta de la necesidad de que el derecho aplicable a los métodos de comunicación, almacenamiento y autenticación de la información sustitutivos de los que utilizan papel sea uniforme;

3. Recomienda también que se haga todo lo posible por promover el conocimiento y la disponibilidad generales de la **Ley Modelo sobre Comercio Electrónico** y de la Ley Modelo sobre las Firmas Electrónicas, junto con sus respectivas Guías para la incorporación al derecho interno.

85ª sesión plenaria

12 de diciembre de 2001

Primera parte. Ley Modelo de la CNUDMI sobre las Firmas Electrónicas (2001)

Artículo 1. Ámbito de aplicación

La presente Ley será aplicable en todos los casos en que se utilicen firmas electrónicas en el contexto *(1)* de actividades comerciales *(2)*. No derogará ninguna norma jurídica destinada a la protección del consumidor.

Artículo 2. Definiciones

Para los fines de la presente Ley:

a) Por *"firma electrónica"* se entenderán 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;

b) Por *"certificado"* se entenderá todo mensaje de datos u otro registro que confirme el vínculo entre un firmante y los datos de creación de la firma;

c) Por *"mensaje de datos"* se entenderá la información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax;

d) Por *"firmante"* se entenderá la persona que posee los datos de creación de la firma y que actúa por cuenta propia o por cuenta de la persona a la que representa;

e) Por *"prestador de servicios de certificación"* se entenderá la persona que expide

certificados y puede prestar otros servicios relacionados con las firmas electrónicas;

f) Por *"parte que confía"* se entenderá la persona que pueda actuar sobre la base de un certificado o de una firma electrónica.

Artículo 3. Igualdad de tratamiento de las tecnologías para la firma

Ninguna de las disposiciones de la presente Ley, con la excepción del artículo 5, será aplicada de modo que excluya, restrinja o prive de efecto jurídico cualquier método para crear una firma electrónica que cumpla los requisitos enunciados en el párrafo 1) del artículo 6 o que cumpla de otro modo los requisitos del derecho aplicable.

Artículo 4. Interpretación

1. En la interpretación de la presente Ley se tendrán en cuenta su origen internacional y la necesidad de promover la uniformidad en su aplicación y de asegurar la observancia de la buena fe.

2. Las cuestiones relativas a las materias que se rigen por la presente Ley que no estén expresamente resueltas en ella se dirimirán de conformidad con los principios generales en los que se basa esta Ley.

Artículo 5. Modificación mediante acuerdo

Las partes podrán establecer excepciones a la presente Ley o modificar sus efectos mediante acuerdo, salvo que ese acuerdo no sea válido o eficaz conforme al derecho aplicable.

Artículo 6. Cumplimiento del requisito de firma

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

2. El párrafo 1) será aplicable tanto si el requisito a que se refiere está expresado en forma de una obligación como si la ley simplemente prevé consecuencias para el caso de que no haya firma.

3. La firma electrónica se considerará fiable a los efectos del cumplimiento del requisito a que se refiere el párrafo 1) si:

a) los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante;

b) los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante;

c) es posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma; y

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

4. Lo dispuesto en el párrafo 3) se entenderá sin perjuicio de la posibilidad de que cualquier persona:

a) demuestre de cualquier otra manera, a los efectos de cumplir el requisito a que se refiere el párrafo 1), la fiabilidad de una firma electrónica; o

b) aduzca pruebas de que una firma electrónica no es fiable.

5. Lo dispuesto en el presente artículo no será aplicable a: *[Y]*.

Artículo 7. Cumplimiento de lo dispuesto en el artículo 6

1. [La persona, el órgano o la entidad, del sector público o privado, a que el Estado promulgante haya expresamente atribuido competencia] podrá determinar qué firmas electrónicas cumplen lo dispuesto en el artículo 6 de la presente Ley.

2. La determinación que se haga con arreglo al párrafo 1) deberá ser compatible con las normas o criterios internacionales reconocidos.

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

Artículo 8. Proceder del firmante

1. Cuando puedan utilizarse datos de creación de firmas para crear una firma con efectos jurídicos, cada firmante deberá:

a) actuar con diligencia razonable para evitar la utilización no autorizada de sus datos de creación de la firma;

b) sin dilación indebida, utilizar los medios que le proporcione el prestador de servicios de certificación conforme al artículo 9 de la presente Ley, o en cualquier caso esforzarse razonablemente, para dar aviso a cualquier persona que, según pueda razonablemente prever el firmante, pueda considerar fiable la firma electrónica o prestar servicios que la apoyen si:

i) el firmante sabe que los datos de creación de la firma han quedado en entredicho; o

ii) las circunstancias de que tiene conocimiento el firmante dan lugar a un riesgo considerable de que los datos de creación de la firma hayan quedado en entredicho;

c) cuando se emplee un certificado para refrendar la firma electrónica, actuar con diligencia razonable para cerciorarse de que todas las declaraciones que haya hecho en relación con el ciclo vital del certificado o que hayan de consignarse en él son exactas y cabales.

2. Serán de cargo del firmante las consecuencias jurídicas que entrañe el hecho de no haber cumplido los requisitos enunciados en el párrafo 1).

Artículo 9. Proceder del prestador de servicios de certificación

1. Cuando un prestador de servicios de certificación preste servicios para apoyar

una firma electrónica que pueda utilizarse como firma con efectos jurídicos, ese prestador de servicios de certificación deberá:

a) actuar de conformidad con las declaraciones que haga respecto de sus normas y prácticas;

b) actuar con diligencia razonable para cerciorarse de que todas las declaraciones importantes que haya hecho en relación con el ciclo vital del certificado o que estén consignadas en él son exactas y cabales;

c) proporcionar a la parte que confía en el certificado medios razonablemente accesibles que permitan a ésta determinar mediante el certificado:

i) la identidad del prestador de servicios de certificación;

ii) que el firmante nombrado en el certificado tenía bajo su control los datos de creación de la firma en el momento en que se expidió el certificado;

iii) que los datos de creación de la firma eran válidos en la fecha en que se expidió el certificado o antes de ella;

d) proporcionar a la parte que confía en el certificado medios razonablemente accesibles que, cuando proceda, permitan a ésta determinar mediante el certificado o de otra manera:

i) el método utilizado para comprobar la identidad del firmante;

ii) cualquier limitación de los fines o del valor respecto de los cuales puedan utilizarse los datos de creación de la firma o el certificado;

iii) si los datos de creación de la firma son válidos y no están en entredicho;

iv) cualquier limitación del alcance o del grado de responsabilidad que haya establecido el prestador de servicios de certificación;

v) si existe un medio para que el firmante dé aviso de que los datos de creación de la firma están en entredicho, conforme a lo dispuesto en el apartado b) del párrafo 1) del artículo 8 de la presente Ley;

vi) si se ofrece un servicio para revocar oportunamente el certificado;

e) cuando se ofrezcan servicios conforme al inciso v) del apartado d), proporcionar un medio para que el firmante dé aviso conforme al apartado b) del párrafo 1) del artículo 8 de la presente Ley y, cuando se ofrezcan servicios en virtud del inciso vi) del apartado d), cerciorarse de que existe un servicio para revocar oportunamente el certificado;

f) utilizar, al prestar sus servicios, sistemas, procedimientos y recursos humanos fiables.

2. Serán de cargo del prestador de servicios de certificación las consecuencias jurídicas que entrañe el hecho de no haber cumplido los requisitos enunciados en el párrafo 1).

Artículo 10. Fiabilidad

A los efectos del apartado f) del párrafo 1) del artículo 9, para determinar si los sistemas, procedimientos o recursos humanos utilizados por un prestador de servicios de certificación son fiables, y en qué medida lo son, podrán tenerse en cuenta los factores siguientes:

a) los recursos humanos y financieros, incluida la existencia de activos;

b) la calidad de los sistemas de equipo y programas informáticos;

c) los procedimientos para la tramitación del certificado y las solicitudes de certificados, y la conservación de registros;

d) la disponibilidad de información para los firmantes nombrados en el certificado y para las partes que confíen en éste;

e) la periodicidad y el alcance de la auditoria realizada por un órgano independiente;

f) la existencia de una declaración del Estado, de un órgano de acreditación o del prestador de servicios de certificación respecto del cumplimiento o la existencia de los factores que anteceden; o

g) cualesquiera otros factores pertinentes.

Artículo 11. Proceder de la parte que confía en el certificado

Serán de cargo de la parte que confía en el certificado las consecuencias jurídicas que entrañe el hecho de que no haya tomado medidas razonables para:

a) verificar la fiabilidad de la firma electrónica; o

b) cuando la firma electrónica esté refrendada por un certificado:

i) verificar la validez, suspensión o revocación del certificado; y

ii) tener en cuenta cualquier limitación en relación con el certificado.

Artículo 12. Reconocimiento de certificados extranjeros y de firmas electrónicas extranjeras

1. Al determinar si un certificado o una firma electrónica producen efectos jurídicos, o en qué medida los producen, no se tomará en consideración:

a) el lugar en que se haya expedido el certificado o en que se haya creado o utilizado la firma electrónica; ni

b) el lugar en que se encuentre el establecimiento del expedidor o del firmante.

2. Todo certificado expedido fuera [del Estado promulgante] producirá los mismos efectos jurídicos en [el Estado promulgante] que todo certificado expedido en [el Estado promulgante] si presenta un grado de fiabilidad sustancialmente equivalente.

3. Toda firma electrónica creada o utilizada fuera [del Estado promulgante] producirá los mismos efectos jurídicos en [el Estado promulgante] que toda firma electrónica creada o utilizada en [el Estado promulgante] si presenta un grado de fiabilidad sustancialmente equivalente.

4. A efectos de determinar si un certificado o una firma electrónica presentan un grado de fiabilidad sustancialmente equivalente para los fines de párrafo 2), o del párrafo 3), se tomarán en consideración las normas internacionales reconocidas y cualquier otro factor pertinente.

5. Cuando, sin perjuicio de lo dispuesto en los párrafos 2), 3) y 4), las partes acuerden entre sí la utilización de determinados tipos de firmas electrónicas o certificados, se reconocerá que ese acuerdo es suficiente a efectos del reconocimiento transfronterizo, salvo que el acuerdo no sea válido o eficaz conforme al derecho aplicable.

---

(1) La Comisión propone el texto siguiente para los Estados que deseen ampliar el ámbito de aplicación de la presente Ley:

La presente Ley será aplicable en todos los casos en que se utilicen firmas electrónicas, excepto en las situaciones siguientes: [Y] .

(2) El término "comercial" deberá ser interpretado en forma lata de manera que abarque las cuestiones que dimanen de toda relación de índole comercial, sea o no contractual. Las relaciones de índole comercial comprenden, aunque no exclusivamente, las operaciones siguientes: toda operación comercial de suministro o intercambio de bienes o servicios; acuerdos de distribución; representación o mandato comercial; facturaje (Afactoring@) ; arrendamiento con opción de compra (Aleasing@); construcción de obras; consultoría; ingeniería; concesión de licencias; inversiones; financiación; banca; seguros; acuerdos o concesiones de explotación; empresas conjuntas y otras formas de cooperación industrial o comercial; transporte de mercancías o de pasajeros por vía aérea, marítima y férrea o por carretera.

Real- Decreto Ley 59/2003, de 19 de diciembre, Sobre la firma electrónica. (España)

Sumario:

- **TÍTULO I. DISPOSICIONES GENERALES.**
  - **Artículo 1.** Objeto.
  - **Artículo 2.** Prestadores de servicios de certificación sujetos a la Ley.
  - **Artículo 3.** Firma electrónica, y documentos firmados electrónicamente.
  - **Artículo 4.** Empleo de la firma electrónica en el ámbito de las Administraciones públicas.
  - **Artículo 5.** Régimen de prestación de los servicios de certificación.
- **TÍTULO II. CERTIFICADOS ELECTRÓNICOS.**
  - **CAPÍTULO I. DISPOSICIONES GENERALES.**
    - **Artículo 6.** Concepto de certificado electrónico y de firmante.
    - **Artículo 7.** Certificados electrónicos de personas jurídicas.
    - **Artículo 8.** Extinción de la vigencia de los certificados electrónicos.
    - **Artículo 9.** Suspensión de la vigencia de los certificados electrónicos.
    - **Artículo 10.** Disposiciones comunes a la extinción y suspensión de la vigencia de certificados electrónicos.
  - **CAPÍTULO II. CERTIFICADOS RECONOCIDOS.**
    - **Artículo 11.** Concepto y contenido de los certificados reconocidos.
    - **Artículo 12.** Obligaciones previas a la expedición de certificados reconocidos.

        - **Artículo 13.** Comprobación de la identidad y otras circunstancias personales de los solicitantes de un certificado reconocido.
        - **Artículo 14.** Equivalencia internacional de certificados reconocidos.
    - **CAPÍTULO III. EL DOCUMENTO NACIONAL DE IDENTIDAD ELECTRÓNICO.**
        - **Artículo 15.** Documento nacional de identidad electrónico.
        - **Artículo 16.** Requisitos y características del documento nacional de identidad electrónico.
- **TÍTULO III. PRESTACIÓN DE SERVICIOS DE CERTIFICACIÓN.**
    - **CAPÍTULO I. OBLIGACIONES.**
        - **Artículo 17.** Protección de los datos personales.
        - **Artículo 18.** Obligaciones de los prestadores de servicios de certificación que expidan certificados electrónicos.
        - **Artículo 19.** Declaración de prácticas de certificación.
        - **Artículo 20.** Obligaciones de los prestadores de servicios de certificación que expidan certificados reconocidos.
        - **Artículo 21.** Cese de la actividad de un prestador de servicios de certificación.
    - **CAPÍTULO II. RESPONSABILIDAD.**
        - **Artículo 22.** Responsabilidad de los prestadores de servicios de certificación.
        - **Artículo 23.** Limitaciones de responsabilidad de los prestadores de servicios de certificación.
- **TÍTULO IV. DISPOSITIVOS DE FIRMA ELECTRÓNICA Y SISTEMAS DE CERTIFICACIÓN DE PRESTADORES DE SERVICIOS DE CERTIFICACIÓN Y DE DISPOSITIVOS DE FIRMA ELECTRÓNICA.**
    - **CAPÍTULO I. DISPOSITIVOS DE FIRMA ELECTRÓNICA.**
        - **Artículo 24.** Dispositivos de creación de firma electrónica.

        - **Artículo 25.** Dispositivos de verificación de firma electrónica.

    - **CAPÍTULO II. CERTIFICACIÓN DE PRESTADORES DE SERVICIOS DE CERTIFICACIÓN Y DE DISPOSITIVOS DE CREACIÓN DE FIRMA ELECTRÓNICA.**

        - **Artículo 26.** Certificación de prestadores de servicios de certificación.
        - **Artículo 27.** Certificación de dispositivos seguros de creación de firma electrónica.
        - **Artículo 28.** Reconocimiento de la conformidad con la normativa aplicable a los productos de firma electrónica.

- **TÍTULO V. SUPERVISIÓN Y CONTROL.**
    - **Artículo 29.** Supervisión y control.
    - **Artículo 30.** Deber de información y colaboración.
- **TÍTULO VI. INFRACCIONES Y SANCIONES.**
    - **Artículo 31.** Infracciones.
    - **Artículo 32.** Sanciones.
    - **Artículo 33.** Graduación de la cuantía de las sanciones.
    - **Artículo 34.** Medidas provisionales.
    - **Artículo 35.** Multa coercitiva.
    - **Artículo 36.** Competencia y procedimiento sancionador.

- **DISPOSICIÓN ADICIONAL PRIMERA.** Fe pública y uso de firma electrónica.
- **DISPOSICIÓN ADICIONAL SEGUNDA.** Ejercicio de la potestad sancionadora sobre la entidad de acreditación y los organismos de certificación de dispositivos de creación de firma electrónica.
- **DISPOSICIÓN ADICIONAL TERCERA.** Expedición de certificados electrónicos a entidades sin personalidad jurídica para el cumplimiento de obligaciones tributarias.
- **DISPOSICIÓN ADICIONAL CUARTA.** Prestación de servicios por la Fabrica Nacional de Moneda y Timbre-Real Casa de la Moneda.

- **DISPOSICIÓN ADICIONAL QUINTA.** Modificación del artículo 81 de la Ley 66/1997, de 30 de diciembre, de medidas fiscales, administrativas y del orden social.
- **DISPOSICIÓN ADICIONAL SEXTA.** Régimen jurídico del documento nacional de identidad electrónico.
- **DISPOSICIÓN ADICIONAL SÉPTIMA.** Emisión de facturas por vía electrónica.
- **DISPOSICIÓN ADICIONAL OCTAVA.** Modificaciones de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- **DISPOSICIÓN ADICIONAL NOVENA.** Garantía de accesibilidad para las personas con discapacidad y de la tercera edad.
- **DISPOSICIÓN ADICIONAL DÉCIMA.** Modificación de la Ley de Enjuiciamiento Civil.
- **DISPOSICIÓN ADICIONAL UNDÉCIMA.** Resolución de conflictos.
- **DISPOSICIÓN TRANSITORIA PRIMERA.** Validez de los certificados electrónicos expedidos previamente a la entrada en vigor de esta Ley.
- **DISPOSICIÓN TRANSITORIA SEGUNDA.** Prestadores de servicios de certificación establecidos en España antes de la entrada en vigor de esta Ley.
- **DISPOSICIÓN DEROGATORIA ÚNICA.** Derogación normativa.
- **DISPOSICIÓN FINAL PRIMERA.** Fundamento constitucional.
- **DISPOSICIÓN FINAL SEGUNDA.** Desarrollo reglamentario.
- **DISPOSICIÓN FINAL TERCERA.** Entrada en vigor.

Juan Carlos I,
Rey de España

A todos los que la presente vieren y entendieren. Sabed:
Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente Ley.

EXPOSICIÓN DE MOTIVOS

I

El Real Decreto-ley 14/1999, de 17 de septiembre, sobre firma electrónica, fue aprobado con el objetivo de fomentar la rápida incorporación de las nuevas tecnologías de seguridad de las comunicaciones electrónicas en la actividad de las empresas, los ciudadanos y las Administraciones públicas. De este modo, se coadyuvaba a potenciar el crecimiento y la competitividad de la economía española mediante el rápido establecimiento de un marco jurídico para la utilización de una herramienta que aporta confianza en la realización de transacciones electrónicas en redes abiertas como es el caso de Internet. El citado Real Decreto-ley incorporó al ordenamiento público español la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica, incluso antes de su promulgación y publicación en el *Diario Oficial de las Comunidades Europeas.*

Tras su ratificación por el Congreso de los Diputados, se acordó la tramitación del Real Decreto-ley 14/1999 como proyecto de ley, con el fin de someterlo a una más amplia consulta pública y al posterior debate parlamentario para perfeccionar su texto. No obstante, esta iniciativa decayó al expirar el mandato de las Cámaras en marzo de 2000. Esta Ley, por tanto, es el resultado del compromiso asumido en la VI Legislatura, actualizando a la vez el marco establecido en el Real Decreto-ley 14/1999 mediante la incorporación de las modificaciones que aconseja la experiencia acumulada desde su entrada en vigor tanto en nuestro país como en el ámbito internacional.

II

El desarrollo de la sociedad de la información y la difusión de los efectos positivos que de ella se derivan exige la generalización de la confianza de la ciudadanía en las comunicaciones telemáticas. No obstante, los datos más recientes señalan que aún existe desconfianza por parte de los intervinientes en las transacciones telemáticas y, en general, en las comunicaciones que las nuevas tecnologías permiten a la hora de transmitir información, constituyendo esta falta de confianza un freno para el desarrollo de la sociedad de la información, en particular, la Administración y el comercio electrónicos.

Como respuesta a esta necesidad de conferir seguridad a las comunicaciones por internet surge, entre otros, la firma electrónica. La firma electrónica constituye un instrumento capaz de permitir una comprobación de la procedencia y de la integridad de los mensajes intercambiados a través de redes de telecomunicaciones, ofreciendo las bases para evitar el repudio, si se adoptan las medidas oportunas basándose en fechas electrónicas.

Los sujetos que hacen posible el empleo de la firma electrónica son los denominados prestadores de servicios de certificación. Para ello expiden

certificados electrónicos, que son documentos electrónicos que relacionan las herramientas de firma electrónica en poder de cada usuario con su identidad personal, dándole así a conocer en el ámbito telemático como firmante.

La Ley obliga a los prestadores de servicios de certificación a efectuar una tutela y gestión permanente de los certificados electrónicos que expiden. Los detalles de esta gestión deben recogerse en la llamada declaración de prácticas de certificación, donde se especifican las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados electrónicos. Además, estos prestadores están obligados a mantener accesible un servicio de consulta sobre el estado de vigencia de los certificados en el que debe indicarse de manera actualizada si éstos están vigentes o si su vigencia ha sido suspendida o extinguida.

Asimismo, debe destacarse que la Ley define una clase particular de certificados electrónicos denominados certificados reconocidos, que son los certificados electrónicos que se han expedido cumpliendo requisitos cualificados en lo que se refiere a su contenido, a los procedimientos de comprobación de la identidad del firmante y a la fiabilidad y garantías de la actividad de certificación electrónica.

Los certificados reconocidos constituyen una pieza fundamental de la llamada firma electrónica reconocida, que se define siguiendo las pautas impuestas en la Directiva 1999/93/CE como la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. A la firma electrónica reconocida le otorga la Ley la equivalencia funcional con la firma manuscrita respecto de los datos consignados en forma electrónica.

Por otra parte, la Ley contiene las garantías que deben ser cumplidas por los dispositivos de creación de firma para que puedan ser considerados como dispositivos seguros y conformar así una firma electrónica reconocida.

La certificación técnica de los dispositivos seguros de creación de firma electrónica se basa en el marco establecido por la Ley 21/1992, de 16 de julio, de Industria y en sus disposiciones de desarrollo. Para esta certificación se utilizarán las normas técnicas publicadas a tales efectos en el *Diario Oficial de las Comunidades Europeas* o, excepcionalmente, las aprobadas por el Ministerio de Ciencia y Tecnología.

Adicionalmente, la Ley establece un marco de obligaciones aplicables a los prestadores de servicios de certificación, en función de si éstos emiten certificados reconocidos o no, y determina su régimen de responsabilidad, teniendo en cuenta los deberes de diligencia que incumben a los firmantes y a los terceros destinatarios de documentos firmados electrónicamente.

III

Esta Ley se promulga para reforzar el marco jurídico existente incorporando a su texto algunas novedades respecto del Real Decreto-ley 14/1999 que contribuirán a dinamizar el mercado de la prestación de servicios de certificación.

Así, se revisa la terminología, se modifica la sistemática y se simplifica el texto facilitando su comprensión y dotándolo de una estructura más acorde con nuestra técnica legislativa.

Una de las novedades que la Ley ofrece respecto del Real Decreto-ley 14/1999, es la denominación como firma electrónica reconocida de la firma electrónica que se equipara funcionalmente a la firma manuscrita. Se trata simplemente de la creación de un concepto nuevo demandado por el sector, sin que ello implique modificación alguna de los requisitos sustantivos que tanto la Directiva 1999/93/CE como el propio Real Decreto-ley 14/1999 venían exigiendo. Con ello se aclara que no basta con la firma electrónica avanzada para la equiparación con la firma manuscrita; es preciso que la firma electrónica avanzada esté basada en un certificado reconocido y haya sido creada por un dispositivo seguro de creación.

Asimismo, es de destacar de manera particular, la eliminación del registro de prestadores de servicios de certificación, que ha dado paso al establecimiento de un mero servicio de difusión de información sobre los prestadores que operan en el mercado, las certificaciones de calidad y las características de los productos y servicios con que cuentan para el desarrollo de su actividad.

Por otra parte, la Ley modifica el concepto de certificación de prestadores de servicios de certificación para otorgarle mayor grado de libertad y dar un mayor protagonismo a la participación del sector privado en los sistemas de certificación y eliminando las presunciones legales asociadas a la misma, adaptándose de manera más precisa a lo establecido en la directiva. Así, se favorece la autorregulación de la industria, de manera que sea ésta quien diseñe y gestione, de acuerdo con sus propias necesidades, sistemas voluntarios de acreditación destinados a mejorar los niveles técnicos y de calidad en la prestación de servicios de certificación. El nuevo régimen nace desde el convencimiento de que los sellos de calidad son un instrumento eficaz para convencer a los usuarios de las ventajas de los productos y servicios de certificación electrónica, resultando imprescindible facilitar y agilizar la obtención de estos símbolos externos para quienes los ofrecen al público. Si bien se recogen fielmente en la Ley los conceptos de *acreditación* de prestadores de servicios de certificación y de *conformidad* de los dispositivos seguros de creación de firma electrónica contenidos en la directiva, la terminología se ha adaptado a la más comúnmente empleada y conocida recogida en la Ley 21/1992, de 16 de julio, de Industria.

Otra modificación relevante es que la Ley clarifica la obligación de constitución de una garantía económica por parte de los prestadores de servicios de certificación que emitan certificados reconocidos, estableciendo una cuantía mínima única de tres millones de euros, flexibilizando además la combinación de los diferentes instrumentos para constituir la garantía.

Por otra parte, dado que la prestación de servicios de certificación no está sujeta a autorización previa, resulta importante destacar que la Ley refuerza las capacidades de inspección y control del Ministerio de Ciencia y Tecnología, señalando que este departamento podrá ser asistido de entidades independientes y técnicamente cualificadas para efectuar las labores de supervisión y control sobre los prestadores de servicios de certificación.

También ha de destacarse la regulación que la Ley contiene respecto del documento nacional de identidad electrónico, que se erige en un certificado electrónico reconocido llamado a generalizar el uso de instrumentos seguros de comunicación electrónica capaces de conferir la misma integridad y autenticidad que la que actualmente rodea las comunicaciones a través de medios físicos. La Ley se limita a fijar el marco normativo básico del nuevo DNI electrónico poniendo de manifiesto sus dos notas más características -acredita la identidad de su titular en cualquier procedimiento administrativo y permite la firma electrónica de documentos- remitiéndose a la normativa específica en cuanto a las particularidades de su régimen jurídico.

Asimismo, otra novedad es el establecimiento en la Ley del régimen aplicable a la actuación de personas jurídicas como firmantes, a efectos de integrar a estas entidades en el tráfico telemático. Se va así más allá del Real Decreto-ley de 1999, que sólo permitía a las personas jurídicas ser titulares de certificados electrónicos en el ámbito de la gestión de los tributos. Precisamente, la enorme expansión que han tenido estos certificados en dicho ámbito en los últimos años, sin que ello haya representado aumento alguno de la litigiosidad ni de inseguridad jurídica en las transacciones, aconsejan la generalización de la titularidad de certificados por personas morales.

En todo caso, los certificados electrónicos de personas jurídicas no alteran la legislación civil y mercantil en cuanto a la figura del representante orgánico o voluntario y no sustituyen a los certificados electrónicos que se expidan a personas físicas en los que se reflejen dichas relaciones de representación.

Como resortes de seguridad jurídica, la Ley exige, por un lado, una especial legitimación para que las personas físicas soliciten la expedición de certificados; por otro lado, obliga a los solicitantes a responsabilizarse de la custodia de los datos de creación de firma electrónica asociados a dichos certificados, todo ello sin perjuicio de que puedan ser utilizados por otras personas físicas vinculadas a la entidad. Por último, de cara a terceros, limita el uso de estos certificados a los actos que integren la relación entre la persona jurídica y las Administraciones públicas y a las cosas o servicios que constituyen el giro o tráfico ordinario de la entidad, sin perjuicio de los posibles límites cuantitativos o cualitativos que puedan añadirse. Se trata de conjugar el dinamismo que debe presidir el uso de estos certificados en el tráfico con las necesarias dosis de prudencia y seguridad para evitar que puedan nacer obligaciones incontrolables frente a terceros debido a un uso inadecuado de los datos de creación de firma. El equilibrio entre uno y otro principio se ha establecido sobre las cosas y servicios que constituyen el giro o

tráfico ordinario de la empresa de modo paralelo a cómo nuestro más que centenario Código de Comercio regula la vinculación frente a terceros de los actos de comercio realizados por el factor del establecimiento.

Con la expresión *giro o tráfico ordinario* de una entidad se actualiza a un vocabulario más acorde con nuestros días lo que en la legislación mercantil española se denomina *establecimiento fabril o mercantil*. Con ello se comprenden las transacciones efectuadas mediata o inmediatamente para la realización del núcleo de actividad de la entidad y las actividades de gestión o administrativas necesarias para el desarrollo de la misma, como la contratación de suministros tangibles e intangibles o de servicios auxiliares. Por último, debe recalcarse que, aunque el *giro o tráfico ordinario* sea un término acuñado por el derecho mercantil, la regulación sobre los certificados de personas jurídicas no sólo se aplica a las sociedades mercantiles, sino a cualquier tipo de persona jurídica que quiera hacer uso de la firma electrónica en su actividad.

Adicionalmente, se añade un régimen especial para la expedición de certificados electrónicos a entidades sin personalidad jurídica a las que se refiere el artículo 33 de la Ley General Tributaria, a los solos efectos de su utilización en el ámbito tributario, en los términos que establezca el Ministerio de Hacienda.

Por otra parte, siguiendo la pauta marcada por la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, se incluye dentro de la modalidad de prueba documental el soporte en el que figuran los datos firmados electrónicamente, dando mayor seguridad jurídica al empleo de la firma electrónica al someterla a las reglas de eficacia en juicio de la prueba documental.

Además, debe resaltarse que otro aspecto novedoso de la Ley es el acogimiento explícito que se efectúa de las relaciones de representación que pueden subyacer en el empleo de la firma electrónica. No cabe duda que el instituto de la representación está ampliamente generalizado en el tráfico económico, de ahí la conveniencia de dotar de seguridad jurídica la imputación a la esfera jurídica del representado las declaraciones que se cursan por el representante a través de la firma electrónica. Para ello, se establece como novedad que en la expedición de certificados reconocidos que admitan entre sus atributos relaciones de representación, ésta debe estar amparada en un documento público que acredite fehacientemente dicha relación de representación así como la suficiencia e idoneidad de los poderes conferidos al representante. Asimismo, se prevén mecanismos para asegurar el mantenimiento de las facultades de representación durante toda la vigencia del certificado reconocido.

Por último, debe destacarse que la ley permite que los prestadores de servicios de certificación podrán, con el objetivo de mejorar la confianza en sus servicios, establecer mecanismos de coordinación con los datos que preceptivamente deban obrar en los Registros públicos, en particular, mediante conexiones telemáticas, a los efectos de verificar los datos que figuran en los certificados en el momento de la expedición de éstos. Dichos mecanismos de coordinación también podrán

contemplar la notificación telemática por parte de los registros a los prestadores de servicios de certificación de las variaciones registrales posteriores.

IV

La Ley consta de 36 artículos agrupados en seis títulos, 10 disposiciones adicionales, dos disposiciones transitorias, una disposición derogatoria y tres disposiciones finales.

El título I contiene los principios generales que delimitan los ámbitos subjetivo y objetivo de aplicación de la ley, los efectos de la firma electrónica y el régimen de empleo ante las Administraciones públicas y de acceso a la actividad de prestación de servicios de certificación.

El régimen aplicable a los certificados electrónicos se contiene en el título II, que dedica su primer capítulo a determinar quiénes pueden ser sus titulares y a regular las vicisitudes que afectan a su vigencia. El capítulo II regula los certificados reconocidos y el tercero el documento nacional de identidad electrónico.

El título III regula la actividad de prestación de servicios de certificación estableciendo las obligaciones a que están sujetos los prestadores -distinguiendo con nitidez las que solamente afectan a los que expiden certificados reconocidos-, y el régimen de responsabilidad aplicable.

El título IV establece los requisitos que deben reunir los dispositivos de verificación y creación de firma electrónica y el procedimiento que ha de seguirse para obtener sellos de calidad en la actividad de prestación de servicios de certificación.

Los títulos V y VI dedican su contenido, respectivamente, a fijar los regímenes de supervisión y sanción de los prestadores de servicios de certificación.

Por último, cierran el texto las disposiciones adicionales -que aluden a los regímenes especiales que resultan de aplicación preferente-, las disposiciones transitorias -que incorporan seguridad jurídica a la actividad desplegada al amparo de la normativa anterior-, la disposición derogatoria y las disposiciones finales relativas al fundamento constitucional, la habilitación para el desarrollo reglamentario y la entrada en vigor.

Esta disposición ha sido sometida al procedimiento de información en materia de normas y reglamentaciones técnicas previsto en la Directiva 98/34/CE, del Parlamento Europeo y del Consejo, de 22 de junio de 1998, por la que se establece un procedimiento de información en materia de normas y reglamentaciones técnicas, modificada por la Directiva 98/48/CE, del Parlamento Europeo y del Consejo, de 20 de julio de 1998, y en el Real Decreto 1337/1999, de 31 de julio, por el que se regula la remisión de información en materia de normas y reglamentaciones técnicas y reglamentos relativos a los servicios de la sociedad de la información.

TÍTULO I.

DISPOSICIONES GENERALES.

Artículo 1. Objeto.

1. Esta Ley regula la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación.

2. Las disposiciones contenidas en esta Ley no alteran las normas relativas a la celebración, formalización, validez y eficacia de los contratos y cualesquiera otros actos jurídicos ni las relativas a los documentos en que unos y otros consten.

Artículo 2. Prestadores de servicios de certificación sujetos a la Ley.

1. Esta Ley se aplicará a los prestadores de servicios de certificación establecidos en España y a los servicios de certificación que los prestadores residentes o domiciliados en otro Estado ofrezcan a través de un establecimiento permanente situado en España.

2. Se denomina prestador de servicios de certificación la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.

3. Se entenderá que un prestador de servicios de certificación está establecido en España cuando su residencia o domicilio social se halle en territorio español, siempre que éstos coincidan con el lugar en que esté efectivamente centralizada la gestión administrativa y la dirección de sus negocios. En otro caso, se atenderá al lugar en que se realice dicha gestión o dirección.

4. Se considerará que un prestador opera mediante un establecimiento permanente situado en territorio español cuando disponga en él, de forma continuada o habitual, de instalaciones o lugares de trabajo en los que realice toda o parte de su actividad.

5. Se presumirá que un prestador de servicios de certificación está establecido en España cuando dicho prestador o alguna de sus sucursales se haya inscrito en el Registro Mercantil o en otro registro público español en el que fuera necesaria la inscripción para la adquisición de personalidad jurídica.

La mera utilización de medios tecnológicos situados en España para la prestación o el acceso al servicio no implicará, por sí sola, el establecimiento del prestador en España.

Artículo 3. Firma electrónica, y documentos firmados electrónicamente.

1. La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

2. 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.

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.

4. 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.

5. Se considera documento electrónico la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.

Sin perjuicio de lo dispuesto en el párrafo anterior, para que un documento electrónico tenga la naturaleza de documento público o de documento administrativo deberá cumplirse, respectivamente, con lo dispuesto en las letras a o b del apartado siguiente y, en su caso, en la normativa específica aplicable.

6. El documento electrónico será soporte de:

a. Documentos públicos, por estar firmados electrónicamente por funcionarios que tengan legalmente atribuida la facultad de dar fe pública, judicial, notarial o administrativa, siempre que actúen en el ámbito de sus competencias con los requisitos exigidos por la ley en cada caso.

b. Documentos expedidos y firmados electrónicamente por funcionarios o empleados públicos en el ejercicio de sus funciones públicas, conforme a su legislación específica.

c. Documentos privados.

7. Los documentos a que se refiere el apartado anterior tendrán el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad con la legislación que les resulte aplicable.

8. El soporte en que se hallen los datos firmados electrónicamente será admisible como prueba documental en juicio. Si se impugnare la autenticidad de la firma electrónica reconocida con la que se hayan firmado los datos incorporados al documento electrónico se procederá a comprobar que se trata de una firma electrónica avanzada basada en un certificado reconocido, que cumple todos los requisitos y condiciones establecidos en esta Ley para este tipo de

certificados, así como que la firma se ha generado mediante un dispositivo seguro de creación de firma electrónica.

La carga de realizar las citadas comprobaciones corresponderá a quien haya presentado el documento electrónico firmado con firma electrónica reconocida. Si dichas comprobaciones obtienen un resultado positivo, se presumirá la autenticidad de la firma electrónica reconocida con la que se haya firmado dicho documento electrónico siendo las costas, gastos y derechos que origine la comprobación exclusivamente a cargo de quien hubiese formulado la impugnación. Si, a juicio del tribunal, la impugnación hubiese sido temeraria, podrá imponerle, además, una multa de 120 a 600 euros.

Si se impugna la autenticidad de la firma electrónica avanzada, con la que se hayan firmado los datos incorporados al documento electrónico, se estará a lo establecido en el apartado 2 del artículo 326 de la Ley de Enjuiciamiento Civil.

9. No se negarán efectos jurídicos a una firma electrónica que no reúna los requisitos de firma electrónica reconocida en relación a los datos a los que esté asociada por el mero hecho de presentarse en forma electrónica.

10. A los efectos de lo dispuesto en este artículo, cuando una firma electrónica se utilice conforme a las condiciones acordadas por las partes para relacionarse entre sí, se tendrá en cuenta lo estipulado entre ellas.

Artículo 4. Empleo de la firma electrónica en el ámbito de las Administraciones públicas.

1. Esta Ley se aplicará 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.

Las Administraciones públicas, con el objeto de salvaguardar las garantías de cada procedimiento, podrán establecer condiciones adicionales a la utilización de la firma electrónica en los procedimientos. Dichas condiciones podrán incluir, entre otras, la imposición de fechas electrónicas sobre los documentos electrónicos integrados en un expediente administrativo. Se entiende por fecha electrónica el conjunto de datos en forma electrónica utilizados como medio para constatar el momento en que se ha efectuado una actuación sobre otros datos electrónicos a los que están asociados.

2. Las condiciones adicionales a las que se refiere el apartado anterior sólo podrán hacer referencia a las características específicas de la aplicación de que se trate y deberán garantizar el cumplimiento de lo previsto en el artículo 45 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. Estas condiciones serán objetivas, proporcionadas, transparentes y no discriminatorias y no deberán obstaculizar la prestación de servicios de certificación al ciudadano cuando

intervengan distintas Administraciones públicas nacionales o del Espacio Económico Europeo.

3. Las normas que establezcan condiciones generales adicionales para el uso de la firma electrónica ante la Administración General del Estado, sus organismos públicos y las entidades dependientes o vinculadas a las mismas se dictarán a propuesta conjunta de los Ministerios de Administraciones Públicas y de Ciencia y Tecnología y previo informe del Consejo Superior de Informática y para el impulso de la Administración Electrónica.

4. La utilización de la firma electrónica en las comunicaciones que afecten a la información clasificada, a la seguridad pública o a la defensa nacional se regirá por su normativa específica.

Artículo 5. Régimen de prestación de los servicios de certificación.

1. La prestación de servicios de certificación no está sujeta a autorización previa y se realizará en régimen de libre competencia. No podrán establecerse restricciones para los servicios de certificación que procedan de otro Estado miembro del Espacio Económico Europeo.

2. Los órganos de defensa de la competencia velarán por el mantenimiento de condiciones de competencia efectiva en la prestación de servicios de certificación al público mediante el ejercicio de las funciones que tengan legalmente atribuidas.

3. La prestación al público de servicios de certificación por las Administraciones públicas, sus organismos públicos o las entidades dependientes o vinculadas a las mismas se realizará

TÍTULO II.

CERTIFICADOS ELECTRÓNICOS.

CAPÍTULO I.

DISPOSICIONES GENERALES.

Artículo 6. Concepto de certificado electrónico y de firmante.

1. Un certificado electrónico es un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad.

2. El firmante es la persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa.

Artículo 7. Certificados electrónicos de personas jurídicas.

1. Podrán solicitar certificados electrónicos de personas jurídicas sus administradores, representantes legales y voluntarios con poder bastante a estos efectos. Los certificados electrónicos de personas jurídicas no podrán afectar al régimen de representación orgánica o voluntaria regulado por la legislación civil o mercantil aplicable a cada persona jurídica.

2. La custodia de los datos de creación de firma asociados a cada certificado electrónico de persona jurídica será responsabilidad de la persona física solicitante, cuya identificación se incluirá en el certificado electrónico.

3. Los datos de creación de firma sólo podrán ser utilizados cuando se admita en las relaciones que mantenga la persona jurídica con las Administraciones públicas o en la contratación de bienes o servicios que sean propios o concernientes a su giro o tráfico ordinario. Asimismo, la persona jurídica podrá imponer límites adicionales, por razón de la cuantía o de la materia, para el uso de dichos datos que, en todo caso, deberán figurar en el certificado electrónico.

4. Se entenderán hechos por la persona jurídica los actos o contratos en los que su firma se hubiera empleado dentro de los límites previstos en el apartado anterior.

Si la firma se utiliza transgrediendo los límites mencionados, la persona jurídica quedará vinculada frente a terceros sólo si los asume como propios o se hubiesen celebrado en su interés. En caso contrario, los efectos de dichos actos recaerán sobre la persona física responsable de la custodia de los datos de creación de firma, quien podrá repetir, en su caso, contra quien los hubiera utilizado.

5. Lo dispuesto en este artículo no será de aplicación a los certificados que sirvan para verificar la firma electrónica del prestador de servicios de certificación con la que firme los certificados electrónicos que expida.

6. Lo dispuesto en este artículo no será de aplicación a los certificados que se expidan a favor de las Administraciones públicas, que estarán sujetos a su normativa específica.

Artículo 8. Extinción de la vigencia de los certificados electrónicos.

1. Son causas de extinción de la vigencia de un certificado electrónico:

a. Expiración del período de validez que figura en el certificado.

b. Revocación formulada por el firmante, la persona física o jurídica representada por éste, un tercero autorizado o la persona física solicitante de un certificado electrónico de persona jurídica.

c. Violación o puesta en peligro del secreto de los datos de creación de firma del firmante o del prestador de servicios de certificación o utilización indebida de dichos datos por un tercero.

d. Resolución judicial o administrativa que lo ordene.

e. Fallecimiento o extinción de la personalidad jurídica del firmante; fallecimiento, o extinción de la personalidad jurídica del representado; incapacidad sobrevenida, total o parcial, del firmante o de su representado; terminación de la representación; disolución de la persona jurídica representada o alteración de las condiciones de custodia o uso de los datos de creación de firma que estén reflejadas en los certificados expedidos a una persona jurídica.

f. Cese en la actividad del prestador de servicios de certificación salvo que, previo consentimiento expreso del firmante, la gestión de los certificados electrónicos expedidos por aquél sean transferidos a otro prestador de servicios de certificación.

g. Alteración de los datos aportados para la obtención del certificado o modificación de las circunstancias verificadas para la expedición del certificado, como las relativas al cargo o a las facultades de representación, de manera que éste ya no fuera conforme a la realidad.

h. Cualquier otra causa lícita prevista en la declaración de prácticas de certificación.

2. El período de validez de los certificados electrónicos será adecuado a las características y tecnología empleada para generar los datos de creación de firma. En el caso de los certificados reconocidos este período no podrá ser superior a cuatro años.

3. La extinción de la vigencia de un certificado electrónico surtirá efectos frente a terceros, en los supuestos de expiración de su período de validez, desde que se produzca esta circunstancia y, en los demás casos, desde que la indicación de dicha extinción se incluya en el servicio de consulta sobre la vigencia de los certificados del prestador de servicios de certificación.

Artículo 9. Suspensión de la vigencia de los certificados electrónicos.

1. Los prestadores de servicios de certificación suspenderán la vigencia de los certificados electrónicos expedidos si concurre alguna de las siguientes causas:

a. Solicitud del firmante, la persona física o jurídica representada por éste, un tercero autorizado o la persona física solicitante de un certificado electrónico de persona jurídica.

b. Resolución judicial o administrativa que lo ordene.

c. La existencia de dudas fundadas acerca de la concurrencia de las causas de extinción de la vigencia de los certificados contempladas en los párrafos c y g del artículo 8.1.

d. Cualquier otra causa lícita prevista en la declaración de prácticas de certificación.

2. La suspensión de la vigencia de un certificado electrónico surtirá efectos desde que se incluya en el servicio de consulta sobre la vigencia de los certificados del prestador de servicios de certificación.

Artículo 10. Disposiciones comunes a la extinción y suspensión de la vigencia de certificados electrónicos.

1. El prestador de servicios de certificación hará constar inmediatamente, de manera clara e indubitada, la extinción o suspensión de la vigencia de los certificados electrónicos en el servicio de consulta sobre la vigencia de los certificados en cuanto tenga conocimiento fundado de cualquiera de los hechos determinantes de la extinción o suspensión de su vigencia.

2. El prestador de servicios de certificación informará al firmante acerca de esta circunstancia de manera previa o simultánea a la extinción o suspensión de la vigencia del certificado electrónico, especificando los motivos y la fecha y la hora en que el certificado quedará sin efecto. En los casos de suspensión, indicará, además, su duración máxima, extinguiéndose la vigencia del certificado si transcurrido dicho plazo no se hubiera levantado la suspensión.

3. La extinción o suspensión de la vigencia de un certificado electrónico no tendrá efectos retroactivos.

4. La extinción o suspensión de la vigencia de un certificado electrónico se mantendrá accesible en el servicio de consulta sobre la vigencia de los certificados al menos hasta la fecha en que hubiera finalizado su período inicial de validez.

CAPÍTULO II.

CERTIFICADOS RECONOCIDOS.

Artículo 11. Concepto y contenido de los certificados reconocidos.

1. Son certificados reconocidos los certificados electrónicos expedidos por un prestador de servicios de certificación que cumpla los requisitos establecidos en esta Ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten.

2. Los certificados reconocidos incluirán, al menos, los siguientes datos:

a. La indicación de que se expiden como tales.

b. El código identificativo único del certificado.

c. La identificación del prestador de servicios de certificación que expide el certificado y su domicilio.

d. La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado.

e. La identificación del firmante, en el supuesto de personas físicas, por su nombre y apellidos y su número de documento nacional de identidad o a través de un seudónimo que conste como tal de manera inequívoca y, en el supuesto de personas jurídicas, por su denominación o razón social y su código de identificación fiscal.

f. Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del firmante.

g. El comienzo y el fin del período de validez del certificado.

h. Los límites de uso del certificado, si se establecen.

i. Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen.

3. Los certificados reconocidos podrán asimismo contener cualquier otra circunstancia o atributo específico del firmante en caso de que sea significativo en función del fin propio del certificado y siempre que aquél lo solicite.

4. Si los certificados reconocidos admiten una relación de representación incluirán una indicación del documento público que acredite de forma fehaciente las facultades del firmante para actuar en nombre de la persona o entidad a la que represente y, en caso de ser obligatoria la inscripción, de los datos registrales, de conformidad con el apartado 2 del artículo 13.

Artículo 12. Obligaciones previas a la expedición de certificados reconocidos.

Antes de la expedición de un certificado reconocido, los prestadores de servicios de certificación deberán cumplir las siguientes obligaciones:

a. Comprobar la identidad y circunstancias personales de los solicitantes de certificados con arreglo a lo dispuesto en el artículo siguiente.

b. Verificar que la información contenida en el certificado es exacta y que incluye toda la información prescrita para un certificado reconocido.

c. Asegurarse de que el firmante está en posesión de los datos de creación de firma correspondientes a los de verificación que constan en el certificado.

d. Garantizar la complementariedad de los datos de creación y verificación de firma, siempre que ambos sean generados por el prestador de servicios de certificación.

Artículo 13. Comprobación de la identidad y otras circunstancias personales de los solicitantes de un certificado reconocido.

1. La identificación de la persona física que solicite un certificado reconocido exigirá su personación ante los encargados de verificarla y se acreditará mediante el documento nacional de identidad, pasaporte u otros medios admitidos en

derecho. Podrá prescindirse de la personación si su firma en la solicitud de expedición de un certificado reconocido ha sido legitimada en presencia notarial.

El régimen de personación en la solicitud de certificados que se expidan previa identificación del solicitante ante las Administraciones públicas se regirá por lo establecido en la normativa administrativa.

2. En el caso de certificados reconocidos de personas jurídicas, los prestadores de servicios de certificación comprobarán, además, los datos relativos a la constitución y personalidad jurídica y a la extensión y vigencia de las facultades de representación del solicitante mediante los documentos públicos que sirvan para acreditar los extremos citados de manera fehaciente y su inscripción en el correspondiente registro público si así resulta exigible. La citada comprobación podrá realizarse, asimismo, mediante consulta en el registro público en el que estén inscritos los documentos de constitución y d4e apoderamiento, pudiendo emplear los medios telemáticos facilitados por los citados registros públicos.

3. Si los certificados reconocidos reflejan una relación de representación voluntaria, los prestadores de servicios de certificación comprobarán los datos relativos a la personalidad jurídica del representado y a la extensión y vigencia de las facultades del representante mediante los documentos públicos que sirvan para acreditar los extremos citados de manera fehaciente y su inscripción en el correspondiente registro público si así resulta exigible. La citada comprobación podrá realizarse, asimismo, mediante consulta en el registro público en el que estén inscritos los mencionados datos, pudiendo emplear los medios telemáticos facilitados por los citados registros públicos.

Si los certificados reconocidos admiten otros supuestos de representación, los prestadores de servicios de certificación deberán exigir la acreditación de las circunstancias en las que se fundamenten, en la misma forma prevista anteriormente.

Cuando el certificado reconocido contenga otras circunstancias personales o atributos del solicitante, como su condición de titular de un cargo público, su pertenencia a un colegio profesional o su titulación, éstas deberán comprobarse mediante los documentos oficiales que las acrediten, de conformidad con su normativa específica.

4. Lo dispuesto en los apartados anteriores podrá no ser exigible en los siguientes casos:

a. Cuando la identidad u otras circunstancias permanentes de los solicitantes de los certificados constaran ya al prestador de servicios de certificación en virtud de una relación preexistente, en la que, para la identificación del interesado, se hubieran empleado los medios señalados en este artículo y el período de tiempo transcurrido desde la identificación es menor de cinco años.

b. Cuando para solicitar un certificado se utilice otro vigente para cuya expedición se hubiera identificado al firmante en la forma prescrita en este artículo y le conste al prestador de servicios de certificación que el período de tiempo transcurrido desde la identificación es menor de cinco años.

5. Los prestadores de servicios de certificación podrán realizar las actuaciones de comprobación previstas en este artículo por sí o por medio de otras personas físicas o jurídicas, públicas o privadas, siendo responsable, en todo caso, el prestador de servicios de certificación.

Artículo 14. Equivalencia internacional de certificados reconocidos.

Los certificados electrónicos que los prestadores de servicios de certificación establecidos en un Estado que no sea miembro del Espacio Económico Europeo expidan al público como certificados reconocidos de acuerdo con la legislación aplicable en dicho Estado se considerarán equivalentes a los expedidos por los establecidos en España, siempre que se cumpla alguna de las siguientes condiciones:

a. Que el prestador de servicios de certificación reúna los requisitos establecidos en la normativa comunitaria sobre firma electrónica para la expedición de certificados reconocidos y haya sido certificado conforme a un sistema voluntario de certificación establecido en un Estado miembro del Espacio Económico Europeo.

b. Que el certificado esté garantizado por un prestador de servicios de certificación establecido en el Espacio Económico Europeo que cumpla los requisitos establecidos en la normativa comunitaria sobre firma electrónica para la expedición de certificados reconocidos.

c. Que el certificado o el prestador de servicios de certificación estén reconocidos en virtud de un acuerdo bilateral o multilateral entre la Comunidad Europea y terceros países u organizaciones internacionales.

CAPÍTULO III.

EL DOCUMENTO NACIONAL DE IDENTIDAD ELECTRÓNICO.

Artículo 15. Documento nacional de identidad electrónico.

1. El documento nacional de identidad electrónico es el documento nacional de identidad que acredita electrónicamente la identidad personal de su titular y permite la firma electrónica de documentos.

2. Todas la personas físicas o jurídicas, públicas o privadas, reconocerán la eficacia del documento nacional de identidad electrónico para acreditar la identidad y los demás datos personales del titular que consten en el mismo, y para acreditar la identidad del firmante y la integridad de los documentos firmados con los dispositivos de firma electrónica en él incluidos.

Artículo 16. Requisitos y características del documento nacional de identidad electrónico.

1. Los órganos competentes del Ministerio del Interior para la expedición del documento nacional de identidad electrónico cumplirán las obligaciones que la presente Ley impone a los prestadores de servicios de certificación que expidan certificados reconocidos con excepción de la relativa a la constitución de la garantía a la que se refiere el apartado 2 del artículo 20.

2. La Administración General del Estado empleará, en la medida de lo posible, sistemas que garanticen la compatibilidad de los instrumentos de firma electrónica incluidos en el documento nacional de identidad electrónico con los distintos dispositivos y productos de firma electrónica generalmente aceptados.

on arreglo a los principios de objetividad, transparencia y no discriminación.

TÍTULO III.

PRESTACIÓN DE SERVICIOS DE CERTIFICACIÓN.

CAPÍTULO I.

OBLIGACIONES.

Artículo 17. Protección de los datos personales.

1. El tratamiento de los datos personales que precisen los prestadores de servicios de certificación para el desarrollo de su actividad y los órganos administrativos para el ejercicio de las funciones atribuidas por esta Ley se sujetará a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en sus normas de desarrollo.

2. Para la expedición de certificados electrónicos al público, los prestadores de servicios de certificación únicamente podrán recabar datos personales directamente de los firmantes o previo consentimiento expreso de éstos.

Los datos requeridos serán exclusivamente los necesarios para la expedición y el mantenimiento del certificado electrónico y la prestación de otros servicios en relación con la firma electrónica, no pudiendo tratarse con fines distintos sin el consentimiento expreso del firmante.

3. Los prestadores de servicios de certificación que consignen un seudónimo en el certificado electrónico a solicitud del firmante deberán constatar su verdadera identidad y conservar la documentación que la acredite.

Dichos prestadores de servicios de certificación estarán obligados a revelar la identidad de los firmantes cuando lo soliciten los órganos judiciales en el ejercicio de las funciones que tienen atribuidas y en los demás supuestos previstos en el artículo 11.2 de la Ley Orgánica de Protección de Datos de Carácter Personal en que así se requiera.

4. En cualquier caso, los prestadores de servicios de certificación no incluirán en los certificados electrónicos que expidan, los datos a los que se hace referencia en el artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Artículo 18. Obligaciones de los prestadores de servicios de certificación que expidan certificados electrónicos.

Los prestadores de servicios de certificación que expidan certificados electrónicos deberán cumplir las siguientes obligaciones:

a. No almacenar ni copiar los datos de creación de firma de la persona a la que hayan prestado sus servicios.

b. Proporcionar al solicitante antes de la expedición del certificado la siguiente información mínima, que deberá transmitirse de forma gratuita, por escrito o por vía electrónica:

    1. Las obligaciones del firmante, la forma en que han de custodiarse los datos de creación de firma, el procedimiento que haya de seguirse para comunicar la pérdida o posible utilización indebida de dichos datos y determinados dispositivos de creación y de verificación de firma electrónica que sean compatibles con los datos de firma y con el certificado expedido.

    2. Los mecanismos para garantizar la fiabilidad de la firma electrónica de un documento a lo largo del tiempo.

    3. El método utilizado por el prestador para comprobar la identidad del firmante u otros datos que figuren en el certificado.

    4. Las condiciones precisas de utilización del certificado, sus posibles límites de uso y la forma en que el prestador garantiza su responsabilidad patrimonial.

    5. Las certificaciones que haya obtenido, en su caso, el prestador de servicios de certificación y los procedimientos aplicables para la resolución extrajudicial de los conflictos que pudieran surgir por el ejercicio de su actividad.

    6. Las demás informaciones contenidas en la declaración de prácticas de certificación.

    La información citada anteriormente que sea relevante para terceros afectados por los certificados deberá estar disponible a instancia de éstos.

c. Mantener un directorio actualizado de certificados en el que se indicarán los certificados expedidos y si están vigentes o si su vigencia ha sido

suspendida o extinguida. La integridad del directorio se protegerá mediante la utilización de los mecanismos de seguridad adecuados.

d. Garantizar la disponibilidad de un servicio de consulta sobre la vigencia de los certificados rápido y seguro.

Artículo 19. Declaración de prácticas de certificación.

1. Todos los prestadores de servicios de certificación formularán una declaración de prácticas de certificación en la que detallarán, en el marco de esta Ley y de sus disposiciones de desarrollo, las obligaciones que se comprometen a cumplir en relación con la gestión de los datos de creación y verificación de firma y de los certificados electrónicos, las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados las medidas de seguridad técnicas y organizativas, los perfiles y los mecanismos de información sobre la vigencia de los certificados y, en su caso la existencia de procedimientos de coordinación con los Registros públicos correspondientes que permitan el intercambio de información de manera inmediata sobre la vigencia de los poderes indicados en los certificados y que deban figurar preceptivamente inscritos en dichos registros.

2. La declaración de prácticas de certificación de cada prestador estará disponible al público de manera fácilmente accesible, al menos por vía electrónica y de forma gratuita.

3. La declaración de prácticas de certificación tendrá la consideración de documento de seguridad a los efectos previstos en la legislación en materia de protección de datos de carácter personal y deberá contener todos los requisitos exigidos para dicho documento en la mencionada legislación.

Artículo 20. Obligaciones de los prestadores de servicios de certificación que expidan certificados reconocidos.

1. Además de las obligaciones establecidas en este capítulo, los prestadores de servicios de certificación que expidan certificados reconocidos deberán cumplir las siguientes obligaciones:

a. Demostrar la fiabilidad necesaria para prestar servicios de certificación.

b. Garantizar que pueda determinarse con precisión la fecha y la hora en las que se expidió un certificado o se extinguió o suspendió su vigencia.

c. Emplear personal con la cualificación, conocimientos y experiencia necesarios para la prestación de los servicios de certificación ofrecidos y los procedimientos de seguridad y de gestión adecuados en el ámbito de la firma electrónica.

d. Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.

e. Tomar medidas contra la falsificación de certificados y, en el caso de que el prestador de servicios de certificación genere datos de creación de firma, garantizar su confidencialidad durante el proceso de generación y su entrega por un procedimiento seguro al firmante.

f. Conservar registrada por cualquier medio seguro toda la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación vigentes en cada momento, al menos durante 15 años contados desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo.

g. Utilizar sistemas fiables para almacenar certificados reconocidos que permitan comprobar su autenticidad e impedir que personas no autorizadas alteren los datos, restrinjan su accesibilidad en los supuestos o a las personas que el firmante haya indicado y permitan detectar cualquier cambio que afecte a estas condiciones de seguridad.

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.

La citada garantía podrá ser sustituida total o parcialmente por una garantía mediante aval bancario o seguro de caución, de manera que la suma de las cantidades aseguradas sea al menos de 3.000.000 de euros.

Las cuantías y los medios de aseguramiento y garantía establecidos en los dos párrafos anteriores podrán ser modificados mediante real decreto.

Artículo 21. Cese de la actividad de un prestador de servicios de certificación.

1. El prestador de servicios de certificación que vaya a cesar en su actividad deberá comunicarlo a los firmantes que utilicen los certificados electrónicos que haya expedido así como a los solicitantes de certificados expedidos a favor de personas jurídicas; y podrá transferir, con su consentimiento expreso, la gestión de los que sigan siendo válidos en la fecha en que el cese se produzca a otro prestador de servicios de certificación que los asuma o, en caso contrario, extinguir su vigencia. La citada comunicación se llevará a cabo con una antelación mínima de dos meses al cese efectivo de la actividad e informará, en su caso, sobre las características del prestador al que se propone la transferencia de la gestión de los certificados.

2. El prestador de servicios de certificación que expida certificados electrónicos al público deberá comunicar al Ministerio de Ciencia y Tecnología, con la antelación indicada en el anterior apartado, el cese de su actividad y el destino que vaya a dar

a los certificados, especificando, en su caso, si va a transferir la gestión y a quién o si extinguirá su vigencia.

Igualmente, comunicará cualquier otra circunstancia relevante que pueda impedir la continuación de su actividad. En especial, deberá comunicar, en cuanto tenga conocimiento de ello, la apertura de cualquier proceso concursal que se siga contra él.

3. Los prestadores de servicios de certificación remitirán al Ministerio de Ciencia y Tecnología con carácter previo al cese definitivo de su actividad la información relativa a los certificados electrónicos cuya vigencia haya sido extinguida para que éste se haga cargo de su custodia a efectos de lo previsto en el artículo 20.1.f. Este ministerio mantendrá accesible al público un servicio de consulta específico donde figure una indicación sobre los citados certificados durante un período que considere suficiente en función de las consultas efectuadas al mismo.

CAPÍTULO II.

RESPONSABILIDAD.

Artículo 22. Responsabilidad de los prestadores de servicios de certificación.

1. Los prestadores de servicios de certificación responderán por los daños y perjuicios que causen a cualquier persona en el ejercicio de su actividad cuando incumplan las obligaciones que les impone esta Ley.

La responsabilidad del prestador de servicios de certificación regulada en esta Ley será exigible conforme a las normas generales sobre la culpa contractual o extracontractual, según proceda, si bien corresponderá al prestador de servicios de certificación demostrar que actuó con la diligencia profesional que le es exigible.

2. Si el prestador de servicios de certificación no cumpliera las obligaciones señaladas en los párrafos b al d del artículo 12 al garantizar un certificado electrónico expedido por un prestador de servicios de certificación establecido en un Estado no perteneciente al Espacio Económico Europeo, será responsable por los daños y perjuicios causados por el uso de dicho certificado.

3. De manera particular, el prestador de servicios de certificación responderá de los perjuicios que se causen al firmante o a terceros de buena fe por la falta o el retraso en la inclusión en el servicio de consulta sobre la vigencia de los certificados de la extinción o suspensión de la vigencia del certificado electrónico.

4. Los prestadores de servicios de certificación asumirán toda la responsabilidad frente a terceros por la actuación de las personas en las que deleguen la ejecución de alguna o algunas de las funciones necesarias para la prestación de servicios de certificación.

5. La regulación contenida en esta Ley sobre la responsabilidad del prestador de servicios de certificación se entiende sin perjuicio de lo establecido en la legislación sobre cláusulas abusivas en contratos celebrados con consumidores.

Artículo 23. Limitaciones de responsabilidad de los prestadores de servicios de certificación.

1. El prestador de servicios de certificación no será responsable de los daños y perjuicios ocasionados al firmante o terceros de buena fe, si el firmante incurre en alguno de los siguientes supuestos:

a. No haber proporcionado al prestador de servicios de certificación información veraz, completa y exacta sobre los datos que deban constar en el certificado electrónico o que sean necesarios para su expedición o para la extinción o suspensión de su vigencia, cuando su inexactitud no haya podido ser detectada por el prestador de servicios de certificación.

b. La falta de comunicación sin demora al prestador de servicios de certificación de cualquier modificación de las circunstancias reflejadas en el certificado electrónico.

c. Negligencia en la conservación de sus datos de creación de firma, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación.

d. No solicitar la suspensión o revocación del certificado electrónico en caso de duda en cuanto al mantenimiento de la confidencialidad de sus datos de creación de firma.

e. Utilizar los datos de creación de firma cuando haya expirado el período de validez del certificado electrónico o el prestador de servicios de certificación le notifique la extinción o suspensión de su vigencia.

f. Superar los límites que figuren en el certificado electrónico en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él o no utilizarlo conforme a las condiciones establecidas y comunicadas al firmante por el prestador de servicios de certificación.

2. En el caso de los certificados electrónicos que recojan un poder de representación del firmante, tanto éste como la persona o entidad representada, cuando ésta tenga conocimiento de la existencia del certificado, están obligados a solicitar la revocación o suspensión de la vigencia del certificado en los términos previstos en esta Ley.

3. Cuando el firmante sea una persona jurídica, el solicitante del certificado electrónico asumirá las obligaciones indicadas en el apartado 1.

4. El prestador de servicios de certificación tampoco será responsable por los daños y perjuicios ocasionados al firmante o a terceros de buena fe si el destinatario de los documentos firmados electrónicamente actúa de forma negligente. Se entenderá, en particular, que el destinatario actúa de forma negligente en los siguientes casos:

a. Cuando no compruebe y tenga en cuenta las restricciones que figuren en el certificado electrónico en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él.

b. Cuando no tenga en cuenta la suspensión o pérdida de vigencia del certificado electrónico publicada en el servicio de consulta sobre la vigencia de los certificados o cuando no verifique la firma electrónica.

5. El prestador de servicios de certificación no será responsable de los daños y perjuicios ocasionados al firmante o terceros de buena fe por la inexactitud de los datos que consten en el certificado electrónico si éstos le han sido acreditados mediante documento público, inscrito en un registro público si así resulta exigible. En caso de que dichos datos deban figurar inscritos en un registro público, el prestador de servicios de certificación podrá, en su caso, comprobarlos en el citado registro antes de la expedición del certificado, pudiendo emplear los medios telemáticos facilitados por los citados registros públicos.

6. La exención de responsabilidad frente a terceros obliga al prestador de servicios de certificación a probar que actuó en todo caso con la debida diligencia.

TÍTULO IV.

DISPOSITIVOS DE FIRMA ELECTRÓNICA Y SISTEMAS DE CERTIFICACIÓN DE PRESTADORES DE SERVICIOS DE CERTIFICACIÓN Y DE DISPOSITIVOS DE FIRMA ELECTRÓNICA.

CAPÍTULO I.

DISPOSITIVOS DE FIRMA ELECTRÓNICA.

Artículo 24. Dispositivos de creación de firma electrónica.

1. Los datos de creación de firma son los datos únicos, como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica.

2. Un dispositivo de creación de firma es un programa o sistema informático que sirve para aplicar los datos de creación de firma.

3. Un dispositivo seguro de creación de firma es un dispositivo de creación de firma que ofrece, al menos, las siguientes garantías:

a. Que los datos utilizados para la generación de firma pueden producirse sólo una vez y asegura razonablemente su secreto.

b. Que existe una seguridad razonable de que los datos utilizados para la generación de firma no pueden ser derivados de los de verificación de

firma o de la propia firma y de que la firma está protegida contra la falsificación con la tecnología existente en cada momento.

c. Que los datos de creación de firma pueden ser protegidos de forma fiable por el firmante contra su utilización por terceros.

d. Que el dispositivo utilizado no altera los datos o el documento que deba firmarse ni impide que éste se muestre al firmante antes del proceso de firma.

Artículo 25. Dispositivos de verificación de firma electrónica.

1. Los datos de verificación de firma son los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica.

2. Un dispositivo de verificación de firma es un programa o sistema informático que sirve para aplicar los datos de verificación de firma.

3. Los dispositivos de verificación de firma electrónica garantizarán, siempre que sea técnicamente posible, que el proceso de verificación de una firma electrónica satisfaga, al menos, los siguientes requisitos:

a. Que los datos utilizados para verificar la firma correspondan a los datos mostrados a la persona que verifica la firma.

b. Que la firma se verifique de forma fiable y el resultado de esa verificación se presente correctamente.

c. Que la persona que verifica la firma electrónica pueda, en caso necesario, establecer de forma fiable el contenido de los datos firmados y detectar si han sido modificados.

d. Que se muestren correctamente tanto la identidad del firmante o, en su caso, conste claramente la utilización de un seudónimo, como el resultado de la verificación.

e. Que se verifiquen de forma fiable la autenticidad y la validez del certificado electrónico correspondiente.

f. Que pueda detectarse cualquier cambio relativo a su seguridad.

4. Asimismo, los datos referentes a la verificación de la firma, tales como el momento en que ésta se produce o una constatación de la validez del certificado electrónico en ese momento, podrán ser almacenados por la persona que verifica la firma electrónica o por terceros de confianza.

CAPÍTULO II.
CERTIFICACIÓN DE PRESTADORES DE SERVICIOS DE CERTIFICACIÓN Y DE DISPOSITIVOS DE CREACIÓN DE FIRMA ELECTRÓNICA.

Artículo 26. Certificación de prestadores de servicios de certificación.

1. La certificación de un prestador de servicios de certificación es el procedimiento voluntario por el que una entidad cualificada pública o privada emite una declaración a favor de un prestador de servicios de certificación, que implica un reconocimiento del cumplimiento de requisitos específicos en la prestación de los servicios que se ofrecen al público.

2. La certificación de un prestador de servicios de certificación podrá ser solicitada por éste y podrá llevarse a cabo, entre otras, por entidades de certificación reconocidas por una entidad de acreditación designada de acuerdo con lo dispuesto en la Ley 21/1992, de 16 de julio, de Industria, y en sus disposiciones de desarrollo.

3. En los procedimientos de certificación podrán utilizarse normas técnicas u otros criterios de certificación adecuados. En caso de utilizarse normas técnicas, se emplearán preferentemente aquellas que gocen de amplio reconocimiento aprobadas por organismos de normalización europeos y, en su defecto, otras normas internacionales o españolas.

4. La certificación de un prestador de servicios de certificación no será necesaria para reconocer eficacia jurídica a una firma electrónica.

Artículo 27. Certificación de dispositivos seguros de creación de firma electrónica.

1. La certificación de dispositivos seguros de creación de firma electrónica es el procedimiento por el que se comprueba que un dispositivo cumple los requisitos establecidos en esta Ley para su consideración como dispositivo seguro de creación de firma.

2. La certificación podrá ser solicitada por los fabricantes o importadores de dispositivos de creación de firma y se llevará a cabo por las entidades de certificación reconocidas por una entidad de acreditación designada de acuerdo con lo dispuesto en la Ley 21/1992, de 16 de julio, de Industria y en sus disposiciones de desarrollo.

3. En los procedimientos de certificación se utilizarán las normas técnicas cuyos números de referencia hayan sido publicados en el *Diario Oficial de la Unión Europea* y, excepcionalmente, las aprobadas por el Ministerio de Ciencia y Tecnología que se publicarán en la dirección de Internet de este Ministerio.

4. Los certificados de conformidad de los dispositivos seguros de creación de firma serán modificados o, en su caso, revocados cuando se dejen de cumplir las condiciones establecidas para su obtención.

Los organismos de certificación asegurarán la difusión de las decisiones de revocación de certificados de dispositivos de creación de firma.

Artículo 28. Reconocimiento de la conformidad con la normativa aplicable a los productos de firma electrónica.

1. Se presumirá que los productos de firma electrónica aludidos en el párrafo d del apartado 1 del artículo 20 y en el apartado 3 del artículo 24 son conformes con los requisitos previstos en dichos artículos si se ajustan a las normas técnicas correspondientes cuyos números de referencia hayan sido publicados en el *Diario Oficial de la Unión Europea.*

2. Se reconocerá eficacia a los certificados de conformidad sobre dispositivos seguros de creación de firma que hayan sido otorgados por los organismos designados para ello en cualquier Estado miembro del Espacio Económico Europeo.

TÍTULO V.

SUPERVISIÓN Y CONTROL.

Artículo 29. Supervisión y control.

1. El Ministerio de Ciencia y Tecnología controlará el cumplimiento por los prestadores de servicios de certificación que expidan al público certificados electrónicos de las obligaciones establecidas en esta Ley y en sus disposiciones de desarrollo. Asimismo, supervisará el funcionamiento del sistema y de los organismos de certificación de dispositivos seguros de creación de firma electrónica.

2. El Ministerio de Ciencia y Tecnología realizará las actuaciones inspectoras que sean precisas para el ejercicio de su función de control.

Los funcionarios adscritos al Ministerio de Ciencia y Tecnología que realicen la inspección a que se refiere el apartado anterior tendrán la consideración de autoridad pública en el desempeño de sus cometidos.

3. El Ministerio de Ciencia y Tecnología podrá acordar las medidas apropiadas para el cumplimiento de esta Ley y sus disposiciones de desarrollo.

4. El Ministerio de Ciencia y Tecnología podrá recurrir a entidades independientes y técnicamente cualificadas para que le asistan en las labores de supervisión y control sobre los prestadores de servicios de certificación que le asigna esta Ley.

Artículo 30. Deber de información y colaboración.

1. Los prestadores de servicios de certificación, la entidad independiente de acreditación y los organismos de certificación tienen la obligación de facilitar al Ministerio de Ciencia y Tecnología toda la información y colaboración precisas para el ejercicio de sus funciones.

En particular, deberán permitir a sus agentes o al personal inspector el acceso a sus instalaciones y la consulta de cualquier documentación relevante para la inspección de que se trate, siendo de aplicación, en su caso, lo dispuesto en el artículo 8.5 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa. En sus inspecciones podrán ir acompañados de expertos o peritos en las materias sobre las que versen aquéllas.

2. Los prestadores de servicios de certificación deberán comunicar al Ministerio de Ciencia y Tecnología el inicio de su actividad, sus datos de identificación, incluyendo la identificación fiscal y registral, en su caso, los datos que permitan establecer comunicación con el prestador, incluidos el nombre de dominio de internet, los datos de atención al público, las características de los servicios que vayan a prestar, las certificaciones obtenidas para sus servicios y las certificaciones de los dispositivos que utilicen. Esta información deberá ser convenientemente actualizada por los prestadores y será objeto de publicación en la dirección de internet del citado ministerio con la finalidad de otorgarle la máxima difusión y conocimiento.

3. Cuando, como consecuencia de una actuación inspectora, se tuviera conocimiento de hechos que pudieran ser constitutivos de infracciones tipificadas en otras leyes, se dará cuenta de los mismos a los órganos u organismos competentes para su supervisión y sanción.

TÍTULO VI.

INFRACCIONES Y SANCIONES.

Artículo 31. Infracciones.

1. Las infracciones de los preceptos de esta Ley se clasifican en muy graves, graves y leves.

2. Son infracciones muy graves:

a. El incumplimiento de alguna de las obligaciones establecidas en los artículos 18 y 20 en la expedición de certificados reconocidos, siempre que se hayan causado daños graves a los usuarios o la seguridad de los servicios de certificación se haya visto gravemente afectada.

   Lo dispuesto en este apartado no será de aplicación respecto al incumplimiento de la obligación de constitución de la garantía económica prevista en el apartado 2 del artículo 20.

b. La expedición de certificados reconocidos sin realizar todas las comprobaciones previas señaladas en el artículo 12, cuando ello afecte a la

mayoría de los certificados reconocidos expedidos en los tres años anteriores al inicio del procedimiento sancionador o desde el inicio de la actividad del prestador si este período es menor.

3. Son infracciones graves:

a. El incumplimiento de alguna de las obligaciones establecidas en los artículos 18 y 20 en la expedición de certificados reconocidos, excepto de la obligación de constitución de la garantía prevista en el apartado 2 del artículo 20, cuando no constituya infracción muy grave.

b. La falta de constitución por los prestadores que expidan certificados reconocidos de la garantía económica contemplada en el apartado 2 del artículo 20.

c. La expedición de certificados reconocidos sin realizar todas las comprobaciones previas indicadas en el artículo 12, en los casos en que no constituya infracción muy grave.

d. El incumplimiento por los prestadores de servicios de certificación que no expidan certificados reconocidos de las obligaciones señaladas en el artículo 18, si se hubieran causado daños graves a los usuarios o la seguridad de los servicios de certificación se hubiera visto gravemente afectada.

e. El incumplimiento por los prestadores de servicios de certificación de las obligaciones establecidas en el artículo 21 respecto al cese de actividad de los mismos o la producción de circunstancias que impidan la continuación de su actividad, cuando las mismas no sean sancionables de conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

f. La resistencia, obstrucción, excusa o negativa injustificada a la actuación inspectora de los órganos facultados para llevarla a cabo con arreglo a esta Ley y la falta o deficiente presentación de la información solicitada por parte del Ministerio de Ciencia y Tecnología en su función de inspección y control.

g. El incumplimiento de las resoluciones dictadas por el Ministerio de Ciencia y Tecnología para asegurar que el prestador de servicios de certificación se ajuste a esta Ley.

4. Constituyen infracciones leves:

El incumplimiento por los prestadores de servicios de certificación que no expidan certificados reconocidos de las obligaciones establecidas en el artículo 18; y el incumplimiento por los prestadores de servicios de certificación de las restantes obligaciones establecidas en esta Ley, cuando no constituya infracción grave o

muy grave, con excepción de las obligaciones contenidas en el apartado 2 del artículo 30.

Artículo 32. Sanciones.

1. Por la comisión de infracciones recogidas en el artículo anterior, se impondrán las siguientes sanciones:

a. Por la comisión de infracciones muy graves, se impondrá al infractor multa de 150.001 a 600.000 euros.

   La comisión de dos o más infracciones muy graves en el plazo de tres años, podrá dar lugar, en función de los criterios de graduación del artículo siguiente, a la sanción de prohibición de actuación en España durante un plazo máximo de dos años.

b. Por la comisión de infracciones graves, se impondrá al infractor multa de 30.001 a 150.000 euros.

c. Por la comisión de infracciones leves, se impondrá al infractor una multa por importe de hasta 30.000 euros.

2. Las infracciones graves y muy graves podrán llevar aparejada, a costa del sancionado, la publicación de la resolución sancionadora en el *Boletín Oficial del Estado* y en dos periódicos de difusión nacional o en la página de inicio del sitio de internet del prestador y, en su caso, en el sitio de internet del Ministerio de Ciencia y Tecnología, una vez que aquélla tenga carácter firme.

Para la imposición de esta sanción, se considerará la repercusión social de la infracción cometida, el número de usuarios afectados y la gravedad del ilícito.

Artículo 33. Graduación de la cuantía de las sanciones.

La cuantía de las multas que se impongan, dentro de los límites indicados, se graduará teniendo en cuenta lo siguiente:

a. La existencia de intencionalidad o reiteración.

b. La reincidencia, por comisión de infracciones de la misma naturaleza, sancionadas mediante resolución firme.

c. La naturaleza y cuantía de los perjuicios causados.

d. Plazo de tiempo durante el que se haya venido cometiendo la infracción.

e. El beneficio que haya reportado al infractor la comisión de la infracción.

f. Volumen de la facturación a que afecte la infracción cometida.

Artículo 34. Medidas provisionales.

1. En los procedimientos sancionadores por infracciones graves o muy graves el Ministerio de Ciencia y Tecnología podrá adoptar, con arreglo a la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y sus normas de desarrollo, las medidas de carácter provisional que se estimen necesarias para asegurar la eficacia de la resolución que definitivamente se dicte, el buen fin del procedimiento, evitar el mantenimiento de los efectos de la infracción y las exigencias de los intereses generales.

En particular, podrán acordarse las siguientes:

a. Suspensión temporal de la actividad del prestador de servicios de certificación y, en su caso, cierre provisional de sus establecimientos.

b. Precinto, depósito o incautación de registros, soportes y archivos informáticos y de documentos en general, así como de aparatos y equipos informáticos de todo tipo.

c. Advertencia al público de la existencia de posibles conductas infractoras y de la incoación del expediente sancionador de que se trate, así como de las medidas adoptadas para el cese de dichas conductas.

En la adopción y cumplimiento de las medidas de restricción a que alude este apartado se respetarán, en todo caso, las garantías, normas y procedimientos previstos en el ordenamiento jurídico para proteger los derechos a la intimidad personal y a la protección de los datos personales, cuando éstos pudieran resultar afectados.

2. En los supuestos de daños de excepcional gravedad en la seguridad de los sistemas empleados por el prestador de servicios de certificación que menoscaben seriamente la confianza de los usuarios en los servicios ofrecidos, el Ministerio de Ciencia y Tecnología podrá acordar la suspensión o pérdida de vigencia de los certificados afectados, incluso con carácter definitivo.

3. En todo caso, se respetará el principio de proporcionalidad de la medida a adoptar con los objetivos que se pretendan alcanzar en cada supuesto.

4. En casos de urgencia y para la inmediata protección de los intereses implicados, las medidas provisionales previstas en este artículo podrán ser acordadas antes de la iniciación del expediente sancionador.

Las medidas deberán ser confirmadas, modificadas o levantadas en el acuerdo de iniciación del procedimiento, que deberá efectuarse dentro de los 15 días siguientes a su adopción, el cual podrá ser objeto del recurso que proceda.

En todo caso, dichas medidas quedarán sin efecto si no se inicia el procedimiento sancionador en dicho plazo o cuando el acuerdo de iniciación no contenga un pronunciamiento expreso acerca de las mismas.

Artículo 35. Multa coercitiva.

El órgano administrativo competente para resolver el procedimiento sancionador podrá imponer multas coercitivas por importe que no exceda de 6.000 euros por cada día que transcurra sin cumplir las medidas provisionales que hubieran sido acordadas.

Artículo 36. Competencia y procedimiento sancionador.

1. La imposición de sanciones por el incumplimiento de lo previsto en esta ley corresponderá, en el caso de infracciones muy graves, al Ministro de Ciencia y Tecnología y en el de infracciones graves y leves, al Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información.

No obstante, el incumplimiento de las obligaciones establecidas en el artículo 17 será sancionado por la Agencia de Protección de Datos con arreglo a lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

2. La potestad sancionadora regulada en esta Ley se ejercerá de conformidad con lo establecido al respecto en la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común y en sus normas de desarrollo.

DISPOSICIÓN ADICIONAL PRIMERA. Fe pública y uso de firma electrónica.

1. Lo dispuesto en esta Ley no sustituye ni modifica las normas que regulan las funciones que corresponden a los funcionarios que tengan legalmente la facultad de dar fe en documentos en lo que se refiere al ámbito de sus competencias siempre que actúen con los requisitos exigidos en la Ley.

2. En el ámbito de la documentación electrónica, corresponderá a las entidades prestadoras de servicios de certificación acreditar la existencia de los servicios prestados en el ejercicio de su actividad de certificación electrónica, a solicitud del usuario, o de una autoridad judicial o administrativa.

DISPOSICIÓN ADICIONAL SEGUNDA. Ejercicio de la potestad sancionadora sobre la entidad de acreditación y los organismos de certificación de dispositivos de creación de firma electrónica.

1. En el ámbito de la certificación de dispositivos de creación de firma, corresponderá al Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información del Ministerio de Ciencia y Tecnología la imposición de sanciones por la comisión, por los organismos de certificación de dispositivos seguros de creación de firma electrónica o por la entidad que los acredite, de las infracciones graves previstas en los párrafos e, f y g del apartado segundo del artículo 31 de la Ley 21/1992, de 16 de julio, de Industria, y de las infracciones leves indicadas en el párrafo a del apartado 3 del artículo 31 de la citada Ley que

cometan en el ejercicio de actividades relacionadas con la certificación de firma electrónica.

2. Cuando dichas infracciones merezcan la calificación de infracciones muy graves, serán sancionadas por el Ministro de Ciencia y Tecnología.

DISPOSICIÓN ADICIONAL TERCERA. Expedición de certificados electrónicos a entidades sin personalidad jurídica para el cumplimiento de obligaciones tributarias.

Podrán expedirse certificados electrónicos a las entidades sin personalidad jurídica a que se refiere el artículo 33 de la Ley General Tributaria a los solos efectos de su utilización en el ámbito tributario, en los términos que establezca el Ministro de Hacienda.

DISPOSICIÓN ADICIONAL CUARTA. Prestación de servicios por la Fabrica Nacional de Moneda y Timbre-Real Casa de la Moneda.

Lo dispuesto en esta Ley se entiende sin perjuicio de lo establecido en el artículo 81 de la Ley 66/1997, de 30 de diciembre, de medidas fiscales, administrativas y del orden social.

DISPOSICIÓN ADICIONAL QUINTA. Modificación del artículo 81 de la Ley 66/1997, de 30 de diciembre, de medidas fiscales, administrativas y del orden social.

Se añaden apartado doce al artículo 81 de la Ley 66/1997, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, con la siguiente redacción.

Doce. En el ejercicio de las funciones que le atribuye el presente artículo, la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda estará exenta de la constitución de la garantía a la que se refiere el apartado 2 del artículo 20 de la Ley 59/2003, de Firma Electrónica.

DISPOSICIÓN ADICIONAL SEXTA. Régimen jurídico del documento nacional de identidad electrónico.

1. Sin perjuicio de la aplicación de la normativa vigente en materia del documento nacional de identidad en todo aquello que se adecúe a sus características particulares, el documento nacional de identidad electrónico se regirá por su normativa específica.

2. El Ministerio de Ciencia y Tecnología podrá dirigirse al Ministerio del Interior para que por parte de éste se adopten las medidas necesarias para asegurar el cumplimiento de las obligaciones que le incumban como prestador de servicios de certificación en relación con el documento nacional de identidad electrónico.

DISPOSICIÓN ADICIONAL SÉPTIMA. Emisión de facturas por vía electrónica.

Lo dispuesto en esta Ley se entiende sin perjuicio de las exigencias derivadas de las normas tributarias en materia de emisión de facturas por vía electrónica.

DISPOSICIÓN ADICIONAL OCTAVA. Modificaciones de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Uno. Adición de un nuevo apartado 3 al artículo 10 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Se añade un apartado 3 con el siguiente texto:

3. Cuando se haya atribuido un rango de numeración telefónica a servicios de tarificación adicional en el que se permita el acceso a servicios de la sociedad de la información y se requiera su utilización por parte del prestador de servicios, esta utilización y la descarga de programas informáticos que efectúen funciones de marcación, deberán realizarse con el consentimiento previo, informado y expreso del usuario.

A tal efecto, el prestador del servicio deberá proporcionar al menos la siguiente información:

a. Las características del servicio que se va a proporcionar.

b. Las funciones que efectuarán los programas informáticos que se descarguen, incluyendo el número telefónico que se marcará.

c. El procedimiento para dar fin a la conexión de tarificación adicional, incluyendo una explicación del momento concreto en que se producirá dicho fin, y

d. El procedimiento necesario para restablecer el número de conexión previo a la conexión de tarificación adicional.

La información anterior deberá estar disponible de manera claramente visible e identificable.

Lo dispuesto en este apartado se entiende sin perjuicio de lo establecido en la normativa de telecomunicaciones, en especial, en relación con los requisitos aplicables para el acceso por parte de los usuarios a los rangos de numeración telefónica, en su caso, atribuidos a los servicios de tarificación adicional.

Dos. Los apartados 2, 3 y 4 del artículo 38 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico se redactan en los siguientes términos:

2. Son infracciones muy graves:

a. El incumplimiento de las órdenes dictadas en virtud del artículo 8 en aquellos supuestos en que hayan sido dictadas por un órgano administrativo.

b. El incumplimiento de la obligación de suspender la transmisión, el alojamiento de datos, el acceso a la red o la prestación de cualquier otro servicio equivalente de intermediación, cuando un órgano administrativo competente lo ordene, en virtud de lo dispuesto en el artículo 11.

c. El incumplimiento significativo de la obligación de retener los datos de tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información, prevista en el artículo 12.

d. La utilización de los datos retenidos, en cumplimiento del artículo 12, para fines distintos de los señalados en él.

3. Son infracciones graves:

a. El incumplimiento de la obligación de retener los datos de tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información, prevista en el artículo 12, salvo que deba ser considerado como infracción muy grave.

b. El incumplimiento significativo de lo establecido en los párrafos a y f del artículo 10.1.

c. El envío masivo de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente o el envío, en el plazo de un año, de más de tres comunicaciones comerciales por los medios aludidos a un mismo destinatario, cuando en dichos envíos no se cumplan los requisitos establecidos en el artículo 21.

d. El incumplimiento significativo de la obligación del prestador de servicios establecida en el apartado 1 del artículo 22, en relación con los procedimientos para revocar el consentimiento prestado por los destinatarios.

e. No poner a disposición del destinatario del servicio las condiciones generales a que, en su caso, se sujete el contrato, en la forma prevista en el artículo 27.

f. El incumplimiento habitual de la obligación de confirmar la recepción de una aceptación, cuando no se haya pactado su exclusión o el contrato se haya celebrado con un consumidor.

g. La resistencia, excusa o negativa a la actuación inspectora de los órganos facultados para llevarla a cabo con arreglo a esta Ley.

h. El incumplimiento significativo de lo establecido en el apartado 3 del artículo 10.

i. El incumplimiento significativo de las obligaciones de información o de establecimiento de un procedimiento de rechazo del tratamiento de datos, establecidas en el apartado 2 del artículo 22.

4. Son infracciones leves:

a. La falta de comunicación al registro público en que estén inscritos, de acuerdo con lo establecido en el artículo 9, del nombre o nombres de dominio o direcciones de Internet que empleen para la prestación de servicios de la sociedad de la información.

b. No informar en la forma prescrita por el artículo 10.1 sobre los aspectos señalados en los párrafos b, c, d, e y g del mismo, o en los párrafos a y f cuando no constituya infracción grave.

c. El incumplimiento de lo previsto en el artículo 20 para las comunicaciones comerciales, ofertas promocionales y concursos.

d. El envío de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente cuando en dichos envíos no se cumplan los requisitos establecidos en el artículo 21 y no constituya infracción grave.

e. No facilitar la información a que se refiere el artículo 27.1, cuando las partes no hayan pactado su exclusión o el destinatario sea un consumidor.

f. El incumplimiento de la obligación de confirmar la recepción de una petición en los términos establecidos en el artículo 28, cuando no se haya pactado su exclusión o el contrato se haya celebrado con un consumidor, salvo que constituya infracción grave.

g. El incumplimiento de las obligaciones de información o de establecimiento de un procedimiento de rechazo del tratamiento de datos, establecidas en el apartado 2 del artículo 22, cuando no constituya una infracción grave.

h. El incumplimiento de la obligación del prestador de servicios establecida en el apartado 1 del artículo 22, en relación con los procedimientos para revocar el consentimiento prestado por los destinatarios cuando no constituya infracción grave.

i. El incumplimiento de lo establecido en el apartado 3 del artículo 10, cuando no constituya infracción grave. Tres. Modificación del artículo 43, apartado 1, segundo párrafo de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

El segundo párrafo del apartado 1 del artículo 43 queda redactado como sigue:

No obstante lo anterior, la imposición de sanciones por incumplimiento de las resoluciones dictadas por los órganos competentes en función de la materia o entidad de que se trate a que se refieren los párrafos a y b del artículo 38.2 de esta Ley corresponderá al órgano que dictó la resolución incumplida. Igualmente, corresponderá a la Agencia de Protección de Datos la imposición de sanciones por la comisión de las infracciones tipificadas en los artículos 38.3 c, d e i y 38.4 d, g y h de esta Ley.

Cuatro. Modificación del artículo 43, apartado 2 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

El apartado 2 del artículo 43 queda redactado como sigue:

2. La potestad sancionadora regulada en esta ley se ejercerá de conformidad con lo establecido al respecto en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y en sus normas de desarrollo. No obstante, el plazo máximo de duración del procedimiento simplificado será de tres meses.

DISPOSICIÓN ADICIONAL NOVENA. Garantía de accesibilidad para las personas con discapacidad y de la tercera edad.

Los servicios, procesos, procedimientos y dispositivos de firma electrónica deberán ser plenamente accesibles a las personas con discapacidad y de la tercera edad, las cuales no podrán ser en ningún caso discriminadas en el ejercicio de los derechos y facultades reconocidos en esta Ley por causas basadas en razones de discapacidad o edad avanzada.

DISPOSICIÓN ADICIONAL DÉCIMA. Modificación de la Ley de Enjuiciamiento Civil.

Se añade un apartado tres al artículo 326 de la Ley de Enjuiciamiento Civil con el siguiente tenor:

Cuando la parte a quien interese la eficacia de un documento electrónico lo pida o se impugne su autenticidad, se procederá con arreglo a lo establecido en el artículo 3 de la Ley de Firma Electrónica.

DISPOSICIÓN ADICIONAL UNDÉCIMA. Resolución de conflictos.

Los usuarios y prestadores de servicios de certificación podrán someter los conflictos que se susciten en sus relaciones al arbitraje.Cuando el usuario tenga la condición de consumidor o usuario, en los términos establecidos por la legislación de protección de los consumidores, el prestador y el usuario podrán someter sus conflictos al arbitraje de consumo, mediante la adhesión de aquéllos al Sistema Arbitral de Consumo competente.

DISPOSICIÓN TRANSITORIA PRIMERA. Validez de los certificados electrónicos expedidos previamente a la entrada en vigor de esta Ley.

Los certificados electrónicos que hayan sido expedidos por prestadores de servicios de certificación en el marco del Real Decreto-ley 14/1999, de 17 de septiembre, sobre firma electrónica, mantendrán su validez.

DISPOSICIÓN TRANSITORIA SEGUNDA. Prestadores de servicios de certificación establecidos en España antes de la entrada en vigor de esta Ley.

Los prestadores de servicios de certificación establecidos en España antes de la entrada en vigor de esta Ley deberán comunicar al Ministerio de Ciencia y Tecnología su actividad y las características de los servicios que presten en el plazo de un mes desde la referida entrada en vigor. Esta información será objeto de publicación en la dirección de internet del citado ministerio con la finalidad de otorgarle la máxima difusión y conocimiento.

DISPOSICIÓN DEROGATORIA ÚNICA. Derogación normativa.

Queda derogado el Real Decreto-ley 14/1999, de 17 de septiembre, sobre firma electrónica y cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en esta Ley.

DISPOSICIÓN FINAL PRIMERA. Fundamento constitucional.

Esta Ley se dicta al amparo del artículo 149.1.8, 18, 21 y 29 de la Constitución.

DISPOSICIÓN FINAL SEGUNDA. Desarrollo reglamentario.

1. El Gobierno adaptará la regulación reglamentaria del documento nacional de identidad a las previsiones de esta Ley.

2. Así mismo, se habilita al Gobierno para dictar las demás disposiciones reglamentarias que sean precisas para el desarrollo y aplicación de esta Ley.

DISPOSICIÓN FINAL TERCERA. Entrada en vigor.

La presente Ley entrará en vigor a los tres meses de su publicación en el *Boletín Oficial del Estado.*

Por tanto, Mando a todos los españoles, particulares y autoridades, que guarden y hagan guardar esta Ley.

Madrid, 19 de diciembre de 2003.

- Juan Carlos R. -

El Presidente del Gobierno,
José María Aznar López

Anteproyecto de Ley de Comercio Electrónico (El Salvador)

CONSIDERANDOS

I.- Las nuevas tecnologías de información y comunicaciones están revolucionando profundamente la forma como las personas e instituciones se relacionan, incidiendo progresivamente en la vida cotidiana de cada uno y transformando ésta a pasos acelerados, abriendo nuevas alternativas de acceso a la información, la cultura, el comercio y la entretención, y marcando estándares más exigentes, cualitativamente y cuantitativamente, en cada uno de estos campos. Dicho fenómeno es una tendencia mundial.

II.- Nuestra sociedad está siendo objeto de estas transformaciones tecnológicas y avances informáticos, a través de lo que conocemos como Internet; que es un vehículo de transmisión e intercambio de todo tipo de información. Por su mismo carácter de red abierta accesible desde cualquier lugar del mundo y la inmediatez de las comunicaciones que permite, Internet se ha convertido en un foro mundial de interrelación social, cultural y económica. Es decir, en una herramienta útil para el ejercicio de múltiples actividades financieras, administrativas, y educativas solo a modo de ejemplo. Internet es una plataforma ideal para las transacciones comerciales. Esto conlleva a la apertura de nuevas oportunidades para el desarrollo económico, así como la creación de nuevas fuentes de empleo, de la cual pueden beneficiarse las empresas para comercializar sus productos o servicios más eficientemente tanto en el mercado local como en otros mercados.

III.- La incertidumbre por la falta de regularización en dicha materia, obstaculiza el desarrollo de nuevos productos y servicios, disuade la inversión, debido a que las normas actuales fueron diseñadas al efecto de una regulación nacional, realizada en la generalidad de casos entre personas presentes en un lugar geográfico establecido, en tanto que el Internet y otros medios de comunicación, han trascendido las fronteras geográficas de los países, sus propias normativas domésticas e internacionales, de ahí que se haga necesario su regulación, adecuándola a las características propias y no dejarlo al desarrollo de cuestiones técnicas. Con dicha regularización se busca dinamizar, modernizar y adaptar nuestra normativa a los mercados internacionales cada vez mas globalizados.

IV.- La incorporación de la sociedad salvadoreña a esta nueva cultura informática necesita de un soporte jurídico que despeje todas las inquietudes que plantea la realización de actividades a través de la red de Internet, así como el uso de medios innovadores que buscan dar celeridad a distinto tipo de transacciones, que le permitirán a las diferentes organizaciones de nuestro país, aumentar su productividad, competitividad y al mismo tiempo reducir sus tiempos y costos.

V.- Es indispensable una ley general que facilite el desarrollo del comercio electrónico, que brinde la confianza necesaria a todos los actores participantes de esta nueva economía, sin merma alguna de las garantías de los usuarios. La importancia de las nuevas tecnologías debe hacer que su introducción en la sociedad Salvadoreña se lleve a cabo dinamizando el tejido empresarial y al, mismo tiempo, protegiendo suficientemente los derechos de los usuarios, estableciéndose, a tal efecto, las oportunas garantías. De conformidad con el artículo 101 de nuestra Constitución es deber del Estado promover el desarrollo económico íntimamente ligado al desarrollo tecnológico en aras del beneficio social.

Sección I
PARTE GENERAL
Disposiciones Generales

Art. 1 Objeto de la Ley

La presente ley tiene por objeto regular 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 manera tal que ellas puedan ser acreditados válidamente, mediante procedimientos de seguridad electrónicos existentes que permitan dar integridad, seguridad, autoría y autenticidad de los mismos.

Art. 2 Ámbito de Aplicación

La presente Ley será aplicable a todo tipo de comunicación o información transmitida en forma de mensaje de datos, salvo 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 en dichos actos o contratos.

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.

Art. 3 Definiciones
Para efectos de esta ley y su aplicación los siguientes términos se entenderán así:

Agente electrónico
Programa computacional, o cualquier otro medio electrónico utilizado independiente y automáticamente para que inicie una acción o responda a mensajes de datos o instrucciones, sin la revisión o acción previa de la persona que tiene el control sobre el actuar de dicho agente.

Certificado Electrónico
Es la certificación electrónica que vincula unos datos de verificación de firma a un iniciador y confirma su identidad vinculándola con su firma digital

Clave Pública
Es aquella que se utiliza para verificar una firma digital, en un sistema criptográfico asimétrico seguro.

Clave privada
Es aquella que se utiliza para firmar digitalmente, mediante un dispositivo de creación de firma digital, en un sistema criptográfico asimétrico seguro.

Comercio Electrónico
Toda transacción comercial o financiera, contractual o no, que se efectúe a través del intercambio de mensajes de datos o medios similares.

Contratos Informáticos:
Todo contrato celebrado sin la presencia física simultanea de las partes, prestando estas su consentimiento en origen y en destino por medio de equipos electrónicos de tratamiento y almacenaje de datos, conectados por medio de cable, radio, medios ópticos o cualquier otro medio electromagnético.

Consumidor
Se entenderá por consumidor toda persona natural que en las comunicaciones electrónicas contempladas en esta Ley actúa con propósito que no sea el de su actividad profesional.

Comunicación
Cualquier mensaje de datos conteniendo información.

Criptografía
Es la codificación de o cifrado de mensajes de datos, cambiándolos de una forma legible a una ilegible y que mediante el uso de algoritmos matemáticos o señales autorizadas puede ser devuelto a su forma original y legible.

Destinatario
Se entenderá por destinatario de un mensaje de datos la persona designada por el iniciador para recibir el mensaje, siempre y cuando no esté actuando a título de intermediario con respecto a él.

Documento Electrónico
Documento en formato electrónico con información electrónica o digital que se almacena, envía, comunica, recibe, archive o genere por cualquier medio electrónico.

Electrónico
Para efecto de la presente Ley se entenderá como electrónico todo medio que utilice tecnología eléctrica, digital, magnética, inalámbrica, alámbrica, óptica, electromagnética o alguna otra similar, conocida o por conocerse.

Entidad Reguladora
Aquella entidad pública que por ley se encarga de supervisar las actividades de las entidades de certificación.

Entidad de Certificación
Es aquella persona que, autorizada conforme a la ley, está facultada para emitir certificados vinculados con las firmas digitales de las personas con el objeto de dar certeza sobre la identidad de una persona, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales, deberá disponer de las herramientas físicas y lógicas necesarias acordes al tipo de servicio a prestar.

Firma Digital
Cualquier medio, método, símbolo o proceso electrónico que es adherido o se asocia lógicamente con un mensaje de datos por la persona que ha aceptado el contenido de dicho mensaje y que permite determinar que dicho mensaje es auténtico, proviene inalterado de dicha persona y sustituyendo a su firma manuscrita impide al signatario desconocer la autoría del mensaje de datos en forma posterior.

Información
Datos, textos, imágenes, sonidos, códigos, programas computacionales, software, bases de datos, voz o similares.

Iniciador de un mensaje de datos
Se entenderá por iniciador de un mensaje de datos, toda persona que, a tenor del mensaje, haya actuado por su voluntad o en cuyo nombre se haya actuado para enviar o generar ese mensaje antes de ser archivado si éste es el caso, pero que no haya actuado a título de intermediario con respecto a él.

Intercambio Electrónico de Datos
La transmisión electrónica de datos de una computadora a otra, estando estructurada la información conforme alguna norma técnica convenida al efecto, entre las partes

Intermediario
Con relación a un determinado mensaje de datos, se entenderá como intermediario a toda persona que, actuando por cuenta de otra, envíe, reciba o archive dicho mensaje o preste algún otro servicio con respecto a él.

Mensaje de Datos
Toda información generada, enviada, recibida, almacenada o comunicada, intercambiada por métodos o medios de comunicación electrónicos, ópticos o cualquier otra tecnología conocida o por conocerse; como pudiesen ser, entre otros, el intercambio electrónico de datos, los sitios de Internet, el correo electrónico, el telegrama, el fax, o el telefax.

Persona
Para efecto de la presente Ley se entenderá como persona, toda persona natural o jurídica, entidades públicas o cualquier otro sujeto de derechos y obligaciones conforme a las leyes.

Prestador de Servicios de Residencia
Es la empresa que realiza el negocio de albergar, servir y mantener archivos de datos para uno o más sitios de Internet.

Proveedor
Persona que suministra un servicio a titulo oneroso, a distancia por vía electrónica y a petición individual del destinatario de la sociedad de información ya sea de comercio electrónico u otro medio. Proceso, método o medio empleado con el propósito de verificar que una firma electrónica, documento o mensaje de datos proviene de una persona específica o para detectar cambios o errores en un documento

electrónico, incluyendo cualquier procedimiento que requiera del uso de algoritmos u otros códigos, palabras o números de identificación o de clave, encriptación o cualquier otro procedimiento de verificación de identidad y contenido.

Sistema criptográfico asimétrico seguro
Es un método criptográfico que utiliza un par de claves compuesto por una clave privada utilizada para firmar digitalmente y su correspondiente clave pública utilizada para verificar esa firma digital, de forma tal que, con las longitudes de claves utilizadas, sea computacionalmente no factible tanto obtener o inferir la clave privada a partir de la correspondiente clave pública como desencriptar aquello que ha sido encriptado con una clave privada sin la utilización de la correspondiente clave pública.

Sistema de Información
Cualquier medio tecnológico utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos.

Transacción automatizada
Significa una acción o serie de acciones ocurridas entre dos o más personas relacionadas con la realización de negocios, comercio o asuntos gubernamentales conducida o realizada electrónicamente, en todo o en parte, en la cual los actos de al menos una de las partes no son revisados por individuo alguno en el tiempo de formación o ejecución de un contrato.

Art. 4 Interpretación
En la interpretación y aplicación de la presente ley habrán de tenerse en cuenta los siguientes principios:

- Otorgarle facilidad y validez a las transacciones por medio de mensajes de datos,
- promover la confianza del público en la validez, integridad y confiabilidad de los mensajes de datos, eliminando barreras resultantes de la no-certeza sobre requerimientos de escritura y firma promoviendo el desarrollo de la infraestructura necesaria para implementar un seguro comercio electrónico.
- su carácter internacional,
- la necesidad de promover la uniformidad de su aplicación,
- la observancia de la buena fe de las partes,
- la libre contratación,

- su concordancia y consistencia con las prácticas comunes y razonables en esta área,
- la predominancia de los aspectos técnicos y las nuevas tecnologías,
- otros principios que aseguren la agilidad, certeza y legalidad de las comunicaciones que sean objeto de la presente ley, y
- la desmaterialización del soporte papel.
- Facilitar el archivo electrónico con autoridades locales y agencias gubernamentales.

Promoviendo un eficiente sistema de servicios gubernamentales. Las cuestiones relativas a materias que se rijan por la presente ley y que no estén expresamente resueltas en ella, se regirán por los principios generales en los cuales esta ley se inspira.

Art. 5 Autonomía de las Partes
Esta ley contiene los derechos y obligaciones mínimas entre las partes que generan, envían, reciben, archivan o procesan de alguna otra forma mensajes de datos. La presente ley habilita el empleo de la firma digital dentro del principio de libertad de contratación.

Las partes tendrán la libertad en sus relaciones de aumentar el número o el alcance de sus derechos y obligaciones no así limitar o eliminar los ya existentes. Una persona que ha acordado utilizar mensajes de datos para sus comunicaciones o transacciones, podrá establecer que tipos de mensajes de datos esta dispuesto a utilizar y aceptar.

Cuando una de las partes acuerde utilizar mensajes de datos para realizar una transacción, puede oponerse a realizar futuras transacciones por esos medios. Este derecho es irrenunciable. La parte que se opone a realizar futuras transacciones por estos medios debe dar aviso a las partes que pudiesen ser afectadas y sujeto a cualquier acuerdo entre ellas. Este aviso deberá comunicarse por cualquier medio de comunicación con acuse de recibo.

Art. 6 Jurisdicción y Ley Aplicable
Las partes podrán fijar libremente y de mutuo acuerdo los términos y condiciones de las cláusulas del contrato informático; el acuerdo debe ser expreso, en caso de controversias se someterán a la jurisdicción estipulada en el contrato, a lo establecido en las leyes de El Salvador o a las normas de arbitraje y mediación si las hubiere. La selección de un foro, no implica la selección de la ley aplicable.

Los mensajes de datos se regirán por la ley que las partes seleccionen para ello. El acuerdo de las partes sobre esta selección deberá ser expreso; en caso de controversias se someterán a la ley estipulada en el contrato, a lo establecido en las leyes de El Salvador o a las normas de arbitraje y mediación si las hubiere.

Art. 7 Incorporación por Remisión
Salvo acuerdo en contrario entre las partes, cuando en un mensaje de datos se haga remisión total o parcial a directrices, normas, estándares, acuerdos, cláusulas, condiciones o términos fácilmente accesibles con la intención de incorporarlos como parte del contenido o hacerlos vinculantes jurídicamente, se presume que esos términos están incorporados por remisión a dicho mensaje de datos. Entre las partes y conforme a la ley, esos términos serán jurídicamente válidos como si hubieran sido incorporados en su totalidad en el mensaje de datos.

No se negarán efectos jurídicos, validez ni fuerza obligatoria a la información por la sola razón de que no esté contenida en el mensaje de datos o en una firma digital que se supone ha de dar lugar a este efecto jurídico, siempre que figure en el mensaje de datos en forma de remisión.

SECCIÓN II -DE LA APLICACIÓN E INTEGRACIÓN DE LAS REGLAS CONCERNIENTES A LOS MENSAJES DE DATOS CON OTRAS NORMAS Y/O REQUISITOS LEGALES DEVALIDEZ DE ACTOS O DOCUMENTOS

Art. 8 Reconocimiento y Consecuencias Jurídicas de las Comunicaciones o los Mensajes de Datos

Un mensaje de datos tendrá efecto, validez y fuerza obligatoria como cualquier otro acto, comunicación o contrato en soporte material.

No se negarán efectos jurídicos, validez o fuerza obligatoria a los actos, comunicaciones o contratos por la sola razón de que parte de su acuerdo estuviese en forma de mensaje de datos.

Los documentos que resulten de la transmisión a distancia vía líneas telefónicas o similares que emanen de un facsímil receptor tendrán legalmente el mismo valor de documento privado que el original enviado desde el fax transmisor, siempre que el original haya sido firmado por el remitente y éste no impugne su firma posteriormente.

Art. 9 Escrito
Cuando alguna disposición legal requiera que una información deba constar por escrito y estar soportada materialmente, o bien establezca la

existencia de consecuencias jurídicas por falta de elaboración en soporte material, se entenderá que un mensaje de datos cumple con el requisito de escrituración si la información contenida en el mismo es legible, si está disponible para ser usada o presentada en cualquier momento, y si existe una razonable seguridad que la información de que da cuenta o que contiene se ha mantenido íntegra desde el momento en que fue generada, salvo los necesarios cambios que sean consecuencia del archivo, de la recuperación y del envío o comunicación del documento.

No se considerará que un mensaje de datos cumple con los requisitos del párrafo anterior, si el iniciador o su sistema electrónico de envío no permite que el destinatario imprima o guarde dicho mensaje o dicho mensaje no pueda ser recuperado posteriormente por algún medio técnico.

Lo dispuesto en el presente artículo no será aplicable a la información que por su naturaleza deba constar en una forma distinta, exigida por la ley ni respecto de las exclusiones previstas en él artículo 2 de la presente ley.

Art. 10 Original e Integridad de los mensajes de datos
Cuando la ley requiera que la información sea conservada y presentada en su forma original, ese requisito quedará satisfecho con un mensaje de datos, si:

- Existe alguna garantía confiable de que la información generada o comunicada con un mensaje de datos por medios electrónicos, ópticos o de cualquier otra tecnología.
- Se ha mantenido integra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva, al margen de los cambios en forma de endoso o cambio normal de la comunicación, archivo o presentación y permanece accesible para su ulterior consulta.
- De requerirse que la información sea presentada, si ésta puede ser mostrada a la persona a quien se deba presentar.

Este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas simplemente prevén consecuencias en el caso de que la información no sea presentada o conservada en su forma original.

Se considerará que la información consignada en un mensaje de datos es íntegra, si ésta ha permanecido completa e inalterada, salvo algún cambio que sea inherente al proceso de comunicación, archivo o presentación que no altere la información original contenida en el mensaje. El grado de confiabilidad requerido, será determinado a la luz de los fines para los que se generó la información y de todas las circunstancias relevantes al caso.

Art. 11 Firma de Documentos
Cuando la ley exija la existencia de una firma manuscrita en un documento en soporte material, se entenderá satisfecho dicho requerimiento en relación con un mensaje de datos, si:

Se ha utilizado un método que permita identificar al iniciador ese mensaje de datos e indicar que el contenido es de su conocimiento y consecuentemente de su aprobación.

Que el método sea tanto confiable como apropiado para el propósito para el cual el mensaje fue generado o comunicado.

El mensaje de datos ha sido firmado con una firma digital de acuerdo a los requisitos dispuestos en la presente ley.

Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas simplemente prevén consecuencias en el caso de que no exista una firma.

Art.12 Admisibilidad y Fuerza Probatoria de los Mensajes de Datos
Los mensajes de datos serán admisibles como medio de prueba y su fuerza probatoria es la otorgada en las disposiciones de la presente Ley.

No se dará aplicación a disposición legal alguna que sea obstáculo para la admisión como medio de prueba de un mensaje de datos.

Art. 13 Criterio para Valorar los Mensajes de Datos
Para la valoración de la fuerza probatoria de los mensajes de datos a que se refiere esta ley, se tendrán en cuenta las reglas de la sana crítica. Por consiguiente habrán de tenerse en cuenta:

- La confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje de datos,
- la confiabilidad en la forma en que se haya conservado la integridad de la información,
- La forma de identificación fehaciente con la cual se identifique al iniciador,
- la utilización de procedimientos de seguridad y,
- Cualquier otro factor pertinente.

Para la valoración de las pruebas, el juez, arbitro o mediador competente que juzgue el caso deberá designar los peritos que considere necesarios para el análisis, debido conocimiento técnico e interpretación de las pruebas presentadas.

Art. 14 Conservación y Archivo de los Mensajes de Datos y Documentos
Cuando cualquier ley requiera que documentos, registros o información sea conservada o archivada, ese requisito quedará satisfecho mediante la conservación de mensajes de datos que contengan dichos documentos, registros o información en cualquier medio electrónico, siempre que se cumplan las condiciones siguientes:

- Que el mensaje de datos sea accesible para su posterior consulta ;
- Que el mensaje de datos sea conservado en el formato en que se haya generado, enviado o recibido o en algún formato que permita demostrar que garantice la integridad del mensaje de datos originalmente enviado;
- Que se conserve, de haber alguna, 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.

No estará sujeta a la obligación de conservación, los documentos, registros o información si los mismos tienen por única finalidad facilitar el envío o recepción de los mensajes de datos. Los libros y documentos de los comerciantes podrán ser conservados en cualquier medio electrónico que garantice su reproducción exacta, inalterabilidad y conservación permanente durante el plazo que la ley requiera.

Toda persona podrá recurrir a los servicios de un tercero para observar o verificar la conservación de sus mensajes de datos, siempre que se cumplan los requisitos enunciados en esta ley.

Cualquier institución gubernamental tendrá la posibilidad de especificar requerimientos adicionales para la retención de mensajes de datos que sean de su competencia.

SECCIÓN III - COMUNICACIÓN DE LOS MENSAJES DE DATOS

Art. 15 Reconocimiento de los Mensajes de Datos entre las partes
En las relaciones entre el iniciador y el destinatario de un mensaje de datos, no se negarán efectos jurídicos, validez o fuerza obligatoria a una manifestación de voluntad u otra declaración por la sola razón de haberse hecho en forma de mensaje de datos.

Las normas contenidas en la presente ley serán aplicables a las personas que han acordado expresa o implícitamente, utilizar mensajes de datos para comunicarse. Cuándo no sea expreso, el acuerdo de las partes respecto del reconocimiento de los mensajes, se determinará por el

contexto, las circunstancias y de acuerdo a los principios contenidos en elArt. 4 de la presente ley.

Art. 16 Atribución de un Mensaje de Datos
Se entenderá que un mensaje de datos proviene del iniciador, cuando éste ha sido enviado por:

El propio iniciador.

Por alguna persona facultada para actuar en nombre del iniciador respecto de ese mensaje.

Por mandatario o representante legal con suficiente representación para ello.

Por un sistema de información programado por el iniciador o en su nombre para que opere automáticamente.

Art. 17 Presunción del Origen de un Mensaje de Datos
A) Se presume que un mensaje datos ha sido enviado por el iniciador, cuando:

El iniciador haya aplicado en forma adecuada el procedimiento acordado previamente con el destinatario, para establecer que el mensaje de datos provenía efectivamente de éste, o el mensaje de datos que reciba el destinatario resulte de los actos de una persona cuya relación con el iniciador, o con algún mandatario suyo, le haya dado acceso a algún método utilizado por el iniciador para identificar un mensaje de datos como propio.

B) La presunción contenida en este artículo no operará:

- A partir del momento en que el destinatario haya sido informado por el iniciador que el mensaje de datos no proviene del iniciador y haya dispuesto de un plazo razonable para actuar en consecuencia; o

- en el caso del numeral dos del literal A, desde el momento en que el destinatario sepa, o debiera saber de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que el mensaje de datos no provenía del iniciador.

Art. 18 Concordancia del Mensaje de Datos Enviado con el Mensaje de Datos Recibido
Siempre que un mensaje de datos provenga del iniciador o que se entienda que proviene de él, o siempre que el destinatario tenga derecho a actuar con arreglo a este supuesto, en las relaciones entre el iniciador y destinatario, éste último tendrá derecho a considerar que el mensaje de datos recibido corresponde al que quería enviar el iniciador, y podrá proceder en consecuencia.

El destinatario no gozará de este derecho si sabía o hubiera sabido, de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que la transmisión habría dado lugar a un error en el mensaje de datos recibido.

Art. 19 Mensajes de Datos Duplicados
Se presume que cada mensaje de datos recibido es un mensaje de datos separado y el destinatario tendrá derecho a considerarlo como tal y a actuar en consecuencia, salvo en la medida en que duplique otro mensaje de datos, y que el destinatario sepa, o debiera saber, de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que el nuevo mensaje de datos era un duplicado.

Art. 20 Acuse de Recibo
Si al enviar o antes de enviar un mensaje de datos, el iniciador unilateralmente solicita o acuerda con el destinatario que se acuse recibo del mensaje de datos, pero no se ha acordado entre éstos una forma o método determinado para efectuarlo, se podrá acusar recibo mediante:

- Toda comunicación del destinatario, sea por medio de agente electrónico o no, o

- Todo acto del destinatario que baste para indicar al iniciador que se ha recibido el mensaje de datos.

Tratándose de la comunicación de mensajes de datos que requieran de un acuse de recibo para surtir efectos entre el iniciador y el destinatario, bien sea por disposición legal o por así requerirlo el iniciador, se considerará que el mensaje de datos ha sido enviado y recibido, cuando se haya recibido el acuse respectivo. Se presumirá que se ha recibido el mensaje de datos cuando el iniciador reciba el acuse correspondiente, salvo prueba en contrario.

Cuando en el acuse de recibo se indique que el mensaje de datos recibido cumple con los requisitos técnicos convenidos o enunciados en alguna norma técnica aplicable, se entenderá que ello es así, salvo prueba en contrario.

Art. 21 Presunción de Recepción de un Mensaje de Datos

Cuando el iniciador reciba el acuse de recibo del destinatario, se presumirá que éste ha recibido el mensaje de datos.

Esta presunción no implicará que el mensaje de datos corresponda al mensaje recibido, salvo prueba en contrario.

Art. 22 Plazo para Acusar Recibo
Tratándose de la comunicación de mensajes de datos que requieran de un acuse de recibo para surtir efectos entre el iniciador y el destinatario, si el iniciador no ha recibido acuse de recibo en el plazo fijado o convenido o no se ha fijado o convenido ningún plazo, en un plazo razonable el iniciador:

Podrá dar aviso al destinatario de que no ha recibido acuse de recibo y fijar un plazo razonable para su recepción; y

De no recibirse acuse dentro del plazo fijado conforme al literal a) de este artículo, el iniciador podrá, previo aviso de ello al destinatario, considerar que el mensaje de datos no ha sido enviado o ejercer cualquier otro derecho que pueda tener.

Art. 23 Efectos Jurídicos del Acuse de Recibo
Los tres artículos anteriores únicamente rigen los efectos relacionados con el acuse de recibo de un mensaje de datos. Las consecuencias jurídicas del contenido de un mensaje de datos se regirán conforme al artículo 8.

La confirmación de la recepción de un mensaje, indicando que este ha cumplido con los requisitos técnicamente reconocidos o acordados, no implicara presunción de aceptación de su contenido.

Art. 24 Tiempo de Envío de un Mensaje de Datos
De no convenir otra cosa entre el iniciador y el destinatario, el mensaje de datos se tendrá por expedido cuando ingrese en un sistema de información que no esté bajo el control del iniciador o de la persona o agente electrónico que envió el mensaje de datos en nombre de éste o del medio programado para el efecto.

Art. 25 Tiempo de Recepción de un Mensaje de Datos
De no convenirse otra cosa entre el iniciador y el destinatario, el momento de la recepción de un mensaje de datos se determinará de la siguiente manera:

Si el destinatario ha designado un sistema de información para la recepción del mensaje de datos, la recepción tendrá lugar:

En el momento en que ingrese el mensaje de datos en el sistema de información designado; o de enviarse el mensaje de datos a un sistema de información del destinatario que no sea el sistema de información designado, en el momento en que el destinatario recupere el mensaje de datos;

Si el destinatario no ha designado un sistema de información, la recepción tendrá lugar cuando el mensaje de datos ingrese a un sistema de información del destinatario independientemente de que sea recuperado el mensaje de datos.

Lo dispuesto en este artículo será aplicable aún cuando el sistema de información esté ubicado en lugar distinto de donde se tenga por recibido el mensaje de datos conforme al artículo siguiente.

Art. 26 Lugar del Envío y Recepción de un Mensaje de Datos
De no convenirse otra cosa entre el iniciador y el destinatario, el mensaje de datos se tendrá por expedido en el lugar donde el iniciador tenga su establecimiento y por recibido en el lugar donde el destinatario tenga el suyo.

Si el iniciador o destinatario tienen más de un establecimiento, su establecimiento será el que guarde una relación más estrecha con la operación subyacente o, de no haber una operación subyacente, su establecimiento principal.

Si el iniciador o el destinatario no tienen establecimiento, se tendrá en cuenta su lugar de residencia habitual.

En caso de existir un certificado de firma digital el mensaje de datos se tendrá por expedido en el domicilio que conste en el certificado de firma digital del iniciador y por recibido en el que conste en el certificado de firma digital del destinatario.

Art. 27 Entrega por Medios Electrónicos o Digitales
Tratándose de la comunicación, notificación o entrega de mensajes de datos u otros documentos, que requieran o estén permitidos que se entreguen físicamente a una persona por razón de una disposición legal, se permitirá que dichos mensajes o documentos se entreguen por medios electrónicos o digitales siempre que dicha persona haya accedido a recibirlos en tal forma.

El efecto y validez legal de la comunicación, notificación o entrega establecida en este artículo será la misma como si se hubiese hecho físicamente o en soporte material.

Sin que la siguiente lista sea taxativa el presente artículo se aplicara a la entrega por medios electrónicos o digitales de programas informáticos, música digitalizada, videos digitalizados y cualquier otro medio que por su naturaleza pueda ser transmitido digital o electrónicamente.

Art. 28 Uso de Procedimientos de Seguridad y Errores o Cambios en un Mensaje de Datos

Si las partes de una comunicación de un mensaje de datos han acordado utilizar cierto procedimiento de seguridad para detectar cambios o errores y una de las personas ha utilizado dicho procedimiento detectando un error o cambio en el mensaje y la otra parte no ha seguido el procedimiento, la persona que siguió el procedimiento tendrá derecho, a hacer valer el mensaje de datos en su forma inalterada o sin errores contra la parte que no siguió el procedimiento, salvo prueba en contrario que exima de responsabilidad a la parte que no cumplió el procedimiento.

SECCIÓN IV - DE LOS CONTRATOS, ACTOS Y DECLARACIONES DE VOLUNTAD

Art. 29 Formación y Validez de los Contratos, Actos y Declaraciones de Voluntad

En la formación de un contrato, de no convenir las partes otra cosa, la oferta o su aceptación podrán ser expresadas por medio de un mensaje de datos sin requerir estipulación previa por escrito para que dichas acciones produzcan efectos.

No se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación un mensaje de datos.

Todos los contratos celebrados por medio de mensajes de datos estarán sujetos a los requisitos de existencia y validez de las leyes, las costumbres y usos nacionales e internacionales, todo en concordancia con la presente Ley.

Cuando las leyes requieran o permitan que un contrato, acto o declaración de voluntad se realice por medios escritos, se permitirá que estos se realicen por medio de mensajes de datos, teniendo estos últimos la misma validez que los escritos.

Los efectos, validez y ejecutividad de un contrato, acto o declaración de voluntad hechos por medio de mensajes de datos será la misma que las realizadas en soporte material.

Art. 30 Condiciones Generales de Contratación
Cuando en una transacción electrónica alguna de las partes contrate bajo condiciones generales de contratación previamente establecidas, estas deben estar redactadas con claridad, concreción y sencillez, cuyo formato no desaliente su lectura y que se encuentren siempre disponibles a la hora de contratar; para que la parte quien redactó dichas condiciones generales pueda oponerlas contra la otra parte, deberá siempre haber alguna aceptación de dichas condiciones por la parte contra quien se oponen.

Al interpretar dichas condiciones, todas aquellas que se consideren como ambiguas, oscuras o incomprensibles se interpretarán contra la parte quien las redactó de acuerdo a las disposiciones de esta ley.

Art. 31 Idioma de los Contratos
Se presume que todas las partes contratantes conocen y comprenden el idioma en el que realizan los contratos por medios electrónicos.

En caso de existir conflictos entre diferentes versiones del mismo contrato prevalecerá la versión del contrato en español siempre y cuando este idioma haya sido uno de los idiomas de contratación originalmente acordados.

Art. 32 Agentes Electrónicos
Un contrato podrá formarse por el intercambio de mensajes de datos entre agentes electrónicos o entre un agente electrónico y una persona, aun si la persona no revisa las acciones del agente electrónico o el resultado de las mismas.

Un contrato electrónico hecho por una persona y un agente electrónico de otra persona no tendrá efectos legales y no será ejecutable:

a) si la persona cometió un error material en el documento y el agente electrónico no otorgo a la persona la oportunidad de corregir el error o prevenirlo y la persona notifica a la otra persona sobre el error tan pronto como sea posible luego de que el individuo toma conocimiento del error respecto del mensaje de datos.

Art. 33 Contratos de Adhesión
Es aquel cuyas cláusulas han sido establecidas unilateralmente por una de las partes, a través de contratos impresos o electrónicos o en

formularios sin que la otra parte, para celebrarlo, haya discutido sustancialmente su contenido.

En este tipo de contrato se estará a lo dispuesto en la Ley de Protección al Consumidor.

Art. 34 Tiempo de validez de la oferta
A criterio del oferente, el mensaje de datos enviado y condicionado a un acuse de recibo o aceptación podrá tener un tiempo de validez durante el cual generara obligaciones para las partes.

Art. 35 Nulidad de los contratos
Se consideraran nulos los contratos informáticos cuando estos adolezcan de alguna causa de nulidad de acuerdo con la legislación vigente.

SECCIÓN V -DE LAS FIRMAS DIGITALES Y LOS SUSCRIPTORES DE LAS MISMAS

Art. 36 Reconocimiento y Efectos Jurídicos de una Firma Digital
Una firma digital, siempre y cuando reúna los requisitos determinados en esta Ley, el cuerpo de leyes de El Salvador y cumpla con los reglamentos que para el efecto se dictaren, tendrá el mismo efecto, validez y efectividad que una firma manuscrita.

Una persona podrá utilizar la firma digital para todos aquellos propósitos para los cuales la ley permite o requiere una firma manuscrita, salvo para los casos en los cuales la firma manuscrita es obligatoria.

Cuando una firma digital haya sido fijada en un mensaje de datos se presume que el suscriptor de la misma tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo, salvo prueba en contrario.

Art. 37 Requisitos Esenciales de una Firma Digital
Se reconocerán las firmas digitales que incorporen los siguientes requisitos:

- Garantizar la confidencialidad del mensaje de datos.
- Ser susceptible de ser verificada la autoría e identidad del emisor.
- Estar bajo el control exclusivo de la persona que la usa.
- Estar ligada a la información o mensaje de datos, de tal manera que si éstos son cambiados, la firma digital es invalidada.

- Ofrecer seguridad suficiente de que no pueda ser falsificada con la tecnología existente en cada momento.

- No alterar la integridad del mensaje.

- Estar conforme a la reglamentación adoptada por el Órgano Ejecutivo.

La firma digital, debidamente certificada por una Entidad de Certificación conforme a lo establecido en la Sección VI de esta ley, se considerara que cumple con los requisitos señalados en este artículo.

Art. 38 Deberes y Responsabilidad de los Suscriptores de Firmas Digitales
Son deberes de los suscriptores de firmas digitales:

Recibir la firma digital de la entidad de certificación o generarla utilizando un método autorizado por esta.

Actuar con la debida diligencia y tomar las medidas de seguridad necesarias para mantener la firma digital bajo su estricto control y evitar toda utilización no autorizada de su firma.

Suministrar la información que requiera la entidad de certificación.

Solicitar oportunamente la revocación de los certificados conforme a los reglamentos que al efecto se dictaren.

Cumplir con las obligaciones derivadas del uso ilegal de su firma, cuando no haya obrado con la debida diligencia para impedir su utilización no autorizada y para evitar que el destinatario desconfíe de ella, salvo que el destinatario conociere o no hubiere actuado con la debida diligencia.

Los suscriptores serán responsables por la falsedad, error u omisión en la información suministrada a la Entidad de Certificación y por el incumplimiento de los deberes antes señalados.

Art. 39 Obligaciones Vinculadas a la firma digital
Mientras el certificado no sea revocado, suspendido o cancelado conforme a los reglamentos que al efecto se dictaren, la firma digital, vincula al titular o a su representado en sus obligaciones frente a terceros de buena fe.

Frente al tercero de buena fe, no cesará la eficacia de la firma digital por muerte, incapacidad, liquidación, quiebra o cualquier otra causa restrictiva

de la capacidad de la persona a quien se imputen los efectos de la misma.

Art. 40 Duración de la firma digital
El período de vigencia estará sujeto a la voluntad del titular de dicha firma, de acuerdo a lo que se estableciere en el Reglamento de esta Ley y/o en cualquier otra Ley que pudiera dictarse a estos efectos.

Art. 41 Prueba
Las firmas digitales serán admisibles como prueba en juicio, valorándose estás de acuerdo a los criterios de valoración contenidos en las normas de la presente ley.

SECCIÓN VI --DE LAS ENTIDADES DE CERTIFICACIÓN Y LOS CERTIFICADOS

Art. 42 De las Entidades de Certificación
Son las personas jurídicas legalmente capacitadas, públicas o privadas, nacionales e internacionales que previa solicitud sean autorizadas por _____ y que cumplan con los demás requerimientos establecidos en los reglamentos emitidos por el Órgano Ejecutivo, con base en las siguientes condiciones:

Ser persona jurídica u organismo público. En caso de ser organismo público estos deberán contar con un presupuesto de gastos y de ingresos que permitan el desarrollo de esta actividad.

Contar con la capacidad económica, financiera y humana suficiente para prestar los servicios autorizados como Entidad de Certificación.

Contar con la capacidad y elementos técnicos necesarios para la generación de firmas digitales, la emisión de certificados sobre la autenticidad de las mismas y la conservación de mensajes de datos en los términos establecidos en esta Ley.

Garantizar un servicio de suspensión, cancelación y revocación, rápido y seguro, de los Certificados que emita.

Un sistema de información de acceso libre, permanente, actualizado y eficiente en el cual se publiquen las políticas y procedimientos aplicados para la prestación de sus servicios, así como los Certificados que hubiere proporcionado, revocado, suspendido o cancelado y las restricciones o limitaciones aplicables a éstos.

La reglamentación de la presente ley establecerá las demás regulaciones que gobernaran las actividades y requerimientos, suspensión de

actividades, garantía, revocación, y otras normas necesarias para la aplicación de la presente ley.

Art. 43 De los Certificados
Un certificado emitido por una Entidad de Certificación autorizada, además de estar firmado por ésta, debe contener por lo menos lo siguiente:

- Nombre, dirección y domicilio del suscriptor.
- Identificación del suscriptor nombrado en el certificado.
- Nombre, dirección y lugar donde realiza sus actividades la entidad de certificación.
- La clave pública del usuario, o cualquier otro método que se pudiese utilizar para identificar al suscriptor.
- La metodología para verificar la firma digital del suscriptor impuesta en el mensaje de datos.
- El número de serie del certificado.
- Fecha de emisión y expiración del certificado.
- La limitación de los fines o del valor con los que pueda utilizarse el certificado, así como de responsabilidad del titular o de la entidad certificadora.
- En los casos de representación, la indicación del documento que acredite las facultades del representante para actuar en nombre de la persona natural o jurídica a la que represente.
- Cualquier otro requisito que se considere esencial según la reglamentación adoptada por el Órgano Ejecutivo.

Artículo 44 Obligaciones de las Entidades de Certificación
Son obligaciones de la Entidades de certificación:

a) Encontrarse legalmente constituidas y registradas en el órgano de control;

b) Justificar de acuerdo al Reglamento, confiabilidad y probidad para prestar servicios de certificación;

c) Ser entidades con solvencia técnica, logística y financiera para prestar óptimos servicios a sus usuarios;

d) Los representantes legales y administradores no podrán ser personas que hayan sido condenadas con pena privativa de la libertad por delitos comunes; Además, las personas que han sido excluidas o suspendidas en el ejercicio de su profesión por falta grave profesional. Esta inhabilidad estará vigente hasta por el tiempo señalado por la Ley para su prescripción;

e) Garantizar la prestación permanente del servicio de Certificación;

f) Atender oportunamente las solicitudes y reclamaciones hechas por los suscriptores;
g) Contar con un servicio de suspensión, cancelación y revocación de certificados, rápido y seguro;
h) Mantener personal técnico, con experiencia y debidamente calificado en la materia;
i) Utilizar sistemas y productos confiables que estén protegidos de toda alteración, además deberán garantizar la seguridad técnica y criptográfica de los procesos que soporten;
j) Mantener sistemas de respaldo de la información relativa a los Certificados;
k) Mantener una publicación en Internet y en otros medios determinados en el contrato de suscripción, en los cuales conste la información relativa a los procedimientos, reglamentos y prácticas aplicadas a los contratos celebrados con los usuarios;
l)) Utilizar herramientas o programas de firma digital que estén protegidas contra la modificación de éstas, de tal forma que no puedan realizar funciones distintas a aquéllas para las que han sido diseñadas. Deben utilizar productos de firma electrónica que, bajo estándares internacionales, garanticen la seguridad y confidencialidad técnica de los procesos de certificación soportados por los productos;
m) Adoptar medidas para evitar la falsificación de Certificados y, en el caso de que la Entidad de Certificación intervenga en la generación de claves privadas, garantizar la seguridad y confidencialidad durante el proceso de generación de dichas claves;
n) Almacenar toda la información relativa a un Certificado por un periodo mínimo de 15 años, especialmente para efectos de prueba en procedimientos judiciales. El almacenamiento podrá hacerse de forma electrónica;
Ñ) No almacenar ni copiar las claves privadas de firma digital de la persona a la cual la entidad de certificación de información ofrezca servicios de administración de claves, a menos que la persona lo solicite expresamente por un medio seguro;

o) Informar a los consumidores antes de iniciar una relación contractual, utilizando un lenguaje entendible y un medio duradero de comunicación, acerca de los términos precisos y condiciones para el uso del certificado, incluyendo cualquier limitación sobre responsabilidad y los procedimientos existentes para resolver cualquier conflicto;
p) Transferir al Organismo de Control para su archivo confidencial, las claves, revocaciones y la documentación que las justifique, en caso de liquidación o terminación de las actividades o quiebra técnica;
q) Garantizar la integridad, disponibilidad y entrega de la información y documentos a su cargo, a fin de que puedan ser usados como

medio de prueba. En especial, suministrarán la información que sea requerida las entidades administrativas competentes o judiciales en relación con las firmas digitales y certificados emitidos; y, en general sobre cualquier mensaje de datos que se encuentre bajo su custodia y administración;

r) La entidad de certificación de información, está obligada, en el acto, a proceder a la revocación, suspensión o cancelación de certificados y a su inmediata publicación de acuerdo con lo dispuesto en esta Ley;
s) Elaborar los reglamentos que definan las relaciones con el suscriptor y la forma de prestación del servicio;
t) Mantener y publicar oportunamente en Internet un listado de fácil y rápido acceso de los certificados de firmas electrónicas suspendidos, cancelados o revocados;
u) Proporcionar a los titulares de certificados de firmas digitales un medio efectivo y rápido para dar aviso que una firma digital tiene riesgo de uso indebido, en cuyo caso el titular deberá solicitar la suspensión del mismo;
v) Certificar la correspondencia de funcionamiento entre la clave pública y la clave privada de acuerdo al certificado expedido y la entrega al titular de ambas claves;
w) Asegurar que el titular del certificado tuvo, en el momento de creación del mismo, el instrumento de generación de firma correspondiente al instrumento de verificación del mismo, reseñado o identificado en el certificado.

Artículo 45 Protección de Datos por parte de las Entidades de Certificación

Las Entidades de Certificación garantizarán, en el archivo, uso y manejo de datos obtenidos en función de su trabajo:

La reserva, privacidad, protección y confidencialidad de la información y datos que manejen. Obtener información únicamente con el consentimiento y voluntad de la persona relacionada con dicha información.

Otros requisitos establecidos en las leyes y reglamentos que regulen la materia. Las Entidades de Certificación, recopilarán datos personales únicamente de los propios sujetos o sus representantes legalmente acreditados y sólo en la medida en que sean necesarios para la emisión de un certificado. Los datos no pueden ser recopilados, procesados, cedidos o distribuidos, sin el consentimiento expreso del titular, para fines distintos de la prestación de servicios de certificación.

Serán sancionadas, conforme a lo dispuesto en esta Ley y otras leyes, la recopilación y cesión ilegal de datos, así como las violaciones de los derechos de confidencialidad y sobre la protección de datos personales.

Art. 46 Cese de actividades
La Entidad de Certificación cesa en tal calidad:

Por decisión unilateral comunicada a la entidad reguladora;

Por revocación de su personalidad jurídica o por cualquier otra causal legal de disolución;

Por revocación de su licencia dispuesta por la entidad de reguladora.

Los certificados emitidos por una Entidad de Certificación que cesa en sus actividades deben ser revocados a partir del día y la hora en que cesa su actividad.

En el caso del literal a) la Entidad de Certificación debe notificar a la a Entidad Reguladora y hacer saber, mediante publicación en el diario oficial por tres días (3) consecutivos, la fecha y la hora de cese de actividades, la cual no puede ser anterior a los noventa (90) días contados desde la fecha de la última publicación.

Igualmente deberán notificar el cese de actividades a todos sus usuarios desde el momento de su decisión o que tome conocimiento de la revocación de su licencia para operar.

SECCIÓN VII -- DE LA ENTIDAD REGULADORA

Art. 47 Funciones de la Entidad Reguladora
__ , ejercerá las facultades que legalmente le han sido asignadas respecto de las Entidades de Certificación y adicionalmente tendrá las siguientes funciones:

- Autorizar la actividad de las entidades de certificación en el territorio nacional otorgando licencias de operación.
- Velar por le funcionamiento y la eficiente prestación del servicio por parte de las Entidades de Certificación.
- Realizar visitas de auditoría a las Entidades de Certificación de acuerdo a lo dispuesto en los reglamentos respectivos.
- Solicitar la información pertinente para el ejercicio de sus funciones.
- Imponer sanciones a las Entidades de Certificación en caso de incumplimiento de las obligaciones derivadas de la prestación del servicio.

- Ordenar la revocación de certificados cuando la Entidad de Certificación los emita sin el cumplimiento de las formalidades legales.
- Designar los repositorios y entidades de certificación en los eventos previstos en la ley.
- Emitir certificados en relación con las firmas digitales en las Entidades de Certificación.
- Velar por la observancia de las disposiciones constitucionales y legales sobre la promoción de la competencia y prácticas comerciales restrictivas, competencia desleal y protección al consumidor, en los mercados atendidos por las entidades de certificación.
- Impartir instrucciones sobre el adecuado cumplimiento de las normas a las cuales deben sujetarse las Entidades de Certificación.
- Revocar o suspender la acreditación otorgada cuando se incumplan las condiciones, requisitos y obligaciones que se establecen en la presente ley.
- Mantener, procesar, clasificar, resguardar y custodiar el Registro de las Entidades de Certificación de acuerdo a lo dispuesto en los reglamentos respectivos.
- Recaudar multas de acuerdo a lo dispuesto en los reglamentos respectivos.
- Actuar como mediador en la solución de conflictos que se susciten entre las Entidades de Certificación y sus usuarios, cuando ello sea solicitado por al menos una de las partes involucradas, sin perjuicio de las atribuciones que tenga el organismo encargado de la protección, educación y defensa del consumidor y el usuario, conforme a esta ley y los reglamentos respectivos.

La reglamentación de la presente ley establecerá las demás regulaciones que gobernaran las actividades y requerimientos, proceso de mediación, creación de registros, aranceles, supervisión, obligaciones, medidas cautelares, sanciones y otras normas necesarias para la aplicación de la presente ley.

Art. 48 Sanciones
La Entidad Reguladora de acuerdo con el debido proceso y el derecho a la defensa, podrá imponer a las Entidades de Certificación, por el incumplimiento de sus responsabilidades, obligaciones y requisitos según la naturaleza y la gravedad de la falta, las siguientes sanciones:

Amonestación escrita.
Multa pecuniaria de hasta _____ tanto para las Entidades de Certificación como para los administradores y representantes legales de las mismas.

Suspender de inmediato todas o algunas de las actividades de la Entidad infractora.

Prohibir a la Entidad de Certificación infractora prestar directa o indirectamente los servicios de entidad de certificación hasta por el término de cinco (5) años.

Revocar definitivamente la autorización para operar como entidad de certificación.

SECCIÓN VIII - DE LA PROTECCIÓN DE LOS CIUDADANOS Y LOS CONSUMIDORES EN EL USO DE COMUNICACIONES ELECTRÓNICAS

Art. 49 Protección de la Privacidad de Ciudadanos y Consumidores
La presente Ley se aplicará sin perjuicio de las normas vigentes en materia de protección al consumidor, en particular de las contenidas en la Ley de Protección al Consumidor.

Si la ley aplicable seleccionada por las partes fuese en detrimento de los derechos de los consumidores conforme a la Ley Salvadoreña, dicha ley se tendrá por no aplicable.

SECCIÓN XII -- DISPOSICIONES VARIAS

Art. 50 Reconocimiento de Certificados, Documentos Electrónicos y Firmas Digitales del Extranjero
Cuando se requiera determinar la validez de un certificado, documento electrónico o firma digital emitida en el extranjero, no se le negará validez por el solo hecho de haber sido emitido o creado en país extranjero; pero para ser reconocidos en los mismos términos y condiciones exigidos por la presente Ley a las Entidades de Certificación nacionales, deberán ser reconocidos por una Entidad de Certificación autorizada por su país de origen, en la misma forma que reconoce sus propios certificados, la regularidad de los detalles del certificado, así como su validez y vigencia.

Los certificados electrónicos extranjeros no garantizados por una Entidad de Certificación debidamente acreditada que cumpla con los requisitos de acreditación en la presente ley, carecerán de los efectos jurídicos que se le atribuyen en la presente ley, sin embargo podrán constituir un elemento de convicción valorable conforme a las reglas de la sana crítica.

Art.51 Reglamentos y Facultad del Órgano Ejecutivo para reglamentar la Ley
El Órgano Ejecutivo por medio del Ministerio de Economía contará con un plazo de doce(12) meses, contados a partir de la publicación de la presente ley para organizar y asignar a _____ para llevar a cabo la función de inspección, control y vigilancia de las actividades realizadas por las entidades de certificación y para emitir todos los reglamentos que considere necesarios para desarrollar el contenido de la presente Ley.

Art. 52 Vigencia y Derogatorias
La presente Ley entrará en vigencia ocho días después de publicada y deroga las disposiciones que le sean contrarias.