

UNIVERSIDAD DE EL SALVADOR
FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES
SEMINARIO DE GRADUACIÓN EN CIENCIAS JURÍDICAS AÑO ACADÉMICO 2004
PLAN DE ESTUDIO 1993



**LA SEGURIDAD JURÍDICA QUE PROPORCIONA EL ESTADO AL
UTILIZAR LA FIRMA DIGITAL COMO MEDIO DE EXPRESIÓN DEL
CONSENTIMIENTO**

**TRABAJO DE GRADUACIÓN PARA OPTAR AL TÍTULO DE:
LICENCIADO EN CIENCIAS JURÍDICAS**

PRESENTAN:

ARRUÉ ECHEGOYÉN, CAROLINA ESMERALDA
MASIN MASIN, NATALIA MARGARITA
VÁZQUEZ LARA, MANUEL ALEJANDRO

DIRECTOR DE SEMINARIO:

LICDA. DELMY RUTH ORTIZ SÁNCHEZ

CIUDAD UNIVERSITARIA, SAN SALVADOR, NOVIEMBRE DE 2004.

UNIVERSIDAD DE EL SALVADOR

RECTORA

DRA. MARÍA ISABEL RODRÍGUEZ

VICE-RECTOR ACADÉMICO

ING. JOAQUÍN ORLANDO MACHUCA GÓMEZ

VICE-RECTORA ADMINISTRATIVO

DRA. CARMEN ELIZABETH RODRÍGUEZ DE RIVAS

SECRETARIA GENERAL

LICDA. ALICIA MARGARITA RIVAS DE RECINOS

FISCAL GENERAL

LIC. PEDRO RESALIÓ ESCOBAR CASTANEDA

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

DECANA

LICDA. MORENA ELIZABETH NOCHEZ DE ALDANA

VICE-DECANO

LIC. OSCAR MAURICIO DUARTE GRANADOS

SECRETARIO

LIC. FRANCISCO ALBERTO GRANADOS HERNÁNDEZ

**COORDINADORA DE LA UNIDAD DE SEMINARIO DE
GRADUACIÓN**

LICDA. BERTA ALICIA HERNÁNDEZ AÁGUILA

DIRECTOR DE SEMINARIO

LICDA. DELMY RUTH ORTIZ SÁNCHEZ

DEDICATORIA

A DIOS:

Quien desde el inicio de mi carrera me enseñó a confiar en Él a pesar de las dificultades, a través de las cuales crecería más y aprendería mucho, a que todo lo que permite en nuestras vidas tiene un propósito y forma parte de un plan divino en el cual Él siempre estará presente para darnos fuerzas y ayudarnos.

A MIS PADRES:

Quienes fueron incondicionales en todo momento mostrándome siempre su ayuda y comprensión a pesar de todos los problemas y pruebas que enfrenté a lo largo de la carrera, que estuvieron presentes cuando los necesitaba, y que siempre, siempre confiaron en mí.

A MIS HERMANOS:

Que a pesar de disgustos que les causaba en los momentos de crisis, creyeron en mí, me apoyaron y siempre estuvieron dándome palabras de ánimo y de apoyo.

A ALGUIEN MUY ESPECIAL:

Que se presentó en mi vida al final de mi carrera, y me dio el apoyo y comprensión que necesitaba en la última y más difícil etapa de mi carrera; y me ayudó a que mi Servicio Social y Práctica Jurídica representaran una etapa muy especial en mi vida y una meta también lograda en mi carrera; y a quien sobre todo me soportó muchas crisis, y nunca se quejó.

A MI FAMILIA:

Abuelos, tíos, primos, quienes con sus bromas y preguntas hacían de mis días difíciles momentos alegres y placenteros.

A MIS AMIGOS Y HERMANOS EN CRISTO:

Quienes estuvieron pendientes de mí, orando y apoyándome con palabras que me reconfortaron.

A MI ASESORA

Licenciada Delmy Ortiz, quien nos apoyo desde el inicio y nos mostró su comprensión a lo largo de todo el proceso de elaboración de nuestra investigación.

A MIS COMPAÑEROS DE GRUPO:

Que durante los cinco años me demostraron ser un grupo genuino en apoyo incondicional y afecto, con quienes reímos y nos afligimos por pruebas muy duras.

Y es a todas estas personas que estuvieron presentes en distintos momentos de mi tesis a quienes quiero agradecer su apoyo y ánimo brindado en el momento necesario y justo.

Carolina Esmeralda Arrué Echegoyén

AGRADEZCO POR EL LOGRO DE ESTA META :

AL REY DE REYES Y SEÑOR DE SEÑORES

Que es dios todopoderoso, por guiar mi camino y mostrar gran misericordia en mi vida, por su fidelidad en cada instante bueno o malo, porque es mi fortaleza y amparo, por la vida misma que me regala, y por todo lo demás que no menciono.

A MI PAPÁ

Por su amor único con el que orienta mi vida, por su apoyo incondicional o su desacuerdo total en determinados momentos, porque cumple con todos los elementos para ser llamado papá.

A MI MAMI

Por su fortaleza y fragilidad, porque su amor no tiene límite y me dedica todos los días de su vida, y está siempre disponible para mí, aguardando que la llame.

A MI MATY

*Porque es la mujer virtuosa y cuento con ella hasta en mis sueños, porque reúne todo para ser llamada **especial**, porque no sabe quererme sino amarme porque es mucho más que una abuela, es mi segunda mamá.*

A MI HERMANO

Que me ha soportado y lo sigue haciendo y que con su sencillez me ha dado grandes lecciones, porque siempre está cuando lo necesito y es en verdad un hermano.

A CAROLINA Y MANUEL

Por ser no solo mis compañeros sino mis AMIGOS por soportarme demasiadas cosas y mostrarme cariño verdadero, porque no tengo cómo agradecerles mucho menos pagarles todo el apoyo brindado.

A MI ESTIMADA ASESORA

Licenciada Delmy Ruth Ortiz Sánchez que ha sido más que una asesora, una verdadera guía y amiga, que nos estuvo apoyando en todo tiempo y gracias a la cual llegamos a finalizar este trabajo

A TODOS MIS AMIGOS

A los que han estado siempre presentes e interesados en el transcurrir de mi vida, por ser incondicionales.

A los que han ido y venido y no por eso dejan de ser amigos, porque cuando están saben serlo.

A TODAS LAS PERSONAS

Que de una u otra forma me ayudaron en momentos determinados no solo en la realización del trabajo de investigación sino en el desarrollo de toda la carrera, brindándome parte de su tiempo y conocimientos.

A MI PAPÁ BELLO

Que en vida nunca me desamparó, tenía una confianza inquebrantable en mí, el cual en cada uno de los últimos días de su vida me inspiraba a seguir y no desfallecer. Al que amé, sigo amando y jamás olvidaré por ser el más BELLO abuelo que ha existido y es a quien dedico todo este éxito.

Natalia Margarita Masin Masin

AGRADECIMIENTOS

***“Ningún logro debe ser el último por alcanzar; no satisface o está completo al olvidar,
las manos que le ayudaron a caminar”***

Gracias, infinitas gracias:

- **A Ti Único Maestro:** en mi andar, la luz y fortaleza en cada adversidad; quien al extender tu mano me permitiste triunfar, **MI DIOS**, Creador de todo motivo de mi agradecer en quien siempre me podré apoyar.
- **A Mis Padres y Hermanos:** por cada gota de sudor que derramaron en su incesante esfuerzo por verme triunfar; por cada aliento que de sus palabras brotó para que pudiera luchar; por sus incansables brazos extendidos que me hicieron siempre levantar.
- **A Nuestra Asesora, Licenciada Delmy Ortiz:** por orientar nuestras ideas con su conocimiento que permitieron alcanzar y terminar esta investigación; además de su apoyo incondicional.
- **A Mis Compañeras de Tesis:** por su esfuerzo, dedicación para que lográramos concebir el presente trabajo; por cada minuto de su tiempo; y por no limitarse únicamente a ser compañeras sino amigas.

Manuel Alejandro Vásquez Lara

DEDICATORIA

A Mi único refugio por todos los siglos mi Dios y Salvador él quien todo lo ha hecho y por quien existo.

A mis padres porque si me hubieran permitido dejar escoger algunos, nunca hubiera encontrado mejores.

Al dulce recuerdo de mi abuelo, imagen de esfuerzo y lucha constante para cualquier adversidad.

A aquellos que me permitieron compartir y sentir los momentos que ahora enmarco como bellos recuerdos guardados con recelo por mi mente centinela; que me saludaran día a día con sonrisas o compañías quienes vivieron mis triunfos, fracasos, alegrías y tristezas, ustedes mis compañeros, hermanos de aula.

Manuel Alejandro Vásquez Lara

ÍNDICE

	Pág.
Introducción.....	i
CAPÍTULO 1	
ORIGEN Y DESARROLLO DEL COMERCIO ELECTRÓNICO Y LA FIRMA DIGITAL	
1.1 Introducción.....	1
1.2 Origen del Comercio Electrónico.....	2
1.3 Desarrollo Internacional del Comercio Electrónico.....	7
1.4 Desarrollo del Comercio Electrónico en El Salvador.....	9
1.5 Origen de la Firma Digital a Nivel Internacional.....	11
1.5.1 Aparecimiento de la Firma Digital en la Legislación Internacional...	13
1.5.2 Incorporación de la Firma Digital en El Salvador.....	19
CAPÍTULO 2	
DE LAS FIRMAS	
2.1 Introducción.....	23
2.2 Origen de la Firma Manuscrita.....	24
2.2.1 Generalidades.....	26
2.2.1.1 Definición.....	26
2.2.1.2 Naturaleza.....	28

2.2.1.3 Características.....	29
2.2.1.4 Elementos.....	30
2.3 Firma Electrónica. Definición.....	32
2.4 Firma Digital.....	33
2.4.1 Generalidades.....	33
2.4.1.1 Definición.....	33
2.4.1.2 Características Técnicas.....	36
2.4.1.3 Atributos de Seguridad de la Firma Digital.....	37
2.4.1.4 Ventajas y Desventajas.....	39
2.4.1.5 Criptografía.....	40
2.4.1.5.1 Historia.....	40
2.4.1.5.2 Concepto.....	47
2.4.1.5.3 Tipos de Criptografía	
Simétrica y Asimétrica.....	56
2.4.2 Proceso de Firma Digital y Verificación	64
2.4.3 La Firma Digital en El Salvador.....	68
2.5 Firma Manuscrita – Firma Electrónica – Firma Digital.....	80

CAPÍTULOS 3

CERTIFICADOS Y AUTORIDADES DE CERTIFICACIÓN

3.1 Introducción.....	83
3.2 Certificados Digitales.....	84

3.2.1 Definición.....	84
3.2.2 Clases.....	85
3.2.3 Requisitos.....	88
3.2.4 Ciclo Vital del Certificado.....	90
3.2.4.1 Generación y Emisión.....	90
3.2.4.2 Distribución del Certificado.....	92
3.2.4.3 Período de Validez del Certificado	
Invalidez Anticipada: Revocación y	
Suspensión del Certificado.....	93
3.3 Autoridades o Entidades de Certificación.....	97
3.3.1 Definición.....	97
3.3.2 Naturaleza.....	98
3.3.3 Funciones.....	99
3.3.4 Clases de Entidades de Certificación.....	102
3.3.5 Importancia de las Entidades de Certificación.....	104
3.4 Firma Digital y su Seguridad Tecnológica: PKI-Infraestructura de	
Clave Pública.....	105
3.5 Otros Mecanismos de Seguridad.....	110
CAPÍTULO 4	
CONSENTIMIENTO POR MEDIOS ELECTRÓNICOS	
4.1 Introducción.....	113

4.2 Del Consentimiento. Definición.....	114
4.3 Elementos del Consentimiento.....	116
4.4 Sujetos del Consentimiento.....	116
4.5 Etapas del Consentimiento.....	117
4.5.1 Oferta.....	118
4.5.2 Aceptación.....	120
4.6 Formas del Consentimiento.....	121
4.7 Momento del Perfeccionamiento.....	122
4.8 Vicios del Consentimiento.....	126
4.8.1 Error.....	126
4.8.2 Fuerza.....	127
4.8.3 Dolo.....	128
4.9 El Consentimiento en las Redes.....	130
4.9.1 Etapas del Consentimiento: Oferta y Aceptación en las Redes.....	130
4.9.2 La Perfección del Contratos Celebrado en la Red.....	137

CAPÍTULO 5

LA SEGURIDAD JURÍDICA DE LA FIRMA DIGITAL

5.1 Introducción.....	141
5.2 Eficacia Jurídica de la Firma Digital	142
5.3 Delitos Informáticos.....	143
5.3.1 Definición.....	144

5.3.2 características.....	144
5.3.3 Clasificación.....	146
5.4 Documento Electrónico.....	150
5.4.1 Definición.....	151
5.4.2 Características.....	152
5.4.3 Clasificación.....	153
5.4.4 Desmaterialización.....	154
5.4.5 Valor Probatorio.....	155
5.5 Análisis de la Legislación de la Firma Digital.....	159
5.5.1 A Nivel Internacional.....	159
5.5.2 A Nivel Nacional.....	175

CAPÍTULO 6

COMPROBACIÓN DE HIPÓTESIS Y ANÁLISIS DE DATOS

6.1 Introducción.....	194
6.2 Comprobación de Hipótesis.....	194
6.3 Análisis de Datos.....	195

CAPÍTULO 7

CONCLUSIONES Y RECOMENDACIONES

7.1 Introducción.....	214
7.2 Conclusiones.....	215

7.3 Recomendaciones.....	219
BIBLIOGRAFÍA.....	221
Anexos.....	227
Anexo 1: Abreviaturas	
Anexo 2: Glosario	
Anexo 3: Ley Modelo de Comercio Electrónico y su Guía para la Incorporación al Derecho Interno. UNCITRAL	
Anexo 4: Ley Modelo para las Firmas Electrónicas. UNCITRAL	
Anexo 5: Ley 59/2003 de 19 de diciembre de Firma Electrónica de España	
Anexo 6: Ley 25.506 de Firma Digital de Argentina	
Anexo 7: Reglamento de la Ley 25.506 de Argentina	
Anexo 8: Ley 527 de Colombia	
Anexo 9: Ley de Firma Digital y Certificados Digitales de Costa Rica	
Anexo 10: Anteproyecto de Ley de Comercio Electrónico de El Salvador (Ministerio de Economía)	
Anexo 11: Ley General Marítimo y Portuaria de El Salvador	
Anexo 12: Ley de Mediación, Conciliación y Arbitraje de El Salvador	
Anexo 13: Ley de Simplificación Aduanera de El Salvador	

INTRODUCCIÓN

Actualmente, con el pleno desarrollo de la denominada revolución de la información, un número cada vez mayor de personas ordenadores, no solo para la búsqueda e intercambio de todo tipo de información, sino también para la realización de operaciones comerciales. Estas comunicaciones, transferencias o transacciones electrónicas en sentido amplio, pueden realizarse en el *sector público* para la comunicación dentro de la administración pública y con las administradas, en el *sector privado* en relaciones interempresariales o entre empresarios y consumidores, o entre *ambos sectores*; tanto en ámbitos nacionales como internacionales. Surgiendo así el fenómeno del comercio electrónico, desarrollándose a través de los mecanismos que proporcionan las nuevas tecnologías de la comunicación como el correo electrónico, el word wide web o el Electronic Data Interchange; cualquiera que sea el caso, esta clase de comercio permite nuevas oportunidades de negocios, una mayor competitividad, una reducción de costes, y una enorme celeridad en el desarrollo de las relaciones comerciales; asimismo, se considera que el comercio electrónico favorece también a los consumidores, pues, al poder comparar instantáneamente entre una amplia variedad de ofertas, gozan de mayor capacidad de elección, tienen a su alcance productos cada vez más especializados, y se pueden beneficiar de una baja de precios a medida que descienden los costes generales.

No obstante, junto a estas evidente ventajas, la utilización de estas nuevas tecnologías, y cambios como la eliminación del papel, pueden generar riesgos e

incertidumbres en los operadores económicos sobre cuestiones jurídicas tan esenciales de entrada como la validez y la eficacia de las transacciones electrónicas; entre otras cuestiones derivadas, como la problemática del perfeccionamiento del contrato celebrado por esos medios, la prueba del mismo, la distribución de riesgos y delimitaciones de responsabilidades entre los distintos sujetos intervinientes, la ley aplicable y la jurisdicción competente en caso de litigio; en definitiva, múltiples problemas derivados de la dificultad de aplicar conceptos y categorías jurídicas tradicionales a contratos realizados por los novedoso medios electrónicos.

Pero eso no es todo, existen también riesgos derivados de los problemas inherentes a los mismos sistemas electrónicos a través de los que se desarrolla el comercio electrónico, los cuales son susceptibles de usos, abusos y errores que puedan provocar graves perjuicios directos o indirectos a los diversos sujetos que participan en el mencionado comercio como lo son los empresarios, los consumidores y también los proveedores de servicios; y dados esos riesgos no existirá entonces garantías acerca de la autoría de los mensajes electrónicos, sobre su contenido y en última instancia sobre su existencia misma, lo que viene a cuestionar la validez y eficacia de ls transacciones electrónicas desde el punto de vista jurídico.

En relación a toda esta problemática es que en este trabajo de investigación se presenta un estudio acerca de la Firma Digital y la Seguridad Tecnológica que representa así como la Seguridad Jurídica que los Estados le brindan a través de su normativa, de esta manera el desarrollo capitular presenta en el *Primer Capítulo* un marco histórico sobre las figuras que constituyen los pilares que sostienen la investigación, tales como el

Comercio Electrónico y al Firma Digital y su desarrollo internacional y nacional, incorporando de forma sencilla las primeras normas jurídicas que en esta materia se han creado; en el *Segundo Capítulo* se contiene las generalidades de la firma manuscrita, firma electrónica y firma digital, sosteniendo un estudio más profundo sobre esta última, por lo cual se incluye a la criptografía como sistema utilizado para brindar seguridad a las nuevas tecnologías, no dejando de lado los indicios del sistema de firma digital que funcionan en El Salvador para concluir con un parangón de los tres tipos de firmas; el *Capítulo Tercero* se dedica a toda la infraestructura que ampara el sistema de firma digital, iniciando con el estudio de los Certificados Digitales, posteriormente se establecen los aspectos básicos de las Autoridades de Certificación explicando cual es el papel que estas juegan en la estructura de funcionamiento de la mencionada firma culminando con aportes que la Infraestructura de Clave Pública hace a la seguridad tecnológica de Firma Digital; en el *Capítulo Cuarto* se da paso a lo relacionado con el consentimiento y la forma en que las etapas de este se presenta en las contrataciones realizadas en red, tratando de ubicar el momento en que se tiene por perfeccionado el consentimiento; es el *Capítulo Quinto* el que se dedica a todo lo referente a la legislación que acerca del tema en estudio se encuentra abordado, el punto de la eficacia jurídica de la Firma Digital, lo concerniente a los delitos informáticos debido a que la importancia que merecen, seguidamente se hace alusión al Documento Electrónico y el valor probatorio que el mismo presenta tanto en el ambiente internacional como el nacional; es en el *Capítulo Seis* que se analizan los datos recogidos de la investigación de campo realizada con la colaboración de los diferentes ámbitos de la sociedad salvadoreña,

asimismo se establece la comprobación de la hipótesis, eje de nuestra investigación; el *Capítulo Siete* es en el que se finaliza el presente trabajo de investigación, con las respectivas conclusiones es acerca del tema y las determinadas recomendaciones que deben de realizarse en busca de que la labor efectuada no sea una más de tantas sino que sirva de inspiración para el mejoramiento de nuestro sistema jurídico y el funcionamiento del mismo Estado.

CAPÍTULO 1

ORIGEN Y DESARROLLO DEL COMERCIO ELECTRÓNICO Y LA FIRMA DIGITAL

Sumario: 1.1. Introducción. 1.2. Origen del Comercio Electrónico. 1.3 Desarrollo Internacional del Comercio Electrónico. 1.4. Desarrollo del Comercio Electrónico en El Salvador. 1.5. Origen de la Firma Digital a Nivel Internacional. 1.5.1 Aparecimiento de la Firma Digital en la Legislación Internacional. 1.5.2. Incorporación de la Firma Digital en El Salvador.

1.1. Introducción

El contenido de este primer capítulo debe de tomarse como lineamientos generales para un mejor entendimiento del presente trabajo de investigación. Se desarrolla de manera breve los aspectos más importantes del origen y desarrollo del Comercio Electrónico que se suscitaron tanto a nivel internacional como a nivel local, sentando con ello las bases para que floreciera un panorama comercial totalmente evolucionado y más dinámico que nunca. Así también se establecen parámetros sobre el origen de la firma digital, en especial la utilización de la criptografía a través de la historia, pues siendo esa un aspecto fundamental para entender lo relacionado con la firma digital se hace necesario contar con una idea inicial de lo que se estará tratando en los siguientes Capítulos. Debido a ello se incluye lo referente a las primeras iniciativas en materia de legislación

que los Estados a nivel mundial han realizado para beneficiar con la utilización de esta tecnología el decidido desarrollo comercial que impera en nuestros días. Se expone además, la manera en que el sistema de firma digital comienza a introducirse en El Salvador para beneficio de diversos sectores del ámbito nacional.

1.2. Origen del Comercio Electrónico

El comercio como tal actividad humana que lo ha acompañado desde tiempos ancestrales, ha evolucionado de muchas maneras; pero debe aclararse que su significado y fin se ha conservado. Se entiende por comercio el proceso y los mecanismos utilizados necesarios para colocar las mercancías, que son elaboradas en las unidades de producción en los centros de consumo en donde se aprovisionan los consumidores, último eslabón de la cadena de comercialización. Es comunicación y trato.¹ En líneas generales y, con un sentido amplio, el comercio implica la investigación de mercado con el fin de interpretar los deseos del consumidor, la publicidad que anuncia la existencia del producto, la posibilidad de adquirirlo, y en que lugar, a la vez que se utilizan medios que permitan persuadir, la venta al por menor y finalmente la adquisición por parte del público.

A través de los años se han desarrollado de acuerdo a las necesidades, diferentes formas o tipos de comercio. A principio de la década de los 20, del siglo anterior, en los Estados Unidos surgió la venta utilizando catálogos, impulsados por grandes tiendas de

¹ “Comercio Electrónico”, www.monografias.com/trabajo12/monografias/monografias.shtml, mayo, 2004.

mayoreo. Este sistema de venta, que para su época se puede considerar de impacto revolucionario; consiste en un catálogo con fotos ilustrativas de los productos a vender; este permite tener mayor llegada, ya que no hay necesidad de tener que atraer a los clientes hacia los locales de venta. Esto posibilitó a las tiendas llegar a los clientes en zonas rurales, que para la época en que se desarrolló dicha modalidad existía una gran masa de personas arraigadas al campo. Además, otro punto importante de esto es que los potenciales compradores pueden escoger los productos en la tranquilidad de sus hogares, sin la asistencia o presión, según sea el caso, de un vendedor. La venta por catálogo tomó mayor impulso con la aparición de las tarjetas de crédito; además de determinar un tipo de relación de mayor anonimato entre el cliente y el vendedor.

El avance tecnológico ha influido en el comercio de manera muy importante, el hecho más sobresaliente de los últimos años se derivó del proyecto llevado a cabo por el Departamento de Defensa de los Estados Unidos de Norteamérica que dio origen a lo que hoy en día se conoce como la red más grande del mundo Internet. Antes de la aparición del Internet las operaciones y transacciones financieras, comerciales y bancarias por medios electrónicos no eran desconocidas, pero si estaban reservados a muy pocas personas y eran de limitada funcionalidad. Estaban reservadas para operaciones interbancarias, gubernamentales o privadas de gran valor.²

Las primeras iniciativas referentes a la utilización de esta red surgen a finales de la década de los 60, pero es en los últimos años en que el Internet ha tenido un gran impacto en la comercialización de productos y servicios, convirtiéndose así en una vía,

² “Nuevas Tecnologías,” <http://homepage.mac.com/eravila/ecommercel.pdf>, mayo, 2004.

no solo una alternativa, de enorme utilización para la realización de muchas actividades económicas.

En esta misma década se realizaron los primeros esfuerzos para el intercambio de datos comerciales en forma estructurada por medios electrónicos tales como el EDI, Electronic Data Interchange, (Intercambio de Datos Electrónicos), el cual se remonta a la época de la industria del transporte en carretera y ferrocarrilera de los Estados Unidos; sin embargo las ideas detrás de la coordinación y estandarización de documentos para el intercambio comercial pueden trazarse hasta 1948 a la transportación aérea de bienes perecederos.³

EDI fue concebido como un reemplazo de órdenes de compra en papel con equivalentes electrónicos. Puede ser comparado y contrastado con el correo electrónico, pero los mensajes cuentan con una estructura definida. Tres elementos definen el EDI: el uso de un elemento electrónico para la transmisión de datos, el uso de mensajes con un formato estándar y consensuado, rápido envío y restricción de mensajes incluyendo la comunicación directa entre aplicaciones y computadoras.

En la década de los 70, los bancos comenzaron a utilizar la Transferencias Electrónicas de Fondo (EFT), que consistía en la transferencia electrónica de documentos de una computadora a otra, encontrándose estructurada mediante mensajes acordados y estandarizados internacionalmente; estas se daban a través de redes

³ Ídem.

privadas, ya que el gobierno y la empresa privada tenían como propósito hacer un mejor uso de computadoras para mejorar las transacciones entre las diversas compañías.⁴

Finalizando la década de los 80 e iniciando la década de los 90 más compañías se fueron involucrando en la mensajería electrónica y diversos sistemas fueron desarrollados para permitir el paso de métodos no electrónicos a plataformas electrónicas con la finalidad de volver los procesos administrativos más eficientes.

Fue en este momento en que se introdujo el comercio electrónico como forma de proveer servicios: on-line (en línea) al público, iniciando de esta manera el desarrollo de aldeas virtuales limitadas a un número reducido de personas.

El avance tecnológico mejoró los mecanismos de uso de las computadoras permitiendo su uso masivo, lo cual aunado a la creación y desarrollo del World Wide Web (www), “La Red que cubre al mundo”, y de tecnologías que garanticen la seguridad de las transacciones electrónicas, facilitan el enorme impacto del comercio electrónico.

Debido a la importancia derivada de lo ya expuesto el comercio electrónico ha sido y sigue siendo objeto de diversos estudios y publicaciones que han abordado distintos aspectos del mismo, tratando algunos de ellos de definir esta nueva e innovadora forma de actividad comercial. En general, esas definiciones se centran o toman como puntos de referencia los medios electrónicos utilizados y la naturaleza de las propias actividades comerciales. En lo que respecta a la evolución de ese fenómeno y

4 GAITÁN CORTEZ, Carlos Ernesto y otros, “Relaciones Contractuales en Internet y su desprotección por la falta de Legislación de Comercio Electrónico”, Tesis UES, 2003, Pág. 3

considerando la rápida evolución de las actividades, se cree conveniente analizar por separado los términos “comercio” y “electrónico”.

Debe entenderse por “electrónico” la infraestructura mundial de tecnologías y redes de la informática, las telecomunicaciones que permiten el procesamiento y la transmisión de datos digitalizados. En las primeras redes privadas, las transacciones económicas fueron realizadas de forma tradicional durante varias décadas hasta el surgimiento de redes abiertas con protocolos de uso público, como por ejemplo Internet. Un rasgo común entre esas redes es que operan sobre la base de propósitos definidos de forma específica y están destinadas exclusivamente para participantes autorizados.

Dentro del contexto en estudio la palabra “comercio” se refiere a una serie cada vez mayor de actividades que tienen lugar en redes abiertas (compraventa, publicidad, comercio y transacciones de toda índole) las cuales conducen a un intercambio de valor entre dos partes.

Al tomar en cuenta lo anterior se puede concluir que comercio electrónico es un concepto amplio que involucra cualquier transacción comercial efectuada por medios electrónicos tales como: el fax, el telex, el teléfono, los EDI e Internet. No obstante nos limitaremos a considerarlo de la siguiente manera: “Comercio electrónico es la parte del comercio que se desarrolla a través de redes (cerradas y abiertas) mediante la relación entre oferta y demanda, para lo cual se utilizan herramientas electrónicas y telecomunicaciones, con el objeto de agilizar el proceso comercial por medio de la reducción de tiempo de costes; abarcando así todas las formas en que se puede

desarrollar el comercio, es decir, entre Estados, entre Estados y Empresas, entre Estados y Particulares, entre empresas, entre empresas y consumidores y entre consumidores.⁵

1.3.Desarrollo Internacional del Comercio Electrónico

Las redes mundiales de información han transformado al mundo y han acercado más a la gente a través de la innovación de las comunicaciones mundiales, se han posibilitado cambios en todos los ámbitos de la actividad, el empleo y la calidad de vida de las naciones. Con las nuevas tecnologías, el tiempo y la distancia dejan de ser obstáculos, los contenidos pueden dirigirse a una audiencia masiva o a un pequeño grupo de expertos y buscar un alcance mundial o meramente local. Las redes mundiales de información como Internet no conocen fronteras.

La rápida difusión y el gran interés en el mundo de la informática en conjunto con el mundo del comercio, ha permitido la creación de ese nuevo mercado que se define como “economía digital”. Los productores, proveedores de bienes/servicios y usuarios logran tener acceso y transmisión mundial de la información y esparcimiento en forma sencilla y económica, sean con fines comerciales o sociales. La apertura de mercados es fundamental para el rápido crecimiento del uso de nuevos servicios y la asimilación de tecnologías nuevas. En la práctica las empresas usan Internet como nuevo canal de ventas, sustituyendo las visitas personales, correo y teléfono por pedidos electrónicos, ya que gestionar un pedido por Internet cuesta 5% menos que hacerlo por vías

⁵ SARRA, Andrea Viviana, “Comercio Electrónico y Derecho”, Editorial Astrea, Edición 2001, Buenos Aires, Argentina, Pág. 279

tradicionales, naciendo entonces con el comercio electrónico, una alternativa de reducción de costes y una herramienta fundamental en le desempeño empresarial.

El comercio electrónico ha contribuido a convertir al mundo en un aldea planetaria, y aunque su evolución principal está en países industrializados, las naciones en desarrollo también pueden beneficiarse con un mejor conocimiento de este elemento de gran potencial en un mundo cada vez más globalizado.⁶

La aparición del comercio electrónico obliga claramente a replantearse muchas de las cuestiones del comercio tradicional, surgiendo nuevos problemas, e incluso agudizando algunos de los ya existentes. En ese catálogo de problemas, se plantean cuestiones que van, desde la validez legal de las transacciones sin papel, la necesidad de acuerdos internacionales que armonicen las legislaciones sobre comercio, el control de impuestos; la protección de los derechos de propiedad intelectual, la protección de los consumidores en cuanto a publicidad engañosa o no deseada, fraude, contenidos ilegales y uso abusivo de datos personales, hasta otros provocados por la dificultad de encontrar información en Internet, comparar ofertas y evaluar la fiabilidad del vendedor y del comprador en una relación electrónica, la falta de seguridad de las transacciones y medios de pago electrónicos, la falta de estándares consolidados, la proliferación de aplicaciones y protocolos de comercio electrónico incompatibles y la congestión de Internet.⁷

6 monografias.com Ob. Cit.

7 monograifas.com Ob. Cit.

1.4. Desarrollo del Comercio Electrónico en El Salvador

Posteriormente al establecimiento pleno del Internet a nivel mundial, en nuestro país en el año de 1994 se dieron los primeros movimientos que llevarían al país a un acceso fijo a la red, entre los precursores de esta iniciativa se encontraban: El Consejo Nacional de Ciencia y Tecnología (CONACYT), la Fundación Salvadoreña para el Desarrollo Económico y Social (FUSADES), Universidad de El Salvador, Universidad Centroamericana Doctor José Simeón Cañas, Universidad Don Bosco, Centro Cultural Salvadoreño, Escuela Superior de Economía y Negocios, Embajada de los Estados Unidos de Norteamérica, CRNet de Costa Rica, y la Organización de Estados Americanos, quienes el 2 de septiembre de ese año acuerdan constituir el grupo coordinador del Proyecto “SUNet”, “Internet en El Salvador”, siendo las primeras cinco instituciones señaladas las fundadoras del proyecto, y las restantes observadoras, teniendo a su cargo posibilitar la conexión de Internet en El Salvador.⁸

En ese mismo mes se gestionó ante la Internet Assigned Numbers Authority (IANA por su siglas en inglés, en castellano Autoridad de Asignación de Números de Internet) y el Internet Network Information Center (INTERNIC por sus siglas en inglés, en castellano Centro de Información de la Red de Internet), respectivamente, un conjunto de direcciones de Protocolo de Internet (IP), equivalentes a una clase B y la administración del dominio correspondiente a El Salvador, reflejando a través de SV.

⁸ GAITÁN CORTEZ, Carlos Ernesto, y Otros, Ob. Cit, pag. 14

En octubre de ese mismo año se estableció un acuerdo con UUNet compañía del Estado de Virginia de los Estados Unidos de América, para manejar el tráfico de correo desde y hacia El Salvador, bajo el dominio antes mencionado. En Diciembre del año en mención se instaló y configuró exitosamente un nodo UUCP (Unix to Unix Copy Program) de correo electrónico en el CONACYT con este propósito, y los primeros mensajes con direcciones terminadas en SV comenzaron a circular en Internet.

El Salvador se encontró inmerso en la World Wide Web desde enero de 1996, cuando ANTEL completó la instalación de los primeros enlaces dedicados a Internet en territorio salvadoreño, siendo estos los pertenecientes a la Universidad Centroamericana Doctor José Simeón Cañas y el de la Universidad Don Bosco.

Desde entonces el crecimiento del Internet ha sido muy acelerado observándose el aumento de proveedores de Internet, tales como: Americatel, AmNet, CyTec, EJJE, El Salvador On Line, GBNet, IFX, Integra, Intercom, Internet Gratis, Netcom, Newcom, Salnet, Saltet, Telecam, Telecom, Telefónica, Telemovil y Tutopía⁹

Las tendencias de relaciones desarrolladas en El Salvador a través del Internet son las denominadas “Business to Business (B2B), Empresa entre Empresa”, y “Business to Consumer (B2C), Empresa y Consumidor”.

La relación Empresa entre Empresa, es aquella en la que la Cámara de Comercio e Industria de El Salvador se ha enfocado y está coordinando tres proyectos EDI, bajo

⁹ Idem

estándares internacionales a nivel nacional en los sectores comercio, aduanal (Teledespacho) y financiero.

En cuanto a la relación Empresa y consumidor, en el país existe un amplio desarrollo de página www pero enfocada principalmente a la publicidad de bienes y servicios. A finales de 1999, surgieron páginas web interactivas (acceso a bases de datos para validar información y/o cálculos, los cuales dan servicio de valor agregado a los clientes). Para citar ejemplos con esta modalidad de comercio electrónico están: Pizza Hut, Almacenes Siman, Kismet, Trans-express, La Tienda.com, Reltex.com y Banco Cuscatlán. Dichos servicios están enfocados a ofrecer productos y servicios a través de la red Internet.

1.5.Origen de la Firma Digital a Nivel Intencional

Una de las cosas que desaparecen en el comercio electrónico son las tradicionales firmas manuscritas que pueden ser reemplazadas usando una variedad de métodos que son incluidos dentro del concepto amplio de firma electrónica. Una firma electrónica sirve a las partes para autenticar todos y cada uno de los mensajes que intercambien en un negocio electrónico.

La definición de “Firma” se ha asociado al “trazado gráfico, conteniendo habitualmente el nombre, apellido y rubrica de una persona, con el cual se suscriben los documentos para darle autoría y obligarse con lo que en ellos se dice. Partiendo de ello se dice que la firma puede componerse del nombre y apellido de la persona y

eventualmente de su rubrica, o consistir en otro “trazado gráfico” o en iniciales, o en grafías ilegibles; lo que importa es la habitualidad de la grafías con su autor. La firma autógrafa no es concebida como la única manera de firmar ya que hay otros mecanismos que constituyen también “trazados gráficos” que dan autoría y obligan, como es el caso de las claves, los códigos, los signos, y en algunos casos, los sellos; de tal manera que el calificativo de “electrónica” referido a la firma y, por ende, la expresión, “firma electrónica” en sentido amplio sería simplemente cualquier método o símbolo basado en medio electrónicos utilizado o adaptado por una parte con la intención actual de vincularse o autenticar un documento, cumpliendo todas o algunas de las funciones características de una firma manuscrita.¹⁰

Al hablar de la firma electrónica como género, puede establecerse la *firma digital* como una especie que ofrece mayor seguridad la cual vendría a ser firma electrónica avanzada las cuales se basan en el Sistema de la Criptografía.

El encriptado, a diferencia de la firma digital es un invento ancestral que tiene como objetivo básico encontrar sistemas que permitan hacer llegar determinada información considerada secreta, desde un lugar de origen a otro destino, de forma tan segura que, si el mensaje es interceptado, el atacante no puede reconocer el mensaje.¹¹

La criptografía debe ser abordada junto al tema de la firma electrónica y en especial con la firma digital para poder comprender todo lo referente a esta. Por lo cual esta se desarrolla con mayor amplitud posteriormente dentro de esta investigación.

10 MARTÍNEZ NADAL, Apollonia, “Comercio Electrónico, firma digital y autoridades de Certificación”, Editorial Civitas, III Edición, Madrid, España, 2001, Pág. 41

11 “Criptografía y Firma Digital”, www.webpanto.com, junio 2004.

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. Puede entonces decirse que las firmas digitales aparecieron por primera vez en 1976 con la llegada de la criptografía de clave pública o asimétrica, sin embargo es hasta hace pocos años que gobiernos y empresas empezaron a usar la tecnología de la firma digital para proteger los documentos confidenciales en la red de redes.

Para septiembre de 1998 el presidente de los Estados Unidos de América Bill Clinton y el primer Ministro irlandés Bertie Ahern firmaron digitalmente un documento de comercio electrónico intergubernamental. Este es registrado como el primer documento de este tipo a nivel mundial que utiliza tecnología de firma digital. Por otro lado, Microsoft utilizó la tecnología de firma digital para desarrollar la tecnología “Authenticode” que asegura los códigos descargables de la web.¹²

1.5.1. Aparecimiento de la Firma Digital en la Legislación Internacional

A causa del desenvolvimiento de relaciones comerciales en el mundo entero a través de los nuevos canales que proporcionan las nuevas tecnologías se genera una serie

¹² Martínez Nadal, Apollonia, Ob. Cit. , Pág. 95

de incertidumbres desde el punto de vista jurídico, las que se derivan, por un lado, de la aplicabilidad de los principios generales de la contratación tradicional a la novedosa contratación electrónica, en cosas tan esenciales como la validez y eficacia de los contratos electrónicos, el perfeccionamiento y la prueba de los mismos. Por otro lado se genera incertidumbre derivada de la misma naturaleza de los medios a través de los cuales esta clase de comercio se desarrolla, planteando problemas de autenticación, integridad, rechazo y confidencialidad de la comunicación.¹³

Como consecuencia de la incertidumbre planteada muchos países alrededor del mundo han realizado esfuerzos encaminados a disminuir dichas incertidumbres jurídicas, de manera tal que han creado legislación atinente al comercio electrónico dando un trato especial al manejo y desarrollo de la firma digital dentro de su regulación. En los cuadros que aparecen a continuación se presentan algunas iniciativas internacionales sobre la materia.

Es en Europa donde se registraron los primeros intentos para regular el comercio electrónico, tomando muy en cuenta el tema de la firma digital, entre estos se mencionan:

¹³ "Firma Digital", www.windowstimag.com, julio, 2004.

PAÍS	LEGISLACIÓN	FECHA	COMENTARIO
Alemania	Ley de Firma Digital	Aprobada el 13 de junio de 1997	Primer país de Europa en presentar proyecto de ley. La ley regula certificados y autoridades de certificación; proporciona una infraestructura segura para el uso de firma digital dentro del país.
Italia	Ley Número 59	15 de marzo de 1997	Recoge el principio de plena validez de los documentos informáticos. Esta ley es desarrollada por reglamentos.
Portugal	Decreto-Ley Número 290-D)99	2 de agosto de 1999	La ley es conformada por 41 artículos, le otorga a la firma digital validez, eficacia y valor probatorio; destaca en ella el hecho de reconocer certificados de estos países.
España	Real Decreto 14/199	Aprobado el 17 de diciembre de 1999. entro en vigencia el 29 de febrero de 2000	Es la primera ley que regula la firma electrónica. Se cuenta con suficiente legislación y jurisprudencia sobre comercio electrónico de forma que regula ampliamente todos los tipos de firma.
Australia	Ley sobre Transacciones Electrónicas	Ingreso al Parlamento de 30 de Julio de 1999. Entró en vigencia el 15 de marzo de 2000	Regula el uso de las transacciones electrónicas, les brinda validez jurídica, establece requisitos formales de firma y escritura, equiparando la firma digital a la firma convencional. La ley se basa en la Ley Modelo de Comercio Electrónico de la UNICITRAL
Austria	Ley sobre Firma Digital	Entró en vigencia el 1 de enero de 2000	Esta ley esta redactada siguiendo las disposiciones de la Unión Europea sobre la materia.

15

De la misma manera, otros estados europeos han formulado proyectos de ley y aprobado legislación en materia de firma digital, algunos de estos Estados son: Dinamarca, Francia, Suecia, Finlandia, Reino Unido, etc.

Algunos países asiáticos también cuentan hoy con legislación sobre firma digital, entre los cuales están:

PAÍS	LEGISLACIÓN	FECHA	COMENTARIO
Japón	Ley de Firma Electrónica	Aprobada el 24 de mayo de 2000. vigente desde el 1 de abril de 2001	Regula lo concerniente a firma electrónica y servicios de certificación.
Corea del Sur	Ley Básica de Comercio Electrónico	En vigencia el 1 de julio de 1999	Otorga efectos jurídicos a las transacciones hechas por medios digitales
India	Ley sobre Tecnología de la Información	Aprobada en junio de 2000	Regula la utilización de firmas digitales y los registros electrónicos a la vez que otorga validez jurídica a transacciones realizadas por medios electrónicos de comunicación
Singapur	Ley de Firmas electrónicas, digitales, registros electrónicos y Comercio Electrónico	Aprobada en junio de 1998	Reconoce y aprueba la utilización de firmas electrónicas, firmas digitales y registros electrónicos.

Ahora, en el continente americano se pueden señalar como algunos de los países más adelantados con respecto a la legislación de firma digital los siguientes:

PAÍS	LEGISLACIÓN	FECHA	COMENTARIO
Estados Unidos de América	Utah Digital Signature Act.	Se aprobó en 1995 se modificó en 1996	Es en el estado de Utah donde se aprueba. Esta ley establece que la firma digital tiene el mismo efecto legal de una firma manuscrita al cumplir con determinados requisitos.
	Federal Electronic Signatures in Global and National Commerce Act.		Debido a la legislación tan diversa de los estados, se vio la necesidad de una ley federal de contenido uniforme aplicable en todo el país.
Argentina	No. 25.506 Ley de Firma Digital	Sanciona el 14 de noviembre de 2001. promulgada de hecho el 11 de diciembre de 2001	Sigue el modelo de principios y reglas generales de la ley de la UNICITRAL. Equipara la firma digital a la firma manuscrita
Colombia	Ley 527	Del 18 de agosto de 1999	Reglamenta el acceso y uso de los mensajes de datos del comercio electrónico y de las firmas digitales, establece las entidades de certificación; da la misma fuerza y efectos jurídicos de la firma manuscrita a la firma digital al cumplir ciertos requisitos
Canadá	Ley 38 sobre Información Electrónica y Documentos	Se aprobó el 21 de junio de 2000	Recoge lo concerniente a la firma electrónica. Este país cuenta con varias iniciativas de ley sobre comercio electrónico
Perú	Ley 27.269 de Firmas y Certificados Digitales	Entró en vigencia en mayo 2000	Iguala los efectos de la firma digital a los de las firmas manuscritas, regula las funciones de las entidades de certificación y registro
Venezuela	Decreto 1.024 Ley sobre Mensajes de Datos y Firmas Electrónicas	Del 10 de febrero de 2001 publicada el 28 de febrero de 2001	Le reconoce eficacia y valor jurídico a la firma electrónica, al mensaje de datos y a toda información inteligible en formato electrónico

Por su parte, también organizaciones internacionales, las cuales se exponen a continuación, han realizado esfuerzos por dictar lineamientos que regulan el comercio electrónico, y por ende la firma digital, que sirva como base para la formulación de normas uniformes que contribuyan a la unificación económica de la región o países que la conforman, algunas de estas organizaciones o entidades son:

ORGANIZACIÓN	DOCUMENTOS O LEGISLACIÓN	FECHA	COMENTARIO
Naciones Unidas	Ley modelo sobre comercio electrónico. Resolución 51/62	16 de diciembre de 1996	Se dio en el seno de la Asamblea General de las Naciones Unidas. Su elaboración estuvo a cargo de la Comisión de las Naciones Unidas en Ley de comercio Internacional, más conocida como UNCITRAL
Unión Europea	Audiencia de la Unión Europea sobre Firma Digital y Encriptación.	23 y 24 de abril de 1998.	Fue realizada en Copenhague, teniendo como objetivo la exploración del uso y desarrollo de la firma digital y la encriptación
	Propuesta para una Directiva del Parlamento y Consejo Europeos para un Marco Común para la Firma Digital	13 de mayo de 1998	Esta propuesta se redactó acorde a las recomendaciones de la dirección general XIII de la Comisión Europea
Organización para la Cooperación y Desarrollo Económico (OCDE)	Recomendación sobre la Utilización de Criptografía	27 de marzo de 1997	Se establece como el primer intento a escala internacional de aportar políticas orientadas en la criptografía. En ella aparecieron principios que sirvieron de base a algunos países al momento de adoptar legislación sobre firma digital.
Cámara de Comercio Internacional (CCI)	Convención General para el Comercio Electrónico y la Firma Digital Internacional (GUIDEC)	Noviembre de 1995 surgió la propuesta	Originalmente se denominó Prácticas Internacionales Uniformes de Autenticación y Certificación, fue cambiada durante la etapa de consulta. Desarrolla lineamientos jurídicos internacionales sobre el Comercio Internacional sobre el Comercio Electrónico y propone el establecimiento de autoridades de certificación

1.5.2. Incorporación de la Firma Digital en El Salvador

El llamado Comercio Electrónico está emergiendo como un negocio imparable. Los catálogos de las principales cadenas y tiendas están siendo paulatinamente reemplazados por páginas web, mientras día a día millones de personas se van decidiendo a realizar sus compras por este medio.

La compra electrónica es otro de los grandes temas comerciales que ha convertido a Internet en un nuevo lugar de especulación para los comercios pequeños y grandes. Las grandes cadenas ya cuentan con shopings virtuales en la red, y las pequeñas se han lanzado a competir con distintas técnicas y buen resultado.

Toda esta serie de cambios en la actualidad han venido a destacar una serie de riesgos derivados de un intercambio de información mediante redes abiertas siendo las mas importantes: que el autor y fuente del mensaje sea suplantado; que el mensaje sea alterado de forma accidental o de forma maliciosa durante la transmisión, que el emisor del mensaje niegue haberlo transmitido o el destinatario haberlo recibido; y que el contenido del mensaje sea leído por una persona no autorizada. A solucionar algunos de estos problemas es hacia donde apunta precisamente la función de la firma electrónica y la firma digital.

El sistema de firma digital es útil tanto para imposibilitar la alteración de esta como para establecer que ella pertenece efectivamente a quien aparece como firmante. Para tener validez jurídica, las firmas digitales deben permitir verificar tanto la identidad

del autor de los datos como comprobar que dichos datos no han sufrido alteración desde que fueron firmados.

En El Salvador la incorporación de la Firma Digital como instrumento dentro del comercio electrónico y como reemplazo de los mecanismos tradicionales que vinculan a sujetos, en relación a un acuerdo de naturaleza comercial ha sido gracias al sector importador, el cual con el fin de facilitar y agilizar su labor ha hecho uso de la tecnología avanzada en materia de comunicación.

Con el decreto legislativo número 523 publicado en el Diario Oficial el 3 de octubre de 2001 que contiene “Reformas a la Ley de Simplificación Aduanera” se implementó de manera obligatoria el sistema de Teledespacho, el cual funciona haciendo uso de Internet.¹⁴ Por medio de este sistema el sector antes mencionado ésta firmando de manera “digital” las declaraciones de mercancías que envían electrónicamente a la Dirección General de Renta de Aduanas. Dicho sistema fue desarrollado por el Ministerio de Hacienda a través de la Dirección General antes señalada, en conjunto con la Cámara de Comercio e Industria de El Salvador a través de la Dirección Estratégica de Comercio Electrónico más conocida como DIESCO, siendo esta última la que ejecuta en su parte técnica dicho sistema, encargándose de autenticar que la persona remitente de la información sea realmente quien dice ser.

Para el sistema de Teledespacho se ha montado una infraestructura a nivel de software y de red de comunicación, que utiliza el servicio de firma digital de llave pública/privada, y la emisión de certificados de firmas digitales con el objeto de

14 GAITÁN CORTÉZ, Carlos Ernesto y otros, Ob. Cit., pág. 17

certificar electrónicamente a los usuarios de este sistema, además se están utilizando redes privadas virtuales para crear canales seguros de comunicación.¹⁵

Es a partir del mes de marzo de 1999 que realmente entró en operaciones el sistema de Teledespacho, funcionando sobre todo con empresas que realizan transacciones virtuales vía EDI con la aduana como por ejemplo: almacenes Siman, Sara Lee, Cajas y Bolsas de El Salvador, ADOC, etc.,¹⁶ y tomando en cuenta que la reducción de los costes de las transacciones realizadas por este medio es significativa cada día más y más empresas son incorporadas a este sistema.

El intercambio de información, en particular, las declaraciones de mercancías y la correspondiente respuesta por parte de la Dirección General de Renta de Aduanas realiza bajo estándares y modelos de seguridad confiables, que implican el uso de Certificados Digitales, Firma Digital.

Se ha implementado el uso de la firma electrónica y certificados digitales emitidos por Certic@mara, filial de la Cámara de Comercio e Industria de El Salvador dentro del sistema de Teledespacho por Internet, esto con el objeto de asegurar las transacciones electrónicas de dicho proyecto.¹⁷ Importante es señalar que los certificados digitales que emite Certi@mara solo certifican al usuario, no la información y su uso es exclusivamente para Teledespacho por Internet.

El Ministerio de Hacienda contrató a partir de octubre de 2002 los servicios de consultoría de DIESCO EAN El Salvador, para el desarrollo de una plataforma de Pago

15 Ídem

16 Ídem

17 “DIESCO,” www.camarasal.com/, mayo, 2004.

Electrónico de Impuestos, conocida como Telepago, esto con el objetivo de facilitar al usuario o contribuyente el realizar una orden de pago de impuestos de importación desde su oficina. Para el mes de febrero del año 2003 Telepago contaba con la participación de 5 bancos: Banco Salvadoreño, Banco Cuscatlán, Banco Americano, Citibank y Banco de Comercio. La seguridad del sistema de Telepago está basado en estándares internacionales, bajo los servicios de autenticidad, no repudio, integridad y confidencialidad, aunado a ello el uso de certificados digitales y el manejo de llaves públicas y privadas. De esta manera, El Salvador ha iniciado la incorporación de tecnologías que utiliza medios electrónicos, para el desarrollo de actividades relacionadas con la Administración Pública.

CAPÍTULO 2

DE LAS FIRMAS

Sumario: 2.1 Introducción. 2.2 Origen de la Firma Manuscrita. 2.2.1 Generalidades: 2.2.1.1 Definición, 2.2.1.2 Naturaleza, 2.2.1.3 Características, 2.2.1.4 Elementos. 2.3 Firma Electrónica. Definición. 2.4 Firma Digital. 2.4.1 Generalidades, 2.4.1.1 Definición, 2.4.1.2 Características Técnicas, 2.4.1.3 Atributos de Seguridad de la Firma Digital, 2.4.1.4 Ventajas y Desventajas, 2.4.1.5 Criptografía, 2.4.1.5.1 Historia, 2.4.1.5.2 Concepto, 2.4.1.5.3 Tipos de Criptografía: Simétrica y Asimétrica, 2.4.2 Proceso de Firma Digital y Verificación, 2.4.3 La Firma Digital en El Salvador 2.5 Firma Manuscrita – Firma Electrónica – Firma Digital.

2.1 INTRODUCCIÓN

La forma tradicional de aceptación se ha caracterizado por ser la firma, cumpliendo con la función a través del tiempo de identificar a una persona, con el avance tecnológico y el desenvolvimiento de las transacciones la firma ha adquirido una singular importancia llegando a desarrollarse diversas modalidades de la misma.

En la actualidad con el comercio electrónico, el clásico documento de papel es sustituido por el novedoso documento electrónico, correlativamente desaparecen las tradicionales firmas manuscritas que pueden ser reemplazadas usando una variedad de métodos que son incluidos en el concepto amplio de firma electrónica, dentro del cual una clave particular sería la Firma Digital, que son tecnológicamente específicas y se crean usando un sistema de criptografía asimétrica o de clave pública. De lo establecido deriva la importancia de este capítulo; y el porque de su denominación, pues se expone lo más relevante, de acuerdo al tema de investigación; acerca de la firma ológrafa o manuscrita, la firma electrónica y la firma digital, resaltando lo referente a esta última,

ya que constituye un punto esencial en la investigación, por ello se incluye, además de los aspectos generales de la misma, lo que se refiere al sistema de criptografía que se utiliza para brindarle el atributo de confidencialidad.

2.1 ORIGEN DE LA FIRMA MANUSCRITA

La Doctrina remonta el origen de la firma manuscrita al Derecho Romano. En Roma no se firmaban los documentos: ni era costumbre, ni necesario. La **manufirmatio** consistía en una ceremonia en que leído el documento por su autor o el notario se le colocaba desenrollado y extendido sobre la mesa del escribano y luego de pasar la mano abierta sobre el pergamino en actitud de jurar, pero sin hacerlo, se estampaba el nombre, signo o una o tres cruces-una por cada persona de la Santísima Trinidad –por el autor o el notario en su nombre, haciéndolo seguidamente de los testigos. Más que un requisito la **manufirmatio** era en sí misma una parte del espectáculo solemne en que se realizaba el acto.¹⁸

Por otra parte en el Sistema Jurídico Visigótico existía la figura de “**Chartam Tangere**”, que consistía en la confirmación de documentos por medio de testigos que ya sea tocaban, signaban o suscribían dicho documento (firmatio, roboratio, stipulatio); este acto no era imprescindible pero sí consistía en una de sus costumbres. Desde la época Euriciana las Leyes Visigodas prestaron atención a las formalidades documentales, regulando detalladamente las suscripciones, signos y comprobaciones de

18 Enciclopedia Jurídica Omeba, Tomo XII, Editorial Driskill S.A., Buenos Aires, Argentina, 1987. Pág. 290

escritura dando origen a las figuras de: “**La subscriptio**”, el cual representaba el nombre del signante y la fecha, esta otorgaba pleno valor probatorio al documento; “**El Signum**”, rasgo que sustituía a la anterior si el siguiente no sabía o no podía escribir, esta no tenía pleno valor probatorio y debía ser completado con juramento de veracidad realizado por uno de los testigos. Si llegara a faltar cualquiera de estas figuras el Documento era inoperante, y para darle valor probatorio debía agregarse el juramento de los testigos sobre la veracidad del documento.¹⁹

En la Edad Media se utilizaron sellos, marcas y signos. Estos últimos se formaban con una cruz con la que se entrelazaban, en forma arbitraria, letras o rasgos, y fueron usados por los fedatarios. Carlomagno, que apenas sabía escribir hacía firmar sus actos por un sello oficial, sus sucesores que no mejoraron la cultura del conquistador utilizaron sellos, hasta que algún tiempo después comenzaron a autenticarse los documentos con sello y firma, aunque por esto se entendían todavía los signos dibujados para individualizarse. En octubre de 1358 Carlos V obligó en Francia a los escribanos – que hacia fines del reinado de San Luis fueron instituidos en oficiales públicos- a suscribir los actos que pasaban ante ellos con sus firmas, además de sus signos. Era en esta época aún tan poco común la escritura que ese mismo año en el Consejo Real eran escasos los que sabían hacerlo, y fue entonces que el mismo Rey dispuso que los actos de ese organismo debían ser autorizados por lo menos por tres de los presentes, los que si no supiesen firmar, estamparían sus marcas o signos.²⁰

19 “Criptografía”, www.htmlweb.net/seguridad/cripto-8.html, junio, 2004.

20 Enciclopedia Jurídica Omeba, Ob. Cit., pag.291

Con la extensión de la instrucción y el mayor desenvolvimiento de las transacciones la firma fue adquiriendo la importancia y las modalidades que ahora tiene.

2.2.1 Generalidades

La firma manuscrita permite certificar el reconocimiento o conformidad sobre un documento por parte del firmante, de forma que tiene una gran importancia desde el punto de vista legal. Aunque existen diferentes formas de mostrar o demostrar conformidad con diferentes actuaciones, o de cerrar acuerdos entre personas o empresas, la firma manuscrita, tiene un reconocimiento particularmente alto. Se considera que la firma, pese a que puede ser falsificada, tiene peculiaridades que la hacen fácil de realizar, fácil de comprobar y vincula a quien la realiza.

2.2.1.1 Definición:

Al establecer un concepto de firma es necesario analizar diferentes puntos de vista.

Para el grupo de estudios en Internet, Comercio Electrónico & Telecomunicaciones e Informática, de la Universidad de Los Andes en su libro “Internet Comercio Electrónico & Telecomunicaciones”, la firma se define tal y como la Real Academia de la Lengua establece *“nombre y apellido o título de un persona que ésta*

pone con rúbrica al pie de un documento escrito de mano propia o ajena, para darle autenticidad, para expresar que se aprueba su contenido o para obligarse a lo que en él se dice."²¹ Esta definición confunde los conceptos de firma y rúbrica, al establecer la dependencia entre ambas, debido a que la rúbrica jurídicamente se entiende como: "*Rasgo, trazo que completa las letras de la firma. En ciertas actuaciones judiciales y otras administrativas, el funcionario Publico se limita a rubricar, sin poner la firma*",²² siendo la firma un concepto mas amplio que esto.

En el vocabulario jurídico de Couture se define como "*Trazado gráfico, conteniendo habitualmente el nombre, los apellidos y la rúbrica de una persona, con el cual se suscriben los documentos para darles autoría y virtualidad y obligarse en lo que en ellos se dice.*"²³ Al igual que la definición anterior ésta confunde el concepto de firma con el de rúbrica como ya se explicó anteriormente.

Según el Art. 3639 del Código Civil argentino "*La firma no es la simple escritura que una persona hace de su nombre o apellido; es el nombre escrito de una manera particular, según el modo habitual seguido por la persona en diversos actos sometidos a esta formalidad*";²⁴ puede considerarse que esta definición es la más adecuada para los fines de esta investigación debido a que distingue entre firma y rúbrica, y a la vez establece un uso de relevancia jurídica.

21 Grupo de Estudios en Internet Comercio Electrónico Telecomunicaciones e Informática, "**Internet Comercio Electrónico & Telecomunicaciones**", Universidad de Los Andes, Facultad de Derecho, Legis S. A., Primera Edición, 2002, Bogotá, Colombia, Pág. 54

22 CABANELLAS, Guillermo, **Diccionario Enciclopédico de Derecho Usual**, Tomo VII, Editorial Heliasta, Buenos Aires, Argentina, 1989, pag. 258.

23 htmlweb.net Ob. Cit.

24 **Código Civil Argentino**, entró en vigor el 1 de Enero de 1871.

De acuerdo con las definiciones anteriores se puede concluir que la firma es el mecanismo tradicional de identificación e indicador de la aprobación del contenido de un documento.

2.2.1.2 Naturaleza

La firma es la afirmación de individualidad, pero sobre todo de voluntariedad. En el primer aspecto ella significa que ha sido la persona firmante y no otra quien ha suscrito el documento. En el segundo que se acepta lo que allí se manifiesta.

Esta fundamentalmente es el vínculo que une a la persona firmante con lo consignado en el documento. Díaz de Guijarro afirma que es “como el testimonio de la voluntad de la parte; es el sello de la verdad del acto; es la que establece la individualización de las partes”.²⁵

Esta circunstancia de ser manifestación de voluntad es lo que le otorga la trascendencia que tiene. Mediante ella se da estabilidad a las transacciones jurídicas y se posibilita el intercambio de noticias y conocimientos en la vida social o cultural ya que permite certeza con respecto al remitente. Si bien en algunos casos excepcionales quien suscribió un documento puede no haber conformado su texto, la comprobación de aquello es suficiente para tenerlo por auténtico, y constituye una prueba principal en juicio. Por esto se exige que sea puesto por la mano misma del interesado, que esté

²⁵ Enciclopedia Jurídica Omeba, Ob. Cit. Pag. 292.

formada por esos rasgos personales, y que sea colocada al pie del escrito careciendo de valor las notas en el margen o a continuación del instrumento ya que no les alcanza a estas la expresión cierta de voluntad.

2.2.1.3 Características

De acuerdo al modo en que se emplea la firma pueden señalarse como sus características:

Identificativa: Sirve para identificar quién es el autor del documento.

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

Probatoria: Permite identificar si el autor de la firma es efectivamente aquél que ha sido identificado como tal en el acto de la propia firma.²⁶

Teniendo en cuenta el fin de la firma puede señalarse como características las siguientes:

Consentimiento: La firma expresa el consentimiento sobre lo escrito o la intención de asignarle efectos jurídicos.

²⁶ “Derecho de las Nuevas Tecnologías- La Firma Digital”, www.tuguialegal.com, julio,2004.

Solemnidad: el hecho de firmar un documento llama a la reflexión al firmante respecto del significado jurídico del acto que realiza, de tal manera, que el hecho de firmar conscientemente evita el adquirir compromisos de manera irresponsable.

Prueba: Una firma es un medio de reconocimiento de la autenticidad del cuerpo de escritura que le precede al identificar a su signatario. Cuando el signatario coloca al pie de un documento un rasgo distintivo que lo caracteriza, la escritura se vuelve prima fácil atribuible a él.

Forma: La firma muchas veces da validez a los actos jurídicos que se celebran.²⁷

Al establecer una diferencia entre las características que posee la firma en cuanto a su uso y fin, se pretende señalar la importancia que ésta reviste de expresar el consentimiento.

2.2.1.4 Elementos :

Hemos de distinguir entre:

Elementos Formales

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

27 MARTÍNEZ NADAL, Apollonia, Ob. Cit., Pág. 369

La Firma como signo personal:

La firma se presenta como un signo distintivo y personal, ya que debe ser puesta de puño y letra del firmante. Refiriéndose a que individualiza a cada sujeto.

El animus signandi:

Es el elemento intencional o intelectual de la firma. Consiste en la voluntad de asumir el contenido de un documento, que no debe confundirse con la voluntad de contratar. Esto quiere decir que la firma es el resultado de la expresión de voluntad de una persona.

Elementos Funcionales

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

Identificadora: La firma asegura la relación jurídica entre el acto firmado y la persona que lo ha firmado. Es decir, la firma manuscrita expresa la identidad, aceptación y autoría del firmante.

Autenticación: El autor del acto expresa su consentimiento y hace propio el mensaje,²⁸ dándole autoría al documento.

²⁸ tuguialegal.com, Ob. Cit.

Los elementos mencionados anteriormente son aquellos que le dan razón de ser a la firma, ya que son ellos quienes permiten que con ésta las personas adquieran obligaciones de relevancia jurídica.

2.3 Firma Electrónica. Definición

La primera cuestión que se debe tratar sobre el tema de la firma electrónica, es que no es firma en los términos tradicionales, es decir, que no es un signo o marquilla que se coloca sobre un objeto material, y que su nombre en realidad se debe a una necesidad de tipo social y cultural, pues resulta más cómodo usar un concepto de fácil manejo para la colectividad.

Una firma electrónica sería “cualquier método o símbolo basado en medios electrónicos utilizados o adoptados por una parte con la intención actual de vincularse o autenticar un documento, cumpliendo todas o algunas de las funciones características de una firma manuscrita.”²⁹

La firma electrónica es solo un paso en el proceso de seguridad del comercio electrónico, debido a que existen otros sistemas o métodos que se emplean para dar mayor seguridad dentro de la red.

29 Art. 7. **Ley Modelo sobre Comercio Electrónico de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI)**, Aprobada en la plenaria en el 29º periodo de sesiones de la Comisión; y la Asamblea General de la ONU la aprobó en resolución 51/162, el 16 de Diciembre de 1996.

2.4 Firma Digital

2.4.1 Generalidades

La Firma Digital es un invento reciente, estimulado por la expansión de las comunicaciones digitales. Permite que el receptor de un mensaje pueda verificar la autenticidad de la firma que aparece en el documento digital. Esta consiste en las transformaciones de un mensaje utilizando un sistema de cifrado asimétrico de manera que la persona que posee el mensaje original y la clave pública del firmante, pueda establecer de forma segura, que dicha transformación se efectuó utilizando la clave privada correspondiente a la pública del firmante, y si el mensaje es el original o fue alterado desde su concepción.

Fueron las transformaciones comerciales y el hecho de tener que interactuar masiva y habitualmente por intermedio de redes de computadoras las que le dieron lugar a la Firma Digital. Pero, solo después que los especialistas en seguridad y los juristas comenzaron a depurarla fue que alcanzó un marco de situación como para ocupar un lugar en las actuaciones entre personas, ya sean jurídicas o naturales.

2.4.1.1 Definición:

El concepto de firma digital nació como una oferta tecnológica para acercar el uso tradicional de la firma ológrafa al marco de lo que se ha dado en llamar el ciberespacio o el trabajo en redes, y para establecer este concepto se hace necesario exponer diferentes puntos de vista:

Para los autores de Tugualegal.com firma digital es “*una secuencia de datos electrónicos (bits) que se obtienen mediante la aplicación a un mensaje determinado de un algoritmo (fórmula matemática) de cifrado asimétrico o de clave pública, y que equivale funcionalmente a la firma autógrafa en orden a la identificación del autor del que procede el mensaje.*”³⁰ Esta definición comete el error de confundir la firma digital con el mismo documento cifrado, al decir, que al aplicar un algoritmo asimétrico a un mensaje se obtiene la firma digital, por lo tanto, se considera deficiente para definir y entender qué es firma digital.

De acuerdo a Polanco Villalobos la firma digital *es el procedimiento por el cual se transforma un mensaje utilizando un criptosistema asimétrico tal que la persona que posea el mensaje inicial y la clave pública del firmante pueda determinar con certeza si la transformación se creó usando la clave privada que corresponde a la clave pública del firmante y si el mensaje ha sido modificado desde que se efectuó la transformación.*³¹ Este autor brinda una definición certera de firma digital, ya que relaciona los aspectos más importantes que la caracterizan, salvo que no establece que es una especie de firma electrónica, además de resultar difícil su entendimiento.

Varias legislaciones se encargan de definir lo que regulan por firma digital para sus países, de los cuales se hace necesario mencionar a los que se consideran más importantes:

30 tugualegal.com Ob. Cit.

31 POLANCO VILLALOBOS, José Antonio y otros “**La Regulación sobre el Comercio Electrónico en el ordenamiento jurídico salvadoreño**”; Tesis UCA, 2001, Pág. 37

El Art. 2 apartado b) del Real Decreto – ley 14-1999 de España define la firma digital como *“la firma electrónica que permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su exclusivo control, de manera que está vinculado únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de estos.”*³²

La Ley 25.506 de Firma Digital de Argentina, en su Art. 2 define la Firma Digital como *“el resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma.”*³³

En el derecho colombiano firma digital es *“el valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje, permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la información”*.³⁴

Por último, la definición adoptada por la Ley peruana en su Art. 3 establece que *“La Firma Digital es aquella firma electrónica que utiliza una técnica de criptografía*

32 Ley 59/2003, de 19 de Diciembre de Firma Electrónica de España. BOE num.304, Sábado 20 de Diciembre de 2003.

33 Ley 25.506, de Firma Digital, Argentina, sancionada el 14 de Noviembre de 2001, y promulgada de hecho el 11 de Diciembre de 2001.

34 CUBILLOS VELANDIA, Ramiro y RINCÓN CARDENAS, Erick. **“Introducción Jurídica al Comercio Electrónico”**. Ediciones Jurídicas Gustavo Ibáñez, Medellín, Colombia, 2002.

asimétrica, basada en el uso de un par de claves únicas; asociadas una clave privada y una clave pública relacionadas matemáticamente entre sí, de tal forma, que las personas que conocen la clave pública no puedan derivar de ella la clave privada.”³⁵

De acuerdo a las definiciones legales expuestas, conviene considerar como las más adecuadas y completas para definir y entender lo que es la firma digital, la establecida por la legislación peruana, debido a que hace hincapié en que es una firma electrónica que utiliza como técnica la criptografía asimétrica, enfatizando el uso de sus dos claves. Pero es importante mencionar que la aclaración realizada al final de esta definición no debe formar parte de ella, por lo tanto, para efectos de esta investigación se adopta la anterior, entendiéndose por firma digital ***“AQUELLA FIRMA ELECTRÓNICA QUE UTILIZA UNA TÉCNICA DE CRIPTOGRAFÍA ASIMÉTRICA BASADA EN EL USO DE UN PAR DE CLAVES ÚNICO; ASOCIADAS UNA CLAVE PRIVADA Y UNA CLAVE PÚBLICA RELACIONADAS MATEMÁTICAMENTE ENTRE SÍ”***.

2.4.1.2 Características Técnicas

De acuerdo a su carácter técnico la firma digital presenta las siguientes características:

Ser un valor numérico que se adhiere al mensaje de datos.

³⁵ Ley 27.269, de Firmas y Certificados Digitales Perú, entro en vigencia en mayo de2000.

Que ese valor numérico se haya obtenido por un procedimiento vinculado a la clave del iniciador, llamado criptografía asimétrica.

Que permita al texto del mensaje determinar que este valor se ha obtenido exclusivamente con la clave del iniciador.

2.4.1.3 Atributos de Seguridad de la Firma Digital:

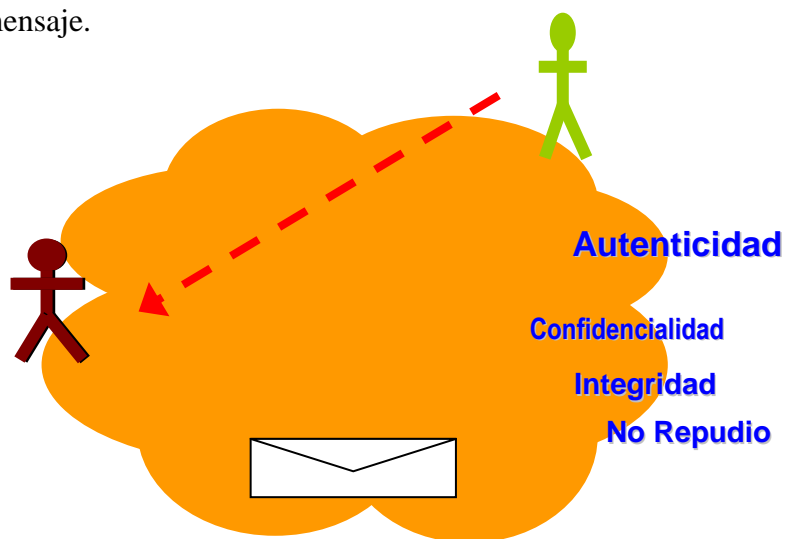
Autenticidad o Identidad: Este atributo de Seguridad protege al receptor del documento garantizándole que dicho mensaje ha sido generado por la parte identificada en el documento como emisor del mismo no pudiendo alguna otra entidad suplantar a un usuario del sistema, es decir garantiza que los sujetos de la transacción realmente son quienes se espera que sean.

Confidencialidad: Consiste en que la información solo está disponible para usuarios autorizados, codifica a la información del mensaje para hacerla ininteligible a todos, excepto al destinatario legítimo, es decir existe seguridad de que ningún tercero podrá acceder a esa información y al conjunto de datos emitidos.

Integridad: Se refiere a la protección contra la modificación de datos en forma intencional o accidental. Es decir, permite que sea detectada cualquier modificación de

los datos firmados por pequeña que sea, proporcionando así una garantía en el contenido del documento.

No Repudio o Rechazo: Este atributo de seguridad protege al receptor del documento de la negativa del emisor de haberlo enviado. Este aspecto de seguridad es más fuerte que los anteriores ya que el emisor no puede negar bajo ninguna circunstancia que ha generado dicho mensaje, transformándose en un medio de prueba que permite repeler la negativa tanto de haber recibido como de haber enviado el mensaje.



Los atributos antes mencionados son expuestos por muchos autores como características de la Firma Digital, y por otros como atributos, requisitos o aspectos de seguridad de la misma, y es a este último criterio al cual se apegó la presente investigación, porque se considera que la autenticidad, confidencialidad, integridad y no

repudio, son aspectos que se originan del uso de la firma digital llegando a ser atributos de seguridad de la misma y no características.

2.4.1.4 Ventajas y Desventajas:

La Firma Digital esta teniendo una aceptación gradual en los procesos financieros y comerciales, y esto ha generando ventajas y desventajas en su uso:

Ventajas

Su procedimiento de verificación es exacto y es imposible en la práctica su falsificación..

La seguridad para realizar transacciones de comercio electrónico e intercambio electrónico de datos.

Permite a los ciudadanos relacionarse con la Administración con la máxima eficacia jurídica.

Desventajas:

No es válida legalmente aún en muchos países, como Canadá, Uruguay, Honduras, Guatemala, El Salvador, etc.

Su seguridad depende de la clave privada, es decir, que si la clave privada se compromete por alguna causa, entonces, se compromete la seguridad de la Firma Digital, esto quiere decir que puede ser usada por individuos y eventos no autorizados.

2.4.1.5 Criptografía

La criptografía es la ciencia que se ocupa de transformar mensajes en formas aparentemente ininteligibles y devolverlos a su forma original. Para su comprensión es indispensable conocer su desarrollo histórico.

2.4.1.5.1 Historia:

Esta técnica ha evolucionado a través de la historia. La primera aplicación conocida de la criptografía se remonta a 4,000 años atrás cuando los Egipcios utilizaban jeroglíficos crípticos para narrar la vida y hazañas de sus faraones, aquí la encriptación no era empleada para esconder el significado del texto sino para volverla más solemnes.

Edad Antigua:

El primer empleo de escritura cifrada data del siglo V a.C. cuando se utiliza a un esclavo como portador de un mensaje en la guerra entre Atenas y Esparta. De este modo, el general Lisandro de Esparta recibe en una cinta una serie de letras con aparente falta de sentido, que al ser enrollada en un determinado rodillo de madera mostraba longitudinalmente los símbolos dispuestos de tal manera que podía leerse el mensaje, que en esta ocasión histórica, sirvió para salvar un imperio y un general.³⁶

³⁶ GALENDE DÍAZ, Juan Carlos, “**Criptografía Historia de la Escritura Cifrada**”, Editorial Complutense, Madrid, España, 1995, Pág. 75

Otra de las primeras noticias que se tiene de la utilización de un método para transmitir información con carácter secreto data de la época de los romanos primer sistema criptográfico conocido como tal se debe a Julio César (100-44 a de C.) Su sistema consistía en reemplazar en el mensaje a enviar cada letra por la situada tres posiciones por delante en el alfabeto latino. En nuestro alfabeto actual tendríamos la siguiente tabla de equivalencias:

<i>A</i>	<i>B</i>	<i>C</i>	<i>D</i>	<i>E</i>	<i>F</i>	<i>G</i>	<i>H</i>	<i>I</i>	<i>J</i>	<i>K</i>	<i>L</i>	<i>M</i>	<i>N</i>	<i>Ñ</i>	<i>O</i>	<i>P</i>	<i>Q</i>	<i>R</i>	<i>S</i>	<i>T</i>	<i>U</i>	<i>V</i>	<i>W</i>	<i>X</i>	<i>Y</i>	<i>Z</i>
<i>D</i>	<i>E</i>	<i>F</i>	<i>G</i>	<i>H</i>	<i>I</i>	<i>J</i>	<i>K</i>	<i>L</i>	<i>M</i>	<i>N</i>	<i>Ñ</i>	<i>O</i>	<i>P</i>	<i>Q</i>	<i>R</i>	<i>S</i>	<i>T</i>	<i>U</i>	<i>V</i>	<i>W</i>	<i>X</i>	<i>Y</i>	<i>Z</i>	<i>A</i>	<i>B</i>	<i>C</i>

Por lo que el mensaje “Hola Mundo” se transformaría en “KRÑD OXPGR”.

Este sistema fue innovador en su época aunque en realidad es fácil de romper ya en todo sistema de transposición simple sólo hay un número de variación si es posible igual al de letras que forman el alfabeto (27 en este caso).³⁷

Edad Media:

Hasta el siglo XII no se tiene mucho conocimiento de la evolución de la criptografía, aunque es presumible que se utilizase, fundamentalmente, con ocasión de guerras o embajadas. En la cancillería carolingia o en Irlanda, durante la Alta Edad Media, el uso de escrituras secretas fue muy simple y consistió, por lo general, en el

³⁷ htmlweb.net Ob. Cit.

empleo de una especie de alfabeto tironiano para sustituir las letras del texto claro, en especial las vocales.

También fue corriente entre los criptográficos los alfabetos pictóricos, que parecían muy misteriosos a los no iniciados. Uno de los más populares fue el “alfabeto zodiacal”, en donde los signos representativos de los cuerpos celestes más conocidos: Venus, Luna, Géminis, Sol, Libra, Aries, Urano, Acuario, Cáncer, Neptuno, etc., cada uno de estos tenía su correspondencia con las diferentes letras que componen el alfabeto.³⁸

Más tarde, la escritura fue practicada desde el siglo XIII en algunas repúblicas italianas y en la curia pontificia. De esta época se conservan las muestras más antiguas de escrituras secretas en unos documentos públicos de Venecia, en los cuales el Sistema de cifrado consistía, por lo general, en sustituir las vocales por puntos, cruces y acentos o por una mezcla de los tres, aunque en ocasiones también se intercalaban en el texto latino varios caracteres griegos y hebraicos para expresar las palabras más importantes. De todas formas, parece ser que las escrituras secretas pontificias son del siglo XII, anteriores, por lo tanto, a los de los estados italianos.

Por otra parte, quizá sea la obra de Gabriel de Lavinde, *Liber Zifrorum*, la más antigua sobre criptografía. Este autor Parmesano era el secretario de las comunicaciones secretas del Papa, y su Sistema de cifrado consiste en utilizar determinados Códigos para Sustituir palabras del mensaje en claro. Este tipo de cifrado será bastante usado durante las centurias siguientes.

38 Ídem

Un empuje decisivo a la criptografía fue dado por el Genovés León Batista Alberti (1404-1472), secretario pontificio de la Corte Romana y autor del célebre *Trattati in cifra* (publicado en Roma en 1470). Se le considera el padre de la criptología, siendo inventor de un criptógrafo basado en el Sistema de Sustitución simple.

Edad Moderna:

Durante la centuria decimosexta, los historiados y religiosos beneditino alemán Tritemio, cuyo verdadero nombre era Johannes Heindererg (1462-1516), publica en 1499 su obra *Polgraphiae*. En ella, aportaba diversos métodos y afirma que Carlomagno cifraba sus comunicaciones. Este tratado aparece primero en latín y después fue traducido al francés y al alemán, lo que indica la necesidad del empleo de la poligrafía. Luego fue acusado de magia negra, y todos los ejemplares fueron quemados.

Luego Giovanni Battista Portu, a quien la historia le ha concedido el título de “padre de la moderna criptografía”, mejora el Sistema de Alberti, en 1535 y aporta nuevos métodos. Años después, este comediógrafo, científico y mago italiano inventó su sistema, que fue publicado en el año 1563 en Nápoles en un tratado titulado *De furtivis litterarum notis vulgo de Ziferis*.

Tanto en el siglo XVI como los siguientes son épocas muy activas, pero sin grandes progresos en la aparición de nuevos métodos. Debido a que se determinaban algoritmos y manipulaciones de mensajes, que se realizaban habitualmente sobre textos escritos y que se recogían en manuales de difusión controlada, de forma que los procedimientos y las claves eran, a su vez, objetos a proteger, ya que en caso de caer en

manos del enemigo, toda la red de comunicaciones quedaba expuesta.³⁹ Con el tiempo además de los métodos manuales aparecieron máquinas simples, como la rueda de Thomas Jefferson. La llegada del telégrafo significó un importante avance en la criptografía, al generalizarse el uso de máquinas electromagnéticas para la encriptación de mensajes.

Época Contemporánea:

El uso de la criptografía contemporánea basada en medios informáticos, comenzó durante la segunda Guerra Mundial. Partiendo de esto se puede establecer que el sistema criptográfico se ha desarrollado en dos pasos. El primero sería con base en la llamada clave secreta, tradicional o simétrica, este es el sistema de encriptado más simple en el que una misma clave sirve tanto para encriptar como para desencriptar.⁴⁰ Esta clave debe ser secreta para evitar el acceso no autorizado a datos confidenciales. Por ello la seguridad de este tipo de criptografía reside en la protección de la clave, pues si ésta se difunde, cualquiera puede descifrar el mensaje. Este sistema generaba el problema de que no se podía determinar quién era el emisor de la información, como tampoco quien era su receptor, por que ambos tenían el mismo sistema de conocimiento del texto aplicado al mensaje de datos; además de que el mantener en absoluto secreto la clave por parte de ambos intervinientes era muy difícil causando como consecuencia la inseguridad del sistema.

39 webpanto.com, Ob. Cit.

40 R. BRIZZIO Claudia, “La informática en el Nuevo Derecho”, Abeledo-Perrot, Buenos Aires, Argentina, 2000, Pág. 88y89

El segundo paso lo da Claude Shannon en el año de 1948 con su obra “A Mathematical Theory of Communication” que ofrece el soporte científico a las bases para una teoría de la información y posteriormente se da el paso decisivo por parte de Whitfield Diffie y Martín Hellman en el año de 1976 con su libro titulado “New directions in Criptography” en el cual establecen un sistema llamado de clave pública conociendo además como sistema moderno o asimétrico, en el cual se utilizan dos claves asociadas entre sí, una de ellas es de conocimiento general a partir de la cual se identifica un sujeto y por otro lado, para que dicho sujeto pueda acceder a la información que se ha enviado en su clase, se requiere la anexión de una clave privada.⁴¹ El nacimiento de la criptografía asimétrica se dio al estar buscando un modo más práctico de intercambiar las llaves simétricas, esto fue lo que propusieron Diffie y Hellman con su sistema de criptografía asimétrica; pero fue hasta que el popular método de Rivest Shamir y Adleman (RSA) publicado en 1978, cuando toma forma la criptografía en cuestión, su funcionamiento esta basado en la imposibilidad computacional de factorizar números enteros grandes.

Época Post-Contemporánea:

Como se ha desarrollado anteriormente, los sistemas criptográficos tradicionales presentaban una dificultad en cuanto a la relación complejidad-longitud de la clave/tiempo necesario para encriptar y desencriptar el mensaje.

41 CUBILLOS VELANDIA, Ramiro y RINCÓN CARDENAS, Erick. Ob. Cit. págs. 209 y 210.

En la era post-contemporánea esta barrera clásica se rompió, debido principalmente a los siguientes factores:

Velocidad de cálculo: con la aparición de los computadores se dispuso de una potencia de cálculo muy superior a la de los métodos clásicos

Avance de las matemáticas: que permitieron encontrar y definir con claridad sistemas criptográficos estables y seguros.

Necesidades de seguridad: surgieron muchas actividades nuevas que precisaban la ocultación de datos, con lo que la criptología experimentó un fuerte avance.

A partir de estas bases surgieron nuevos y complejos sistemas criptográficos, que se clasificaron en dos tipos o familias principales, los de clave simétrica y los de clave pública. Los modernos algoritmos de encriptación simétricos mezclan la transposición y la permutación, mientras que los de clave pública se basan más en complejas operaciones matemáticas.

En la práctica la criptografía simétrica y asimétrica se usan conjuntamente. La simétrica para intercambiar grandes volúmenes de información por su rapidez y la asimétrica para el intercambio de las claves simétricas y la firma digital.

2.4.1.5.2 Concepto:

Entendemos por criptografía (Kriptos = ocultar, Graphos = escritura) la técnica de transformar un mensaje inteligible, denominado texto en clave, en otro que sólo puedan entender las personas autorizadas a ello, que llamaremos criptograma o texto cifrado.

El objetivo básico de la criptografía es encontrar sistemas que permitan hacer llegar determinada información considerada secreta, desde un lugar origen a otro destino, de forma tan segura que, si el mensaje es interceptado, un atacante no puede reconocer el mensaje.

De esta forma la encriptación es un modo de autenticación digital, que permite ante todo mantener la integridad del mensaje. Mediante ella se transforman los datos en signos ilegibles para quien no disponga de la clave para descryptarlos, asegurando de tal modo la privacidad del usuario al ocultar la información a los terceros a quienes no está dirigida. Posibilita que el texto original (texto plano), una vez encriptado (texto cifrado), sólo puede ser leído luego de su descryptación, para lo cual se requiere de cierta clave.⁴²

42 R. BRIZZIO, Claudia, Ob. Cit. Pág. 88

Algoritmos Criptográficos:

La criptografía se basa en problemas matemáticos verdaderamente difíciles; más difíciles de los que se encuentran en una clase de álgebra. Un algoritmo es el conjunto de pasos necesarios para resolver un problema matemático. En el campo de la ciencia de las computadoras, los algoritmos se implementan como partes de un programa que se conoce como una rutina o biblioteca. Usualmente, el programa principal realiza la operación matemática sobre varios conjuntos de datos llamados repetidas veces las bibliotecas de algoritmos.⁴³

Los algoritmos criptográficos, son algoritmos matemáticos y están diseñados de manera que se puedan llamar con diferentes conjuntos de datos para entrar en funcionamiento.

Existen tres clases de algoritmos criptográficos: simétricos, asimétricos y Hash. La criptografía simétrica ha existido desde hace mucho tiempo, incluso la usaron los egipcios.

Las claves son partes importantes de los algoritmos criptográficos, tanto simétricos como asimétricos. Una clave criptográfica es similar a una llave física que se usa para cerrar o abrir una puerta. Para cada tipo de cerradura existe una llave con una forma específica que se ajusta a aquélla, debe tener una cierta longitud, y unas ranuras para ubicarse en la posición correcta. Por lo general, una llave de un fabricante en

⁴³ NASH, Andrew y otros, “PKI Infraestructura de Claves Públicas”, McGraw-Hill, Bogotá, Colombia, 2002, Pág. 15

particular se ajustará a la cerradura de ese tipo, pero solamente si es la llave correcta. La llave con el patrón apropiado de muecas girará y abrirá la cerradura.⁴⁴

Las claves criptográficas son similares a las llaves físicas de muchas maneras. Cada algoritmo criptográfico necesita una clave con la extensión correcta en otras palabras, el número correcto de bits. Se puede procesar un algoritmo criptográfico con cualquier clave que tenga la longitud apropiada, pero solo la que tenga el patrón correcto de bits hará que el algoritmo descifre un documento cifrado.

Por otra parte la seguridad del algoritmo va en relación directa a su tipo, tamaño, tiempo de cifrar y a la no violación del secreto.

Algoritmos simétricos:

Los algoritmos simétricos son aquellos que utilizan una misma clave con la cual se encripta y desencripta el documento. Todo documento encriptado con una clave deberá desencriptarse, en el proceso inverso, con la misma clave. Es importante destacar que la clave debería de viajar con los datos, lo que hace arriesgada la operación e imposible de utilizar en ambientes donde interactúan varias interlocutoras.

Estos algoritmos emplean claves con un elevado número de bits, y usualmente se mide su calidad por la cantidad de esfuerzo que se necesita para romperlos.⁴⁵

44 Ídem. Pág. 21

45“Firma Digital Criptografía. Metodología de la Programación. Autenticación. Informática. Computación. Seguridad. Comercio Electrónico. Certificación. Electrónica. Datos Cifrados,” html.rincondelvago.com/certificados_vfirmas_digitales.html, mayo, 2004.

Dentro de estos algoritmos se encuentran:

DES (Data Encryption Standard)

Es un algoritmo diseñado por IBM a principios de los años 70 y que, originariamente, se conocía con el nombre de LUCIFER. En 1977, el gobierno de los Estados Unidos de América modificó este algoritmo y lo adoptó para realizar sus comunicaciones secretas encriptadas. A partir de aquí, y después de que la Oficina Nacional de Estandarización (NBS) hubiese publicado abiertamente el algoritmo. DES se convirtió en el algoritmo de cifrado más extendido y estudiado de todos los algoritmos existentes hasta el momento.⁴⁶

DES utiliza una clave simétrica de 64 bits, de los cuales 56 son usados para la encriptación, mientras que los 8 restantes son de paridad, y se usan para la detección de errores en el proceso.

Este sistema se considera muy fuerte, es decir, que no presenta debilidades aparentes. Sin embargo, el tamaño relativamente pequeño de las claves ha permitido romper por fuerza bruta este sistema en varias ocasiones. Es por eso que DES ha dejado de considerarse seguro. Aunque se debe decir también que para romper DES se requiere de una capacidad computacional que no está al alcance de cualquiera. Así que, en la actualidad, DES todavía protege de la mayoría de criptoanalistas (o hackers informáticos) con pocos recursos.

⁴⁶ “Algoritmos Simétricos,” <http://personal.telefonica.terra.es/web/criptologia/recerca4.html>, agosto, 2004.

BLOWFISH

Fue creado por Bruce Schneier, autor del libro “Applied Cryptography” (considerado por muchos como la “Biblia” en cuestiones de criptografía). Utiliza claves de hasta 448 bits, y, hasta el momento, ha resistido con éxito todos los ataques. Por ello y por su estructura se le considera uno de los algoritmos más seguros, a pesar de lo cual no se utiliza masivamente. Su autor no ha patentado el método para que pueda ser empleado sin limitaciones.⁴⁷

IDEA (International Data Encryption Algorithm)

Desarrollado en 1990 por Xuejia Lai y James Massey. Este algoritmo está considerado en la actualidad el mejor sistema criptográfico simétrico. Emplea claves de 128 bits para cifrar bloques de 64 bits y, al igual que pasa con DES, utiliza el mismo algoritmo para cifrar y para descifrar.

RC2

El RC2 es un cifrador en bloque. La serie RC de cifras fue desarrollada por Ron Rivest (la R en RSA) y RC equivale a Rivest Cipher o Ron’s Code. El RC2 se desarrolló como un reemplazo continuado para el DES, pero es de dos a tres veces más rápido que este último.

⁴⁷ “La Seguridad de los Protocolos Criptográficos”, www.ugr.es/~aquiran/cripto/informes/info002.htm, agosto,2004.

Es un código protegido bajo secreto comercial (aunque no patentado) por RSA Data Security Inc. Existen ataques criptonalíticos que, aunque requieren de gran cantidad de texto cifrado, muestran las vulnerabilidades de RC-2. Existen versiones mejoradas y hoy día RC2 tiende a utilizarse cada vez menos en beneficio.

RC4

Es un intento de reemplazar RC2 por un algoritmo más sólido. También es un secreto comercial, aunque al igual que RC2, su código fuente ha sido ubicado en grupos de discusión. Forma una parte vital del sistema de cifrado de capas SSL, ampliamente utilizados en navegadores de Internet tales como Netscape Navigator y Microsoft Internet Explorer. La versión explorable de RC4 tiene una clave de solamente 40 bits, lo que lo hace altamente vulnerable a ataques de fuerza bruta (simplemente se trata de ir probando una a una todas las claves). La versión EE.UU., con clave de 128 bits, es segura.⁴⁸

RC5

Es otra cifra de Rivest. Por lo general, utiliza bloques de 64 ó 128 bits y puede soportar longitudes variables de clave hasta 2,048 bits. RC5 también es un algoritmo muy sencillo de implantar.

⁴⁸ urg.es.htm Ob. Cit.

RC6

Este se desarrolló como un reemplazo potencial del DES y es un cifrador en bloque que se basa en el RC5, soporta bloques de 128 bits tiene un tamaño de clave de 128 bits.⁴⁹

TRIPLE DES

El 3-DES, es la abreviatura de triple DES. Se basa en tres iteraciones sucesivas de algoritmo DES con lo que se consigue una longitud de clave de 128 bits, y que es compatible con DES simple.

Los algoritmos simétricos son más rápidos y eficientes que los algoritmos asimétricos y su principal característica es que habitualmente son simples sustituciones alfabéticas junto con técnicas de transposición (alteración del orden lógico de las letras del mensaje). De esta forma, consiguen ocultar la relación que existe entre el texto en claro y el texto cifrado, siendo así realmente difícil deducir el texto original y la clave a partir del texto cifrado.

Algoritmos Asimétricos

Los algoritmos asimétricos o de Llave Pública emplean generalmente longitudes de clave mucho mayores que los simétricos; requieren dos claves una privada y otra

⁴⁹ NASH, Andrew, y otros, Ob. Cit.

llamada pública, ambas relacionadas por una fórmula matemática compleja muy difícil de reproducir.⁵⁰

En comparación con los algoritmos simétricos, los algoritmos asimétricos requieren de claves mucho más grandes para garantizar la seguridad, lo cual provoca que en la práctica sean mucho más lentos. Por esta razón, los algoritmos asimétricos no han desbancado a los algoritmos simétricos y en la actualidad se utilizan los dos con la misma frecuencia.

Los algoritmos asimétricos más conocidos son:

RSA

Este algoritmo fue desarrollado en 1978 por Ron Rivest, Adi Shamir y Leonard Adleman, cuyos apellidos dan nombre al algoritmo. Este sistema ha sido utilizado durante muchos años por mucha gente y en la actualidad sigue siendo uno de los algoritmos más populares. Esto sucede porque hoy por hoy, al contrario de lo que pasa con DES, RSA continúa considerándose seguro.

La seguridad de RSA recae en el hecho de factorizar números grandes, es decir, que la clave pública y la clave privada se calculan a partir de un número que resulta de multiplicar dos números que son primos y además son grandes (de más de cien cifras): Por ello, las claves de RSA no pueden ser escogidas al azar ni pueden ser formadas por cualquier número aleatorio.

⁵⁰ rincondelvago.com Ob. Cit.

La patente fundamental del algoritmo RSA expiró en septiembre del año 2000 y, como resultado, ahora se está incorporando en muchos protocolos como algoritmo criptográfico asimétrico de carácter obligatorio, garantizándole una larga vida.⁵¹

DIFFIE-HELLMAN

Nacido en 1976 de las manos de Whitfield Diffie y Martín Helman, éste fue el primero (y por lo tanto, revolucionario) de los algoritmos asimétricos. Se considera tan seguro o más que RSA, por eso en la actualidad todavía es utilizado para el intercambio de claves de sistemas de cifrado simétricos.

Diffie-Hellman basó su seguridad en el llamado problema de los logaritmos discretos, que se cree que es computacionalmente tan complejo como el de la factorización de números primos grandes.

Su importancia se debe sobre todo al hecho de ser el inicio de los sistemas asimétricos.

Función Hash

La función hash es un algoritmo que transforma una secuencia de bits en otra menor efectuando sobre un gran bloque de datos que constituyen el documento un cálculo matemático, obteniendo como resultado un resumen o reseña (digest) al que se le

⁵¹ NASH, Andrew, y otros, Ob. Cit.

conoce como “Huella Digital” (fingerprint), este se aplica tanto para la creación como para la verificación de la firma digital.

Estos algoritmos son unidireccionales, debido a que a partir del resumen no se puede obtener el mensaje original, porque no existe la función inversa de hash.

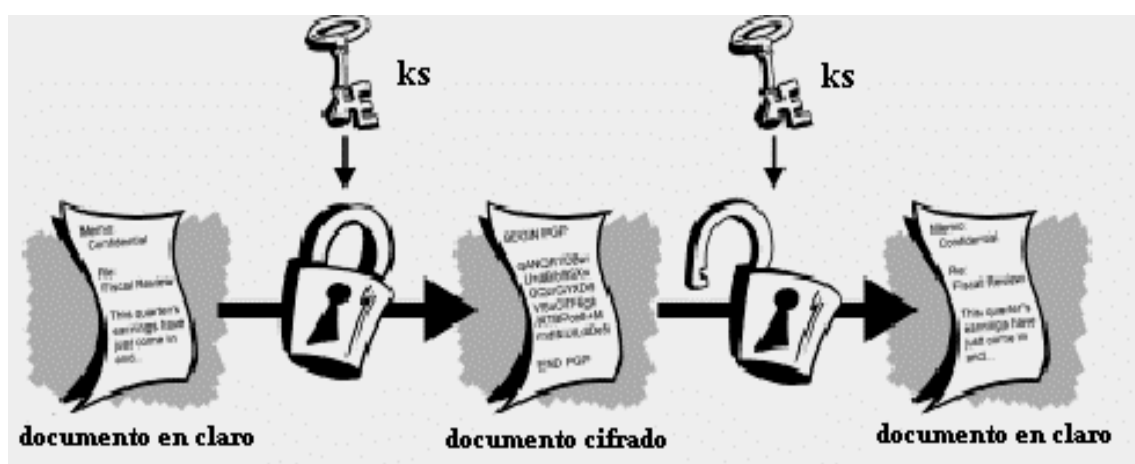
Existen varios algoritmos hash dentro de los cuales se encuentran: MD2 Message Digest # 2, produce un digest de 128 bits, MD4 Message Digest 4 , MD5 Message Digest 5, todos desarrollados por Ron Rivest, y SHA-1, desarrollado por la Agencia de Seguridad Nacional Norteamericano, produce un digest de 160 bits.

2.4.1.5.3 Tipos de Criptografía: Simétrica y Asimétrica.

Criptografía Simétrica o de Clave Privada:

Es un sistema criptográfico que en el proceso de cifrado y descifrado las partes deben compartir una clave común que es usada para cifrar y descifrar, y que se ha acordado de forma previa. Dicha clave es secreta para evitar acceso no autorizado a datos confidenciales, y de la protección de esa clave depende la seguridad de este tipo de criptografía.

De esta manera una operación criptográfica que utiliza un algoritmo de clave única o simétrica consiste en un proceso mediante el cual se produce el cifrado de un determinado documento, utilizando para ello una clave que es la misma que posteriormente se utilizará para descifrarlo. El cifrado simétrico es el más fácil de entender, por que se parece a la forma en que guardamos las cosas en la vida real.⁵²



Con esta figura perfectamente se puede esquematizar lo antes mencionado, acerca de la utilización de la criptografía simétrica ya que la misma llave (ks) en este caso la clave privada, utilizada para cerrar (cifrar) el documento, es la misma utilizada para abrirlo (descifrarlo); es decir los algoritmos simétricos encriptan y descifran con la misma llave.

52 webpanto.com, Ob. Cit.

Características

Utiliza la misma clave para cifrar y descifrar

Es rápido, por que el cifrado de grandes cantidades de datos puede avanzar a un ritmo veloz.

Es compacto, por que no genera un impacto significativo en la carga del procesador, usualmente, tiene el mismo tamaño del texto original.

Es seguro, por que el cifrado simétrico ha existido durante algún tiempo, y los algoritmos han podido sobrevivir en todo ese tiempo a varias pruebas.

La criptografía simétrica no se ajusta a las Firmas Digitales, por que no soluciona la cuestión del no rechazo o no repudio, debido a que la clave Privada podría dejar de ser “Privada”⁵³ al llegar al conocimiento de un tercero

Las anteriores características son las que han permitido que la criptografía simétrica siga existiendo, a pesar de la incorporación de tecnologías más avanzadas como la criptografía asimétrica.

Ventajas y Desventajas

Dentro de las *ventajas* se encuentran:

Su velocidad, por que este tipo de algoritmos son los más apropiados para el cifrado de grandes cantidades de datos.

53 Nash Andrew y otros, Op. Cit., Pág. 26-28

Proporciona Integridad, debido a que si el mensaje ha sido manipulado, al descifrarlo con la clave secreta no tendrá sentido.

Es útil y adecuada para dar confidencialidad a la información, pues solo las dos partes que comparten la clave secreta pueden descifrar el mensaje.⁵⁴

Por otra parte dentro de las *desventajas* se puede mencionar que:

Plantea un grave problema de seguridad al no garantizar privacidad de la clave secreta.

Puede ser inoperativa para grandes comunidades, ya que estos algoritmos necesitan que la clave sea conocida en ambos extremos.

No constituye firma, por que el mensaje frente a terceros, es atribuible a las dos partes que comparten la clave secreta, debido a que un tercero no podría atribuir la autoría del mensaje cifrado con certeza a alguna de las partes.

La necesidad de que exista una clave para cada par de personas que vayan a intercambiarse mensajes cifrados entre sí.⁵⁵

Como puede observarse, la distribución, el almacenamiento y la administración de claves, y la falta de soporte de las firmas digitales, son problemas que se enfrentan con la criptografía simétrica.

54 MARTÍNEZ NADAL, Apollonia, Ob. Cit. Pág. 46

55 Idem.

Criptografía Asimétrica o de Clave Pública:

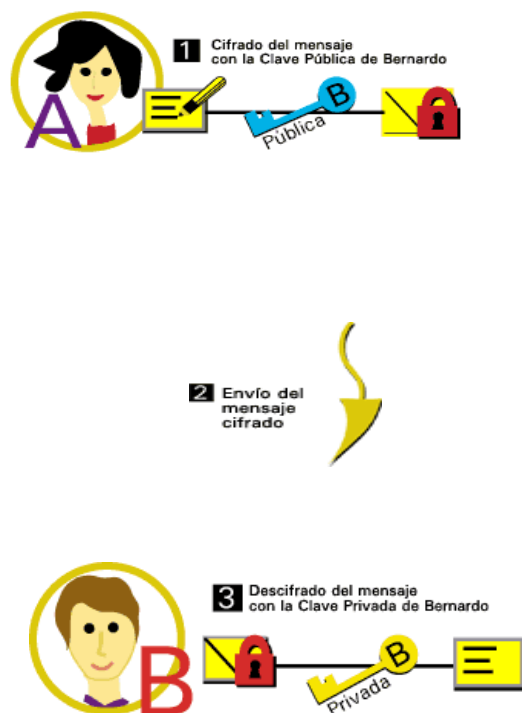
Este tipo de criptografía se basa en el uso de dos claves diferentes, claves que poseen una propiedad fundamental: una clave puede descifrar lo que la otra ha encriptado.

Generalmente una de las claves, denominada Clave Privada, es usada por el propietario para encriptar los mensajes, mientras que la otra, llamada Clave Pública, es usada para descifrar el mensaje cifrado.

Las claves Pública y Privada tienen características matemáticas especiales, de tal forma que se generan siempre a la vez, por parejas, estando cada una de ellas ligada intrínsecamente a la otra, de tal forma que si dos llaves públicas son diferentes, entonces sus llaves privadas asociadas también lo son, y viceversa.⁵⁶

Mientras que la Clave Privada debe mantenerla en secreto su propietario, ya que es la base de la seguridad del sistema, la Clave Pública es difundida ampliamente por Internet, para que este al alcance del mayor número de personas, existiendo servidores que guardan, administran y difunden dichas claves. El nacimiento de la Criptografía Asimétrica se dio al estar buscando un modo más práctico de intercambiar las llaves simétricas.

⁵⁶ htmlweb.net, Ob. Cit.



Características:

Con la Criptografía Asimétrica que cifra con una clave (pública o privada) solo se puede descifrar con la otra clave (privada o pública), es decir ambas claves, privada y pública, sirven tanto para cifrar como para descifrar mensajes.

Es segura, debido a que cada propietario puede realizar operaciones matemáticas con su clave privada, tan complejas que nadie más en el mundo puede realizarlas, debido a que no se puede deducir ni obtener matemáticamente la clave privada partiendo de la clave pública.

La codificación asimétrica no sufre interceptación de clave, dado que no se necesita enviar una clave al receptor.

El número de claves que se necesita distribuir es el mismo número de participantes, por ello la criptografía asimétrica sirve también en escalas de poblaciones muy grandes.

La criptografía asimétrica es la base para las firmas digitales.

Es relativamente lento.

Reduce el texto al cifrarlo y lo expande al descifrarlo.

A pesar de la característica de lentitud que a la criptografía asimétrica, esta adquiere mayor importancia al constituir la base para la realización de las firmas digitales.

Ventajas y Desventajas:

Dentro de las *ventajas* se puede mencionar:

No se puede obtener la clave privada a partir de la clave pública o viceversa.

No se necesita tener una relación prioritaria con alguien para poder enviarle información cifrada.

La clave pública y el algoritmo de cifrado son o pueden ser de dominio público y no es necesario poner en peligro la clave privada en tránsito, ya que esta siempre oculta en poder únicamente de su propietario.

Este tipo de criptografía evita perfectamente los problemas administrativos de clave.

Por otra parte dentro de las **desventajas** se encuentran:

Los algoritmos asimétricos son relativamente lentos.

Cifrado asimétrico expande el texto cifrado.

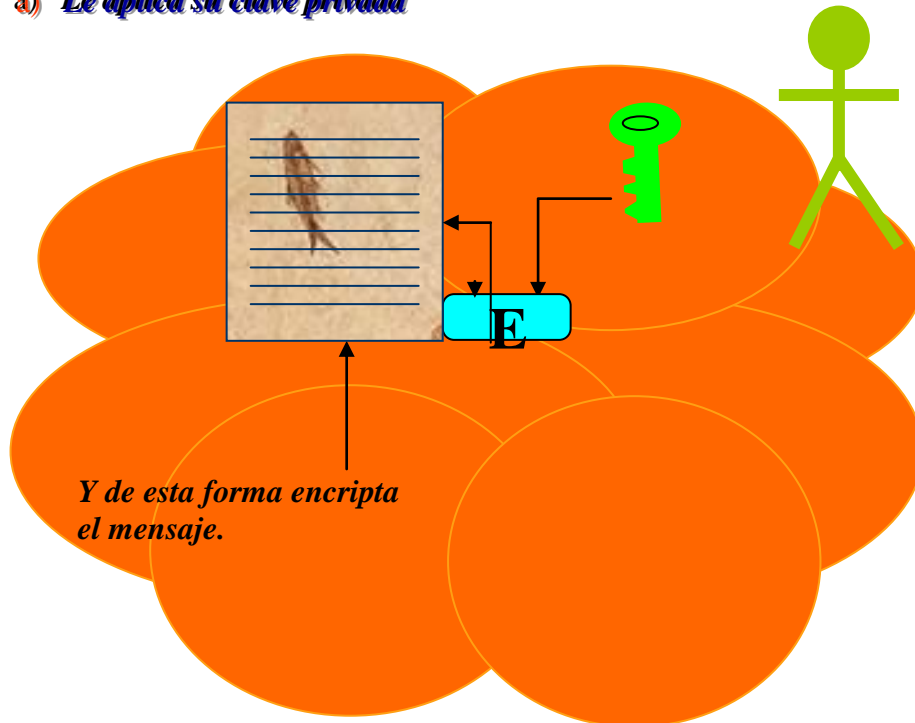
Observando las ventajas brindadas por la criptografía asimétrica se puede concluir que su seguridad es mayor que la de la criptografía simétrica y que es esto lo que le da credibilidad y certeza a la firma digital en su utilización y a la vez otorga confidencialidad e integridad a los documentos en la cual esta se utiliza, pasando por alto las desventajas que esta presenta.

2.4.2 Proceso de Firma Digital y Verificación

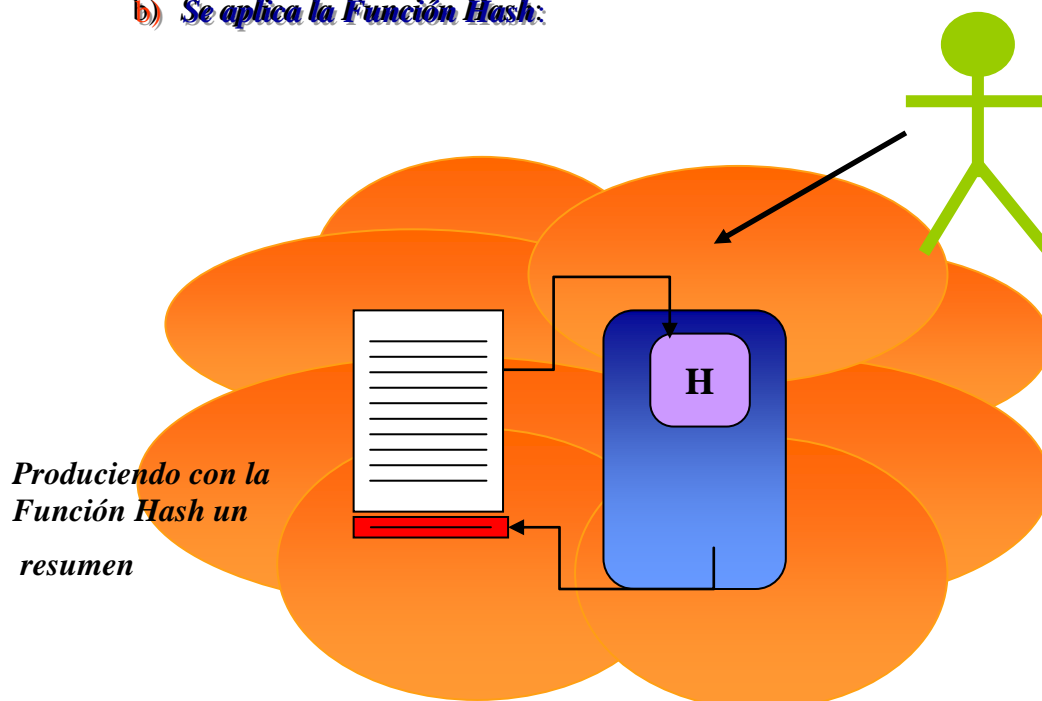
PROCESO DE FIRMA DIGITAL

1º EL USUARIO PREPARA EL MENSAJE A ENVIAR

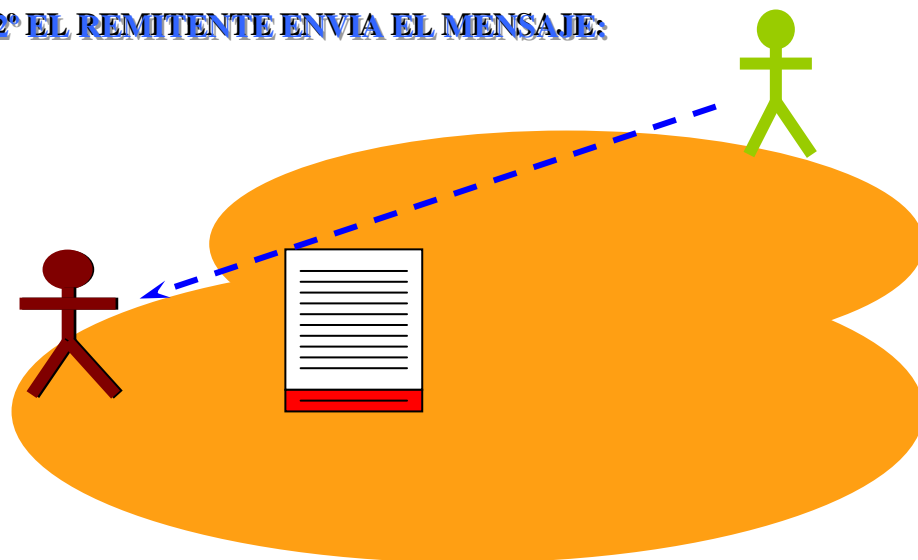
a) *Le aplica su clave privada*



b) *Se aplica la Función Hash:*



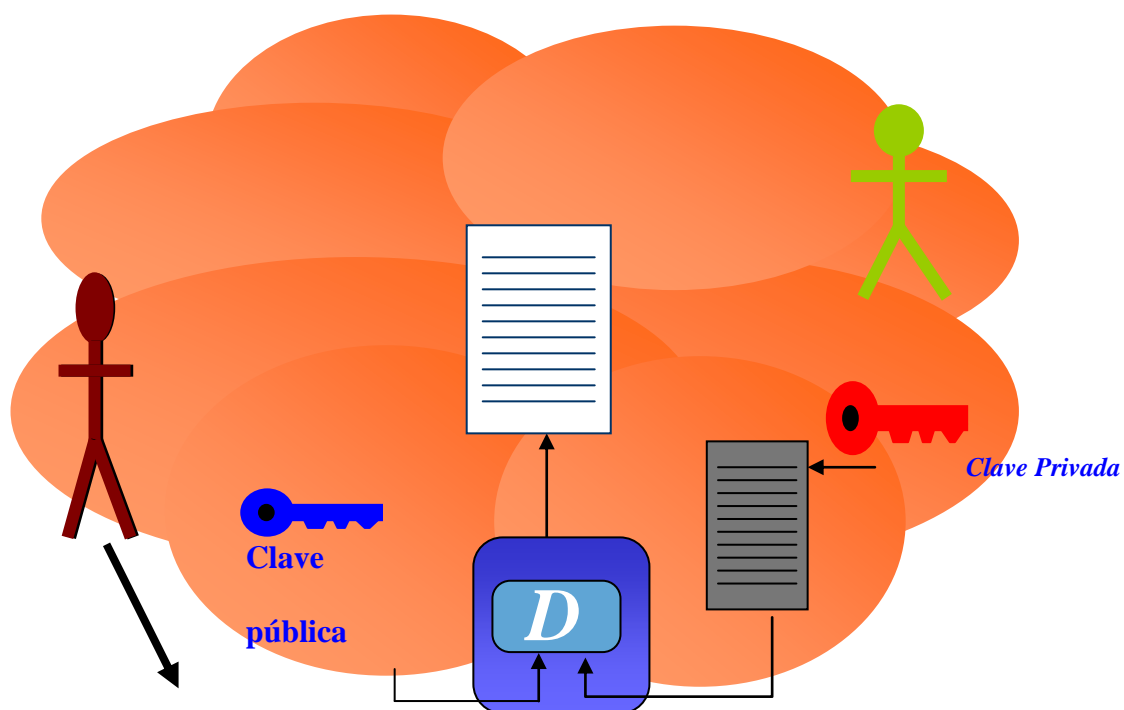
2º EL REMITENTE ENVIA EL MENSAJE:



En el proceso de firmar digitalmente un documento, la utilización del par de claves implica que el emisor cifra un mensaje utilizando para ello su clave privada y, una vez cifrado, lo envía al receptor. Partiendo de un mensaje determinado que puede tener cualquier tamaño, dicho mensaje se convierte mediante la función Hash en un mensaje con una dimensión fija (entre 128 y 160 bits). Para ello, el mensaje originario, se divide en varias partes cada una de las cuales oscilará entre aquella dimensión, y una vez dividido se combinan elementos tomados de cada una de las partes resultante de la división para formar el mensaje-resumen o Hash, que también tendrá una dimensión fija y constante. Este resumen es el que se cifra utilizando la clave privada del emisor del mensaje.

PROCESO DE VERIFICACION DE FIRMA DIGITAL

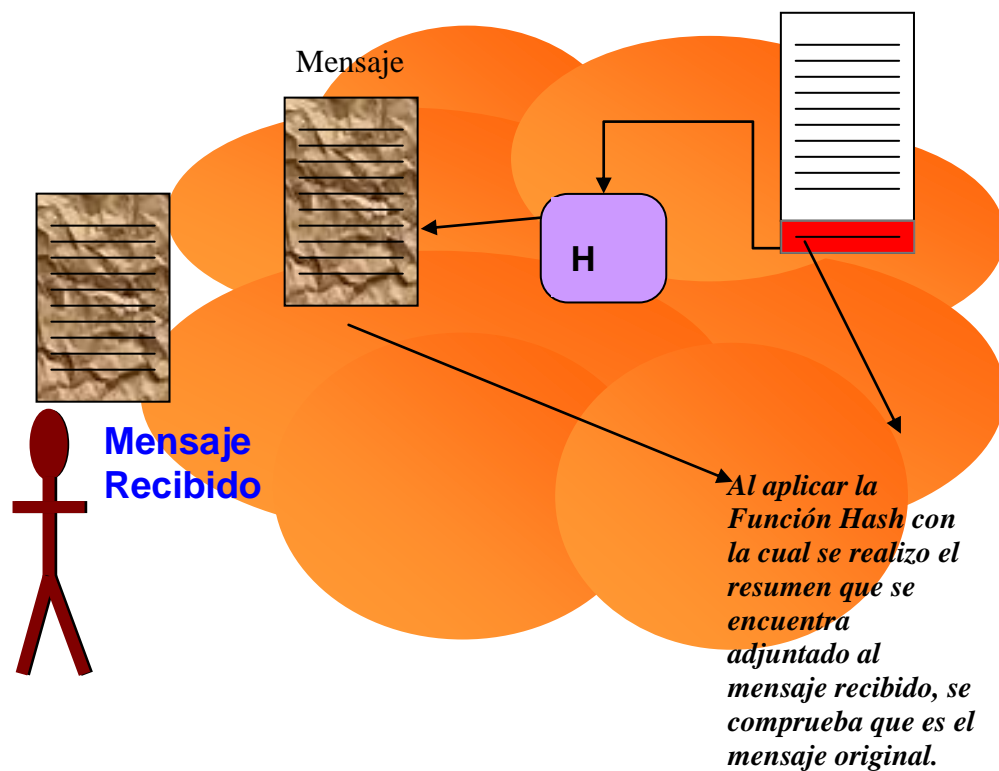
1º El destinatario recibe el mensaje



*El destinatario
desencripta el mensaje
aplicando la clave
publica del remitente.*

*Cuando el destinatario recibe el mensaje, lo descifra con
la Clave Publica del emisor, para comprobar la firma.*

2º El destinatario compara el mensaje que ha recibido ya descifrado aplicando al mensaje que se le ha enviado la Función Hash, empleada para el resumen del mensaje original



El destinatario calcula el resumen del mensaje recibido repitiendo el proceso que usó el emisor. Si los dos resúmenes (el del emisor descifrado y el calculado ahora por el destinatario) coinciden, la firma se considera válida y el destinatario puede estar seguro de la integridad del mensaje: Si el mensaje hubiera sido alterado por su paso por la red, el resumen calculado por el destinatario no coincidirán con el original.

2.4.3 La Firma Digital en El Salvador

A pesar de que Internet nació en nuestro país en 1996, las empresas tienen poco tiempo de realizar negocios en la red. La mayoría de las empresas salvadoreñas que realizan comercio por medio de Internet son las más fuertes en su giro de negocios.

Las empresas que actualmente realizan comercio electrónico reflejan muy pocas utilidades, existiendo empresas cuyo giro de negocios es solamente la venta por Internet; pero a pesar de que los porcentajes de ventas no son muy significativos, las visitas a las páginas web son altas, siendo este un inicio para el ciclo de ventas.

El cobro de los productos y/o servicios son efectuados por las empresas de carácter financiero que captan fondos a través de las tarjetas de crédito, luego de la realización de compras.

Los consumidores tienen la oportunidad de poder adquirir sus productos y servicios desde su casa u oficina mediante el uso de Internet. Existen varias tiendas virtuales como son: www.gevesa.com, www.siman.com, www.netcomsa.com, www.compramerica.com, www.grupotvoffer.com, www.omnihits.com, www.tiendavirtual.com.sv, y dentro del centro comercial electrónico: www.virtualmall.com.sv.

El pago por los productos y/o servicios son efectuados a través de cualquiera de las tarjetas de crédito mayoritarias y con respaldo a nivel mundial como son: Aval Card, Master Card, VISA, Dinners Club y American Express en cualquiera de sus presentaciones: nacional, regional e Internacional.

No obstante la implementación y desarrollo del comercio electrónico en nuestro país, actualmente no existe un método seguro que garantice la autenticidad de las relaciones por internet; y es por esto posible afirmar que actualmente no existe la firma digital en el sentido amplio desarrollado en esta investigación. Lo único existente hasta el momento, son tipos de firmas electrónicas que están siendo utilizadas ya por nuestra banca y al mismo tiempo un incipiente cifrado de clave doble, implementado por DIESCO EAN.

Los Bancos que se encuentran más avanzados en la digitalización de sus transacciones bancarias son el Banco Cuscatlan y el Banco Agrícola, los cuales poseen un servicio de algunas de sus transacciones por internet, y otras de ellas a través de cajeros automáticos que utilizan impulsos electrónicos que constituyen tipos de Firma Electrónica.

Banco Cuscatlan:

El Banco Cuscatlan cuenta con un espacio en Internet, el cual se denomina ***NetBankin***, este servicio está diseñado para que se realicen directamente, vía Internet, consultas, transacciones y todo tipo de gestiones con el Banco, desde el hogar y la oficina. Adicionalmente NetBanking ofrece Servicios Empresariales, donde se pueden realizar todas las operaciones bancarias tales como el Pago de Planilla o el Pago a Proveedores, sin riesgos ni demoras. También con NetBanking se puede pagar más de 70 servicios públicos y privados como son luz, agua, teléfono, cable, colegios, entre otros. Estas pueden ser realizadas las 24 horas del día y los 365 días del año.

Algunas de las operaciones que se pueden realizar a través de Netbankin son:

Consultas de saldo, pagos y transferencias de sus Cuentas, <Inversiones, Préstamos y pago de servicios diversos.

Realizar operaciones bancarias de empresa tales como: transferencias de dinero a Cuentas de terceros, pago de planillas, proveedores y operaciones de crédito. Solicitar diversos servicios como conciliación de Cuentas, cambio de claves, reserva de fondos, suspensión y consulta visual de cheques, anulación de libreta de ahorro. Todo tipo de gestiones de Tarjetas de Crédito como ampliación de límite de

crédito, solicitud de Tarjeta adicional y reposición de Tarjeta o Clave de Acceso de Cajero Automático.

Para la seguridad y conveniencia, todo el sistema está diseñado para salvaguardar la información mediante mecanismos de seguridad de los datos. Además, cuenta con dispositivos de seguridad que verifican la identidad de quien utiliza el sistema.

Banco Agrícola:

El Banco Agrícola cuenta con un programa denominado PCBAC, por medio del cual pueden realizarse diferentes transacciones en línea como las siguientes:

Consultas de Saldos, Estados de Cuentas de Ahorro, Corriente, Préstamos, Tarjetas de Crédito y Líneas de Crédito.

Pago de Planilla y Proveedores.

Pago de Tarjetas de Crédito.

Pago de Prestamos.

Pago de Servicios.

Transferencias entre Cuentas.

Reservas y suspensiones de Pago de Cheques.

Conciliación de Cuenta Corriente.

Solicitud de Transferencias Internacionales.

Notificaciones de Libreta y/o Chequera extraviada.

Solicitud de Chequeras.

Información sobre productos y servicios del Banco Agrícola.

Correo Electrónico interno del programa, para comunicarse directamente con el Banco Agrícola.

También el Banco Agrícola cuenta con el servicio de “Red de Cajero Automaticos 7/24,” el cual permite realizar a los usuarios retiros, consultas, etc. de su cuenta.

DIESCO EAN

Diesco es una empresa contratada por la Cámara de Comercio de El Salvador, y la única que actualmente está poniendo en práctica la firma digital utilizando criptografía asimétrica o de clave pública en nuestro país con base y aplicación de La Ley Aduanera, la cual se explicará posteriormente. Para su implementación ha creado ciertos lineamientos que se denominan “Prácticas de Certificación Digital” y dentro de los cuales establece algunos criterios importantes de mencionar como:

Ámbito de Aplicación

CERTI-C@MARA es una Autoridad Certificadora/Registradora Cerrada, es de carácter privado y los certificados emitidos son utilizados para el Sistema de Teledespacho por Internet y ha sido creado para la emisión de certificados personales o jurídicas.

La finalidad de los servicios de certificación digital ofrecidos por CERTI-C@MARA, es crear un marco razonable de seguridad jurídica y tecnológica, en el que CERTI-C@MARA, se constituye en un tercero confiable para las partes involucradas en una transacción electrónica con la Aduana.

Servicios

Los Servicios de Certificación Digital que serán prestados por CERTI-C@MARA comprenderán entre otros, los siguientes:

Emisión de Certificados: personales o Personas Jurídicas.

Revocación de Certificados: para efecto de dar por terminada anticipadamente la vigencia de un certificado, ya sea por voluntad de su titular o porque concurrieron una o más de las causales descritas e la sección correspondiente de este documento.

Publicación de Certificados: una vez que el certificado digital haya sido emitido, éste será publicado en un directorio bajo especificaciones X.509, u otra bajo cualquier otra especificación, de manera que terceros interesados pueda tener acceso a él.

Almacenamiento de Certificados: los certificados digitales emitidos y la lista de certificados revocados (CRL's), son almacenados por un período determinado de tiempo

debido a que el documento firmado digitalmente, por sí mismo, puede poseer un período de validez o vigencia más amplio que el del certificado utilizado para firmar.

Tipos de Certificados

Por sí misma como Autoridad Certificadora, CERTI-C@MARA podrá emitir la siguiente clase de Certificados Personales o Jurídicos.

Certificados Nivel 0: son certificados personales para efectos de PRUEBAS, no tienen valor legal alguno, son emitidos con el único fin de facilitar las pruebas de transmisión de información entre partes que utiliza Internet y desean un entorno más seguro en el envío y recepción de mensajes.

Por su propia naturaleza, al no ser necesaria la presencia física del solicitante, generalmente se emiten, suspenden, revocan o renuevan en línea y con respecto a ellos CERTI-C@MARA no reconoce responsabilidad alguna de ninguna naturaleza.

Certificados Nivel 1: son certificados personales para E-MAIL, su valor legal deriva del contrato entre las partes y se emiten por instrucción o bajo la responsabilidad de entidad interesada.

Son emitidos con el único fin de facilitar la transmisión de información entre partes que utilizan Internet y desean un entorno más seguro en el envío y recepción de mensajes, básicamente por medio de correo electrónico. La seguridad que proporcionan solo está referida a la confirmación del nombre de una persona y la dirección de correo

electrónico con la que esa persona ha sido vinculada. Ambos elementos constituyen el único objeto de validación que CERTI-C@MARA les reconoce.

Certificados Nivel 2: son certificados personales, su valor legal deriva del contrato entre las partes y se emiten por instrucción o bajo la responsabilidad de la entidad interesada para entornos APLICATIVOS.

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

Certificados Nivel 3: son certificados personales o Jurídicos, con valor legal pleno. Son emitidos en un entorno más seguro y revestido de ciertos formalismos no solo respecto de la identificación del solicitante del certificado, sino incluso respecto del proceso de emisión, ya que para ello resulta indispensable la comparecencia personal (física) del titular ante el Agente Certificador. Estas formalidades, realizadas en el contexto del marco jurídico existente proporciona una mayor seguridad en las transacciones de comercio electrónico y garantizan al mismo tiempo la posibilidad de exigir su cumplimiento mediante los procedimientos jurisdiccionales tradicionales.

Tecnología Utilizada

Los certificados emitidos en el ámbito de Teledespacho por Internet están basados en los sistemas de criptografía de clave pública de RSA y cumplen con los estándares definidos para la versión 3 del formato X.509.

La tecnología aplicada en los productos utilizados por CERTI-C@MARA ha sido desarrollada por su socio tecnológico SeguriDATA y han sido creadas utilizando el más alto nivel de criptografía, siguiendo el modelo de criptografía de clave pública más reconocido y utilizado a nivel internacional (RSA) y de acuerdo a los estándares emergentes. Los productos no violan ningún derecho de gobierno o compañías extranjeras, así como tampoco están sujetos a sus restricciones.

De esta forma, CERTI-C@MARA puede ofrecer el más alto nivel de seguridad (claves RSA de hasta 2048 bits de extensión y claves simétricas de 128 bits de longitud).

Las claves privadas de las Autoridades Certificadoras de CERTI-C@MARA han sido generadas y almacenadas en dispositivos de seguridad que cumplen con las especificaciones internacionales FIPS 140-1 en cuanto a su nivel de seguridad.

Procedimientos de Certificación

Todo servicio y/o proceso de certificación digital ofrecido por CERTI-C@MARA está sujeto y regulado además por la celebración de un convenio expreso entre CERTI-C@MARA y sus clientes.

Generación de Claves

La generación de las claves pública y privada necesarias para la emisión de un certificado digital deberá realizarse bajo el absoluto control de quien será el titular de dicho certificado y será exclusiva responsabilidad de éste el tomar las medidas de seguridad que considere necesarias para el resguardo de la clave privada y la contraseña de acceso a ésta.

Tratándose de certificados personales o de personas Jurídicas, la generación de dichas claves podrá realizarse a través del sitio web de ésta (www.diescoean.com.sv), o si el usuario lo requiere podrá solicitar a Certi-C@mara que le genere dichas claves (es opcional), pero bajo la estricta responsabilidad del usuario.

Emisión de Certificados

Cumplidos los requisitos para la obtención de los certificados digitales, CERTI-C@MARA, procederá a emitirlos y su caso o ponerlos a disposición de su titular en el sitio Web, previa notificación que se haga a éste por medio de correo electrónico.

El proceso de solicitud de un certificado digital puede iniciarse a través del sitio web de CERTI-C@MARA, o el usuario puede presentarse a las oficinas de dicha institución a solicitar la emisión de dicho documento electrónico, pero invariablemente deberá concluirse en los términos indicados en los procesos anteriores.

Responsabilidades

En la prestación de los servicios de certificación digital por parte de CERTI-C@MARA, la responsabilidad estará delimitada por las consecuencias legales y económicas que deriven del cumplimiento o incumplimiento de los requisitos establecidos para los distintos procesos y niveles de certificación.

La definición de dicha responsabilidad deberá partir de la base de considerar el rol que cada parte ejerce en el proceso de certificación, y que tiene como finalidad:

Por parte de los **Agentes Certificadores** verificar y validar:

Que un sujeto determinado acredita su identidad y su capacidad legal para obligarse;

Que un sujeto determinado manifiesta su voluntad de que se le certifique la correspondencia de veracidad entre su identidad y la que dice ser su clave pública.

Que un sujeto determinado manifiesta expresamente su sujeción a los términos y condiciones contenidas en esta Declaración de Prácticas de Certificación.

Para las **Autoridades Certificadoras** verificar y validar:

Que un Agente Certificador ha cumplido con todos y cada uno de los requisitos necesarios para ejercer dicha función;

Que existe correspondencia de veracidad entre la identidad de un Agente Certificador y su clave pública, con respecto a un certificado digital emitido por éste.

Para **CERTI-C@MARA** verificar y validar que en la operación de los servicios de certificación digital:

Que ha implementado y aplicado los estándares de seguridad y criptografía necesarios con un nivel razonable de confiabilidad;

Que los servicios estarán en operación las 24 horas del día, durante los 365 días del año; y

Que aplicará su mejor esfuerzo para garantizar la permanente actualización de la tecnología utilizada y la consecuente aplicación de los estándares nacionales e internacionales que corresponda.

Estas Practicas han sido elaboradas en el contexto de la declaración de practicas de certificación a que se refiere el proyecto de régimen uniforme para las firmas digitales, en correlación con la ley modelo sobre comercio electrónico, elaborados por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (UNCITRAL) y su finalidad es constituirse en el mecanismo formal de difusión y comunicación, para con los titulares de un certificado digital emitido por CERTI-C MARA, así como para con cualquier persona que pretenda usar y/o confiar en dichos certificados.

Es importante mencionar que la firma digital empleada por la Diesco, que utiliza criptografía asimétrica o de clave publica, no es la misma que se ha desarrollado a lo largo de esta investigación, debido a que ellos combinan otros mecanismos.

2.5 Firma Manuscrita – Firma Electrónica – Firma Digital

A partir de lo que se ha establecido sobre cada una de estas clases de firmas se puede señalar ciertos criterios que claramente distinguen una firma de otra pero que también pueden hallar semejanzas entre las mismas. Eso es lo que con el siguiente cuadro pretende mostrarse.

CRITERIO	FIRMA MANUSCRITA	firma electrónica	firma digital
Constituye un signo personal	X	X	X
Declara la voluntad personal	X	X	X
Cumple una función identificadora	X	X	X
certifica el reconocimiento o conformidad del documento que la contiene	X	X	X
Proporciona integridad al documento o mensaje			X
Cumple la función de autenticación			X
Proporciona seguridad en el comercio electrónico		X	X
El documento firmado tiene fuerza legal	X	X	
El procedimiento de verificación es exacto		X	X
Puede ser falsificada fácilmente	X		
puede ser realizada de forma simultánea en diferentes partes del mundo			X
Utiliza tecnología		X	X
Utiliza sistema criptográfico		X	X

Generalmente la conforman los nombres y apellidos de una persona	X		
Constituye una cadena de bits		X	X
Puede compararse con otra firma de su tipo	X		
Por naturaleza es secreta		X	X
Suponen una serie de características añadidas al documento que la contiene		X	X
Generan en definitiva derechos y obligaciones	X	X	X
Se utiliza como forma de expresión del consentimiento	X	X	X
Tiene aplicación a nivel mundial	X		
Utiliza cualquier método basado en medios electrónicos		X	
No puede ser imitada		X	X
Necesita, en ocasiones, ser autenticada por Notario	X		
Necesita estar amparada por una autoridad de certificación			X
Es utilizada como condición de validez	X	X	X
Son admitidas como medio de prueba	X	X	X
Se encuentra regulada jurídicamente de manera específica en nuestro país	X		

Los criterios que se han tomado en cuenta son cuestiones generalizadas a nivel internacional, con respecto a las características y usos de las firmas objeto de estudio; vale aclarar que respecto del criterio que señala “el documento firmado tiene fuerza legal” debe entenderse que se refiere a la fuerza ejecutiva y precisamente en el caso de nuestro país; ya que en otros países donde tiene uso y regulación jurídica el sistema de firma digital, también cuenta con este atributo.

Así en el cuadro anterior trata de precisarse lo que la tecnología ha logrado equiparar a la firma manuscrita; es decir, a la forma o sistema tradicional de firma; en lo que esta ha sobresalido y lo que no ha logrado conseguir aún.

CAPÍTULO 3

CERTIFICADOS Y AUTORIDADES DE CERTIFICACIÓN

Sumario 3.1 Introducción- 3.2 Certificados Digitales: 3.2.1 Definición, 3.2.2 Clases, 3.2.3 Requisitos, 3.2.4 Ciclo Vital del Certificado, 3.2.4.1 Generación y Emisión, 3.2.4.2 Distribución de Certificado, 3.2.4.3 Período de Validez del Certificado. Invalidez Anticipada: Revocación y Suspensión del Certificado- 3.3 Autoridades o Entidades de Certificación 3.3.1 Definición, 3.3.2 Naturaleza, 3.3.3 Funciones, 3.3.4 Clases de Entidades de Certificación, 3.3.5 Importancia de las Entidades de Certificación- 3.4 Firma Digital y su Seguridad Tecnológica: PKI-Infraestructura de Clave Pública. 3.5 Otros Mecanismos de Seguridad.

3.1 Introducción

Como se ha señalado, la criptografía asimétrica y las firmas digitales son elementos esenciales del comercio electrónico seguro; y para la aplicación de estas tecnologías de forma segura y a gran escala es que surgen los denominados certificados de clave pública emitidos por las autoridades de certificación; pues, efectivamente, cuando una parte desea verificar la firma digital generada por la otra parte, la parte verificadora necesita una copia de la clave pública de la parte firmante y necesita tener certeza de la correspondencia entre la clave pública y esa concreta persona determinada, en otras palabras, su correspondencia con la clave privada; y esto puede conseguirse y resolverse con los certificados de clave pública emitidos por una autoridad de certificación que actúa como tercera parte de confianza de la parte firmante y la parte verificadora.

Es así como en este capítulo se dedica a estudiar los certificados digitales enumerando los aspectos más generales y básicos de los mismos y tratando de brindar un conocimiento inicial de las diferentes etapas de su existencia efectiva desde su generación hasta su “muerte”, es decir, hasta que deja de ser válido y proporcionar seguridad. También se incluyen apartados en los que se estudian las Autoridades de Certificación que se constituyen en terceros de confianza que amparan certificados; finalizando este capítulo resaltando la seguridad tecnológica que toda la infraestructura de Clave Pública brinda al mecanismo de Firma Digital.

3.2 Certificados Digitales

3.2.1 Definición

En el mundo electrónico, para asegurar que una determinada clave pública pertenece a un usuario en concreto se utilizan los certificados digitales, que son documentos electrónicos que contienen un conjunto de información a la que se ha fijado una firma digital por alguna entidad que es reconocida y en la que confía alguna comunidad de usuarios de certificados.⁵⁷ El Certificado Digital permite que el par de claves obtenido por una persona este siempre vinculado a una determinada identidad personal, y si se sabe que el mensaje ha sido cifrado con la clave privada de esa persona, se sabe también quién es la persona titular de esa clave privada. En este sentido

⁵⁷ MARTÍNEZ NADAL, Apollonia, Ob. cit., Pág. 145

certificado digital se puede definir como: “ Un documento electrónico emitido y firmado digitalmente por una autoridad de certificación, que identifica una clave pública con su propietario”.

Un certificado debe estar identificado por un número de serie único y además contener los datos de identificación del propietario, su clave pública, y la firma privada del propietario Prestador de Servicios de Certificación.

Los certificados son un elemento esencial para la aplicación segura y a gran escala de tecnología de las firmas digitales en el ámbito del comercio electrónico, tecnología necesaria para dar seguridad a este tipo de comercio. Revistiendo también, importancia debido a que contribuye a solventar el problema de una distribución fiable de claves públicas que presentan las firmas digitales, con una adecuada comprobación de la identidad del titular.⁵⁸

3.2.2 Clases:

Los Certificados Digitales son equivalentes a un Documento de Identidad ya que permiten identificarse, y firmar, es decir cifrar electrónicamente documentos y mensajes. Sus principales aplicaciones son para autenticar identidad y firmar digitalmente. Dependiendo del uso que se vaya a dar al certificado y de qué persona o entidad lo solicita, las Autoridades Certificadoras han dividido los certificados en varios tipos. Del

⁵⁸ Ídem. Pág. 148

tipo de certificado a emitir van a depender las medidas de comprobación de los datos y el precio del mismo.

Los **certificados, según las comprobaciones de los datos que se realizan**, se dividen en cuatro clases:

Certificados de Clase 1: corresponde a los certificados más fáciles de obtener e involucran pocas verificaciones de los datos que figuran en él: sólo el nombre y la dirección de correo electrónico del titular.

Certificados de Clase 2: en los que la Autoridad Certificadora comprueba además el DNI o permiso de conducir, el número de la Seguridad Social y la fecha de nacimiento.

Certificados de Clase 3: en la que se añaden a las comprobaciones de la Clase 2 la verificación de crédito de la persona o empresa mediante un servicio del tipo Equifax o Duns&Bradstreet.

Certificados de Clase 4: que a todas las comprobaciones anteriores suma la verificación del cargo o la posición de una persona dentro de una organización (todavía no formalizados los requerimientos; está en estudio).

Desde el punto de vista de la finalidad, los certificados electrónicos se dividen en:

Certificados SSL para cliente: usados para identificar y autenticar a clientes ante servidores en comunicaciones mediante el protocolo Secure Socket Layer, y se expiden normalmente a una persona física, bien un particular, bien un empleado de una empresa.

Certificados SSL para servidor: usados para identificar a un servidor ante un cliente en comunicaciones mediante el protocolo Secure Socket Layer, y se expiden generalmente a nombre de la empresa propietaria del servidor seguro o del servicio que éste va a ofrecer, vinculando también el dominio por el que se debe acceder al servidor. La presencia de éste certificado es condición imprescindible para establecer comunicaciones seguras SSL.

Certificados S/MIME : usados para servicios de correo electrónico firmado y cifrado, que se expiden generalmente a una persona física. El mensaje lo firma digitalmente el remitente, lo que proporciona Autenticación, Integridad y No Repudio. También se puede cifrar el mensaje con la clave pública del destinatario, lo que proporciona Confidencialidad al envío.

Certificados para la firma de código: usados para identificar al autor de ficheros o porciones de código en cualquier lenguaje de programación que se deba ejecutar en red (Java, JavaScript, CGI, etc). Cuando un código de éste tipo puede resultar peligroso para

el sistema del usuario, el navegador lanza un aviso de alerta, en el que figurará si existe certificado que avale al código, con lo que el usuario puede elegir si confía en el autor, dejando que se ejecute el código, o si por el contrario no confía en él, con lo que el código será rechazado.

Certificados para AC: que identifican a las propias Autoridades Certificadoras, y es usado por el software cliente para determinar si pueden confiar en un certificado cualquiera, accediendo al certificado de la AC y comprobando que ésta es de confianza.

Toda persona o entidad que desee obtener un certificado debe pagar una cuota a las Autoridades de Certificación, cuota que irá en función de la clase del certificado y del uso que se le vaya a dar al mismo (ambas están relacionadas). A mayor nivel de comprobación de datos (clase mayor) o seguridad, más costará el certificado.

3.2.3 Requisitos:

Para que los certificados digitales gocen de validez deben cumplir con los siguientes requisitos:

Ser emitidos por un certificador autorizado; quien se constituye en un tercero de confianza que administra la certificación en el sistema de firma digital.

Responder a formatos estándares reconocidos internacionalmente, los cuales son fijados por la autoridad de certificación basados en los lineamientos establecidos por la ITU-T (International Telecommunication Union-Telecommunication Standardization

Sector) y el ISO/IEC (International Standards Organization/ International Electrotechnical Comisión), quienes son a nivel internacional los encargados de establecer parámetros referente a certificados digitales, y que en la actualidad exige el formato V3 del X.509.

Contener como mínimo los elementos siguientes:

Sujeto; los nombres y apellidos, dirección, domicilio y correo electrónico del individuo o entidad que se van a identificar con el certificado. Se puede incluir información de identificación adicional en el nombre del sujeto.

Clave Pública; esta se refiere a la clave pública del usuario la cual corresponde con su clave privada.

Entidad Certificadora; identifica la fuente de confianza que generó y firmó el certificado indicando su nombre, dirección, lugar donde realiza sus actividades y su período de vigencia.

Número de serie; un número de serie permite que este certificado se identifique como único, incluso si se emite otro certificado con la misma información..

Período de validez; este campo indica el período de tiempo durante el cual el certificado es válido y la autoridad certificadora está obligada a mantener información sobre el estado del mismo. El campo consiste en una fecha inicial, la fecha en la que el certificado empieza a ser válido y la fecha después de la cual el certificado deja de serlo.

Uso de claves; esta información describe los usos válidos para la pareja de claves pública/privada del sujeto.

Firma Digital; se refiere a la firma que le imprime la entidad certificadora.

Identificador del algoritmo de firmado; en este espacio se identifica el algoritmo empleado para firmar.

Versión; contiene el número de versión del certificado. Pudiendo ser V1, V2, V3 de X.509.⁵⁹

Estos elementos son los que generalmente debe contener un certificado digital, pero estos no se convierten e taxativos, debido a que cada país en su legislación puede exigir otro tipo de datos que a su criterio juzgue necesarios para brindar mayor seguridad al emitir un certificado.

3.2.4 Ciclo Vital del Certificado:

3.2.4.1 Generación y Emisión

Solicitud y registro

Como requisito previo para el inicio del procedimiento de generación de un certificado es necesaria la recepción por parte de la autoridad de certificación de una solicitud de emisión firmada por el futuro suscriptor en la que éste suministra cierta información que la autoridad de certificación necesita para registrarlo e incluir en el certificado. Generalmente, se puede acudir a dicha entidad personalmente o por medio de Internet utilizando la página web de la entidad de certificación.⁶⁰

⁵⁹ Nash Andrew, Op. Cit. Pág. 72 y 73

⁶⁰ MARTÍNEZ NADAL, Apollonia, Ob. Cit. Pág. 177

Comprobación de la solicitud

Una vez recibida la solicitud la autoridad de certificación procede a la aprobación de la misma previa a su comprobación, exigiéndole a una persona natural sus documentos de identidad, y al representante de una sociedad (administrador, apoderado, etc.) o de cualquier otra persona jurídica, su acreditación documental del cargo y facultades, logrando con esto su autenticación como aspecto más relevante para la aprobación del certificado.

Emisión y firma del certificado

Verificada la exactitud de la información suministrada por el solicitante y contenida en el certificado, la autoridad de certificación crea con los dispositivos técnicos adecuados el par de claves pública y privada y genera el certificado digital correspondiente a esas claves, firmándolo digitalmente utilizando la clave privada de la que es titular.

Entrega del certificado

La entidad de certificación entrega una tarjeta semejante a una tarjeta de crédito que tiene una banda magnética en la que están gravados tanto el par de claves como el certificado digital. El acceso al par de claves y al certificado digital gravados en la tarjeta está protegido mediante una clave como los que se utilizan en las tarjetas de crédito o en las tarjetas de cajero automático. En otras ocasiones, en lugar de la tarjeta la entidad de

certificación deja almacenado el certificado digital en su propia página web, a fin de que el destinatario copie el archivo y lo instale en su ordenador.

Con esa tarjeta magnética y un lector de bandas magnéticas adecuado conectado a un ordenador, el propietario del certificado podrá leer y utilizar la información gravada en la tarjeta para firmar digitalmente los mensajes electrónicos que envíe a otras personas.⁶¹

Publicación y archivo del certificado:

La autoridad de certificación incluye una copia del certificado en un directorio de certificados para su publicación. Un **directorio** es una base de datos de certificados y otra información relevante accesible on-line. La publicación del certificado en el directorio significa para la comunidad de usuarios que el suscriptor lo ha aceptado.

También esta autoridad archiva una copia del certificado. Este archivo es utilizado para tener un registro de lo que ha sido firmado por ella, en caso de que el certificado emitido se traspase a un directorio, así como para permitir verificar que no se emitan dos certificados con las mismas claves; y a la vez para el suscriptor presenta la utilidad de solicitar una copia en caso de pérdida del certificado que le fue entregado.

3.2.4.2 Distribución del Certificado

Antes de que los certificados se puedan usar para establecer identidades, se deben distribuir en diferentes formas a los usuarios:

⁶¹ tuguialegal.com, Ob. Cit.

El propietario del certificado puede transmitirlo: a través de su correo electrónico adjuntándolo a un documento.

La autoridad de certificación lo puede almacenar en un directorio llamado también repositorio: el cual contiene información accesible y disponible sobre los certificados.

La distribución del certificado dependerá del tipo de servicio que ofrezca la entidad de certificación, los cuales estarán sujetos al régimen jurídico que se les aplica a estas entidades en cada país.

3.2.4.3 Período de Validez del Certificado. Invalidez Anticipada: Revocación y Suspensión del Certificado.

Período de Validez del Certificado:

Duración

Los certificados no pueden tener una validez indefinida debido a que si estos no se están renovando constantemente se vuelven vulnerables a robos, falsificaciones, etc. es por eso, que estos tienen una vida limitada, indicada por una fecha/hora de comienzo y una fecha/hora de finalización, que están incluidas en el certificado.⁶²

La duración del período de validez del certificado es una cuestión política de la autoridad de certificación, y esta puede variar dependiendo de la política bajo la que se rija la autoridad.

62 MARTÍNEZ NADAL, Apollonia, Ob. cit. Pág. 211

Efectos de la expiración

Una vez que finalice el período de vida previsto, el certificado ha expirado y no es válido y ya no debe de utilizarse, y de hacerlo es por cuenta y riesgo del usuario. Finalizado el período de vida del certificado, cabe entender que cesan también las obligaciones y responsabilidades de la autoridad y del suscriptor.

Renovación

Cuando el certificado ya ha expirado, la autoridad de certificación puede emitirle un nuevo certificado al suscriptor.

Invalidez Anticipada

Revocación

Aunque inicialmente, el certificado se emite para ser utilizado durante su período de validez, puede ocurrir que los usuarios deben dejar de confiar en un certificado antes de la finalización de su período de validez por diversas causas. El instrumento para ello es la **revocación**, la cual provoca que un certificado deje de ser operativo de forma permanente, finalizando su período operacional, desde un determinado momento en adelante.⁶³

63 Idem. Pág. 218

Dentro de las causas por las cuales se puede revocar un certificado estan:

Los datos han dejado de ser válidos, por ejemplo: cambio de nombre de la persona autorizada (persona jurídica), revocación del poder de representación que constaba en el certificado.

La clave privada ha sido comprometida, por ejemplo: cuando el suscriptor pierde la tarjeta inteligente que contiene la clave privada, por robo.

El certificado ha dejado de tener validez dentro del contexto para el que había sido emitido.

La autoridad de certificación ha determinado que un certificado no fue emitido de acuerdo con los procedimientos exigidos por esta, por ejemplo exhibición de un documento que posteriormente a la exhibición se comprueba que es falso, la no solicitud de documento acreditado de identidad.

El sujeto del certificado ha incumplido una obligación material de la declaración de prácticas de certificados, por ejemplo la negligencia en la custodia de la clave privada.

Cuando el suscriptor la solicita.⁶⁴

Después de comprobada la causa para revocar un certificado digital, y efectuada la misma, debe ser publicada como requisito indispensable para que la revocación quede consumada.

64 “Introducción a los Certificados Digitales”, http://revista.robotiker.com/articulos/articulo_51/página1.jsp, agosto,2004.

Lista de certificados revocados (certificate revocations list):

Es el método más común para dar publicidad a la revocación y que consiste en la publicación por parte de la autoridad de certificación de una lista de certificados revocados (**certificate revocations list**, abreviadamente **CRL**, y, descriptiva y significativamente, lista negra), definida, en el Standard X.509, como una lista sellada temporalmente de certificados revocados que ha sido firmada digitalmente por una autoridad de certificación y hecha accesible a los usuarios de certificados. Cada lista de certificados revocados contiene los números de serie de los certificados que se han revocado, junto con la fecha de revocación y un estatus que identifica la razón para dicha revocación, la cual esta firmada con la clave privada de un servicio de revocación de confianza, para garantizar que no se puede modificar, y a la vez identifica la fecha en que se publicó y cuando se puede esperar que sea la siguiente publicación, para garantizar que se utiliza la lista de certificados revocados más reciente.⁶⁵

Suspensión

En ocasiones, la cuestión de si un certificado debe finalizar su período de vigencia de forma anticipada no esta clara, bajo tales circunstancias, el suscriptor o la autoridad puede que no quieran revocar el certificado posiblemente, para evitar, dado el

65 NASH, Andrew y otros, Ob. cit., Pág. 106

carácter permanente e irreversible de la revocación, un innecesario procedimiento de recertificación. Es por que existe la **suspensión** que consiste en *hacer inoperativo de forma temporal el certificado digital*, sin necesidad de llegar a una revocación permanente del mismo.

3.3 Autoridades o Entidades de Certificación

3.3.1 Definición

La utilización de la firma digital solo es útil si existe una forma de demostrar quien ha sido el autor de la firma. Nace aquí la necesidad de la existencia de un ente encargado de comprobar la identidad de los usuarios que le solicitan certificados.

Este ente recibe diferentes denominaciones tales como: **Autoridad de certificación, Entidad certificadora, Autoridad emisora, Proveedor o prestador de servicios de certificación o simplemente Certificador;** y es *aquella que se dedica a la emisión de certificados de clave pública que contienen información sobre algún hecho o circunstancia del sujeto del certificado.*⁶⁶

Para efectos de la presente investigación a estas instituciones se les denominará Autoridad de Certificación o Entidad de Certificación, debido a la presente tendencia que en nuestro país están adoptando y que se cree seguirán teniendo, la cual se explicará al abordar la naturaleza de las mismas. De esta manera se entenderá por Autoridad o

66 MARTÍNEZ NADAL, Apollonia, Ob. cit., Pág. 149

Entidad de Certificación “*aquella persona natural o jurídica que emite certificados digitales en relación con las firmas digitales de las personas, ofrece o facilita los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos y realiza otras funciones relativas a las firmas digitales*”.⁶⁷

3.3.2 Naturaleza:

Una de las cuestiones más debatidas respecto de las entidades encargadas de la provisión de servicios de certificación es la relativa a su naturaleza, pública o comercial.

En efecto, las autoridades de certificación pueden tener una naturaleza diversa, en función de cada particular opción legislativa. Las autoridades de certificación pueden ser **Entidades Privadas o Públicas**; siendo públicas las que se puede considerar de mayor confianza, por que se presume que una administración o una entidad pública actuarán en función del interés público, además de ser más estables que las privadas. Además cabe plantearse la posibilidad de que puedan ser personas naturales o jurídicas.

Las autoridades de certificación *públicas* pueden desempeñar distintos papeles: pueden actuar como autoridad de certificación a raíz de la estructura de autoridad de certificación de un país, certificando al resto de autoridades de certificación comercial, o bien, pueden actuar como autoridad de certificación para los ciudadanos únicamente para las relaciones administración-administrado; mientras que las autoridades *privadas* pueden dedicarse a la certificación ofreciendo ese servicio a terceros como parte de su

⁶⁷ “Entidades de Certificación, Certificados y Firmas Electrónicas,” www.mici.gob.pa/comercio-electronico/sobre_entidad.html, junio,2004.

actividad empresarial principal. Es por esto, que se considera que en nuestro país estas entidades acogen una naturaleza pública porque hasta el momento es Certi-C@mara, como dependencia de la Cámara de Comercio e Industria de El Salvador, la encargada de fungir como Autoridad de certificación en nuestro país.

La naturaleza de estas entidades se encuentra íntimamente ligada con la terminología utilizada para referirse a estas terceras partes de confianza, ya que al tener un carácter público éstas se denominan **Autoridad o Entidad de Certificación**, porque se considera que reviste de una cierta fuerza, seguridad y garantías a la actividad que realizan; mientras que al gozar de un carácter privado, a éstas generalmente se les conoce como **Proveedores o Prestadores de Servicios de Certificación**, debido a que esa connotación les atribuye una naturaleza estrictamente comercial evitando la apariencia de naturaleza pública.⁶⁸

3.3.3 Funciones:

Las entidades de certificación, son las encargadas entre otras cosas, de facilitar y garantizar las transacciones comerciales por medios electrónicos o medios diferentes a los estipulados en papel e implican un alto grado de confiabilidad, y es por eso, que una vez autorizadas podrán realizar actividades tales como:

Generación y Registro de Calves:

En el sistema de generación de claves, es esencial que las claves sean únicas y estén a prueba de manipulaciones, por ello las autoridades de certificación deben utilizar

68 MARTÍNEZ NADAL, Apollonia, Ob. Cit. Pág. 149 y 150

un sistema seguro para crear las claves, en caso de ser ellas quienes las crean. Pero si es el caso de que las claves de firma han sido creadas por el titular de la clave, entonces, es la autoridad de certificación quien sólo debe de verificar que las claves han sido creadas usando los elementos técnicos adecuados y que los datos de estos para almacenar y usar la clave privada son auténticos. Una vez generadas las claves la autoridad de certificación debe de registrarlas elaborando un certificado digital.

Identificación de solicitantes de certificados:

La emisión de certificados exige el reconocimiento previo de todos aquellos elementos característicos y únicos que son propios del solicitante; a estos caracteres se les denomina “Identificadores Intrínsecos”, tales como: fotografía, firma manuscrita, huellas dactilares, timbre de voz, fondo de ojos, marcas de nacimiento, etc.

Emisión de certificado

La entidad de certificación emite los certificados digitales únicos y perfectamente identificables a través de su número de serie.⁶⁹

Almacenamiento en la Autoridad de Certificación de su Clave Privada

Las autoridades de certificación son firmantes digitales en la emisión de certificados digitales, para ello deben disponer de una clave privada que sólo conocen

⁶⁹ “Autoridades de Certificación y Confianza Digital- Tercera Parte” www.fundaciondike.org.ar/seguridad/firmadigital-autoridades2.html, junio 2004.

ellos y que custodian con niveles de seguridad iguales o superiores a los declarados públicamente, dado que todo el valor reside en que cada agencia de certificación es la única capaz de generar las firmas que llevan su identificador, es de mucha importancia que esas claves privadas se almacenen y gestionen de forma segura. Cualquier falla en la seguridad de las claves privadas no sólo pone en entredicho a la institución, sino que invalida todos los certificados emitidos por ella.

Mantenimiento de las claves vigentes y revocadas

Deben de almacenar los certificados emitidos mientras estos son válidos, de este modo, en el caso de que uno de los suscriptores pierda su certificado, podrá pedirle a la autoridad emisora que la envíe de nuevo una copia.⁷⁰

Cuando un certificado ha sido revocado el ente emisor debe de incluirlo en su lista de certificados revocados porque es desde ese momento en que la revocación del certificado tiene efecto y que puede invalidar cualquier operación que se haga con fecha posterior.

Servicios de Directorio

Este servicio de directorio es ofrecido por todas las autoridades de certificación, y es aquél en el que pueden obtener la clave pública certificada de cualquier miembro con quien quiere ponerse en contacto o establecer relaciones de algún tipo. Un servicio

⁷⁰ Ídem

de directorio consiste en una gran base de datos en la que cada entrada de usuario en el directorio contiene los certificados de las claves públicas de las que es titular.

Las anteriores funciones no son las únicas que deben desempeñar las autoridades de certificación debido a que cada una de ellas debe definir y elaborar ciertos lineamientos conocidos como: **“Declaración de Prácticas de Certificación”** (Certification Practices Statement, CPS), que originalmente fue concebido por la Asociación Americana de Abogados, en su sección de Pautas para firmas digitales; los cuales consisten en reglas que describen la manera cómo éstas operan y están limitadas en sus funciones.⁷¹ Además deben siempre sujetarse a la legislación que las rige en cada país en que operan.

3.3.4 Clases de Entidades de Certificación:

Las Entidades de Certificación son aquellas empresas nacionales y extranjeras que otorgan firmas digitales o certificados digitales, generados por medios electrónicos seguros. Estos pueden dividirse de acuerdo a sus **facultades** en:

Entidades de Certificación Abiertas: Son aquellas que ofrecen los servicios propios de las Entidades de Certificación, su uso no se limita al intercambio de mensajes entre la entidad y el suscriptor, recibiendo remuneración por ello. Sus servicios están dirigidos al público en general y no limitan el intercambio de mensajes de datos.

⁷¹ NASH, Andrew y otros, Ob. Cit. Pág. 83

Entidades de Certificación Cerrada: Al igual que la anterior ofrece los servicios de una Entidad de Certificación, solo para el intercambio de mensajes entre esta y el suscriptor, sin exigir remuneración por ello. Este tipo de entidad, tiene por objeto mejorar el nivel de seguridad entre los usuarios de los servicios de certificación y la entidad. Sin embargo, esta no constituye la actividad principal de la Entidad de Certificación.

También pueden clasificarse de acuerdo a la naturaleza del ente que presta los **servicios:**

Entidades Publicas: son aquellos organismos o dependencias del sector publico creadas o facultadas por el Estado, para realizar las mismas actividades de una entidad de certificación.

Entidades Privadas: es aquella persona natural o jurídica que es autorizada por el ente encargado, para realizar las funciones de un entidad de certificación.

Una entidad de certificación puede adaptarse a cualquiera de las clasificaciones establecidas anteriormente, para el caso, una entidad de naturaleza privada puede ser abierta o cerrada, dependiendo de la clase de certificados que este facultada a emitir; de igual manera una entidad de carácter publico podrá ser clasificada como abierta o cerrada.

3.3.5 Importancia de las Entidades de Certificación:

Las entidades de certificación, por su connotación en la circulación de los mensajes de datos, se convierten en la pieza fundamental del engranaje comercial, pues son las que brindan certeza sobre el autor y contenido de un mensaje de datos, y por lo mismo, de ellas depende el desarrollo de este tipo de canales de comunicación dentro un marco de seguridad jurídica esencial para la proliferación del comercio por esta vía.

Además de constituir una especie de fedatario, también se convierte en un tercero disipador de conflictos al determinar la originalidad y autoría de los mensajes de datos es así que el desarrollo correcto de la actividad implica adicionalmente la tranquilidad por parte del Estado, respecto al orden público en las relaciones de sus subordinados.⁷²

Por lo tanto, las entidades juegan un papel definitivo tanto para brindar seguridad en la red, como para asegurar la confianza en el mundo físico respecto a algunos de los actos que tengan efectos jurídicos que en ella se den. Esto significa para un pequeño empresario que podrá realizar convenios y transacciones comerciales sin necesidad de viajar fuera del país e incluso sin moverse de su puesto de trabajo, pues todas las operaciones las podrá realizar desde su computador. Obtendrá la seguridad de que conoce la identidad de aquél con quien está negociando, tendrá certeza de que el

⁷² CUBILLOS VELANDIA, Ramiro y RINCÓN CÁRDENAS, Erick. Ob. Cit. Pág. 257

documento enviado no ha sido manipulado ni alterado, confidencialidad total, y una vez la otra persona reciba el mensaje, este hecho no podrá ser negado.

3.4 Firma Digital y su Seguridad Tecnológica: *PKI-Infraestructura De Clave Pública.*

El modelo de confianza basado en terceras partes confiables es la base de la definición de **PKI** son las siglas de “**Public Key Infrastructure**” (**Infraestructura de Clave Pública**”, expresión que se refiere a toda la infraestructura necesaria para poder poner en marcha y explotar sistemas y aplicaciones que utilizan técnicas de criptografía asimétrica.

Una infraestructura de clave pública es un conjunto de protocolos, servicios y estándares que soportan aplicaciones basadas en criptografía de clave pública. Es el hardware, software, personas, políticas y procedimientos necesarios para crear, gestionar, guardar, entregar, y revocar certificados.⁷³

Esta infraestructura se compone por distintas terceras partes en las que todos los demás usuarios de la infraestructura confían, las cuales son:

Autoridad de Registro

Una **Autoridad de registro (RA)** es una entidad opcional dentro de la Infraestructura de Clave Pública responsable de las tareas administrativas asociadas con

⁷³ tuguialegal.com Ob. Cit.

el registro del suscriptor, que es el sujeto del certificado expedido por la Autoridad de Certificación. Si en la Infraestructura de Clave Pública no se encuentra una Autoridad de Registro, se supone que la autoridad de certificación tiene el mismo conjunto de capacidades definidas que aquella.⁷⁴

Esta entidad identifica de forma inequívoca al solicitante de un certificado; suministra a la autoridad de certificación los datos verificados del solicitante a fin de que ésta emita el correspondiente certificado.

Las funciones que una autoridad de registro en particular implanta variarán con base en la necesidad de la instalación de la Infraestructura de Clave Pública, pero deben soportar el principio de establecer o verificar la identidad del suscriptor. Es probable que estas funciones influyan:

Autenticación personal del sujeto que se registra para un certificado.

Verificación de la validez de la información suministrada por el sujeto.

Validar el derecho del sujeto a los atributos del certificado solicitado.

Verificar que el sujeto en realidad posee la clave privada que se va a registrar.

Informar los casos de determinación o compromiso de clave donde se requiera la renovación.

Asignación de nombres con propósitos de identificación.

Generación de la pareja de claves pública/privada.

Almacenamiento de la clave privada.

⁷⁴ NASH, Andrew, y otros, Ob. Cit. Pág. 189

*Distribución de señales físicas (como las tarjetas inteligentes) que contienen las claves privadas.*⁷⁵

En general, la autoridad de registro maneja los intercambios (con frecuencia involucran interacciones del usuario) entre el sujeto y la Infraestructura de Clave Pública para el registro, la entrega del certificado y otros procesos de la administración del ciclo de vida del certificado y la clave; pero lo que nunca hará es expedir un certificado debido a que esto solamente le corresponde a la autoridad de certificación.

Autoridad de Certificación:

La autoridad de certificación es responsable de crear y expedir certificados. Estos asocian la identidad del sujeto por medio de su nombre que se registró con la clave pública correspondiente a la clave privada que posee ese mismo sujeto. Además esta autoridad es responsable de administrar todos los aspectos del ciclo de vida del certificado después de su expedición, lo cual incluye seguir el estado de un certificado y las noticias de revocación y suspensión del mismo. Esta entidad ya fue desarrollada anteriormente, por lo tanto, este apartado sólo se limita a definirla.

Autoridad de Fechado:

La autoridad de fechado es la encargada de certificar que un evento en particular sea producido en un determinado momento, basan su funcionamiento en la posición de un certificado digital emitido por una autoridad de certificación y ofrece su

⁷⁵ Ídem. Pág. 190

servicio a usuarios de la misma infraestructura de la clave pública a la que estos pertenecen. Esta autoridad no forma parte de todas las Infraestructuras de Clave Pública, pero es importante aclarar que la función desempeñada por ésta puede ser también proporcionada por una autoridad de certificación.

La función mencionada anteriormente se conoce como “Sello Temporal” y consiste en introducir marcas temporales en el documento electrónico, esto quiere decir introducirle fecha y hora al momento de enviarlo, de forma que sea imposible cambiar incluso un solo bit sin que el cambio se ponga de manifiesto; el sellado temporal implica también que es posible sellar un documento con una hora y una fecha diferente de la actual.⁷⁶

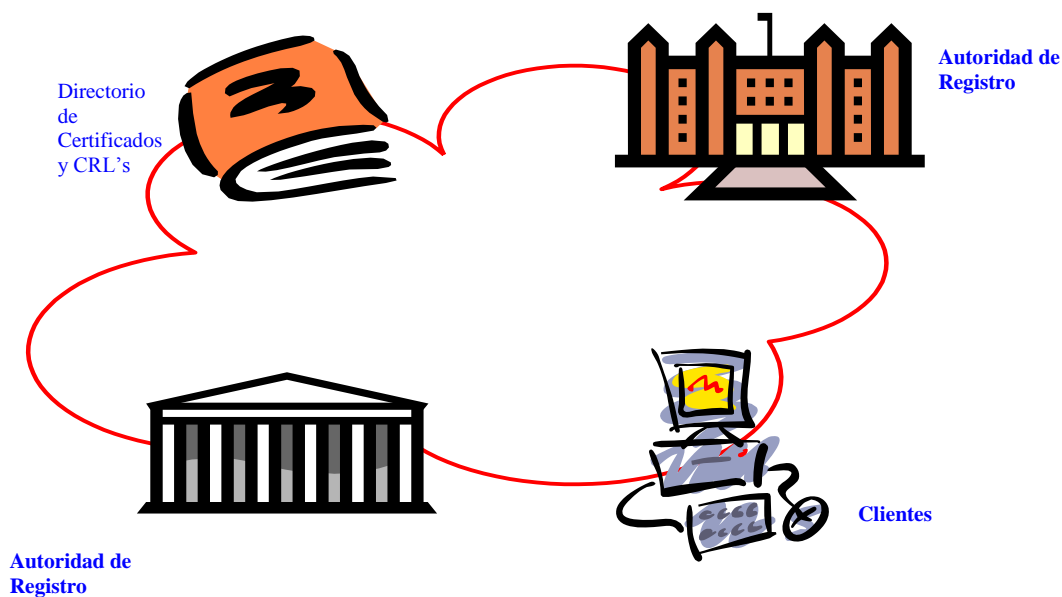
Directorio o Repositorio:

Un directorio ofrece información sobre los certificados digitales que emite una autoridad de certificación, en el que se encuentran publicados los certificados de clave pública, y es consultado para probar el estado de los mismos y así obtener la información necesaria para cifrar documentos para determinados usuarios. Lo referente a éste ya fue desarrollado anteriormente.

⁷⁶ MARTÍNEZ NADAL, Apollonia, Ob. Cit. Pág. 82

Lista de Certificados Revocados (CRL):

La autoridad de certificación publica en el Directorio lo que se denominan Listas de Revocación, las cuales contienen los números de serie de los certificados que han sido revocados así como el motivo de su revocación. De esta manera, cuando se desee comprobar el estado de un certificado, se accederá a la lista de revocación asociada al mismo y se comprobará si su número de serie pertenece a la lista, en cuyo caso se considerará que el certificado ya no es confiable. Este punto se ha tratado con profundidad en un apartado anterior.



En definitiva, una PKI incluirá una o varias autoridades de registro para certificar la identidad de los usuarios; una o varias autoridades de certificación que emitan los certificados de clave pública; un depositario de certificados, accesible vía web u otro

medio, donde se almacenen los certificados; las listas de revocación de certificados (CRL), donde se listan los certificados suspendidos o revocados; y, por supuesto, los propios certificados.⁷⁷

3.5 Otros Mecanismos de Seguridad:

La seguridad en Internet consiste en implementar mecanismos para que cuando se reciba un mensaje o se realice una transacción por medios electrónicos, se asegure la integridad del contenido y la identidad del remitente y del receptor. Las contraseñas y palabras claves ya no son un mecanismo suficientemente fiables y seguras, ya que éstas pueden ser interceptadas durante su transmisión. Pero existen soluciones seguras.

En el plano técnico, ya hay en el mercado mecanismos que pueden asegurar los contenidos y la identidad de las partes que se comunican y realizan transacciones en Internet, dentro de los cuales se pueden mencionar:

Biométrica

Es la ciencia de la identificación de personas sobre la base de sus datos físicos. El Consorcio sobre Biométrica es una organización sin fines de lucro del gobierno de los Estados Unidos para la Investigación, desarrollo, pruebas y aplicaciones de la biométrica a la identificación y verificación de personas. Un ejemplo de biométrica es el sistema de clasificación de las huellas digitales descubierto por el argentino Juan Vucetivh y que es

⁷⁷ “PKI o los Cimientos de una Criptografía de Clave Pública” www.iec.csic.es/criptonomicon/susurros/susurros11.html, agosto,2004.

hasta el presente el sistema más difundido de identificación de personas, por ser simple y preciso pues no existen dos huellas digitales iguales.⁷⁸

Hoy se están investigando otros sistemas relacionados con el iris del ojo, la geometría de la mano, la voz y las facciones. Los sistemas que se están investigando son:

Huellas digitales: En esta línea algunas técnicas emulan el clásico sistema policial mencionado, algunas tratan de detectar cuando la huella corresponde a un dedo “vivo”. Estas técnicas son de buena precisión, salvo errores de uso. La verificación por huella digital puede ser para sistemas del hogar donde los usuarios pueden ser adecuadamente entrenados y por sus bajos costos y pequeños tamaños de los detectores, que por ejemplo pueden ser integrados a los teclados de las computadoras.

Geometría de la mano: Se trata de la medición de las características físicas de manos y dedos desde una perspectiva tridimensional. Estos sistemas son adecuados a bases de muchos usuarios con acceso infrecuente y pueden estar menos predispuestos y disciplinados a ser detectados. La precisión puede ajustarse hasta ser elevada y son técnicas muy flexibles a los escenarios.

Verificación por voz: Potencialmente muy atractivo para las actividades de negocios, pero al momento son muy sensibles a las condiciones de aproximación y externas, por ejemplo, la acústica del recinto. Por otra parte, la colección de los registros puede ser conflictiva y compleja.

⁷⁸ “Biométrica”, www.aunmas.com/guias/criptologia/biometrica.htm, Septiembre, 2004.

Barrido de la Retina: Una conocida tecnología muy precisa en la que la delicada retina es barrida por una luz de baja intensidad vía un acoplador óptico, pero requiere que la persona mire dentro de un receptáculo y enfoque su mirada hacia un punto. Esto es un inconveniente si la persona usa anteojos o tiene escrúpulos en contactar el receptáculo.

Barrida del Iris: El barrido del iris es sin lugar a dudas la tecnología menos intrusa pues se utiliza una cámara CCD convencional y no requiere contacto íntimo entre el sistema de registro y la persona. Su precisión es buena y no hay problemas en los registros de personas con anteojos o lentes de contacto. Ha sido probada con varios grupos étnicos.⁷⁹

Reconocimiento facial: Una técnica controvertida. Desde el punto de vista del usuario es atractiva, pero presenta muchas dificultades prácticas, tales como reconocer una cara dentro de un grupo, algo diferente a realizar el contraste entre dos imágenes. Resueltos los inconvenientes técnicos es evidentemente una tecnología de auspicioso futuro.

Existen otras técnicas tales como el uso de perfumes, marcas indelebles y los lóbulos de las orejas, pero no son considerados como aplicables en forma masiva.

79 Ídem

CAPÍTULO 4

CONSENTIMIENTO POR MEDIOS ELECTRÓNICOS

Sumario 4.1 Introducción. 4.2 Del Consentimiento: Definición. 4.3 Elementos del Consentimiento. 4.4 Sujetos del Consentimiento. 4.5 Etapas del Consentimiento: 4.5.1 Oferta, 4.5.2 Aceptación. 4.6 Formas del Consentimiento 4.7 Momento del Perfeccionamiento. 4.8 Vicios del Consentimiento: 4.8.1 Error, 4.8.2 Fuerza, 4.8.3 Dolo. 4.9 El Consentimiento en las Redes.4.9.1 Etapas del Consentimiento: Oferta y Aceptación en las Redes.4.9.2 La Perfección del Contrato Celebrado en la Red.

4.1. Introducción

El consentimiento como base de cualquier contrato, es sin lugar a dudas, aspecto indispensable dentro de esta investigación. Así la Teoría del Consentimiento debe ser comprendida en su forma tradicional para luego aplicarse a la formación del consentimiento en materia de contratación electrónica, tomando aquí en cuenta ciertas circunstancias que presentan dificultades adicionales en este tipo de contratación como el hecho de que las partes nunca están en presencia una de la otra. Por ello este capítulo inicia con el estudio del consentimiento de la manera que la doctrina tradicional lo

presenta, para que, solamente después, se inicie con la adecuación del consentimiento y sus etapas en el mundo de la contratación electrónica, determinando los puntos o consideraciones esenciales que deben de tenerse en cuenta para la presentación de este trabajo de investigación.

4.2 Del Consentimiento. Definición

Tradicionalmente, el consentimiento es el requisito más importante para la existencia y validez del acto jurídico, pues en definitiva este elemento afecta directa o indirectamente a los demás requisitos.

El consentimiento como se deduce de su propia raíz etimológica (cum sentire “sentir con”), es la coincidencia (conformidad o acuerdo) de dos o más voluntades distintas y contrapuestas sobre el contenido del contrato que celebran. Este es un acto bilateral a diferencia de la voluntad que es un acto unilateral.⁸⁰

El concepto señalado anteriormente, es el más conveniente para definir el consentimiento, por hacerlo de una forma sencilla y clara, y a la vez por apegarse a lo establecido por consentimiento en el Art. 1316 No. 2 de nuestro Código Civil, que dice: “Para que una persona se obligue a otra por un acto o declaración de voluntad es necesario: 2º Que consienta en dicho acto o declaración y su consentimiento no adolezca de vicio”.

Para que se dé el consentimiento se requieren determinadas condiciones a las que la doctrina las llama requisitos, los cuales son:

80 CLARO SOLAR, Luis. “**Explicaciones de Derecho Civil Chileno y Comparado**”. Tomo X. De las Obligaciones, Santiago, Chile, 1992, pág. 54.

Pluralidad de sujetos: Por ser el consentimiento, la concurrencia de dos o más voluntades, se exige una pluralidad de sujetos o partes contratantes.

Capacidad de las partes: Este requisito no es un presupuesto de la existencia del consentimiento propiamente dicho, sino de la validez y eficacia del negocio jurídico; pero en definitiva viene a determinar la validez y eficacia de la concurrencia de voluntades.

Existencia de una voluntad contractual: La voluntad interna e individual de cada contratante ha de dar lugar al consentimiento o voluntad contractual, por el cual se establece una reglamentación de intereses. Estas voluntades deben ser conscientes, deliberadas y libres, pues si falta el discernimiento o la libertad de alguna de las partes el consentimiento está viciado.

La manifestación del consentimiento o Declaración de voluntad contractual: La voluntad carece de eficacia jurídica en tanto o se manifiesta mediante una declaración; es decir, la voluntad interna debe manifestarse para que pueda ser conocida por la otra parte y los demás terceros.

Concordancia entre lo declarado y lo internamente querido: Para que este requisito se cumpla debe valorarse la intención de cada contratante y que ésta corresponda con su manifestación.⁸¹

81 LETE del RÍO José M., “**Derecho de Obligaciones**” volumen II, Segunda Edición, Tecnos, Madrid, España, 1995. Pág. 35-37

4.3 Elementos del Consentimiento:

Para comprender el consentimiento se tienen que conocer algunas nociones generales sobre los elementos que lo constituyen, los cuales según la doctrina, son dos:

Intención: Llamada por algunos autores voluntad interna, por formar parte del fuero interno de la persona, se requiere de que sea seria, consciente del resultado jurídico, que persigue, esto implica que deben desestimarse todas aquellas situaciones en que se obra o actúa, por cortesía o complacencia desde luego que no dan nacimiento a situaciones de Derecho.

Manifestación de la Intención: El derecho no toma en cuenta, lo que sucede en el fuero interno del individuo, por lo tanto, no basta la sola intención, para hablar de voluntad jurídica, es preciso que esa intención se exteriorice, en cualquier forma, siempre y cuando se descubra claramente la intención del autor, salvo, por supuesto, que se requiera una manera determinada de hacerlo, como sucede en los actos y contratos solemnes.⁸²

El consentimiento, de acuerdo a estos elementos puede manifestarse expresa o tácitamente, tanto una como otra forma tienen igual valor, con excepción de que la ley o las mismas partes exija o requiera un modo especial de manifestación.

4.4 Sujetos del Consentimiento:

Todo contrato, cualquiera que sea su naturaleza o calificación, cualquiera que sea la obligación que engendre para una o ambas partes, supone el consentimiento de las

⁸² COREAS BENAVIDES, Miguel Ángel y otros, “El consentimiento en el Derecho Civil Salvadoreño”, Tesis, UNSSA, Noviembre, 2000, Pág. 41 y 42

mismas, porque nace del acuerdo de voluntades; sin él no hay contrato. Sólo quedan afectados los que han concurrido con su voluntad a celebrarlo; son las partes contratantes que han expresado su voluntad a celebrarlo, quienes pueden beneficiarse con los derechos que engendre o ser afectadas por las obligaciones que crea. Estas partes siempre estarán constituidas por uno o más que ofrecen y uno o más que aceptan, a los cuales se les denominará: **oferente o peticente, y aceptante.**

Oferente o Peticente: Es toda persona que propone a otra, la celebración de un negocio jurídico, sobre bases ciertas y determinadas.

Aceptante: Es aquella persona a quien va dirigida la oferta y ésta a la vez manifiesta su aceptación, ya sea en forma expresa o tácita.

Estas partes son las que le dan fisonomía al consentimiento, y cada una de ellas puede formarse de la voluntad o acuerdo de voluntades de una o más personas; es del concurso de estas voluntades que se forma el consentimiento. Es por eso que quien no ha concurrido con su voluntad, es decir, quien no ha expresado su consentimiento para generar un contrato, es un tercero ajeno al mismo, y no goza de ningún derecho ni responde a obligación alguna generada de la expresión del consentimiento.⁸³

4.5 Etapas del Consentimiento:

El consentimiento no es otra cosa que el acuerdo de voluntades de parte de los contratantes, quiere decir que en su formación tienen que existir dos etapas, representada

83 ALESSANDRI RODRÍGUEZ, Arturo y SOMARRIVA UNDURRAGA, Manuel, “Curso de Derecho Civil”, Tomo IV, Fuente de las Obligaciones, Editorial Nascimento, Santiago de Chile, 1842. Pág. 27

cada una por la voluntad de cada uno de los contratantes. Estas etapas tienen un nombre propio: la *oferta*, constituida por la voluntad del que propone el contrato, y la *aceptación*, constituida por la voluntad de la persona a quien se ofrece el contrato.

4.5.1 Oferta, Policitación o Propuesta: Es una declaración de voluntades por medio de la cual una persona propone a otra u otras la celebración de un negocio jurídico. Se trata de una propuesta completa, precisa y definitiva que expresa la intención de celebrar un contrato en el caso de que la otra parte, a quien va dirigida, la acepte. Por consiguiente, si la oferta no es aceptada tal y como ha sido formulada, sino que la persona a quien va dirigida introduce cambios o modificaciones en la misma, se habrá generado una **segunda oferta o contraoferta**.⁸⁴

Para que una iniciativa sea considerada como oferta debe tener los siguientes requisitos:

Debe ser voluntaria: Es decir, emitida libremente, ya que constituye la voluntad de uno de los contratantes.

Debe ser seria: Con la intención de producir efectos jurídicos.

Debe ser completa: Hecha en forma tal, que para el nacimiento del contrato solo falte el sí de la otra parte; es decir, debe contener todos los elementos esenciales del negocio.

Debe Exteriorizarse: Lo que puede hacerse en dos formas:

84 CLARO SOLAR, Luis. Ob. Cit. Pág. 56

Expresa: Cuando es hecha en términos explícitos que revelan la intención inequívoca del proponente de contratar. Esta manifestación de voluntad puede ser hecha verbalmente o por escrito, personalmente o por medio de mandatario.

Tácita: Cuando se deduce de determinados sucesos o actos emanados del proponente.

Debe ser Emitida con intención de concluir el contrato: Se refiere a que la declaración de voluntad por parte del ofertante ha de manifestarse de un modo que inequívocamente revele el propósito de vincularse contractualmente.

Debe ir dirigida a la persona con la cual el ofertante desea concluir el contrato: Es decir, a la persona que el proponente conoce o con quien desea contratar, aunque también puede dirigirse a persona indeterminada o al público en general.⁸⁵

Generalmente estos requisitos son los expresados por la doctrina, la cual los retoma de los lineamientos generales del Derecho Civil.

Una vez manifestada la oferta puede **extinguirse** en los siguientes casos:

Cuando es rechazada expresamente por el destinatario.

Cuando es revocada o retirada por el ofertante, antes de la perfección del contrato.

Cuando transcurre el tiempo o plazo establecido por el proponente para la aceptación. Si no se hubiere fijado plazo, deberá considerarse en vigor durante el tiempo necesario, atendida a la naturaleza del contrato, según la buena fe o los usos.

Cuando se produce la muerte o la incapacidad sobrevenida del ofertante.

⁸⁵ LETE del RÍO José M., Ob. Cit. Pág. 62

La oferta no requiere una forma especial o determinada, salvo cuando se trate de aquellos contratos para los que se exige una cierta forma, como por ejemplo, aquellos que requieren de determinadas formalidades para volverlos más solemnes.

4.5.2 Aceptación: Es una declaración de querer celebrar el contrato tal y como había sido propuesto por el ofertante. Es la respuesta afirmativa a una oferta; no es necesario que contenga todos y cada uno de los puntos esenciales del contrato, simplemente se requiere conteste afirmativamente o asiente mediante algún gesto.⁸⁶

La aceptación requiere de los siguientes requisitos:

Ser seria: Con la determinada intención de producir efectos jurídicos.

Ser voluntaria: Emitida sin coacción alguna, en libertad completa por la persona que la expresa.

Debe coincidir en todas sus partes con la oferta: Debe ser aceptada tal y como fue propuesta originalmente, de no ser así, se constituye en una nueva oferta.

Dirigirla al ofertante.

Realizarla dentro del plazo: Debe hacerse antes de que se revoque la oferta.

Debe Exteriorizarse: Al igual que la oferta debe realizarse de dos maneras:

Expresa: Cuando se hace en términos explícitos y formales, sea verbalmente o por escrito, personalmente o por medio de un mandatario.

⁸⁶ Ídem. Pág. 63

Tácita: Cuando se deduce de ciertos actos que manifiestan inequívocamente la intención de aceptar.⁸⁷

Para que se lleve a cabo la aceptación, tal como en el caso de la oferta, deben de concurrir los requisitos antes señalados, los cuales son analizados a partir de la regulación que de la Aceptación hace el Derecho Civil.

Si la propuesta es aceptada pura y simplemente, tal como es formulada, y sin la menor variación o agregación, se verifica el concurso real de las voluntades de las dos partes, y el contrato queda en el acto perfeccionado y listo para producir efectos legales.

4.6 Formas del consentimiento:

Las partes son libres para someter a los contratos que celebren, los requisitos de forma, que les plazcan, siempre que no prescindan de los exigidos por la ley; así lo contempla el Art. 23 de la Constitución de la República al decir: “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 determinar sus asuntos civiles o comerciales por transacción a arbitramento...”, al mismo tiempo el Art. 22 de la misma contiene el Principio de Libre Disposición de los Bienes cuando dice: “Toda persona tiene derecho a disponer libremente de sus bienes conforme a la ley. La propiedad es transmisible en la forma en que determinen las leyes...”; con base en estos las personas puede decidir

⁸⁷ Ídem Pág. 64

libremente el querer ser o no sujetos de derechos y obligaciones, a través del acuerdo de voluntades, es por esto que para las formas de manifestación del consentimiento la voluntad de cada una de las partes puede expresarse de diversas maneras, personalmente o por medio de mandatario, representantes, intérpretes, corredores o mensajeros, sea de palabra, emitida verbalmente, por teléfono, radio, o Internet, sea por escrito mediante instrumento público o privado, manuscrito, impreso, dactilografiado o reproducido o transmitido por cualquier medio mecánico (fotografía, telegrama, etc.) sea por hechos, signos o actitudes que la revelan de un modo inequívoco.⁸⁸

La voluntad de las partes puede manifestarse de dos formas:

En Forma Expresa: Es cuando el consentimiento se manifiesta, mediante términos formales y explícitos, es decir, lenguaje hablado, escrito o mímico.

En Forma Tácita: Es el consentimiento que se deduce, de hechos o actos que la manifiestan o permitan suponerla de un modo inequívoco. Se exterioriza por actos concluyentes, cuando el sujeto no manifiesta de un modo directo su voluntad sino que realiza una determinada conducta que, por suponer necesariamente tal voluntad, es valorada por el ordenamiento jurídico como declaración.⁸⁹

4.7 Momento del Perfeccionamiento:

La determinación del momento en que el contrato se perfecciona no plantea problemas cuando éste se celebra entre personas presentes. La cuestión se complica

88 COREAS BENAVIDES, Miguel Ángel, Ob. Cit. Pág. 45

89 LETE del RÍO José M. Ob. Cit. Pág. 64

cuando las personas que han de consentir se encuentran ausentes, o encontrándose en el mismo lugar no quieren reunirse.

Entre Presentes: Cuando se celebra el contrato entre personas presentes, la participación del consentimiento se confunde con su manifestación; hablar y oír son entonces hechos simultáneos; la oferta es dada a conocer y su aceptación debe acompañarla en el acto mismo para que el contrato se forme; no mediando esta aceptación inmediata la oferta se extingue como tal y el oferente queda libre de todo compromiso, como si no hubiera hecho la oferta. Entre presentes, además, la aceptación, tan pronto como es manifestada, llega al conocimiento del proponente quien queda así impuesto inmediatamente de la celebración del contrato.⁹⁰

Entre Ausentes: Este contrato es el celebrado entre personas lejanas, y el problema que presenta es el determinar cuando queda perfeccionado el contrato; porque la carta del proponente puede haber sido escrita y expedida, el telegrama del proponente puede haber sido enviado, sin que el destinatario sepa nada de ello; y la carta o el telegrama de aceptación de la oferta recibida por la persona a quien iba dirigida, pueden haberse hecho y estar aun en viaje, o bien el aceptante puede haber procedido a ejecutar el contrato ofrecido, sin que el proponente se halle enterado de nada de esto. Por consiguiente, hay necesidad de indagar en qué momento y en qué lugar se ha realizado la participación del consentimiento y con ella el vínculo contractual, si en el momento y lugar en que se produce la aceptación de la oferta, o en el momento y lugar en que el proponente recibe y queda impuesto de la aceptación.

90 CLARO SOLAR, Luis, Ob. Cit. Pág. 75

Las legislaciones positivas, los escritores y la jurisprudencia se han dividido al tratar de resolver el problema antes planteado en dos sistemas: **El Sistema de Declaración y el Sistema de Información.**⁹¹

El Sistema de la Declaración: Este sistema es conocido también de Aceptación o Emisión y establece que el contrato se forma por la simple aceptación de la oferta. Cuando la aceptación se junta a la oferta, hay concurso de dos voluntades; esta unión constituye el consentimiento por sí sola; y por lo mismo, la convención queda formada.

El Sistema de la Declaración no es presentado, sin embargo, por todos los autores de la misma manera; y puede subdividirse en tres clases diversas: **La declaración sensu strictu, la expedición y la recepción.**

La Declaración en sentido estricto, es aquella en la que el vínculo contractual se perfecciona en el momento mismo en que la aceptación de la oferta se declara de cualquier manera; es decir, la aceptación hace el contrato perfecto desde el instante en que tiene lugar, y no solamente a partir del momento en que llega al conocimiento de aquel que ha hecho la oferta.

La Expedición: Según esta teoría no basta la manifestación de la aceptación, sino que es necesario que ésta sea dirigida al oferente, aunque no es necesario que éste la haya recibido. En este caso el consentimiento se formará cuando el

91 Ídem. Pág. 75

destinatario envíe o remita su aceptación, en otras palabras, cuando se desprende de ella.⁹²

La Recepción: Esta exige que el documento material que contiene la aceptación llegue a poder del proponente, entendiéndose perfeccionado el contrato por el hecho de llegar la aceptación a su casa, aunque el proponente, por ausencia, enfermedad o cualquier otra causa no adquiriera conocimiento de la misma.

Este sistema es muy criticado por el contenido de sus dos primeras teorías ya que estas dejan en manos del aceptante la formación del negocio jurídico lo cual acarrea perjuicios al oferente; y es para salvar esta crítica que surge la tercera teoría partiendo de la base de que el consentimiento se perfecciona cuando la aceptación llega a su destino.

Sistema de la Información: Llamado también de la cognición o del conocimiento, exige para el perfeccionamiento del contrato entre ausentes, no solo que se haya declarado la voluntad de aceptar la oferta, sino también que la declaración de la aceptación haya llegado a noticia del proponente; es decir no basta que el destinatario acepte o envíe la aceptación, sino que esta debe ser conocida por el oferente.⁹³

Este sistema adopta una postura contraria al sistema de declaración, pero siempre es criticado por que la información del consentimiento queda en manos de un solo sujeto, que en este caso es el que propone el negocio jurídico.

92 Ídem. Pág. 78

93 Ídem.

4.8 Vicios del Consentimiento:

Para la validez del acto jurídico, no solo se requiere que las partes consientan en dicho acto, sino que su consentimiento no adolezca de vicio el cual es aquel que se presenta en la manifestación o declaración de la voluntad como todo hecho contrario a la libertad y conocimiento con que la declaración debe ser formulada. Los vicios de los cuales puede adolecer el consentimiento son: Error, Fuerza y Dolo, así lo establece el Art. 1322 de nuestro Código Civil.

4.8.1 Error:

El Error es la falsa noción que se tiene de una cosa o de un hecho. Consiste, por lo tanto, en ese estado intelectual en que la idea de la realidad se halla oscurecida u ocultada por una idea falsa. En cambio la ignorancia es la ausencia de toda noción de una cosa o de un hecho; sin embargo, jurídicamente error e ignorancia se valoran igual, puesto que la noción errónea sobre una cosa o un hecho es ignorancia de la verdad, y, en consecuencia, la ley se refiere indistintamente con una expresión u otra al supuesto de insuficiente conocer de las cosas o de los hechos.⁹⁴

Se distinguen dos clases de errores: *el error de derecho y el error de hecho.*

Error de Derecho, es el falso concepto que se tiene de la ley, o su ignorancia. Esta clase de error no vicia el consentimiento según lo regula el Art. 1323 C.C.

⁹⁴ LETE del RÍO, Ob. cit, Pág. 41.

Error de Hecho, es el falso concepto o ignorancia que se tiene de una cosa, de una persona o de un acontecimiento. Este lo contemplan los Art. 1324, 1325 y 1326C.C y se tiene como efectivo vicio del consentimiento cuando recae sobre aspectos esenciales o determinantes de las personas, actos o cosas que influyen en la voluntad de los sujetos para decidirse a consentir; más no será así, cuando el error recaiga sobre aspectos hasta cierto punto insignificantes dentro de la formación del consentimiento.

El error de derecho recae, por consiguiente, sobre una regla de derecho, es decir, sobre el derecho objetivo; el error de hecho recae sobre hechos jurídicos, es decir, sobre las condiciones exigidas para la aplicación de una regla de derecho.

4.8.2 La Fuerza:

La Fuerza, violencia o intimidación es el constreñimiento o presión ejercido sobre la voluntad del que hace la declaración, y que resulta de la amenaza de un mal considerable y grave. La Fuerza puede ser *física* o *moral*, siendo *física* la que reduce a la víctima a un estado puramente pasivo y *moral* aquella acción ejercida sobre la voluntad por medio de amenazas, es decir, un temor inspirado con cierto fin.

Para que la fuerza asuma el carácter de vicio del consentimiento y pueda invalidar el acto o contrato, debe reunir tres requisitos:

Debe ser Determinante: Es decir, que la violencia empleada debe ser expresamente para imponerle la obligación de dar el consentimiento.

Debe ser Injusta: Esto se refiere a que la fuerza debe ser contraria a derecho que consista en hechos ilícitos, estén o no penados por la ley.⁹⁵

Debe ser Grave: Producir una impresión fuerte en una persona de sano juicio, tomando en cuenta su edad, sexo y condición.

Estos requisitos son los que toma en cuenta el Art. 1327 C.C. que dice: “La Fuerza no vicia el consentimiento, sino cuando es capaz de producir una impresión fuerte en una persona de sano juicio, tomando en cuenta su edad, sexo y condición. Se mira como una fuerza de este género todo acto que infunde a una persona un justo temor de verse expuesta a ella, su consorte o alguno de sus ascendientes a un mal irreparable y grave. El temor reverencial, esto es, el solo temor de desagradar a las personas a quienes se debe sumisión y respeto, no basta para viciar el consentimiento”.

4.8.3 El Dolo:

Es toda especie de maniobras reprobadas por la buena fe, que una persona emplea para hacer que otra persona incurra en un error que la determine a contratar. Es decir que constituye un acto o una omisión, dañosa a otro, que ha sido ejecutada con el propósito de perjudicarlo, sea por pura maldad, sea con el deseo de realizar un provecho. Este vicio del consentimiento se encuentra regulado expresamente en los Arts. 1329 y 1330 C.C.

El Dolo puede dividirse en: **principal o determinante y Accidental o Incidental.** El primero de ellos es el que ha sido el motivo determinante de la

⁹⁵ COREAS BENAVIDES, Miguel Ángel y otros, Ob. cit, Pág. 53

declaración de voluntad, el que ha determinado a la parte engañada a contratar, y el que efectivamente vicia el consentimiento y da lugar a la rescisión del contrato en virtud de la acción de la parte que ha sido víctima del dolo. Este es el que regula el Art. 1329 Inc. 1º C.C. que establece: “El dolo no vicia el consentimiento sino cuando es obra de una de las partes, y cuando además aparece claramente que sin él no hubieran contratado”. El segundo es aquel en virtud del cual una persona, determinada por lo demás a contratar es engañada sobre algunos accesorios o accidentes del contrato; este no vicia el consentimiento porque no lo determina, solo da lugar a la indemnización de perjuicios que debe pagar la persona que se ha aprovechado de él. Es el Inc. 2º del Art. 1329 C.C. el que lo contempla de la manera siguiente: “En los demás casos el dolo da lugar solamente a la acción de perjuicios contra la persona o personas que lo han fraguado o que se han aprovechado de él; contra los primeros por el total valor de los perjuicios, y contra las segundas hasta concurrencia del provecho que han reportado del dolo.

De lo expuesto anteriormente se puede concluir que los vicios del consentimiento suponen, pues, que la convención ha podido formarse, porque el acuerdo de voluntades se ha producido; pero el consentimiento de las partes o de una de ellas se halla viciado hasta el punto de que pueda anularse el contrato.

4.9 El consentimiento en las Redes:

La contratación y el consentimiento electrónico representan una nueva modalidad constitutiva de obligaciones, no se trata de una nueva fuente de la obligación, sino 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.

Par la formación del consentimiento en materia de contratación electrónica, se debe determinar que para que este quede expresado electrónicamente y sea válido, las partes deben ser capaces, lo cual en materia de negocios electrónicos implica serias dificultades, teniendo en cuenta que las partes nunca están en presencia una de la otra; sin embargo en este caso las precauciones para que no se cometan defraudaciones estarán a cargo del proveedor de productos o servicios a través de la red, es decir de la persona que a través por ejemplo de una página web ofrece determinados bienes.⁹⁶

El consentimiento en las redes, como se puede colegir de lo antes mencionado, no presenta mayores cambios que el consentimiento tradicional, debido a que lo innovador es que se realiza mediante la utilización de algún elemento electrónico, con influencia decisiva, real y directa sobre la formación de la voluntad.

4.9.1 Etapas del Consentimiento: Oferta y Aceptación en las Redes.

La oferta electrónica, es definida como aquella declaración unilateral de voluntad que una persona realiza a través de medios de comunicación y/o medios informáticos,

96 CUBILLOS VELANDIA, Ramiro y RINCÓN CARDENAS, Erick, Ob. Cit. Pág. 158.

invitando a otra persona a la celebración de una convención que quedará perfeccionada con la sola aceptación de esta.⁹⁷

La oferta, en general, puede ser hecha en forma verbal o escrita. A su vez también existen la oferta expresa y la oferta tácita. En particular, es importante mencionar la oferta electrónica, que es hecha en forma escrita por regla general. Sin embargo, no debe dejarse de lado que existen ofertas electrónicas que también se pueden efectuar en forma verbal, o mediante el uso de comunicaciones electrónicas siendo específicas la oferta telefónica, vía fax, etc.

Debe considerarse que la oferta electrónica constituye una oferta escrita, ya que constituye un texto alfanumérico o gráfico en lenguaje de bits y por lo tanto no existe razón válida para no considerarla como una oferta escrita. En todo caso este es un problema que tiene directa relación con el documento electrónico entendido como documento escrito. Lo mismo se aplica a la aceptación electrónica y que se considera, según lo expresado, como aceptación escrita.

Entre las ofertas electrónicas, se puede clasificar las ofertas realizadas a través de Internet, en los siguientes términos:

Realizadas vía *e-mail* o *correo electrónico*: Son aquellas que se envían a ordenadores determinados. Es de tener en cuenta que la mayoría de los casos el usuario de una cuenta de correo electrónico es quien solicita que le sea enviada tal clase de información.

Realizadas *on line*: son ofertas que se encuentran en forma permanente en las redes y a las cuales se tiene acceso navegando por diferentes páginas, pero estas no llegan a los

⁹⁷ Ídem, Pág. 160.

ordenadores, sino que se accede a ellas a través de visitas a ciertos *web sites*. Constituyen ofertas a personas indeterminadas.⁹⁸

Desde el punto de vista jurídico, la oferta electrónica es perfectamente admisible en el sentido de que no necesita ninguna formalidad específica para su emisión, así lo establece el Art. 11 de la Ley Modelo de UNCITRAL sobre comercio electrónico al expresar: “En la formación de un contrato de no convenir las partes otra cosa la oferta y la aceptación podrán ser expresadas por medio de un mensaje de datos”; pero es necesario mencionar que para que esta oferta sea considerada como verdadera y obligue al oferente es de vital importancia que quede de manifiesto de manera indubitada la intención de este de obligarse, lo cual exige el cumplimiento de los siguientes requisitos:

Ser completa: de manera que el destinatario pueda limitarse simplemente a aceptar. Esta circunstancia reviste aun mayor importancia en la contratación celebrada vía Internet, en razón de que en la mayoría de los casos el destinatario de la oferta se limita a “**pinchar o hacer clic**” sobre un icono en la página web para emitir su aceptación sin posibilidad de modificación de las cláusulas contenidas en la oferta. Debe quedar de manifiesto la voluntad del oferente de concluir un contrato con el destinatario o destinatarios de las ofertas.⁹⁹

Ser precisa: cumplir con todos los elementos esenciales del tipo de contrato que se desea llevar a cabo; en los casos de las ventas en Internet se deben cumplir los requisitos establecidos en la normativa sobre las ventas a distancia.

98 Ídem, Pág. 162.

99 Ídem, Pág. 164.

Debe tener un plazo de duración: es importante que los oferentes establezcan el período 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.

No obstante estos requisitos, cabe señalar que el oferente debe actuar de buena fe, es decir, el derecho a modificar la oferta que se reserva el oferente debe ser comunicado debidamente al destinatario, quien podrá aceptar o no la modificación de la oferta. Todo ello en el bien entendido de que todavía no hay aceptación y por tanto el contrato no se ha perfeccionado.¹⁰⁰

La oferta por Internet debe reunir determinadas condiciones de validez, dentro de las cuales se encuentran:

Identidad del Proveedor: Esta identidad debe entenderse en forma amplia, es decir incluyendo sus signos distintivos, especificaciones de su ubicación física, situación por demás importante en el caso de que se trate de un establecimiento netamente virtual careciente de sede física.

Características Especiales de los Productos: Los productos ofertantes deben precisarse de forma clara, así también las funciones y especificaciones de los mismos.

Precio: Esta determinado de forma clara o deben establecerse inequívocamente los criterios para su determinación.

100 FERNÁNDEZ FERNÁNDEZ, Rodolfo, “Contratación Electrónica: La Prestación del Consentimiento en Internet”. J. M. Bosch Editor, Barcelona, España, 2001, Pág. 37.

Gastos de transporte: Deben estar separados del precio, y están determinados en base a la distancia, el costo, cualidades especiales del producto y la rapidez en la recepción del mismo.

Forma de pago: Las modalidades de pago deben estar determinadas con claridad, o en su caso las condiciones de crédito posible.

Modalidades de Entrega: Pudiendo ser de *forma instantánea* (al tratarse de un software o un producto de forma digital), o través del *envío de mercancía* (al tratarse de un objeto físico).

Plazo de validez de la oferta: La oferta debe de permanecer abierta durante un período de tiempo razonable dependiendo de las circunstancias, del tipo de transacción o del deseo del oferente de obtener una respuesta rápida.

Plazo de ejecución del pedido: Los plazos deben estar de antemano por el vendedor según la distancia en que se encuentra el comprador y sobre la base de los medios de transporte escogidos.¹⁰¹

Estas condiciones de validez son las que sirven de parámetros para diferenciar la oferta contractual de una simple publicidad en la web la cual no es más que una parte del espacio que esta dirigido a divulgar los productos o servicios de una empresa en general, esta tiene un carácter genérico y va dirigido a exteriorizar una conducta empresarial, divulgando conceptos.

101 CUBILLOS VELANDIA, Ramiro y RINCÓN CÁRDENAS, Erick, Ob. cit. Pág. 165-168.

A efectos de la aceptación, esta puede definirse como aquella declaración unilateral de voluntad que una persona realiza a través de medios de comunicación y/o medios informáticos manifestando su conformidad a una propuesta recibida.

Al igual que la oferta, la aceptación puede ser expresa o tácita y también puede ser pura y simple o estar bajo término o condición. La aceptación pura y simple es aquella en que se demuestra total concordancia con la oferta realizada. En cambio, la aceptación condicional se emite con reservas o condicionamientos que modifican los términos de la oferta, en otras palabras una contraoferta.

Esta técnica contractual clásica se conoce como *teoría del espejo*, ya que 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 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 de ella.

Existen ciertas circunstancias o requisitos que son necesarios para que se forme el consentimiento electrónico y ellos son los siguientes:

Debe ser congruente con la oferta: El contenido de la aceptación debe coincidir con el de la oferta para que pueda darse la declaración conjunta común del oferente y el aceptante.

Debe ser oportuna: Ser hecha mientras la oferta se encuentre vigente, es decir a tiempo, debiendo ser recibida por el oferente durante el tiempo de vigencia de la oferta fijada por el oferente o por la ley.

Debe ser dirigida al oferente: No puede ser dirigida a otra persona diferente a este, o sea que quien ha formulado la propuesta.¹⁰²

Respecto a las modalidades que se pueden presentar en la aceptación *on-line*, se tiene:

Se puede manifestar por vía e-mail, partiendo de la base de que la oferta se hizo por este medio;

Por medio de mensajes electrónicos a través de sistemas EDI;

A través de un “clic” en el botón de una página de Internet que contenga una oferta;

Bajando los contenidos de la red, y que se entienda por parte del proveedor de servicio y por parte del usuario, que esta es una forma de aceptación.

Las mayores dificultades que se derivan de la aceptación en entornos electrónicos se relacionan directamente con la inclusión de condiciones generales de contratación en el entendido de que gran parte de los contratos celebrados vía Internet, son contratos de adhesión que impiden la negociación de las cláusulas en ellos

102 Ídem, Pág. 172.

contenidas, cláusulas que por lo general no se encuentran insertadas en forma directa, clara y visible en la misma página web sino que se incluyen de manera indirecta a través de un link que envía al usuario a otro sitio de la red. El problema se agrava en razón de que en la aceptación por medio de impulsos electrónicos, en los denominados contratos clic-wrap agreements o point-and-click agreements, estas condiciones ni siquiera son de acceso al aceptante llegando en algunos casos a emitirse la aceptación con total desconocimiento de las condiciones generales que rigen el contrato, ocasionando graves perjuicios a los usuarios de la red.¹⁰³

4.9.2 La Perfección del Contrato Celebrado en la Red:

La contratación electrónica se caracteriza por la ausencia y distancia entre las partes en la perfección del negocio, aunque no en términos absolutos debido a que el tiempo transcurrido entre oferta y aceptación puede llegar a ser muy reducido, por lo que para muchos autores parecería una nueva modalidad de contrato entre ausentes o a distancia, con condicionantes y características totalmente novedosas que la distinguen de la contratación a distancia tradicional o realizada por medios distintos.

Para otros autores, no puede considerarse una contratación a distancia porque esta deja de reunir aspectos típicos de la misma cuando se contrata en tiempo real, ya sea porque las partes se encuentran conectadas a una misma *web site* simultáneamente y expresan sus declaraciones de voluntad en línea, o porque estas incluyen a sus

103 Ídem. Pág. 170

comunicaciones voz e imagen, permitiendo que la contratación en línea se acerque cada vez más a una contratación presencia.¹⁰⁴

Estos planteamientos antes mencionados conllevan a concluir que, si bien es cierto las posturas doctrinales clásicas pueden enmarcar aspectos característicos de estas nuevas contrataciones, ninguna de ellas puede aplicárseles; debido a que si una contratación se realiza por correo electrónico sería similar a la aceptación hecha por carta o por cualquier otro medio de contratación entre ausentes, donde no necesariamente existe inmediatez en la prestación de los respectivos consentimientos contractuales, en cambio cuando si pueda producirse la inmediatez y exista un intercambio sucesivo y continuado de mensajes entre las partes contratantes se podría asimilar a un contrato entre presentes, dejando claro que las figuras tradicionales de la forma en que se da el consentimiento han quedado desfasadas haciendo necesaria la creación de nuevas figuras.

Momento de la Perfección:

Es importante destacar, que es fundamental pactar el momento exacto en que la oferta se considera realizada y aceptada. Para el caso específico de las contrataciones efectuadas por redes abiertas, si las partes no acuerdan el momento en que se considera realizada la aceptación, debería entenderse que ha sido hecha cuando el oferente recibe un mensaje del aceptante expresando su acuerdo sobre la propuesta realizada.

104 FERNÁNDEZ FERNÁNDEZ, Rodolfo. Ob. cit. Pág. 34

Para solventar ciertos problemas que presenta lo anterior, se ha sentado un nuevo principio de perfección en el contrato electrónico denominado “*Principio de Acuse de Recibo*” o “*Teoría de la Confirmación*”, que exige para la perfección del contrato celebrado electrónicamente, no solo la recepción y conocimiento por el oferente, sino además también la notificación de la recepción de nuevo al aceptante, por medio de mensaje.¹⁰⁵

Este sistema de perfección es el más novedoso hasta el momento, y a la vez práctico ya que no presenta mayor complejidad y resulta más sencillo probar su existencia, lo que dota de seguridad jurídica a la contratación electrónica, con lo cual esta se distancia de las teorías de los momentos de perfeccionamiento por los que pasan las declaraciones de voluntad del oferente y aceptante que informa la contratación bajo la comunicación no inmediata, esto debido principalmente a la naturaleza de los medios empleados.

Lugar de la Perfección

El concepto del lugar de realización o perfeccionamiento del contrato, es decir, del lugar donde se forma el consentimiento tiene gran relevancia porque normalmente la ley que rige al contrato es la del lugar donde se forma. Lo mismo pasa con la costumbre que debe aplicarse dependiendo del lugar, también tiene importancia para las cuestiones penales pues dependiendo del lugar se declara el tribunal competente.

105 Ídem. Pág. 67

No existe problema alguno partiendo del hecho que oferente y aceptante residen en un mismo lugar. La problemática surge cuando ambos residen en lugares distintos; y es aquí donde el principio de Libertad Contractual juega un papel importante, ya que la práctica comercial y sobre todo la contratación a través de medios electrónicos se caracteriza por adoptar la figura de un contrato de adhesión, como fue expresado anteriormente, en los cuales el ofertante a través de las cláusulas pre constituidas del mismo incluye la determinación de la normativa aplicable la cual por lógica comercial será aquella que más le favorece y por consiguiente ese será el lugar de perfeccionamiento del contrato, quedando de esta manera pactado de forma expresa. A falta de esta clase de pacto y de normativa aplicable que establezca cosa distinta, podría deducirse atendiendo al Principio de Acuse de Recibo que el lugar de perfeccionamiento del consentimiento será el lugar de domicilio del aceptante, esto en virtud de lo determinado por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (UNCITRAL) en el Art. 15.4 de la Ley Modelo sobre Comercio Electrónico de dicha Comisión, el cual establece: ***“De no convenir otra cosa el iniciador y el destinatario, el mensaje de datos se tendrá por expedido en el lugar de donde el iniciador tenga su establecimiento y por recibido en el lugar donde el destinatario tenga el suyo”***, constituyéndose así en un lineamiento general que siguen la mayoría de países que cuentan con regulación de este tipo.

CAPÍTULO 5

LA SEGURIDAD JURÍDICA DE LA FIRMA DIGITAL

Sumario 5.1 Introducción. – 5.2 Eficacia Jurídica de la Firma Digital.- 5.3 Delitos Informáticos. 5.3.1 Definición, 5.3.2 Características, 5.3.3 Clasificación.- 5.4 Documento Electrónico, 5.4.1 Definición, 5.4.2 Características, 5.4.3 Clasificación. 5.4.4 Desmaterialización. 5.4.5 Valor Probatorio.

5.1 Introducción

Algunos de los recientes problemas jurídicos han surgido porque muchas de nuestras leyes fueron desarrolladas a través de largos períodos de tiempo durante los cuales los medios físicos eran los únicos mecanismos, o por lo menos los más comunes e importantes, para realizar transacciones jurídicamente válidas.

Hoy en día, con ocasión del uso de las tecnologías digitales de comunicación están realizándose analogías a fin de evitar que la validez de una comunicación electrónica o de cualquier documento electrónico se supedite a su reproducción o un medio físico (ejemplo de ello el papel). En consecuencia este fenómeno ha generado la necesidad de reexaminar algunos conceptos fundamentales que ahora deben ser extendidos a un mundo digital.

5.2 Eficacia Jurídica de la Firma Digital

Actualmente el ritmo de los negocios ha impuesto que la manera de exteriorizar acuerdos de voluntad sea más ágil y dinámica, al realizar transacciones o celebrar contratos entre partes que ni siquiera se conocen, y por medios totalmente digitales. Pero para que se pueda dar el consentimiento en este tipo de contratación, las partes necesitan, además de un elemento al que pueda atribuírsele los mismos propósitos que los de la firma convencional, de un sustento por medio del cual el Estado les brinde la debida seguridad y eficacia como base para la utilización de esta clase de medios.

La eficacia jurídica de la firma digital va a estar determinada por la normativa existente sobre la misma en cada contexto en que se desarrolle, así el principio del que debe partir esta normativa es que el documento firmado digitalmente tiene la misma validez y eficacia que un documento tradicional en soporte papel debidamente firmado.

La firma ológrafa o manuscrita ha sido reconocida entre otras cosas como mecanismo de expresión del consentimiento, como requisito de validez para algunos actos y como forma de autenticación de documentos; aspectos que no son ajenos a la firma digital salvo con la única diferencia que se aparta un poco más de su representación habitual, ello debido a que es el resultado de la realización de un proceso

matemático desarrollado con soporte tecnológico;¹⁰⁶ ya que en esencia, la naturaleza de la firma digital es la de expresar la autoría de la declaración de voluntad del signatario, siendo lo mismo en el caso de la firma manuscrita diferenciándose en la forma en como se representan.

En definitiva puede establecer que la utilización de la firma digital puede ser tanto o más útil, válida y eficaz en el comercio electrónico y en el derecho, como la firma escrita sobre papel.

5.3 Delitos Informáticos

Las redes de comunicación electrónica y los sistemas de información forman parte integrante de la vida diaria de los ciudadanos en el mundo y juegan un papel fundamental en la economía universal; ello sin duda tiene evidentes ventajas, las cuales no han sido acompañadas por un desarrollo equivalente de defensas adecuadas contra su mala utilización, llegando a generar hechos ilícitos que se cometen o facilitan mediante el empleo de ordenadores, viniendo estos a ser los mismos que desde hace milenios las sociedades han castigado de una forma u otra, y aunque algunas categorías penales tradicionales muestran cierto grado de inadecuación respecto a las nuevas modalidades delictivas, estos se han denominado “Delitos Informáticos”.¹⁰⁷

106 SARRA, Andrea Viviana, Ob. cit., Pág. 366.

107 GUIBOURG, Ricardo y otros, Ob. cit., Pág. 221.

Establecer un concepto sobre delitos informáticos no es labor fácil y esto en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de delitos, es decir, las acciones contempladas en textos jurídico-penales, se requiere que la expresión delitos informáticos este consignada en los códigos penales o alguna otra ley especial, lo cual en algunos países, para el caso el nuestro, no ha sucedido aún; y es por esto que se hace necesario establecer parámetros que conduzcan a la tipificación de estos delitos.

5.3.1 Definición:

Por Delito Informático se entenderá: “cualquier acción ilegal en la que el ordenador sea el instrumento o el objeto del delito; es decir son conductas típicas, antijurídicas y culpables que se cometen a través de medios electrónicos o contra ellos”.¹⁰⁸ De este concepto, puede inferirse que la esencia del concepto de Delito sigue siendo la misma que tradicionalmente se conoce debido a que, lo que siempre se busca es la protección de un bien jurídico. Lo que se consigue, en este caso, ampliando la tutela del mismo en razón de la inclusión de medios electrónicos ya sea como el lugar en el que se cometen o como el instrumento que se utiliza para cometerlos.

5.3.2 Características:

Entre las características de los Delitos Informáticos se pueden mencionar:

Son conductas delictivas de cuello blanco, pues solo determinado número de personas con ciertos conocimientos pueden llegar a cometerlos.

108 Idem. Pág. 274.

Son acciones ocupacionales, porque en ocasiones se realizan cuando los sujetos están trabajando.

Son acciones de oportunidad porque aprovechan una ocasión creada.

Provocan serias pérdidas económicas para los afectados y casi siempre producen grandes beneficios económicos a quienes lo realizan.

Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundo y sin la necesaria presencia física puede llegar a cometerse.

Son muchos los casos y pocas las denuncias, todo ello debido a la falta de la misma regulación jurídica a nivel internacional.

Son sumamente sofisticados y frecuentes en el ámbito militar.

Presentan grandes dificultades para su comprobación, por su mismo carácter técnico.

En su mayoría son dolosos o intencionales, aunque también hay muchos de carácter culposos o imprudenciales.

Ofrecen facilidades para su comisión a los menores de edad.

Tienden a proliferarse cada vez más, por ello requieren una urgente regulación jurídica.¹⁰⁹

109 TÉLLEZ VALDÉZ, Julio, “**Derecho Informático**”, Tercera Edición, Instituto Tecnológico y de Estudios Superiores de Monterrey, Mc Graw Hill, México, D.F., 2004. Pág. 163.

Las personas que cometen ese tipo de delitos son aquellos que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible o bien son hábiles en el uso de los sistemas informatizados, aún cuando, en muchos de los casos, no desarrollan actividades laborales que facilitan la comisión de este tipo de delitos.

5.3.3 Clasificación:

Los Delitos Informáticos han sido objeto de las más variadas clasificaciones, según el punto de vista de los autores que las han propuesto. Así, han sido agrupados según el perjuicio causado, o el papel que el computador desempeña en su perpetración o el modo de actuar, o el tipo penal en el que se encuadran, o la clase de actividades que cada delito implique respecto de los datos involucrados.¹¹⁰

Debido a que este trabajo de investigación no tiene como objeto un estudio detallado de los delitos informáticos, no se hará un estudio amplio de los mismos, y es por ello que la clasificación que se presenta a continuación representa solo un panorama de las acciones que se consideran como delitos informáticos.

¹¹⁰ GUIBOURG, Ricardo, Ob. cit. Pág. 274.

Clasificación de Delitos Informáticos

CARACTERÍSTICAS	
Delitos	Fraudes cometidos mediante manipulación de computadoras
Manipulación de los datos de entrada	Este tipo de fraude informático, conocido también como sustracción de datos, representa el delito informático más común, ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.
La manipulación de programas	Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.
Manipulación de los datos de salida	Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a partir de tarjetas bancarias robadas, sin embargo, en la actualidad se usan equipos y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias.
Fraude efectuado por manipulación informática	Aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina técnica del salami en la que “rodajas muy finas” apenas perceptibles de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

CARACTERÍSTICAS	
Delitos	Falsificaciones Informáticas
Como objeto	Cuando se alteran datos de los documentos almacenados en forma computarizada.
Como instrumento	Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras puede hacer copias de alta resolución, pueden modificar documentos e incluso crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.
Acceso no autorizado a sistemas o servicios	Por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hacker) hasta el sabotaje o espionaje informático.
Piratas informáticos o hackers	El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema, esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.
Reproducción no autorizada de los programas informáticos	Ésta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, reproducción no autorizada de programas informáticos es un delito informático debido a que el bien jurídico a tutelar es al propiedad intelectual.

CARACTERÍSTICAS	
Delitos	Daños o modificaciones de programas o datos computarizados
Sabotaje informático	<p>Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:</p> <p>Virus</p> <p>Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.</p> <p>Gusanos</p> <p>Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos, podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus; por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.</p> <p>Bomba lógica o cronológica</p> <p>Exige conocimientos especializados, ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.</p>

Los Delitos desarrollados en el cuadro anterior no constituyen la totalidad de los que se pueden realizar en este medio, pero son los que han alcanzado un alto grado de difusión; y frente a esto algunos juristas proponen la sanción de nuevas normas para encuadrarlos más específicamente, mientras algunos otros opinan que se deben aplicar las normas jurídicas preexistentes a esta nueva forma de cometer delitos. Independientemente de estas dos posturas, lo importante es que estas conductas sean contempladas en un contexto jurídico lo suficientemente completo y uniforme a nivel internacional para que todas las formas de ataques contra los sistemas de información puedan ser objeto de investigaciones mediante técnicas y métodos disponibles en Derecho Penal.¹¹¹

5.4 Documento Electrónico:

Tradicionalmente, el concepto de documento se vincula a un cuerpo o soporte material que plasma, representa o incorpora una expresión, un derecho, una obligación, entre otros. Ese cuerpo se ha considerado como la base esencial o el ser mismo del documento, en su sentido amplio es toda representación material destinada e idónea para reproducir cierta manifestación de pensamiento.

La fusión de la informática y las nuevas técnicas de comunicación, así como la transferencia electrónica de datos, que permite intercambiar mensajes electrónicos en

111 TÉLLEZ VALDÉZ, Julio. Ob. cit. Pág. 175

lugar de documentos escritos, son elementos del actual contexto digital que revalúan la concepción tradicional del documento y da lugar a los documentos electrónicos.

5.4.1 Definición:

Técnicamente el Documento Electrónico es un conjunto de impulsos electrónicos que recaen en un soporte de computadora, y que sometidos a un adecuado proceso, permite su traducción al lenguaje natural a través de una pantalla o una impresora. Cabe aclarar que lo que se lee en la pantalla o lo impreso no son el documento electrónico original sino copias, ya que el original no se podrá utilizar directamente, debido a que su contenido no puede ser aprehendido por nuestros sentidos.¹¹²

Al referirnos al documento electrónico se alude a que el lenguaje magnético constituye la acreditación, materialización o documentación de una voluntad ya expresada en las formas tradicionales, y en que la actividad de una computadora o de una red solo comprueban o consignan electrónica, digital o magnéticamente un hecho, una relación jurídica o una regulación de intereses preexistentes. Se caracterizan porque solo pueden ser leídos o conocidos por el hombre gracias a la intervención de sistemas o dispositivos traductores que hacen comprensibles las señales digitales.

El análisis de la temática del documento electrónico debe abarcar la necesidad de otorgar la más eficaz y basta utilización de los medios de información que se intercambian electrónicamente y la necesidad de tutelar la confianza de los usuarios en la seguridad de los nuevos documentos; razón por la cual, deben recibir el mismo

112 Ídem. Pág. 247

tratamiento de los documentos consignados en papel, es decir, debe dársele la misma eficacia jurídica, por cuanto el documento electrónico comporta los mismos criterios de un documento.¹¹³

5.4.2 Características:

El documento en soporte electrónico, informático y telemático posee las mismas características en cuanto a su validez jurídica que el documento tradicional que consta en soporte papel, y dentro de estas se encuentran:

Inalterabilidad: Hace referencia a que el contenido del documento no se puede alterar, y que si esto ocurre existen medios para comprobar dicha alteración, llegando a carecer de valor real el documento, convirtiéndose en falso.

Autenticidad: Un documento es auténtico cuando es generado por quien dice ser su autor.

Durabilidad: El documento electrónico perdura en el tiempo debido a que el soporte en el que se da su reproducción, es de carácter indeleble, es decir, que permanece estable en el tiempo y no puede ser alterado sin dejar huella alguna.

Seguridad: Con el desarrollo de algunas técnicas que se emplean en el documento electrónico, este es al menos, equivalente en cuanto a seguridad, al instrumento escrito y firmado sobre un soporte papel.¹¹⁴

113 CUBILLOS VELANDÍA, Ramiro y RINCÓN CÁRDENAS, Erick, Ob. Cit. Pág. 223

114 TÉLLEZ VALDÉZ, Julio. Ob. Cit. Pág. 248

Estas características del documento electrónico permiten que éste no sea la simple transcripción sino la reproducción completa y fiel de la forma y contenido del documento original preexistente.

5.4.3 Clasificación:

De acuerdo al grado de conservación de los documentos electrónicos estos pueden clasificarse en:

De carácter Volátil: Como los datos contenidos en las memorias de circuitos RAM (Random Access Memory), los cuales se pierden inmediatamente al cortar la energía a la computadora.

Permanentes: Son aquellos contenidos en algunas memorias de masa como discos compactos, cintas y floppy disk. A diferencia de la anterior categoría, los datos allí almacenados desaparecen sólo al ser borrados, en caso contrario se mantienen en el tiempo.

Inalterables: Son aquellos que una vez grabados no pueden ser alterados, sólo leídos. Dentro de estos encontramos las memorias RAM (Read Only Memory), que consiste en un circuito o chip integrado a la computadora o que se le puede incorporar a la voluntad y los CD-ROM, que son una memoria de masa contenida en un disco láser.¹¹⁵

Esta clasificación representa uno de los tantos criterios con base en los cuales se clasifican los documentos electrónicos, y debido a que se considera que es la más sencilla y clara para su entendimiento, razón por la cual se han retomado en la presente investigación.

115 Ídem. Pág. 251

Desmaterialización:

Se llama “Desmaterialización”, al proceso por medio del cual un documento de papel es transformado en un documento electrónico. La principal ventaja de este proceso es la reducción de los típicos asociados con el envío de documentos de papel y el ahorro de tiempo y dinero; es por ello que muchas compañías están abandonando la práctica de realizar negocios a través de papel, inclinándose a favor del uso del intercambio electrónico de datos (EDI), ya que es prácticamente un aspecto intrínseco de la desmaterialización pues en definitiva un documento desmaterializado es un grupo de récords creados a partir de mensajes electrónicos.

La Desmaterialización puede ser *total* o *parcial*:

Total: Es aquella en la que el documento es creado, circulando y negociando electrónicamente sin que el mismo sea el producto de la transformación de un documento de papel a un documento electrónico.

Parcial: En ésta el documento es creado en forma física, pero las transacciones sobre él se realizan electrónicamente. En este caso, usualmente el documento de papel es depositado en un banco o en una central de registro donde es convertido en documento electrónico para realizar operaciones sobre el mismo.

Existen críticas sobre la utilización del término desmaterialización cuando éste se emplea en el caso de documentos que son creados electrónicamente sin que previamente fuesen emitidos en medios materiales. Estas tienen base en el hecho de que

sólo puede desmaterializarse lo que previamente está dotado de materia; y todo aquél que nunca ha sido materia (desmaterialización total) es un documento inmaterializado.¹¹⁶

Se puede concluir, que la desmaterialización en la actualidad es el mecanismo más utilizado por los países tanto en la Administración Pública como en el sector privado porque facilita y agiliza las transacciones electrónicas.

5.4.4 Valor Probatorio:

La noción de documento desde el punto de vista jurídico es el resultado de una larga evolución consuetudinaria, legislativa y científica que se ha ligado a la valoración legal de los medios de prueba en materia contractual. Por tanto, para estos fines la prueba documental debe ser entendida en el sentido más amplio posible comprendiendo, en consecuencia, también los modernos medios electrónicos de información, sean estos circuitales o constituidos por mensajes electrónicos sobre soportes magnéticos, o sean documentos formados por el elaborador.

Si bien el tema probatorio ha avanzado significativamente en nuestra sociedad las implicaciones de este en medios electrónicos digitales representa un reto conceptual y práctico para los organismos que imparten justicia¹¹⁷.

Al momento de enfrentar un proceso judicial, los medios probatorios tradicionales son elementos fundamentales para determinar y configurar la imagen

¹¹⁶ Grupo de Estudios en Internet, Comercio Electrónico & Telecomunicaciones e Informática. Ob. Cit. Pág. 23 y 24
¹¹⁷ Ídem. Pág. 84

completa de los hechos y valorar los mismos para establecer la sentencia sobre el caso en la investigación.

Sin embargo, al aportarse elementos digitales al caso en estudio, se plantea una revisión diferente de los medios, dado que las instituciones judiciales no cuentan con suficiente conocimiento para analizarla y valorarla. Si bien la normativa actual establece directrices y estrategias para la valoración de prueba en los casos, no presenta elementos particulares sobre material en medios tecnológicos, haciendo un vacío procedimental y normativo en estos temas.

El documento electrónico es admisible en aquellos países donde está consentido el sistema de libre apreciación de la prueba, esto, siguiendo a las reglas de la sana crítica para aquellos medios de prueba que no están excluidos de forma expresa en la ley. En este sentido, el juzgador deberá atribuirle a ese medio de prueba no contemplado en la ley, validez y fuerza probatoria luego de la adecuada valoración del mismo. Por ello, algunos países han tomado a bien la admisión de los medios electrónicos como instrumentos probatorios, afirmando que los computadores y los medios electrónicos deben sumarse a las herramientas jurídicas procesales, puesto que son una expresión de la realidad que el derecho no puede desconocer.¹¹⁸

Entre todas las legislaciones, aquella que dio un paso adelante en esta materia fue la Legislación Francesa, al promulgar en 1980 una ley que modificaría su Código Civil, y otorgándole a los documentos electrónicos la misma validez y eficacia probatoria que

118 VARGAS FRONTERA, Ginay del Valle. “Valor Probatorio de los medios electrónicos en el Derecho Comparado, particularmente en las legislaciones mexicana, española, francesa, chilena, argentina y venezolana”, Informe de investigación jurídica, Guayana, 2003.

aquellos que constan en soporte de papel. Luego fue la Legislación Española, en 1992, con la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común; pero no es sino hasta 1997 que se incorpora en Estados Unidos, en Utah, Georgia, California y Washington. En Europa, fue Alemania el primero en considerar esta materia.

En cuanto a la validez del documento electrónico y su equivalencia al documento tradicional, la ley modelo sobre comercio electrónico señala en su Art. 5 bajo el título de “Reconocimiento Jurídico de los mensajes de datos”, el principio de equivalencia funcional al decir: “No se negarán efectos jurídicos, validez o fuerza obligatoria a la información por sola razón de que esté en forma de mensajes de datos”, así es como este principio implica fundamentalmente la no discriminación respecto de las declaraciones de voluntad independientemente de la forma en que haya sido expresadas; en consecuencia, los efectos jurídicos surten efecto indistintamente del soporte en papel o electrónico conste la declaración.¹¹⁹

En nuestro país, en materia procesal civil no existe norma alguna que otorgue valor probatorio al documento electrónico, debido a que el sistema de valoración de prueba obedece a la regla tasada; por ello la regla general a seguir consiste en la no aceptación de documento electrónico alguno como medio probatorio. Sin embargo, existen leyes especiales que si le otorgan este valor.

Existen normas que, principalmente en materia financiera, hacen referencia a la utilización de medios electrónicos en esta rama, y que desde luego aunque no lo

119 Ídem.

contempla expresamente, sí le otorgan valor probatorio a los documentos electrónicos; algunas de estas son: La Ley de Bancos, La Ley Orgánica de la Superintendencia de Valores, La Ley del Mercado de valores, La Ley General Marítimo y Portuaria, La Ley de Mediación, Conciliación y Arbitraje, las cuales serán desarrolladas posteriormente.

En materia penal, con las reformas de 1998, se incorporan nuevos elementos de prueba, admitiéndose en el proceso las siguientes: las grabaciones y elementos de prueba audiovisuales, de acuerdo con el Art. 351 del Código Procesal Penal,¹²⁰ además de la incorporación de modernas disposiciones sobre la prueba: la libertad de prueba y la valoración de la misma (Art. 162 Pr.Pn.), donde todos los hechos y circunstancias pertinentes relacionadas con el delito, podrán ser probadas por cualquier medio legal de prueba, y los jueces deberán valorarlas de acuerdo a las reglas de la sana crítica.

Es así, como en El Salvador sólo se presume el valor probatorio de los documentos electrónicos en algunas leyes, no así en materia procesal civil en donde ninguna norma incluye estas nuevas modalidades de prueba, haciendo urgente y necesario que se le otorgue al documento electrónico el valor probatorio que se merece.

120 Recopilación de Leyes en Materia Penal, 4ª edición, Editorial Jurídicas LIS, El Salvador, 2001.

5.5 Análisis de la Legislación de la Firma Digital:

5.5.1 A nivel internacional:

En el mundo, el comercio electrónico es un fenómeno que está creciendo y desarrollándose rápidamente, principalmente por las facilidades que brinda a los usuarios, entre ellas la flexibilidad y la disminución en el costo de las operaciones. No obstante el notable incremento en las relaciones comerciales, existen factores que impiden un mayor desarrollo del comercio electrónico, uno de ellos es la inseguridad al momento de realizar transacciones electrónicas, debido a un sistema jurídico que no está suficientemente instrumentado para recoger las exigencias del mismo.

Algunos países más desarrollados ya tienen normas en funcionamiento, las cuales permiten crear documentos seguros, mediante el denominado sistema de firmas electrónicas, basado en certificados electrónicos emitidos por entidades de certificación. La regulación de la firma electrónica y la digital significa un avance en el establecimiento de un marco jurídico respecto de las tecnologías de la información.

En relación con la situación del uso de las mencionadas firmas, cabe señalar que aunque está plenamente justificada su existencia, a partir de la celebración de contratos o de transacciones económicas o compras que se realice a través de medios electrónicos, todavía es perceptible que existe un rechazo social a la utilización de estos; lo cual se debe, en parte, al nivel de inseguridad que impera entre los usuarios al momento de realizar una operación de ese tipo, por desconocer la identidad del destinatario y receptor

de los mensajes o documentos electrónicos, en la veracidad y autenticidad de su contenido y en cuanto a la validez del documento electrónico, entre otros.

Con la finalidad de tener un panorama general de la situación en que se encuentra la firma digital, a continuación se presenta un breve detalle de la legislación que algunos países han emitido con respecto al tema:

Organismos Internacionales

Unión Europea (UE)

Los lineamientos generales en torno de los cuales se enmarcan los proyectos normativos sobre firma digital, encriptación y promoción del comercio electrónico, dentro de la Unión Europea, están contenidos en diversas directivas, resoluciones y comunicaciones del Parlamento y Consejo europeos.

Resolución del Parlamento Europeo del 19 de septiembre de 1996. en ella el Parlamento por resolución A4-244/96, solicitó a la Comisión de Iniciativa Europea sobre Comercio Electrónico la preparación de lineamientos concernientes a la seguridad de la información, la confidencialidad, la firma digital y la protección de la privacidad.

Resolución del Consejo de Ministros de la Unión Europea. El 21 de noviembre de 1996, el Consejo de Ministros adoptó una serie de medidas para asegurar la integridad y

autenticación de instrumentos transmitidos digitalmente, mediante resolución 96/C376/01.

Comunicación del Comité Económico y Social del Comité de las Regiones al Parlamento Europeo y al Consejo Europeo del 16 de abril de 1997. En su comunicado sobre comercio electrónico COM (97) 157, la Comisión de Iniciativa Europea sobre Comercio Electrónico anunció su intención de elaborar una política encaminada a garantizar la libre circulación de las tecnología y los productos de encriptación e instó al desarrollo de un marco político al efecto, para lo cual se establecieron pautas generales sobre la regulación de la criptografía en orden a fomentar la utilización de la firma y la moneda digital, de entre las cuales resalta el establecer un marco jurídico-tecnológico para la firma digital dentro de la Unión Europea, y aseguran el funcionamiento del mercado interno para los productos y servicios sobre criptografía.

Audiencia de la Unión Europea sobre firma digital y encriptación. Fue realizada en Copenhague el 23 y 24 de abril de 1998 y tuvo como objetivo la exploración del uso y desarrollo de la firma digital y la encriptación. Este encuentro tuvo la característica de que, además, de participar en él los países miembros de la Unión Europea, estuvieron presentes representantes de Australia, Canadá, Estados Unidos de América, Japón, Noruega y Suiza.

Propuesta para una directiva del Parlamento y Consejo europeo para un marco común para la firma digital. La propuesta COM (98) 297, del 13 de mayo de 1998, fue redactada acorde con las recomendaciones de la dirección general XIII de la Comisión Europea que, a principios de 1998, había formulado el Anteproyecto de Directiva de un Marco para los Servicios de Certificación Electrónica. La Directiva de la Unión Europea propone una regulación general de la prestación de servicios de la sociedad de la Información, de las comunicaciones comerciales, la validación jurídica de la celebración de contratos por vías electrónicas, la protección de los consumidores extrajudicial de litigios y la celeridad en vía judicial.

Organización para la Economía, Cooperación y Desarrollo (OECD)

El 27 de marzo de 1997 se establecieron los principios que sirvieron de base a los países miembros para la formulación de sus propias políticas relacionadas con el uso de la criptografía. Estos intentos a escala internacional son los primeros en tratar de aportar políticas orientativas en varios aspectos de la criptografía.

Entre el 2 y 4 de junio de 2000, en California, el Comité de Políticas para la Información Computadoras y Comunicaciones de la OECD, llevó a cabo una reunión de trabajo sobre tecnologías de autenticación electrónica. Algunos de los temas analizados fueron similitudes y disparidades existentes entre los métodos tradicionales de autenticación y los electrónicos, en relación con el entorno en que son utilizados, y los

diferentes métodos de autenticación, como los mecanismos de autenticación electrónica, las firmas basadas en criptografía de clave pública y los métodos biométricos.

Organización de las Naciones Unidas (ONU)

Dentro de esta organización se han dado diferentes documentos, con la finalidad de ayudar a la unificación de la normativa en materia de Comercio Electrónico y sobre esta base la regulación de la firma digital, entre los cuales destacan:

Ley Modelo sobre Comercio Electrónico de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (UNCITRAL por sus siglas en inglés). Fue aprobada por el plenario de esta comisión en su 29º período de sesiones, celebrado en New York del 28 de mayo al 14 de junio de 1996 y la Asamblea General de la ONU la aprobó mediante resolución 51/162 el 16 de diciembre de 1996. Esta ley constituye un modelo de referencia para fomentar la armonización y unificación progresivas del derecho mercantil internacional, garantiza la seguridad jurídica y provee una legislación que facilite el uso del comercio electrónico en Estados con sistemas jurídicos diferentes. A su vez propicia el reconocimiento jurídico de los documentos electrónicos estableciendo estándares mínimos de requisitos de forma y establece definiciones referidas al proceso de comunicación de “mensajes de datos”.

Ley Modelo de Firma Electrónica de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional: En el año 1997, dentro del período 30 de sesiones de esta Comisión se empezó con la inquietud de conformar un régimen uniforme sobre cuestiones relativas a las firmas digitales, las entidades certificadoras y asuntos conexos; pero hasta en junio de 2001, fue presentada a consideración de los miembros de la comisión para su aprobación en el período de 34 sesiones, junto con su respectiva Guía para la incorporación, la cual al igual que la ley fueron preparadas a partir del supuesto previsto en el artículo 7 de la Ley Modelo sobre Comercio Electrónico, correspondiente a las consideraciones jurídicas relacionadas con la firma.

La Ley Modelo en comento, es una propuesta a los Estados para que incorporen a su derecho interno, algunas disposiciones relacionadas con estos mecanismos de seguridad tecnológica, teniendo en cuenta sus limitaciones, procedimientos y las condiciones propias de su ordenamiento jurídico. Aborda lineamientos relacionados a las técnicas denominadas firmas electrónicas y de la manera de proporcionarles a estas equivalentes funcionales de las firmas manuscritas y de otros tipos de mecanismos de autenticación empleados en el soporte de papel; así como también pautas referidas a los servicios de certificación digital, fijando criterios para evaluar la conducta de las partes involucradas, es decir, el firmante, el tercero que confía en el certificado y el prestador de servicios de certificación.

Cámara de Comercio Internacional (ICC)

La propuesta de la ICC de desarrollar lineamientos internacionales sobre los aspectos jurídicos del comercio electrónico y el establecimiento de una cadena internacional de registración y autoridades de certificación, surgió en noviembre de 1995 en el contexto de un grupo de trabajo abocado a la temática del comercio electrónico. Después de denominar las Prácticas Internacionales Uniformes de Autenticación y Certificación (UIACP), se decidió llamarla Convención General para el Comercio electrónico y la Firma Digital Internacional (GUIDEC), la cual pretende delinear los elementos esenciales del comercio electrónico, que puedan servir como indicador de términos y una exposición del entorno general de la temática.

Europa

Alemania

Desde hace algunos años, el comercio electrónico está siendo objeto de estudio en diversos foros internacionales y nacionales a nivel mundial, siendo Alemania el país pionero en implementar su regulación y en elaborar el primer proyecto de ley de firma digital en Europa. Es así como el 20 de diciembre de 1996, el gobierno alemán presentó al Parlamento una legislación sobre firma digital. Ella contiene los detalles técnicos del uso de firmas digitales en Alemania, así como las normas para el funcionamiento de las autoridades de certificación (que son denominadas “certificadores”), la validez de los

certificados, los componentes técnicos utilizados para firmas digitales y otros asuntos similares.

Esta ley fue aprobada el 13 de junio de 1997, y está vigente a partir del 1º de agosto de ese año. Las primeras autoridades certificantes en el marco de la nueva ley fueron licenciadas en 1998 y el primer notario público digital alemán está en funcionamiento como autoridad certificante en el Instituto para Telemática en Trier¹²¹.

La ley en cuestión, es bastante técnica y no regula la validez legal de las firmas digitales. Su finalidad es proporcionar las condiciones para una infraestructura segura para el uso de firmas digitales en Alemania; aunque el cumplimiento de la ley es voluntario, la intención del gobierno alemán es que actúe *estándar de facto* para el uso de firmas digitales; a pesar del intenso debate, se decidió finalmente, no incluir previsión alguna relativa a la responsabilidad. Muchas cuestiones de detalle están contenidas en la *Digital Signature Ordinance* y en catálogos de seguridad para componentes técnicos y autoridades de certificación; además, el Ministerio de Justicia está trabajando en otras normativas relativas al efecto legal y la validez de las firmas digitales.

Debido a la necesidad de adaptación a la directiva comunitaria de firma electrónica, se halla en fase avanzada de elaboración una nueva ley sobre la materia.

España:

En España han surgido en los últimos tiempos distintas iniciativas en materia de firma digital y autoridades de certificación; la mayoría de ellas, sin embargo, al menos

121 SARRA ANDREA, Viviana. Ob. Cit. Pág. 178

inicialmente, en el ámbito de las administraciones públicas, y como consecuencia de la apertura hacia la mayor tecnificación y modernización de las administraciones, basada en la utilización de medios electrónicos y Telemática, propugnada por el artículo 45 de la Ley 30/1992, de 26 de diciembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento administrativo común, desarrollado por el Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de tales técnicas por la Administración General del Estado, delimitando las garantías, requisitos y supuestos de utilización de las mismas¹²².

Con base en estos lineamientos y a las iniciativas a nivel internacional ya existentes como el Proyecto de Directiva del Parlamento Europeo sobre firma electrónica por el Consejo de Ministros de Telecomunicaciones de la Unión Europea, aprobado el 22 de abril de 1999; es el 16 de Julio de 1999 cuando se aprueba en España el Anteproyecto de ley de firma digital para adecuar la legislación interna a las exigencias del Proyecto del Parlamento Europeo. Pero este se aprueba hasta el 18 de septiembre de 1999 como Real Decreto ley 14/1999 de 17 de Septiembre, tras la urgencia de la regulación española de firma electrónica, con la peculiaridad de que al momento que esta se aprueba, la propuesta comunitaria no estaba definitivamente aprobada; arriesgándose a que se produjeran divergencias entre la legislación española y la comunitaria cuando esta se aprobara.¹²³

122 Ídem Pág. 103

123 Ídem. Pág. 106 y107

El Real Decreto 14/1999 estaba formado por 28 artículos, agrupados en 5 títulos, una disposición adicional única, una disposición transitoria única y tres disposiciones finales; regulaba de forma general, la firma electrónica, -el uso de certificados y el papel de los prestadores de servicios de certificación.

Sin embargo, a la vista del contenido del Real Decreto, podía concluirse que la normativa española no cumplía al menos de forma inmediata, su objetivo de regular y dar seguridad al tema de la validez de los efectos jurídicos de la firma electrónica, pues existían numerosas cuestiones pendientes de regulación. Y es por ello que se crea en el año 2003 una nueva legislación atinente a la firma electrónica.

La ley 59/2003, de 19 de Diciembre, de firma electrónica,¹²⁴ constituye una nueva propuesta para la firma digital en España, esta sustituye al Real Decreto-Ley 14/1999 de 17 de Septiembre, (el cual desde que fue aprobado el Parlamento determinó que tendría que someterlo a una más amplia consulta pública), y adopta la directiva comunitaria 1999/93/CE, de Diciembre de 1999. Esta ley fue elaborada por el Ministerio de Ciencia y Tecnología y aprobada por el Consejo de Ministros, para su posterior ratificación por parte del parlamento, en una búsqueda por reforzar el marco jurídico existente de firma digital, incorporando algunas novedades respecto de Real Decreto Ley 14/1999 que contribuirán a dinamizar el mercado de la prestación de servicios de certificación.

¹²⁴ Ley de España 59/2003. de 19 de diciembre de Firma Electrónica. BOE núm. 304, Sábado 20 de diciembre 2003.

La ley en comento, consta de 36 artículos agrupados en seis títulos, 10 disposiciones adicionales, dos disposiciones transitorias, una disposición derogatoria y tres disposiciones finales. Contiene los principios generales que delimitan 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, así como la regulación de certificados reconocidos y el documento nacional de identidad electrónico. También establece 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; supliendo de esta forma algunos vacíos en cuanto a seguridad y validez de la firma que presentaba la anterior ley.

AMÉRICA

Estados Unidos

En Estados Unidos, es donde más avanzada está la legislación sobre firma electrónica, aunque el proyecto de estandarización del **NIST, The National Institute of Science and Technology** (Instituto Nacional de Ciencia y Tecnología), no lo consiga. El NIST ha introducido dentro del proyecto Capstone, **el DSS, Digital Signature Standard** (Estándar de Firma Digital), como estándar de firma, y a la vez ha equiparado la firma manuscrita y la firma digital.¹²⁵

¹²⁵ <http://dev.abanet.org/scitech/ec/isc/dsgfree.html>. The American Bar Association Section of Science and Technology

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

El valor probatorio de la firma ha sido ya admitido en Utah, primer estado en dotarse de una ley de firma digital. La firma digital de Utah (**Digital Signature Act Utah** del 27 de Febrero de 1995, modificada en 1996) se basa en un “Criptosistema Asimétrico” definido como un algoritmo que proporciona una pareja de claves segura. Sus objetivos son, facilitar el comercio por medio de mensajes electrónicos fiables, minimizar las incidencias de la falsificación de firmas digitales y el fraude en el comercio electrónico. Esta ley establece la presunción de que una firma digital tiene el mismo efecto legal que una firma manuscrita si se cumplen ciertas exigencias; una de las exigencias es que la firma digital sea verificada por referencia a una clave pública incluida en un certificado válido emitido por una autoridad de certificación con licencia. El estado de Utah también ha redactado un proyecto de Ley (The Act on Electronic Notarización) en 1997.

Mientras algunos estados consideran como modelo la ley de **Utah**, algunos estados se mueven hacia sistemas menos reguladores, y no tan específicos tecnológicamente. Así por ejemplo, California y Arizona han aprobado legislaciones que permiten el uso de firmas digitales para transacciones con las entidades públicas de cada estado, autorizando al secretario de estado a dictar normas para alcanzar la finalidad de la ley; otros estados tienen leyes que permiten el uso de firmas electrónicas con finalidades específicas, médicas (Connecticut) o financieras (Delaware). Y hoy día se

está desarrollando una nueva tendencia, como la del estado de Massachussets, que da efecto legal a las firmas y documentos electrónicos, no sólo las firmas digitales, teniendo en cuenta la naturaleza dinámica e impredecible de la evolución tecnológica.¹²⁶

En este sentido, la **Florida Electronic Signature Act** de 1996, que tiene como objetivo el desarrollo del comercio electrónico en el sector público y privado, a diferencia de la ley de Utah, California y Washington, que sólo se refieren a la firma digital, da a las firmas electrónicas la misma fuerza y efectos que las firmas manuales, de forma que todos los tipos de firmas electrónicas existentes y futuras, incluidas las firmas digitales, son ahora iguales legalmente a las firmas manuscritas.

Dada la diversidad de las iniciativas legislativas de los distintos estados, se planteó la necesidad de una ley federal con un contenido uniforme aplicable en todo el país. Y, en este sentido, se ha aprobado, la **Federal Electronic Signatures in Global and National Commerce Act** (2000), conocida, abreviadamente, como «Federal E- Sign Act». Esta ley adopta la técnica legislativa de la CNUDMI estableciendo la no discriminación jurídica de las transacciones realizadas por medios electrónicos- firmas, documentos, registros-; o establecer los estándares técnicos específicos para satisfacer los requisitos mínimos de forma, con resguardo de su neutralidad tecnológica.

126 SARRA, Andrea Viviana, Ob.Cit. pág. 97 y 98.

Argentina

La legislación Argentina con el afán de regular exhaustivamente los temas relativos a la seguridad en los medios electrónicos ha creado un sinnúmero de leyes, decretos, estándares, orientados a proporcionar la protección debida en esta área.

Actualmente se encuentra vigente la Ley No. 25.506 denominada “Ley de Firma Digital”, la cual fue aprobada por el Senado y la Cámara de Diputados de la nación Argentina el 14 de noviembre de 2001 y promulgada el 11 de diciembre del mismo año. Esta ley regula la utilización de la firma digital y de cualquier otro tipo de firma electrónica para la Administración Pública.

La ley No. 25.506, equipara de valor jurídico de la firma digital y de la firma tradicional manuscrita, salvo que se trate de disposiciones de última voluntad (Ej. testamentos, legados), actos jurídicos en las relaciones de familia (Ej. reconocimiento de hijos), actos personalísimos en general (Ej. Donación de órganos), cualquier tipo de actos que sean incompatibles con la utilización de la firma digital, y aquellos en los que dicha incompatibilidad sea establecida por la ley o por las partes. También establece una diferencia entre firma electrónica digital; al igual que desarrolla los certificados de validez, sus requisitos de validez, del certificador licenciado, la creación de la Comisión Asesora para la Infraestructura de Firma Digital, y el establecimiento de la Jefatura de Gabinete de Ministros como autoridad de aplicación de esta ley; a la vez contempla su utilización por parte del Estado Nacional, quien a través del poder Ejecutivo deberá emitir un Reglamento para esta ley.

Con el fin de establecer una Infraestructura de Firma Digital que ofrezca autenticación, y garantía de integridad para los documentos digitales o electrónicos y constituir la base tecnológica que permita otorgarles validez jurídica, en Argentina se emite el decreto 2628/2002, el cual constituye el Reglamento que desarrolla la Ley 25/506, y en este se establecen y desarrollan las facultades tanto de la Jefatura de Gabinete de Ministros, como autoridad de aplicación, al igual que las de la Comisión Asesora para la infraestructura de Firma Digital. También se establece el Sistema de Auditoría, la revocación de los Certificados Digitales, las funciones de las autoridades de Registro, y se detalla un glosario atinente al mismo reglamento.

Colombia

Entre 1996 y 1998 el gobierno de Colombia asistió como observador a la Comisión de Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) y conoció de primera línea los trabajos realizados en materia de comercio electrónico. Con base en los antecedentes legislativos de Colombia y los lineamientos plasmados por el gobierno nacional de fomentar el uso de las tecnologías de la información y comunicación (TIC), así como el deber de las entidades públicas por adoptar mecanismos de transmisión electrónica que permite una mejor prestación del servicio, la delegación observadora resaltó la importancia de adecuar el ordenamiento jurídico colombiano a las tendencias jurídicas universales.¹²⁷

¹²⁷ Grupo de Estudios en Internet Comercio Electrónico & Telecomunicaciones e Informática, Ob. Cit. Pág. 184 y 185.

De tal manera que a través de una Comisión Interinstitucional se abordó la tarea de estudiar la Ley Modelo sobre Comercio Electrónico y de diseñar los mecanismos para su adecuación e incorporación en el ordenamiento interno. La Comisión Redactora fue conformada por funcionarios de los Ministerios de Justicia y del Derecho, Transporte, Desarrollo Económico y Comercio Exterior, y en sus deliberaciones tuvieron una nutrida participación el sector privado, académico y otras entidades públicas.

El fruto de esta labor, que duró cerca de un año, se vio reflejado en el Proyecto de Ley N° 527 presentado a la Cámara de Representantes y culminado el 18 de agosto de 1999 cuando el presidente de la República, Dr. Andrés Pastrana Arango, sancionó la Ley 527 de Comercio Electrónico aprobada por el Congreso de la República; “mediante la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, se establecen las entidades de certificación, y se dictan otras disposiciones”.

Esta Ley contiene 47 artículos, los primeros 27 son la adaptación a Colombia de la Ley Modelo de la UNCITRAL, y presenta exactamente los mismos temas, los demás artículos, tratan de las firmas digitales, los suscriptores, las entidades de certificación y el organismo encargado de vigilarlas. También regula los mensajes de datos, establece algunas definiciones con respecto a la ley y regula a las entidades de certificación.

Costa Rica:

La Ley de Firma Digital y Certificados Digitales (N° 14, 276) que es la que se encuentra vigente en Costa Rica, y que fue promulgada el 22 de febrero de 2001, tiene como objetivo regularla de forma tal, que existan los elementos jurídicos fundamentales para el desarrollo de la Economía Digital en un contexto razonable, más no infalible de seguridad jurídica.

Esta Ley establece primeramente una diferencia entre Firma Digital y Electrónica, establece los entes encargados de regularla, y a la vez determina cual será el órgano rector que se encargará de vigilar los certificados digitales y sus requisitos.

5.5.2 A Nivel Nacional:

El Salvador no está en condiciones de dar respuestas jurídicas apropiadas para las necesidades que requieren los sistemas de implementación del comercio electrónico y las tecnologías vinculadas; sin embargo, existen aproximaciones para regular el tipo de transacciones electrónicas que se están llevando a cabo en nuestro país y éstas son:

Ley de Bancos

La Ley de Bancos que tiene por objeto regular la función de Intermediación Financiera y las otras operaciones realizadas por los bancos, propiciando que estos brinden a la población un servicio transparente, confiable y ágil, que contribuya al

desarrollo del país, establece en su CAPÍTULO II, de las “OPERACIONES PASIVAS”, Art. 56 literal “I”, denominado “Términos de referencia aplicables”, que:

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

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

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

*caso el banco estará obligado a explicar al cliente las implicaciones del contrato, previo a su suscripción”.*¹²⁸

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

En el capítulo III, de las “OPERACIONES ACTIVAS”, Art. 60 inc. 1º, “De los Sistemas de Pagos y las Transacciones Electrónicas”, también se establece:

“Las operaciones activas y pasivas que efectúen los bandos y otras instituciones a través de las cuentas que se manejan en el Banco Central, podrán realizarse mediante el intercambio electrónico de datos. Para tal efecto, tendrá validez probatoria los registros o bitácoras contenidas en los sistemas informáticos, las impresiones que reflejan las transacciones efectuadas por los mismos registros de **firmas digitales** o de números de identificación personal de los participantes autorizados en dichos sistemas. Las certificaciones extendidas, por el funcionario autorizado por el Banco Central para llevar registros y controles de lo anteriormente referido, tendrán fuerza ejecutiva contra la parte que incumplió . Las instrucciones que dicten los bancos al Banco Central, serán de carácter irrevocable”.

Este artículo establece los registros que se llevarán de firmas digitales, aunque en realidad se refiere a firmas electrónicas, confundiéndolas y por lo tanto, regulando protección solamente para las firmas y no las digitales.

¹²⁸ Ley de Bancos, aprobada el 10 de sep. de 1999, sancionada el 27 de sep. de 1999 y publicada en el Diario Oficial No. 181, Tomo 334, del 30 de sep. de 1999.

Ley de Anotaciones Electrónicas de Valores En cuenta:

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

Ley del Mercado de Valores:

La Ley del Mercado de valores tiene como objeto regular la oferta pública de valores y a estos, sus transacciones, sus respectivos mercados e intermediarios y a los emisores, con la finalidad de promover el desarrollo eficiente de dichos mercados y velar por los intereses del público inversionista, disponiendo en sus artículos 27 lit. “b” y 45 que las transacciones se pueden llevar a cabo por **medios electrónicos**, y estos literalmente expresan:

“AUTORIZACIÓN DE OPERACIONES

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

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

OPERACIONES BURSÁTILES

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

- a) Al contado;
- b) A plazo;
- c) Operacionales, de compra o venta; y
- d) Otro tipo de operaciones que autorice previamente la Junta Directiva de cada bolsa mediante la correspondiente incorporación en su reglamento”.

En estas disposiciones la Ley de Mercado de Valores otorga plena validez a las transacciones bursátiles que sean realizadas por medios o procedimientos electrónicos, y como consecuencia de la misma, la necesidad de su respectiva y efectiva regulación, es así como en el reglamento de esta ley se establece los requisitos que deberán reunir los registros electrónicos para brindar la seguridad necesaria a todos los sujetos intervinientes dentro de las actividades del Mercado de Valores.

Ley Orgánica de la Superintendencia de Valores:

Este cuerpo normativo establece y regula las funciones de la Superintendencia de Valores, y dentro de ellas establece en su Art. 38 la facultad que ésta tiene de fiscalizar las contrataciones bursátiles que sean realizadas por medios electrónicos y

telemáticos, efectivos representantes del Comercio Electrónico como forma de contratación y actividad mercantil.

Ley General Marítimo Portuaria:

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

“INTERCAMBIO ELECTRÓNICO DE DATOS

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

La firma podrá ser manuscrita, o bien estampada mediante facsímil o **autenticada por un código electrónico**”¹²⁹.

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

129 Ley General Marítimo Portuaria aprobada el 19 de sep. de 2002

Ley de Mediación, Conciliación y Arbitraje:

Esta ley establece el régimen jurídico aplicable al arbitraje, sin perjuicio de lo dispuesto en los tratados o convenios internacionales vigentes, asimismo, reconoce la eficacia de otros medios alternativos de solución de diferencias, que facultativamente pueden adoptar las personas naturales o jurídicas capaces, en asuntos civiles o comerciales, sobre los cuales tengan la libre disposición de sus bienes y que sean susceptibles transacción o desistimiento. Dentro de todo lo referente al arbitraje que regula la presente ley, al referirse a las modificaciones y comunicaciones preliminares, permite que estas sean por medios electrónicos, y así lo establece el Art. 27 lit. “d”:

“Notificaciones y Comunicaciones Preliminares

Art. 27. Las notificaciones y comunicaciones escritas previas a la iniciación del procedimiento arbitral se registrarán por las siguientes reglas:

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

También cuando esta ley se refiere al Convenio Arbitral en el Art. 29 deja la libertad para que las partes lo realicen por cualquier medio que inequívocamente deje constancia documental de la voluntad de las partes de someterse a arbitraje, y este artículo 29 inc. 3º establece:

“SECCIÓN SEGUNDA DEL ARBITRAJE NACIONAL

CAPÍTULO I

DEL CONVENIO ARBITRAL

Formalidades

Art. 29- El Convenio arbitral deberá constar por escrito inc. 3º Se entenderá que el convenio se ha formalizado por escrito no solamente cuando esté contenido en documento único suscrito por las partes, sino también cuando resulte del intercambio de cartas **o de cualquier otro medio de comunicación o correspondencia** que inequívocamente deje constancia documental de la voluntad de las partes de someterse a arbitraje”.

Si bien es cierto este artículo no establece específicamente que los medios por el que se puede exteriorizar el convenio arbitral son electrónicos, este lo deja la posibilidad abierta para “cualquier otro medio de comunicación o correspondencia”, concluyendo que si es posible utilizar medios de comunicación electrónica.

Ley de Simplificación Aduanera

En El Salvador es esta ley la que más claramente establece un sistema para la implementación del uso de Firma Digital por que tiene por objeto establecer el marco jurídico básico para la adopción de mecanismos de simplificación, facilitación y control de las operaciones aduaneras, a través del uso de sistemas automáticos de intercambio de información. Constituye la base jurídica para el funcionamiento del sistema de Teledespacho, que consiste principalmente en intercambiar información, particularmente de la Declaración de Mercancías, para con la Dirección General de la Renta de Aduanas, lo cual lo define mejor el Art. 6 al establecer: “El despacho de las mercancías podrá ser

solicitado por procedimientos informáticos, mediante el intercambio de información por vía electrónica, a través del sistema conocido como Teledespacho.

Para efecto de esta ley, Teledespacho constituye el conjunto sistematizado de elementos tecnológicos de carácter informático y de comunicaciones que permiten dentro de un marco de mutuas responsabilidades, y mediante los procedimientos autorizados, el intercambio por vía electrónica de información de trascendencia tributaria entre la dirección general, importadores, exportadores y los operadores e instituciones contraloras del comercio exterior en general”.

Esto constituye el inicio en nuestro medio de la introducción de nuevas tecnologías que viene a facilitar y desarrollar las actividades que implican participación tanto de la administración pública como del sector privado, fundando con ello las bases para la dinamización de las actividades del Estado salvadoreño.

Punto importante es que esta ley otorga pleno valor probatorio al documento electrónico constituido por los datos y registros recibidos y archivados en el sistema informático, así lo rige el Art. 9, a ello también hace referencia el Art. 7 del mismo cuerpo legal.

ANTEPROYECTO DE LEY DE COMERCIO ELECTRÓNICO DEL MINISTERIO DE ECONOMÍA

El Ministerio de Economía ha elaborado anteproyecto de Ley de Comercio Electrónico y la Fundación Salvadoreña para el Desarrollo Económico y Social (FUSADES) a través del Departamento de Estudios Legales, ha sido invitada a

participar en la comisión revisora de dicho anteproyecto, la cual la conformarán: Ministerio de Economía, Asociación Nacional de la Empresa Privada, Cámara de Comercio e Industria de El Salvador Superintendencia del Sistema Financiero.

La Ley de Comercio Electrónico establecerá el marco regulatorio que vendrá a normar la contratación electrónica. El comercio electrónico no es solamente compra electrónica, es la producción, publicidad, venta y distribución de productos y servicios a través de las redes de comunicaciones. Se da entre empresas y consumidor, entre empresa y empresa, entre empresa y administración pública, y entre consumidor y administración; a través de elementos como el teléfono, la transferencia electrónica de fondos y el Internet.

Los problemas que pueden plantearse desde el punto de vista legal son:

Jurisdicción y competencia para resolver los conflictos derivados de la contratación electrónica;

Legislación aplicable, y

Lugar, tiempo y forma de perfeccionamiento de los contratos electrónicos (oferta y aceptación).

Para que funcione satisfactoriamente el comercio electrónico se requiere de ciertos requisitos:

Reglas claras para identificar los objetos intercambiables;

Un sistema de pago seguro, y

Mecanismos de protección que permitan sancionar las transgresiones a dichas reglas.

Objeto de la ley: normar la utilización de mensajes de datos y comunicaciones electrónicas, cualquiera sea la forma utilizada, en el contexto de actividades comerciales en el ámbito nacional e internacional, de tal manera que ellas puedan ser acreditadas válidamente, mediante procedimientos de seguridad ya existentes y que a su vez permitan dar claridad, seguridad, autoría y autenticidad a las mismas.

Ámbito de aplicación: todo tipo de comunicación o información transmitida en forma de mensaje de datos, salvo en los siguientes casos:

Derecho sucesoral;

Derecho de familia;

Aquellos actos que las leyes exijan expresamente alguna solemnidad, o que requieran la presencia de algunas de las partes;

Las advertencias escritas que por disposición legal deban ir impresas en cierto tipo de productos en razón del riesgo que implica su comercialización, uso o consumo, y

Obligaciones contraídas por el Estado en virtud de tratados internacionales.

Jurisdicción y ley aplicable: en caso de controversias se someterán a la jurisdicción estipulada en el contrato, a lo establecido en las leyes vigentes o a las normas de arbitraje y mediación. Los contratos contendrán una cláusula compromisoria que indique la manera en que se van a resolver los conflictos.

Reconocimiento y consecuencias jurídicas de los mensajes de datos: un mensaje de datos tendrá efecto, validez y fuerza obligatoria como cualquier acto o contrato en forma material.

Formación y validez de los contratos, actos y declaraciones de voluntad: en la forma de los contratos, la oferta o su aceptación podrán ser expresadas por medio de un mensaje de datos.

Reconocimiento y efectos jurídicos de una firma electrónica: siempre y cuando reúna los requisitos determinados en la ley y cumpla con los **reglamentos** que al efecto se dictaren, tendrá el mismo efecto, validez y efectividad que una firma manuscrita.

Requisitos de la firma electrónica:

Garantizar la confidencialidad del mensaje de datos;

Ser susceptible de verificación en la autoría e identidad del emisor;

Estar bajo el control exclusivo de la persona que la usa, del mandatario o representante legal;

Estar ligadas a la información o mensaje de datos, de tal manera que si son cambiados, la firma electrónica es invalidada;

Ofrecer seguridad suficiente de que no pueda ser falsificada con la tecnología existente, y

No alterar la integridad del mensaje.

Entidades de Certificación: es aquella entidad que legalmente está facultada para emitir certificados digitales, con el objeto de dar certeza sobre la identidad y firmas

electrónicas de una persona. Dichas entidades deben estar jurídica y tecnológicamente capacitadas para emitir los certificados electrónicos, y deberán contar con la previa autorización de la respectiva autoridad.

Requisitos de las Entidades de Certificación:

Ser persona jurídica de interés público o privado;

Contar con la capacidad económica, financiera y humana suficiente para prestar los servicios autorizados;

Contar la capacidad y elementos técnicos necesarios para la generación de firmas electrónicas, la emisión de certificados sobre la autenticidad de las mismas y la conservación de los mensajes de datos;

Garantizar un servicio de suspensión, cancelación y revocación, rápido y seguro, de los certificados que emita, y

Tener un sistema de información de acceso libre, permanente, actualizado y eficiente en el cual se publiquen las políticas y procedimientos aplicados, así como los certificados que hubiere proporcionado, revocado, suspendido o cancelado.

Principales obligaciones de las Entidades de Certificación:

Utilizar sistemas y productos confiables que estén protegidos de toda alteración, que garanticen la seguridad técnica de los procesos que soporten;

Utilizar programas de firma electrónica que estén protegidos contra su modificación, 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;

Adoptar medidas para evitar la falsificación de los certificados;

Certificar la correspondencia de funcionamiento entre la clave pública y la clave privada.

Entidad Reguladora: es la encargada de supervisar las actividades de las Entidades de Certificación.

Principales funciones de la Entidad Reguladora:

Autorizar la actividad de las Entidades de Certificación otorgando licencias de operación;

Velar por el buen funcionamiento de las Entidades de Certificación;

Imponer sanciones a las Entidades de Certificación;

Revocar certificados cuando sean emitidos sin cumplir los requisitos legales;

Velar porque las Entidades de Certificación emitan conforme a la ley certificados de firma electrónica;

Revocar o suspender las licencias de operación cuando se incumplan los requerimientos legales;

Llevar el Registro de las Entidades de Certificación;

Recaudar multas de conformidad al Reglamento de la Ley, y

Actuar como mediador en la solución de conflictos entre las entidades certificadoras y los usuarios, cuando le sea solicitado.

Sanciones:

Amonestación escrita;

Multa (no se ha determinado el monto máximo);

Suspensión todas o alguna de las actividades;

Prohibición de prestar los servicios hasta por cinco años, y

Revocación definitiva de la autorización.

DERECHO COMPARADO

Nuestro país carece en la actualidad, de una normativa jurídica especializada en relación al comercio electrónico y el formato digital para la celebración de actos jurídicos; únicamente presenta de forma aislada la regulación de aspectos que permiten de una manera inicial la incorporación de mecanismos electrónicos en ciertas transacciones. Es por ello que se hace necesario creación de una ley que regule la generalidad de esta materia y de lo que hasta este momento solo tiene un incipiente anteproyecto, el cual se comparará con normativa existente en otros países que han tenido como prioridad la creación de este tipo de normas.

CRITERIOS	ESPAÑA	COLOMBIA	ARGENTINA	COSTA RICA	EL SALVADOR
Concepto	Art. 3 No. 1, 2, 3 - Firma Electrónica - Firma Electrónica Avanzada - Firma Reconocida	Art. 2 lit. c) Firma Digital	Art. 2 Inc. 1° Firma Digital	Art. 4 - Firma Digital - Firma Digital Avanzada.	Art. 3 Firma Electrónica
Definición	Art. 3 No.2 y 3 “La firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que esta vinculada al firmante, de manera única y a los datos a que se verifica y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control. Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma”.	Art. 2 lit. c) “Firma Digital se entenderá como un valor numérico que se adhiere a un mensaje de datos, y que utilizando procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje, permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación”.	Art. 2 “Firma Digital. Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose esta bajo su absoluto control...”	Art. 12 No 11 y 12 “Firma Digital: es el conjunto de datos, anexos a otros datos o datos asociados funcionalmente, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge. Firma digital avanzada: es la firma digital certificada por un prestador de servicios de certificación debidamente acreditado ante la autoridad competente de acreditación”.	Art. 3 “Firma electrónica es cualquier medio, método, símbolo o proceso electrónico que sustituye la firma manuscrita y se adhiere o se asocia lógicamente con un mensaje de datos aceptados y aprobado por una persona dándolo por autentico impidiendo que el signatario pretenda desconocer la autoría de la misma posteriormente”.

Ámbito de Aplicación	Art. 4 Se aplica en el ámbito de la Administración Pública	Art. 1 Se entiende para el sector privado	La ley se entiende para el sector privado y público. Art. 37. Regula, señala la aplicación en el sector público nacional.	No señala ámbito de aplicación específico. Se entiende que es para el sector privado.	Art. 1 No hace distinción para su aplicación.
Exclusiones del Ámbito de Aplicación		Art. 1 - Obligaciones contraídas por el Estado colombiano en virtud de convenios y tratados internacionales. - Advertencias suscritas por disposición legal deban ir necesariamente impresas en cierto tipo de productos en razón al riesgo de comercio, uso y consumo.	Art. 4 - Derecho sucesorial - Derecho de familia. - Actos personalísimos. Solemnidades legales.	.	Art. 2 - Derecho sucesorial - Derecho de familia - Solemnidades legales - Advertencias de ley en razón del comercio, uso y consumo.
Valor Probatorio	Art. 3 No. 8 Otorga valor probatorio a los datos firmados electrónicamente	Art. 10 “Los mensajes de datos serán admisibles como medio de prueba y su fuerza probatoria es la otorgada en el Código de Procedimiento Civil”.	Art. 11 Da valor probatorio a los documentos firmados digitalmente.		Art. 12 Da valor probatorio a los mensajes de datos que le otorga la ley.
Autoridades de Registro		Art. 41 y 42 Superintendencia de industria y comercio.	Art. 1 (Decreto 1028/2003) Oficina Nacional de Tecnologías de Información.	Art. 8 Es el Ministerio de Ciencia y Tecnología.	Art. 47 y 48 Entidad reguladora.
Autoridades de Certificación	Art. 2 No. 2 Prestador de servicios de certificación.	Art. 29 al 34 Entidades de certificación	Art. 17 Certificador licenciado	Art. 9 Autoridades de acreditación	Art. 44, 45 y 46 Entidades de certificación
Seguros de Autoridades de Certificación	Art. 20 No. 2		Art. 30 Regl.		
Certificados Digitales	Art. 6	Art. 35	Art. 13	Art. 10	Art. 43
Certificados Extranjeros	Art. 14		Art. 16 Art. 28 y 38 Regl.	Art. 12	

Período de Validez de los Certificados	Art. 8 No. 1 lit. a) No lo determina		Art. 15 Art. 26 Regl Son 5 años		
Revocación de los Certificados	Art. 8 No. 1 lit. b)	Art. 37	Art. 23 Regl.	Art. 11	
Acuse de Recibo		Art. 20			Art. 20
Regulación de Conductas Delictivas			Art. 51 Equiparación a los efectos del Derecho Penal		
Equiparación de la Firma Digital Electrónica a la Firma Manuscrita	Art. 3 No. 4	Art. 7		Art. 1	Art. 11
Comentario	La ley española distingue entre dos clases de firma que son electrónica y firma electrónica avanzada siendo esta la que encaja como Firma Digital pero únicamente se equiparará a la Firma Manuscrita cuando cumpla otros requisitos y solo entonces es que tendrá la calidad de Firma Electrónica reconocida. No se incluye la figura de la Autoridad de Registro, solo se le delegan algunas de sus funciones al Ministerio de Ciencia y tecnología Esta ley es bastante corta e incluye apartados que no deberían ser campo regulado en ella..	Por ser colombiana uno de los países más avanzados en América en el tema de la Firma Digital, su regulación deja en claro; al desarrollo ampliamente el valor probatorio de la Firma, su equiparación de validez con la Firma Autógrafa, el acuse de recibo, las entidades de certificación, los certificados, y la autoridad encargada de aplicar esta ley.	La ley 25.506, es bastante completa; salvo en aspectos puntuales, a los cuales puede hacersele observaciones así en la verificación de la Firma Digital, tiende hacerse incompleta, y además remite a un reglamento la regulación de aspectos importantes como por ejemplo el sistema de auditoria	En razón de ser una ley corta que solo cuenta con 20 artículos, tiende a dejar de lado ciertos aspectos como el valor probatorio, el acuse de recibo; y al regular a las entidades de certificación solo se encarga de mencionarlas, no de desarrollarlas ni establecer sus funciones.	El anteproyecto con que se cuenta es de Comercio Electrónico y en este se da la regulación de Firma Electrónica, se abstiene de utilizar el término Firma Digital y se centra en regular determinados puntos de manera muy amplia dejando mucha materia por regular dentro del o los reglamentos, pretendiendo suplir los vacíos de ley vía reglamentaria. Además, carece de regular un régimen sancionatorio, entre otras cosas contiene muchas deficiencias. La opinión es que debería regular en una ley especial lo referente a las firmas.

Las leyes o reglamentos que en el cuadro anterior se relacionan y de las cuales se citan los artículos son las siguientes:

Alemania:

España: *Ley 59/2003. de 19 de diciembre de Firma Electrónica. BOE núm. 304,

Sábado 20 de diciembre 2003.

Estados Unidos de América:

Colombia: * Ley N° 527 del 18 de agosto de 1999.

Argentina: * Ley N° 25.506 de Firma Digital, sancionada el 14 de noviembre de

2001, Promulgada de Hecho el 11 de diciembre de 2001.

* Decreto 2628/2002, del 20 de diciembre de 2002 Reglamento de la Ley
N° 25.506.

Costa Rica: * Ley de Firma Digital y Certificados Digitales. Expediente N° 14.276.

El Salvador: * Anteproyecto de Ley de Comercio Electrónico (Ministerio de
Economía).

CAPÍTULO 6

COMPROBACIÓN DE HIPÓTESIS Y ANÁLISIS DE DATOS

Sumario: 6.1 Introducción- 6.2 Comprobación de Hipótesis- 6.3 Análisis de Datos.

6.1 Introducción

Este apartado es el que se dedica a establecer la comprobación o no de la hipótesis que dirigió la investigación realizada explicando los términos en que se llegó a su comprobación; además se incluye de manera sencilla la explicación de los datos que se recogieron a partir de la realización de las entrevistas a informantes claves, con lo cual se da cobertura a este apartado de enorme importancia para determinar si verdaderamente en El Salvador se emplea la Firma Digital y que grado de seguridad le brinda la regulación nacional.

6.2 Comprobación de Hipótesis:

Debido a que en El Salvador la firma digital no ha sido desarrollada aún como aquella especie de firma electrónica que utiliza la técnica de criptografía asimétrica, la

presente investigación ha podido realizarse y así comprobar la hipótesis únicamente a nivel teórico.

La hipótesis que sirvió de parámetro para esta investigación fue: “A mayor grado de seguridad proporcionado por el Estado en el uso de la firma digital, mayor será su aplicación como medio de expresión del consentimiento”, su comprobación se ha realizado a través de una investigación de tipo Descriptiva y Explicativa desarrollada tanto a nivel teórico como empírico. Teóricamente al analizar la doctrina y la normativa internacional de firma digital se ha comprobado que en los países que esta goza de protección jurídica si es un buen medio de expresión del consentimiento y muy utilizado. En El Salvador por no existir la firma digital en todo el sentido de la palabra, solo se ha podido llevar a cabo la investigación a nivel empírico, de las formas híbridas de firmas electrónicas existentes en nuestro país.

6.3 Análisis de Datos:

para la realización de la investigación empírica el método a emplear fue el “Muestro No Probabilística” de tipo “Intencional o Selectivo”, desarrollado a través de entrevistas a informantes claves, utilizando la técnica de la “Encuesta” por medio del instrumento denominado “Cédula de Entrevista”; consiguiendo con este determinar cuales son los empleos que se le da a la firma electrónica en el país y a la vez obtener una opinión generalizada de la aceptación que la firma digital gozaría al emplearla en El Salvador.

Las opiniones recogidas por medio de las veintiún entrevistas realizadas con las siguientes:

*** LICENCIADOS EN CIENCIAS JURÍDICAS**

- 1. ¿CONOCE USTED LA** *a esta interrogante todos los informantes claves*
EXISTENCIA DE LA *respondieron que sí*
FIRMA DIGITAL?

“Esta pregunta era la base para la realización de la entrevista, debido a que si los informantes claves no conocían acerca del tema, la entrevista se volvería infructuosa”.

<p>2. ¿Cómo la calificaría como medio de expresión del consentimiento</p>	<p>ÓRGANO JUDICIAL</p>	<ul style="list-style-type: none"> - Como una forma novedosa, y plena expresión del consentimiento.
	<p>DOCENTES UES</p>	<ul style="list-style-type: none"> - Mecanismo tecnológico de homologación tanto de la oferta como de la aceptación:
	<p>BANCA</p>	<ul style="list-style-type: none"> - Si hay consentimiento
	<p>SSF</p>	<ul style="list-style-type: none"> - Es eficaz.
	<p>MINISTERIO DE ECONOMÍA</p>	<ul style="list-style-type: none"> - Es adecuado en el momento de globalización en que vivimos
	<p>ABOGADOS</p>	<ul style="list-style-type: none"> - Es un medio inequívocamente para expresar el consentimiento. - Es necesario que se regule para que tenga todos los requisitos de existencia y validez. - Materialización de una voluntad.

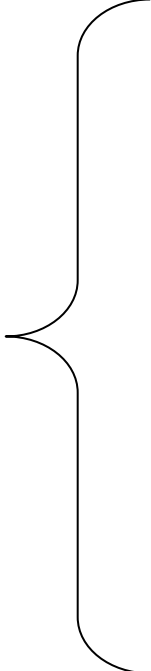
“Debido a que esta investigación se basa en que la firma digital constituye un novedoso medio de expresión del consentimiento, en un mundo digital, el grupo de investigación se adhiere a todas las opiniones brindadas en este sentido”

3. ¿CREE QUE CUMPLE CON TODOS LOS REQUISITOS PARA OBLIGARSE?	ÓRGANO JUDICIAL	- Sí - No, porque falta la calidad personal.
	DOCENTES UES	- Sí
	BANCA	- Sí
	SSF	- Sí cumple con los requisitos
	MINISTERIO DE ECONOMÍA	- Sí
	ABOGADOS	- No, porque no tiene sustento legal. - Sí, las cumple. - La Firma no es lo que obliga.


“Partiendo de la idea de que la Firma Digital identifica a una persona, y que esto conlleva a que al momento de celebrar un contrato esta constituya el medio de expresión del consentimiento, se puede determinar que sí cumple con todos los requisitos para obligarse”.

<p>4. DENTRO DE LA CLASIFICACIÓN TRADICIONAL DEL MOMENTO DE LA PERFECCIÓN DEL CONSENTIMIENTO. ¿CÓMO CALIFICARÍA A LOS CONTRATOS DONDE SE UTILIZA FIRMA DIGITAL?</p>	ÓRGANO JUDICIAL	<ul style="list-style-type: none"> - <i>No encaja en ninguna sería un contrato de adhesión</i> - <i>Entre presentes.</i>
	DOCENTES UES	<ul style="list-style-type: none"> - <i>Entre ausentes</i>
	BANCA	<ul style="list-style-type: none"> - <i>ambas son válidas (presentes u ausentes).</i>
	SSF	<ul style="list-style-type: none"> - <i>depende de la forma de contratar, y del momento en que se manifieste el consentimiento.</i>
	MINISTERIO DE ECONOMÍA	<ul style="list-style-type: none"> - <i>Entre ausentes.</i>
	ABOGADOS	<ul style="list-style-type: none"> - <i>No puede encajar en figuras tradicionales.</i> - <i>Entre ausentes.</i> - <i>Es contratación con presencia física o no.</i>

“Por ser los contratos electrónicos algo demasiado novedoso muchas veces algunas figuras del derecho quedan obsoletas, no pudiendo las relaciones encajar en estas. Esta pregunta estaba dirigida a realizar un sondeo acerca de la amplitud de criterio que se tenga sobre la forma de celebración de contratos por medios electrónicos”.

5. ¿EXISTEN NORMAS REGULEN SU USO?		ÓRGANO JUDICIAL	- <i>No.</i>
		DOCENTES UES	- <i>Sí.</i>
		BANCA	- <i>Sí, de forma incipiente.</i>
		SSF	- <i>No hay normas específicas.</i>
		MINISTERIO DE ECONOMÍA	- <i>Entre ausentes.</i>
		ABOGADOS	- <i>No puede encajar en figuras tradicionales.</i> - <i>Entre ausentes.</i> - <i>Es contratación con presencia física o no.</i>

“Desde el inicio se conocía que no existe una ley de comercio electrónico y menos aún una que regula la Firma Digital, pero se contaba con la noción de la existencia de artículos dispersos que regularán las formas incipientes de firma electrónica que se están empleando en el país, y que a lo largo de la investigación se pudieron determinar.

6. ¿CREE QUE ES NECESARIO CREAR UNA NUEVA NORMATIVA O ADOPTAR LA YA EXISTENTE?		ÓRGANO JUDICIAL	- <i>Sí, hay que crear.</i>
		DOCENTES UES	- <i>Ley especial.</i>
		BANCA	- <i>Normativa nueva.</i>
		SSF	- <i>Nueva ley.</i>
		MINISTERIO DE ECONOMÍA	- <i>Depende de la política legislativa</i>
		ABOGADOS	- <i>Si es necesario crear una nueva normativa.</i>

“El grupo de investigación siempre ha sostenido la opinión de que es necesaria la creación de una norma especial que regule el comercio electrónico y la firma digital; pero que a la vez es imprescindible, tal y como se ha realizado en muchos países, que se reforme los artículos que en el Código Civil y el de Comercio servirían de base para la implementación de este mecanismo en nuestro país”.

7. ¿CREE QUE UN DOCUMENTO ELECTRÓNICO GOZA DE VALOR PROBATORIO EN EL SALVADOR?	ÓRGANO JUDICIAL	- Sí, depende del juez. - No, porque no esta reglamentado.
	DOCENTES UES	- Sí.
	BANCA	- Sí.
	SSF	- Sí.
	MINISTERIO DE ECONOMÍA	- No.
	ABOGADOS	- Sí. - Actualmente no. - No por la prueba tasada en civil. Solo constituye u indicio.

“En nuestro país por el momento un documento electrónico no goza d valor probatorio en todas las áreas del Derecho, pero este es un punto que al igual que otros e que El Salvador se ha quedado un poco retrasado, debería de reformarse y dársele en todos los campos valor probatorio que este posee; ya que determinadas áreas”.

8. ¿CREE QUE EL ESTADO SALVADOREÑO BRINDA LA PROTECCIÓN NECESARIA PARA LA UTILIZACIÓN DE LA FIRMA DIGITAL?	ÓRGANO JUDICIAL	- No. - SI.
	DOCENTES UES	- No.
	BANCA	- No, actualmente.
	SSF	- Poca.
	MINISTERIO DE ECONOMÍA	- No.
	ABOGADOS	- No, solo en el sector privado.

“Por ser el sector privado quien ha realizado la implementación del comercio electrónico y la firma digital en nuestro país, se podría criticar al Estado salvadoreño por su falta de interés en proporcionar el marco jurídico que proteja y de seguridad a las actuaciones que la sociedad realice en el ámbito de los avances tecnológicos”.

<p>9. ¿CREE QUE LAS DEPENDENCIAS DEL ÓRGANO JUDICIAL QUE CONOCEN EN MATERIA MERCANTIL ESTÁN CAPACITADOS PARA CONOCER DE PROCESOS EN LOS QUE SE EXIJA EL CUMPLIMIENTO DE UN CONTRATO EN EL QUE SE HAYA UTILIZADO LA FIRMA DIGITAL?.</p>	<p>ÓRGANO JUDICIAL</p>	<p>- No. - No se puede asegurar.</p>
	<p>DOCENTES UES</p>	<p>- No.</p>
	<p>BANCA</p>	<p>- Tendrían que estar capacitados.</p>
	<p>SSF</p>	<p>- No.</p>
	<p>MINISTERIO DE ECONOMÍA</p>	<p>- No.</p>
	<p>ABOGADOS</p>	<p>- No.</p>

“Debido al poco conocimiento que la sociedad en general tiene a cerca del tema, es muy difícil pretender que el Órgano Judicial este en la capacidad de dirimir un conflicto de esta naturaleza”.

10. ¿CUÁL ES LA REPERCUSIÓN EN LA FE PÚBLICA DE LA UTILIZACIÓN DE ESTE TIPO DE FIRMA?

ÓRGANO JUDICIAL - *Se ampliaría el campo.*

DOCENTES UES - *Ninguna.*

BANCA - *No se ve afectada.*

SSF - *No hay repercusión alguna.*

MINISTERIO DE ECONOMÍA - *Repercusión favorable se les tomaría en cuenta.*

- *Primero tiene que delimitarse la función de ellos.*

- *Se mejorará la Fe Pública.*

“La repercusión en la Fé Pública utilizar de la Firma Digital es algo muy difícil de determinar sin conocer la regulación que de esta determinará el Estado y el grado de participación que se le de al Sector Notarial”.

INGENIEROS EN SISTEMAS INFORMÁTICOS.

- 1) **¿CONOCE USTED A** *A esta interrogante todos los*
EXISTENCIA DE LA FIRMA *informantes claves respondieron*
DIGITAL? *que sí.*

<p>2. CONOCE EL MECANISMO DE OPERACIÓN DE LA FIRMA DIGITAL? ¿CUÁL ES?</p>	<p>docentes UES</p>	<ul style="list-style-type: none"> - Funciona a través de certificados digitales. - No exactamente. - Generada por una clave privada que se encripta y en el destino se describe con una clave pública.
	<p>DIESCO EAN EL SALVADOR</p>	<ul style="list-style-type: none"> - Sí, funciona mediante cálculos matemáticos (algoritmos).
	<p>INGENIEROS</p>	<ul style="list-style-type: none"> - A través de dos claves, una pública y privada; unida a la infraestructura de PKI.
	<p>MINISTERIO DE ECONOMÍA</p>	<ul style="list-style-type: none"> - Criptografía asimétrica.

“El mecanismo de operación de la Firma Digital, tal y como se ha determinado a lo largo de esta investigación, se basa en la criptografía de la Clave Pública, la cual emplea dos claves una privada y una pública. Pero tal y como se puede determinar con el análisis de estos con el análisis de estos datos en nuestro medio no es muy conocido”.

**3) ¿CÓMO SE HACE
PARA FIRMAR
DIGITALMENTE
UN DOCUMENTO
ELECTRÓNICO?**

docentes UES

- *Por medio del uso de dos llaves, una privada y otra pública.*
- *Por el uso de un software brindado por una empresa.*

**DIESCO EAN
EL SALVADOR**

- *Por medio de el uso de un par de claves.*

INGENIEROS

- *Desconoce el proceso exacto.*
- *Por el uso de la llave privada.*

**MINISTERIO
DE ECONOMÍA**

- *Con el empleo de algoritmos.*

“Para firmar digitalmente un documento primero debe de encriptarse con una clase privada o con una clave pública, de acuerdo al caso; lo cual como refleja es conocido”.

4. ¿PARA QUE SE UTILIZA LA FIRMA DIGITAL?

docentes UES

- *Se utiliza para identificar y validar al remitente de un mensaje.*
- *Realizar transacciones o analizar información electrónica.*
- *Los usos de la firma manuscrita, con enfoque electrónico.*
- *Brindar seguridad a los datos enviados.*
- *Firmar información sin que se puede acceder a ella.*

DIESCO EAN EL SALVADOR

- *Por el sistema de teledespacho y telepago.*

INGENIEROS

- *Por garantizar datos.*

MINISTERIO DE ECONOMÍA

- *Seguridad en las transacciones.*
- *Para firmar un documento sin que pueda existir repudio.*

“La utilización de la Firma Digital se centra en proporcionar seguridad en las transacciones garantizando la autoría del documento o mensaje y la integridad del mismo”.

5. ¿CÓMO FUNCIONA EN NUESTRO PAÍS?	docentes UES	<ul style="list-style-type: none"> - <i>Se desconoce.</i> - <i>Funciona con dos llaves una privada y una pública.</i>
	DIESCO EAN EL SALVADOR	<ul style="list-style-type: none"> - <i>Teledespacho y telepago.</i>
	INGENIEROS	<ul style="list-style-type: none"> - <i>Pago de impuestos.</i>
	MINISTERIO DE ECONOMÍA	<ul style="list-style-type: none"> - <i>No funciona en aduana</i>

“Actualmente en nuestro país la Firma Digital no funciona tal y como se ha establecido en doctrina en la presente investigación, siendo la única referencia que se acerca a este sistema es el Teledespacho y Telepago en el sector Aduanero”.

6. ¿CREE QUE UN SISTEMA DE ESTE TIPO PODRÍA IMPLEMENTARSE EN NUESTRO PAÍS?	docentes UES	<ul style="list-style-type: none"> - <i>Es factible.</i> - <i>Los sistemas de seguridad deben ser mejor.</i>
	DIESCO EAN EL SALVADOR	<ul style="list-style-type: none"> - <i>Sí.</i>
	INGENIEROS	<ul style="list-style-type: none"> - <i>No.</i>
	MINISTERIO DE ECONOMÍA	<ul style="list-style-type: none"> - <i>Posiblemente.</i> - <i>Sí.</i>

“En nuestro país implementar un sistema de este tipo sería demasiado costoso y difícil por no contar con medios adecuados; y si en algún momento se llegara a implementar sería parcialmente en relación a su infraestructura”.

<p>7. ¿QUÉ SEGURIDAD TÉCNICA PROPORCIONA LA FIRMA DIGITAL?</p>	<p>docentes UES</p>	<ul style="list-style-type: none"> - <i>Es seguro por el uso de algoritmos de encriptamiento.</i> - <i>Es difícil de terminarla cuantitativamente.</i> - <i>Depende de la educación del usuario, en cuanto a su custodia.</i> - <i>Funciona correcto y seguro en el cumplimiento de normas jurídicas.</i>
	<p>DIESCO EAN EL SALVADOR</p>	<ul style="list-style-type: none"> - <i>Un porcentaje de 99.95% seguro.</i>
	<p>INGENIEROS</p>	<ul style="list-style-type: none"> - <i>Es seguro.</i>
	<p>MINISTERIO DE ECONOMÍA</p>	<ul style="list-style-type: none"> - <i>No mucha seguridad técnica y la jurídica dependerá de la ley.</i> - <i>Si dependiendo del uso que se le de.</i>

“La seguridad técnica proporcionada por la Firma Digital es muy elevada debido a que se encuentra basada en una infraestructura que brinda bastante confianza”.

8. ¿CONOCE LA EXISTENCIA DE UNA LEY QUE LA REGULE?	docentes UES	- <i>Desconoce.</i>
	DIESCO EAN EL SALVADOR	- <i>Ley de simplificación aduanera.</i>
	INGENIEROS	- <i>Desconoce.</i>
	MINISTERIO DE ECONOMÍA	- <i>No existe legislación.</i>

“No, existe actualmente una ley que regule el uso de Firma Digital tal y como se establece en legislaciones extranjeras”.

CAPÍTULO 7

CONCLUSIONES Y RECOMENDACIONES

Sumario: 7.1 Introducción- 7.2 Conclusiones- 7.2 Recomendaciones

7.1 Introducción

Esta investigación se ha desarrollado a través de un estudio amplio y sistemático de la figura de la Firma Digital y la seguridad técnica jurídica con la que cuenta, tomando estos, como lineamientos centrales que se delimitaron a partir de haber realizado un análisis somero y de carácter bibliográfico; se ha llegado a la conclusión que el implementar el uso globalizado de la Firma Digital acarrea grandes beneficios además de facilitar las comunicaciones, a tal grado que aquellas donde la aproximación física de las partes no existe con el uso de las nuevas tecnologías la interacción en tiempo real permite que se comuniquen como si existiera esa aproximación. A pesar de estas ventajas surgen inquietudes generalizadas entre las cuales se destaca como una de las más importantes la inseguridad en redes abiertas, la cual constituye el eje de esta investigación.

7.2 Conclusiones

Los modernos medios de comunicación se han difundido con notable rapidez en el desarrollo de las operaciones comerciales internacionales previéndose que sea cada vez mayor su difusión a medida que se globalicen, con la única finalidad de simplificar y facilitar la comunicación; y esto ha originado la necesidad imperante que sean adoptados todos los mecanismos y sistemas que garantizaron las tradicionales formas de comunicación para que estas interacciones puedan ser reconocidas y por ello validadas dentro de la sociedad.

Con el afán de volver más segura la comunicación a través de redes abiertas como la que se da en Internet y el EDI, se han ido buscando métodos o técnicas que ofrezcan mayor grado de autenticidad e integridad de los mensajes para que estos no puedan ser negados por su autor, brindándole un alto grado de confianza a las relaciones que se realizan utilizando medios electrónicos, uno de estos métodos o técnicas lo constituye la criptografía asimétrica o de clave pública.

En El Salvador la introducción de los avances tecnológicos principalmente en materia de comercio y la iniciativa de contar con tecnología de punta se ha logrado gracias al sector privado quienes interesados en el desarrollo de la relación empresa-

consumidor han hecho posible que el país involucre en el movimiento mundial del comercio electrónico cerrado pero sobre todo en el abierto basado en el EDI e Internet.

El paso del comercio tradicional al comercio electrónico introduce un ambiente en el que se impone la despapelización de los actos, lo que conlleva a que la firma no solo se vuelva prácticamente inoperante sino que conspira contra la automatización de las actuaciones, provocando la urgente adecuación del Derecho a las exigencias del nuevo tiempo.

Que el objetivo primordial de la Firma Digital es brindar autenticidad al documento que suscribe, garantizando de esta manera que quien se muestra como autor del mensaje es quien dice ser, sin temor de que otra persona lo haya suplantado, pues de haberlo hecho el mensaje dejaría al descubierto tal situación en el momento de la verificación.

La criptografía como ciencia que se ocupa de la transformación de mensajes en formas aparentemente ininteligibles para el lenguaje humano y posteriormente devolverlos a su forma original constituye un modo casi perfecto de autenticación digital utilizada en medios informáticos que permiten ante todo proteger la integridad de los mensajes porque transforma los datos en signos ilegibles y solo los revela si se le aplica a clave para descryptarlos y de esta forma asegura la privacidad del mensaje.

Que dentro del término firmas electrónicas pueden incluirse una diversidad de técnicas que utilizan distintos mecanismos para establecer la autoría; pero aquella que utiliza la criptografía asimétrica o de clave pública basada en la relación entre un par de claves es la que encaja en el sistema de Firma Digital y es la que goza de credibilidad y certeza y por ello la que se asemeja en más aspectos a la Firma Manuscrita.

A nivel mundial se han implementado los modelos basados en terceras partes de confianza lo que se denomina Infraestructura de Clave Pública (PKI) referida a todo el aparataje necesario para poner en marcha, sistemas y aplicaciones que utilizan técnicas de criptografía asimétrica; y estas constituyen parte importante para el funcionamiento de la Firma Digital porque conforman una cadena de confianza en la que los usuarios se amparan.

La seguridad en Internet consiste en implementar mecanismos como la criptografía asimétrica o de clave pública, para que cuando se reciba un mensaje o se realice una transacción por medios electrónicos, se asegure la integridad y la identidad del remitente y del receptor.

Las nuevas tecnologías de la información se adaptan sin ninguna dificultad como

medios de expresión de la voluntad para formación del consentimiento entre partes no presentes físicamente desarrollándose una nueva modalidad de constituir derechos y obligaciones no porque la fuente sea la nueva sino porque la forma de expresar la voluntad es lo novedoso, pues deviene de utilizar un medio electrónico.

Teorías tradicionales que explican la forma en que se perfecciona el consentimiento y por consiguiente los contratos, como son las teorías entre partes presentes y entre partes ausentes ya no se ajustan a la manera innovadora de celebración de contratos; pues el incluir medios electrónicos que permiten actuar en tiempo real, inmediatez de los actos, e incluso contar con imágenes y sonido en los mismos, conlleva a pensar en una nueva clasificación de contratar que se ajuste a los parámetros que el desarrollo tecnológico va imponiendo.

En nuestro país se pueden catalogar como mínimos los intentos de regulación en materia de Comercio Electrónico principalmente de Firma Digital los cuales se limitan a establecer circunstancias especiales adaptables en casos específicos los cuales no son suficientes para proteger jurídicamente y determinar los mecanismos necesarios que permitan a los usuarios de estos novedosos sistemas de información y comunicación tener seguridad al usar dichos sistemas.

7.3 Recomendaciones

El Estado salvadoreño debe analizar y posteriormente adoptar los mecanismos y sistemas que a nivel internacional y principalmente en los países desarrollados se están generando, con el fin de brindar protección y garantía a todos aquellos que interactúan dentro de los modernos medios de comunicación.

En el ámbito de la adquisición de obligaciones y la tutela de derechos, el país debe adherirse a los nuevos sistemas que internacionalmente se están retomando, con el único fin de que a través de estos sistemas que actúan en el medio electrónico como por ejemplo en el sistema de Firma Digital que utiliza criptografía de clave pública o asimétrica, para que con ello se logre un mayor grado de autenticidad e integridad de los mensajes por los que son atribuidos derechos y obligaciones a los sujetos.

La administración pública en nuestro país debe comenzar a mostrar mayor interés e importancia debida a los nuevos avances tecnológicos en materia de comercio; y, ya que ha sido el sector privado el único impulsador de estas ideas, unir esfuerzos encaminados

a que nuestro país pueda retomar estas tecnologías para facilitar y asegurar de mejor manera las comunicaciones.

Es menester de nuestros legisladores encaminar la ideología normativa con la que se deberá crear y posteriormente aprobar las leyes que deberán regular las relaciones a través de medios electrónicos, adecuándolos a estas nuevas tecnologías con el único fin de brindar seguridad y validez jurídica a dichos actos.

Es necesario hacer un análisis exhaustivo, sistemático, serio y coherente de la actual legislación tanto sustantiva como procesal con la finalidad de concluir cual es idóneo y cual debería ser derogado para establecer un nuevo cuerpo legal más válido, sólido y que brinde una mejor protección jurídica a las relaciones que dan por medio electrónicos y a la vez que establezca mecanismos procesales que permitan exigir en el cumplimiento de obligaciones pactadas por aquellos medios.

La doctrina jurídica que como función primordial tiene brindar apoyo para un mejor entendimiento de las instituciones jurídicas, bases para cualquier normativa, debe mutar de igual forma, debiendo adaptarse a las nuevas formas, sistemas y mecanismos tecnológicos que son utilizados en las relaciones de todo tipo dentro de la sociedad y que tienen relevancia jurídica, para poder superar posturas clásicas o tradicionalistas que cada vez se adecuan menos a las nuevas formas y figuras que están surgiendo.

BIBLIOGRAFÍA

Libros:

ALESSANDRI RODRÍGUEZ, Arturo y SOMARRIVA UNDURRAGA, Manuel, **“Curso de Derecho Civil”**, Tomo IV, Fuentes de las Obligaciones, Editorial Nacimiento, Santiago, Chile, 1842.

CLARO SOLAR, Luis, **“Explicaciones de Derecho Civil Chileno y Comparado”**, Tomo X, De las Obligaciones, Santiago, Chile, 1992.

CUBILLOS VELANDIA, Ramiro y RINCÓN CÁRDENAS, Erick, **“Introducción Jurídica al Comercio Electrónico”**, Ediciones Jurídicas Gustavo Ibáñez, Medellín, 2002.

FERNÁNDEZ FERNÁNDEZ, Rodolfo, **“Contratación Electrónica: La Prestación del Consentimiento en Internet”**, J. M. Bosch Editor, Barcelona, 2001.

GALENDE DÍAS, Juan Carlos, **“Criptografía, Historia de la Escritura Cifrada”**, Editorial Complutense, Madrid, 1995.

GRUPO DE ESTUDIOS EN INTERNET, COMERCIO ELECTRÓNICO, TELECOMUNICACIONES E INFORMÁTICA, **“Internet, Comercio electrónico, Telecomunicaciones”**, Universidad de los Andes, Facultad de Derecho, Legis S. A., Primera Edición, Bogotá, 2002.

LETE DEL RÍO, José M. **“Derecho de Obligaciones”**, Volumen II, Segunda Edición, Tecnos, Madrid, 1995.

MARTÍNEZ NADAL, Apollonia, **“Comercio Electrónico, Firma Digital y autoridades de Certificación”**, Editorial Civitas, III Edición, Madrid, 2001.

NASH Andrew y otros, **“PKI Infraestructura de Claves Públicas”**, McGraw-Hill, Colombia, Bogotá, 2002.

R. BRIZZIO, Claudia, **“La Informática en el Nuevo Derecho”**, Abeledo-Perrot, Buenos Aires, 2002.

SARRA, Andrea Viviana, **“Comercio Electrónico y Derecho”**, Editorial Astrea, Edición 2001, Buenos Aires.

TÉLLEZ VALDÉZ, Julio, **“Derecho Informático”**, Tercera Edición, Instituto Tecnológico y de Estudios Superiores de Monterrey, McGraw-Hill, México, D.F., 2004.

Tesis:

COREAS BENAVIDES, Miguel Ángel y otros, **“El Consentimiento en el Derecho Civil Salvadoreño”**, Tesis Universidad Nueva San Salvador, 2000.

GAITÁN CORTÉZ, Carlos Ernesto y otros, **“Relaciones Contractuales en Internet y su Desprotección por la falta de Legislación de Comercio Electrónico”**, Tesis Universidad de El Salvador, 2003.

POLANCO VILLALOBOS, José Antonio y otros, **“La Regulación sobre Comercio Electrónico en el Ordenamiento Jurídico Salvadoreño”**, Tesis Universidad Centroamericana Doctor José Simeón Cañas, 2001.

VARGAS FRONTERA, Ginay del Valle, “**Valor Probatorio de los Medios Electrónicos en el Derecho Comparado, particularmente en las legislaciones, Mexicana, Española, Francesa, Chilena, Argentina y Venezolana**”, Informe de Investigación Jurídica, Guayana, 2003.

Enciclopedias:

BUENO, Marta, **El Pequeño Larousse Ilustrado 2001**, Séptima Edición 2ª reimpresión, Larousse, Santa Fe de Bogotá, Colombia, 2001.

CABANELLAS, Guillermo, **Diccionario Enciclopédico de Derecho Usual**, Tomo VII, Editorial Heliastas, Buenos Aires, 1989.

Enciclopedia Jurídica Omeba, Tomo XII, Editorial Driskill S. OXFORD., Buenos Aires, argentina, 1987.

GUIRAO, Pedro, **Diccionario de la Informática**, Inglés-Español, Ediciones Prisma, México, D.F.1995.

OXFORD UNIVERSITY PRESS, **Diccionario de Informática**, Segunda Edición, Diaz de Santos, Madrid, España, 1993.

PAFFENBERGER, Bryan, **QUE Diccionario Para Usuarios de Computadoras e Internet**, Sexta Edición, México D.F., 2000.

STEWART, Charles O., **QUE Diccionario Para Usuarios de Computadoras**, Tercera Edición, Prentice Hall. 2000.

Sitos Web:

“Algoritmos Simétricos,” <http://personal.telefonica.terra.es/web/criptologia/recerca4.html>, agosto, 2004.

“Autoridades de Certificación y Confianza Digital- Tercera Parte” www.fundaciondike.org.ar/seguridad/firmadigital-autoridades2.html, junio 2004.

“Biométrica”, www.aunmas.com/guias/criptologia/biometrica.htm, Septiembre, 2004.

“Comercio Electrónico”, www.monografias.com/trabajo12/monografias/monografias.shtml, mayo, 2004.

“Criptografía”, www.htmlweb.net/seguridad/cripto-8.html, junio, 2004.

“Criptografía y Firma Digital”, www.webpanto.com, junio 2004.

“Derecho de las Nuevas Tecnologías- La Firma Digital”, www.tuguialegal.com, julio, 2004.

“DIESCO,” www.camarasal.com/, mayo, 2004.

“Entidades de Certificación, Certificados y Firmas Electrónicas,” www.mici.gob.pa/comercio-electronico/sobre_entidad.html, junio, 2004.

“Firma Digital”, www.windowstimag.com, julio, 2004.

“Firma Digital Criptografía. Metodología de la Programación. Autenticación. Informática. Computación. Seguridad. Comercio Electrónico. Certificación. Electrónica. Dato Cifrado,” html.rincondelvago.com/certificados_yfirmas_digitales.html, mayo, 2004.

“Introducción a los Certificados Digitales”, <http://revista.robotiker.com/articulos/articulo51/página1.jsp>, agosto,2004.

“La Seguridad de los Protocolos Criptográficos”, www.ugr.es/~aquiran/cripto/informes/info002.htm, agosto,2004.

“Nuevas Tecnologías,” <http://homepage.mac.com/eravila/ecommercel.pdf>, mayo, 2004.

“PKI o los Cimientos de una Criptografía de Clave Pública” www.iec.csic.es/criptonomicon/susurros/susurros11.html, agosto,2004.

LEGISLACIÓN INTERNACIONAL:

Ley Modelo sobre Comercio Electrónico de la Comisión de las Naciones Unidas por el Derecho Mercantil Internacional. Aprobada en Asamblea General de la ONU por resolución 51/162, el 16 de diciembre de 1996.

Ley 59/2003 de Firma Electrónica de España del 19 de diciembre de 2003, BOE núm. 304, sábado 20 de diciembre de 2003.

Ley 25.506 de Firma Digital, Argentina, Sancionada el 14 de noviembre de 2001 y promulgada de Hecho el 11 de diciembre de 2001.

Ley 27.269 de Firma y Certificados Digitales de Perú, entró en vigencia en mayo de 2000.

Ley N° 527 de Colombia del 18 de agosto de 1999.

Ley de Firma Digital y Certificados Digitales de Costa Rica, Expediente N° 14.276.

LEGISLACIÓN NACIONAL:

Constitución, Leyes Civiles y de Familia, Tercera Edición, Editorial LIS, San Salvador, 1999.

Ley General Marítima Portuaria, D.L.N° 994, aprobada el 19 de septiembre de 2002, publicada el 1 de Octubre del 2002, D.O. 182, Tomo 357.

Ley de Bancos, aprobada el 10 d septiembre de 1999, sancionada el 27 de septiembre de 1999 y publicada en D.O No 181, Tomo 334 del 30 de septiembre de 1999.

Ley de Mediación, Conciliación y Arbitraje, D.L.N° 914, aprobada el 11 de Julio del 2002, publicada el 21 de agosto del 2002, D.O. 157, Tomo 356.

Recopilación de Leyes en Materia Penal, 4ª edición, Editorial Jurídica LIS, El Salvador, 2001.

A N E X O S

A N E X O 1

A b r e v i a t u r a s

ABREVIATURAS

- a. C. = Antes de Cristo
- a. de C. = antes de Cristo
- Pág. = página
- Ob. Cit. = Obra Citada
- Op. Cit. = Obra Citada
- Idem. = Mismo autor citado en la nota anterior
- etc. = etcétera
- C. C. = Código Civil
- Cn. = Constitución de la República
- Pr. Pn. = Código Procesal Penal
- Art = Artículo
- Inc. = Inciso
- lit. = literal
- Ud. = Usted
- D. O. = Diario Oficial
- B. O. E = Boletín Oficial de España
- www. = World Wide Web

A N E X O 2

G l o s a r i o

GLOSARIO

- **Algoritmo:** Procedimiento matemático o lógico para resolver un problema. Un algoritmo es un método para encontrar la respuesta a un problema difícil, mediante la separación del problema en un número específico de pasos sencillos.
- **Bit:** Contracción de las palabras inglesas Binary Digit (cifra binaria). Es la unidad elemental de información que solo puede tomar uno de los dos valores 0 ó 1. los bits se emplean universalmente en los sistemas electrónicos para codificar la información, instrucciones o datos.
- **Certificados:** Es un documento electrónico que contiene un conjunto de información a la que se ha fijado una Firma Digital por alguna entidad que es reconocida y en la que confía alguna comunidad de usuarios de certificados.
- **Click-wrap:** Término utilizado para la contratación por internet, el cual da a entender que con solo presionar la tecla del ratón se adquieren derechos o se contraen obligaciones.
- **Correo Electrónico:** Uso de comunicaciones electrónicas para enviar mensajes textuales (como cartas, memorando e informes). Se le conoce también como e-mail.

Comprende una comunicación de uno a uno, en el que una persona envía a otra, o una de uno a muchos conectados a la red.

- **Datos de Entrada:** (input) Cualquier información introducida a la computadora.

- **Datos de Salida:** Datos que muestran o imprimen los resultados de las operaciones de procedimiento.

- **Desencriptar:** Proceso de interpretar o convertir u texto encriptado a su estado original mediante el uso de la clave que desencripta el texto.

- **Desmaterialización:** Aniquilación de las partículas materiales y correlativa aparición de energía.

- **Encriptar:** La transformación de un texto legible en otro totalmente diferente e inteligible a simple vista por medio de un proceso matemático y el cual solo pueda ser leído por quien tiene la clave que desencripta el texto.

- **Facsímil:** Transmisión y recepción de una página impresa entre dos localizadas enlazadas a través de un sistema de telecomunicaciones.

- **Fax:** El término fax es una forma abreviada de facsímil.

- **Hacker:** Entusiasta aficionado a las computadoras con bastos conocimientos técnicos cuya diversión estriba en hacerle modificaciones a los programas o sistemas de computación y romper el sistema de seguridad de un sistema por el mero reto que ello ofrece.
- **Hardware:** Componentes electrónicos, tarjetas, periféricos y equipo que conforman un sistema de cómputo. El hardware debe distinguirse del software (o programas). Que es el que le indica a los componentes mencionados lo que deben hacer.
- **Internet:** Amplio sistema de enlaces de cómputo, faculita el envío de correo a todo el mundo.
- **Link:** Establecer una conexión entre dos archivos o elementos de información para que la modificación que se haga en uno se refleje en el otro.
- **Nodo:** En una red de área local, punto de conexión capaz de crear, recibir o repetir mensajes.
- **On-line:** En línea; en directo; conectado. Conectado al sistema y utilizable.

- **Ordenador:** Un ordenador comprende una parte física (hardware), constituida por circuitos electrónicos de alta relación, y una parte física (software).

- **Poligrafía:** Actividad de escribir sobre diversas materias.

- **Protocolo:** Sistema de reglas o estándares para comunicarse a través de una red, en especial a través de Internet. Los equipos y las redes interactúan de acuerdo con los protocolos que determinan el comportamiento que cada lado espera del otro en la transferencia de información.

- **Signatarios:** (Firmante) Que firma.

- **Software:** Programa de sistema, utilería o aplicaciones expresados en un lenguaje legible para las computadoras.

- **Soporte Telemático:** Medio material, tarjeta perforada, disco, cinta magnética, capaz de recibir una información, transmitirla o conservarla y, después, restituirla a petición.

- **Standar:** (Estándar), conjunto de reglas o especificaciones que, en conjunto, definen la arquitectura de un dispositivo de hardware, programa o sistema operativo.

- **Telex:** Servicio telegráfico con conexión directa entre los usuarios por medio de teleimpresores.

- **Vicio:** Defecto que anula o invalida un acto o contrato; sea de fondo o forma.

- **Virus:** Programa de computación, diseñado como un elemento llamativo o un saboteador, que se copia asimismo, para lo cual se adjunta a otros programas y lleva a cabo operaciones indeseables y en ocasiones dañinas.

- **Web:** (Telaraña). En World Wide Web (www) o cualquier sistema de hipertexto, un conjunto de documentos relacionados entre sí que conforman juntos una presentación con hipertexto.

A N E X O 3

**L e y M o d e l o d e
C o m e r c i o E l e c t r ó n i c o
y s u G u í a p a r a l a
I n c o r p o r a c i ó n a l
D e r e c h o I n t e r n o
U N C I T R A L**

**Comisión de las Naciones Unidas para el Derecho
Mercantil Internacional
(CNUDMI)**

***LEY MODELO DE LA CNUDMI SOBRE COMERCIO
ELECTRÓNICO CON LA GUÍA PARA SU
INCORPORACIÓN AL DERECHO INTERNO 1996***

con la adición del Artículo 5 bis en la forma aprobada en 1998

ÍNDICE

RESOLUCIÓN 51/162 DE LA ASAMBLEA GENERAL DE 16 DE DICIEMBRE DE
1996
LEY MODELO DE LA CNUDMI SOBRE COMERCIO ELECTRÓNICO

Primera parte. Comercio electrónico en general

Capítulo I. Disposiciones generales

- Artículo 1. Ámbito de aplicación
- Artículo 2. Definiciones
- Artículo 3. Interpretación
- Artículo 4. Modificación mediante acuerdo

Capítulo II. Aplicación de los requisitos jurídicos a los mensajes de datos

- Artículo 5. Reconocimiento jurídico de los mensajes de datos
- Artículo 5 bis. Incorporación por remisión
- Artículo 6. Escrito
- Artículo 7. Firma
- Artículo 8. Original
- Artículo 9. Admisibilidad y fuerza probatoria de los mensajes de datos
- Artículo 10. Conservación de los mensajes de datos

Capítulo III. Comunicación de los mensajes de datos

- Artículo 11. Formación y validez de los contratos
- Artículo 12. Reconocimiento por las partes de los mensajes de datos
- Artículo 13. Atribución de los mensajes de datos
- Artículo 14. Acuse de recibo
- Artículo 15. Tiempo y lugar del envío y la recepción de un mensaje de datos

Segunda parte. Comercio electrónico en materias específicas

Capítulo I. Transporte de mercancías

- Artículo 16. Actos relacionados con los contratos de transporte de mercancías
- Artículo 17. Documentos de transporte

GUÍA PARA LA INCORPORACIÓN AL DERECHO INTERNO DE LA LEY MODELO DE LA CNUDMI SOBRE COMERCIO ELECTRÓNICO párrs. 1-150

Finalidad de la presente Guía párr. 1

I. Introducción a la Ley Modelo párrs. 2-23

- A. Objetivos párrs. 2-6
- B. Ámbito de aplicación párrs. 7-10
- C. Estructura párrs. 11-12
- D. Una ley "macro" que habrá de ser completada por un reglamento técnico párrs. 13-14
- E. Criterio del equivalente funcional párrs. 15-18
- F. Reglas de derecho supletorio y de derecho imperativo párrs. 19-21
- G. Asistencia de la Secretaría de la CNUDMI párrs. 22-23

II. Observaciones artículo por artículo párrs. 24-122

Primera parte. Comercio electrónico en general párrs. 24-107

Capítulo I. Disposiciones generales párrs. 24-45

- Artículo 1. Ámbito de aplicación párrs. 24-29
- Artículo 2. Definiciones párrs. 30-40
- Artículo 3. Interpretación párrs. 41-43
- Artículo 4. Modificación mediante acuerdo párrs. 44-45

Capítulo II. Aplicación de los requisitos legales a los mensajes de datos párrs. 46-75

Artículo 5. Reconocimiento jurídico de los mensajes de datos párr. 46

Artículo 5 bis. Incorporación por remisión párrs. 46-1 - 46-7

Artículo 6. Escrito párrs. 47-52

Artículo 7. Firma párrs. 53-61

Artículo 8. Original párrs. 62-69

Artículo 9. Admisibilidad y fuerza probatoria de un mensaje de datos párrs. 70-71

Artículo 10. Conservación de los mensajes de datos párrs. 72-75

Capítulo III. Comunicación de mensajes de datos párrs. 76-107

Artículo 11. Formación y validez de los contratos párrs. 76-80

Artículo 12. Reconocimiento por las partes de los mensajes de datos párrs. 81-82

Artículo 13. Atribución de los mensajes de datos párrs. 83-92

Artículo 14. Acuse de recibo párrs. 93-99

Artículo 15. Tiempo y lugar del envío y la recepción de un mensaje de datos párrs. 100-107

Segunda parte. Comercio electrónico en materias específicas párrs. 108-122

Capítulo I. Transporte de mercancías párrs. 110-122

Artículo 16. Actos relacionados con los contratos de transporte de mercancías párrs. 111-112

Artículo 17. Documentos de transporte párrs. 113-122

III. Historia y antecedentes de la Ley Modelo párrs. 123-150

Resolución aprobada por la Asamblea General

[sobre la base del informe de la Sexta Comisión (A/51/628)]

51/162. Ley Modelo sobre Comercio Electrónico aprobada por 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 medio del intercambio electrónico de datos y por otros medios de comunicación, habitualmente conocidos como "comercio electrónico", en los que se usan métodos de comunicación y almacenamiento de 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.º período de sesiones, celebrado en 1985,¹ y el inciso *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 Comisión¹ 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,

Convencida de que la elaboración de una ley modelo que facilite el uso del comercio electrónico y sea aceptable para Estados que tengan sistemas jurídicos, sociales y económicos diferentes podría contribuir de manera significativa al establecimiento de relaciones económicas internacionales armoniosas,

Observando que la Ley Modelo sobre Comercio Electrónico fue aprobada por la Comisión en su 29.º período de sesiones después de examinar las observaciones de los gobiernos y de las organizaciones interesadas,

Estimando que la aprobación de la Ley Modelo sobre Comercio Electrónico por la Comisión ayudará de manera significativa a todos los Estados a fortalecer la legislación que rige el uso de métodos de comunicación y almacenamiento de información sustitutivos de los que utilizan papel y a preparar tal legislación en los casos en que carezcan de ella,

1. *Expresa su agradecimiento* a la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional por haber terminado y aprobado la Ley Modelo sobre Comercio Electrónico que figura como anexo de la presente resolución y por haber preparado la Guía para la Promulgación de la Ley Modelo;
2. *Recomienda* que todos los Estados consideren de manera favorable la Ley Modelo cuando promulguen o revisen 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;
3. *Recomienda también* que no se escatimen esfuerzos para velar por que la Ley Modelo y la Guía sean ampliamente conocidas y estén a disposición de todos.

LEY MODELO DE LA CNUDMI SOBRE COMERCIO ELECTRÓNICO

[Original: árabe, chino, español, francés, inglés, ruso]

Primera parte. Comercio electrónico en general

Capítulo I. Disposiciones generales

*Artículo 1. Ámbito de aplicación**

La presente Ley** será aplicable a todo tipo de información en forma de mensaje de datos utilizada en el contexto***de actividades comerciales****.

* La Comisión sugiere el siguiente texto para los Estados que deseen limitar el ámbito de aplicación de la presente Ley a los mensajes de datos internacionales:

La presente Ley será aplicable a todo mensaje de datos que sea conforme a la definición del párrafo 1) del artículo 2 y que se refiera al comercio internacional.

** La presente ley no deroga ninguna norma jurídica destinada a la protección del consumidor.

*** La Comisión sugiere el siguiente texto para los Estados que deseen ampliar el ámbito de aplicación de la presente Ley:

La presente Ley será aplicable a todo tipo de información en forma de mensaje de datos, salvo en las situaciones siguientes: [...].

**** El término "comercial" deberá ser interpretado ampliamente de forma que abarque las cuestiones suscitadas por toda relación de índole comercial, sea o no contractual. Las relaciones de índole comercial comprenden, sin limitarse a ellas, las operaciones siguientes: toda operación comercial de suministro o intercambio de bienes o servicios; todo acuerdo de distribución; toda operación de representación o mandato comercial; de

facturaje ("factoring"); de arrendamiento de bienes de equipo con opción de compra ("leasing"); de construcción de obras; de consultoría; de ingeniería; de concesión de licencias; de inversión; de financiación; de banca; de seguros; todo acuerdo de concesión o explotación de un servicio público; de empresa conjunta y otras formas de cooperación industrial o comercial; de transporte de mercancías o de pasajeros por vía aérea, marítima y férrea, o por carretera.

Artículo 2. Definiciones

Para los fines de la presente Ley:

a) 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;

b) Por "intercambio electrónico de datos (EDI)" se entenderá la transmisión electrónica de información de una computadora a otra, estando estructurada la información conforme a alguna norma técnica convenida al efecto;

c) Por "iniciador" de un mensaje de datos se entenderá toda persona que, a tenor del mensaje, haya actuado por su cuenta 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;

d) Por "destinatario" de un mensaje de datos se entenderá la persona designada por el iniciador para recibir el mensaje, pero que no esté actuando a título de intermediario con respecto a él;

e) Por "intermediario", en relación con un determinado mensaje de datos, se entenderá toda persona que, actuando por cuenta de otra, envíe, reciba o archive dicho mensaje o preste algún otro servicio con respecto a él;

f) Por "sistema de información" se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos.

Artículo 3. Interpretación

1) En la interpretación de la presente Ley habrán de tenerse en cuenta su origen internacional y la necesidad de promover la uniformidad de su aplicación y la observancia de la buena fe.

2) Las cuestiones relativas a materias que se rijan por la presente Ley y que no estén expresamente resueltas en ella serán dirimidas de conformidad con los principios generales en que ella se inspira.

Artículo 4. Modificación mediante acuerdo

1) Salvo que se disponga otra cosa, en las relaciones entre las partes que generan envían, reciben, archivan o procesan de alguna otra forma mensajes de datos, las disposiciones del capítulo III podrán ser modificadas mediante acuerdo.

2) Lo dispuesto en el párrafo 1) no afectará a ningún derecho de que gocen las partes para modificar de común acuerdo alguna norma jurídica a la que se haga referencia en el capítulo II.

Capítulo II. Aplicación de los requisitos jurídicos a los mensajes de datos

Artículo 5. Reconocimiento jurídico de los mensajes de datos

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

Artículo 5 bis. Incorporación por remisión

(En la forma aprobada por la Comisión en su 31.º período de sesiones, en junio de 1998)

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 que se supone ha de dar lugar a este efecto jurídico, sino que figure simplemente en el mensaje de datos en forma de remisión.

Artículo 6. Escrito

- 1) Cuando la ley requiera que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos si la información que éste contiene es accesible para su ulterior consulta.
- 2) El párrafo 1) será aplicable tanto si el requisito en él previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que la información no conste por escrito.
- 3) Lo dispuesto en el presente artículo no será aplicable a: [...].

Artículo 7. Firma

- 1) Cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos:
 - a) Si se utiliza un método para identificar a esa persona y para indicar que esa persona aprueba la información que figura en el mensaje de datos; y
 - b) Si ese método es tan fiable como sea apropiado para los fines para los que se generó o comunicó el mensaje de datos, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo pertinente.
- 2) El párrafo 1) será aplicable tanto si el requisito en él previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que no exista una firma.
- 3) Lo dispuesto en el presente artículo no será aplicable a: [...].

Artículo 8. Original

- 1) Cuando la ley requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos:
 - a) Si existe alguna garantía fidedigna de que se ha conservado la integridad de la información a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma;
 - b) De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona a la que se deba presentar.
- 2) El párrafo 1) será aplicable tanto si el requisito en él previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que la información no sea presentada o conservada en su forma original.
- 3) Para los fines del inciso a) del párrafo 1):

- a) La integridad de la información será evaluada conforme al criterio de que haya permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de su comunicación, archivo o presentación; y
 - b) El grado de fiabilidad requerido será determinado a la luz de los fines para los que se generó la información y de todas las circunstancias del caso.
- 4) Lo dispuesto en el presente artículo no será aplicable a: [...].

Artículo 9. Admisibilidad y fuerza probatoria de los mensajes de datos

- 1) En todo trámite legal, no se dará aplicación a regla alguna de la prueba que sea óbice para la admisión como prueba de un mensaje de datos:
- a) Por la sola razón de que se trate de un mensaje de datos; o
 - b) Por razón de no haber sido presentado en su forma original, de ser ese mensaje la mejor prueba que quepa razonablemente esperar de la persona que la presenta.
- 2) Toda información presentada en forma de mensaje de datos gozará de la debida fuerza probatoria. Al valorar la fuerza probatoria de un mensaje de datos se habrá de tener presente la fiabilidad de la forma en la que se haya generado, archivado o comunicado el mensaje, la fiabilidad de la forma en la que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente.

Artículo 10. Conservación de los mensajes de datos

- 1) Cuando la ley requiera que ciertos documentos, registros o informaciones sean conservados, ese requisito quedará satisfecho mediante la conservación de los mensajes de datos, siempre que se cumplan las condiciones siguientes:
- a) Que la información que contengan sea accesible para su ulterior consulta; y
 - b) Que el mensaje de datos sea conservado con el formato en que se haya generado, enviado o recibido o con algún formato que sea demostrable que reproduce con exactitud la información generada, enviada o recibida; y
 - c) Que se conserve, de haber alguno, todo dato que permita determinar el origen y el destino del mensaje, y la fecha y la hora en que fue enviado o recibido.
- 2) La obligación de conservar ciertos documentos, registros o informaciones conforme a lo dispuesto en el párrafo 1) no será aplicable a aquellos datos que tengan por única finalidad facilitar el envío o recepción del mensaje.
- 3) Toda persona podrá recurrir a los servicios de un tercero para observar el requisito mencionado en el párrafo 1), siempre que se cumplan las condiciones enunciadas en los incisos a), b) y c) del párrafo 1).

Capítulo III. Comunicación de los mensajes de datos

Artículo 11. Formación y validez de los contratos

- 1) En la formación de un contrato, de no convenir las partes otra cosa, la oferta y su aceptación podrán ser expresadas por medio de un mensaje de datos. No se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación un mensaje de datos.
- 2) Lo dispuesto en el presente artículo no será aplicable a: [...].

Artículo 12. Reconocimiento por las partes de los mensajes de datos

- 1) 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.
- 2) Lo dispuesto en el presente artículo no será aplicable a: [...].

Artículo 13. Atribución de los mensajes de datos

- 1) Un mensaje de datos proviene del iniciador si ha sido enviado por el propio iniciador.
- 2) En las relaciones entre el iniciador y el destinatario, se entenderá que un mensaje de datos proviene del iniciador si ha sido enviado:
 - a) Por alguna persona facultada para actuar en nombre del iniciador respecto de ese mensaje; o
 - b) Por un sistema de información programado por el iniciador o en su nombre para que opere automáticamente.
- 3) En las relaciones entre el iniciador y el destinatario, el destinatario tendrá derecho a considerar que un mensaje de datos proviene del iniciador, y a actuar en consecuencia, cuando:
 - a) Para comprobar que el mensaje provenía del iniciador, el destinatario haya aplicado adecuadamente un procedimiento aceptado previamente por el iniciador con ese fin; o
 - b) 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.
- 4) El párrafo 3) no se aplicará:
 - a) A partir del momento en que el destinatario haya sido informado por el iniciador de que el mensaje de datos no provenía del iniciador y haya dispuesto de un plazo razonable para actuar en consecuencia; o
 - b) En los casos previstos en el inciso b) del párrafo 3), 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.
- 5) 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 el destinatario, el destinatario tendrá derecho a considerar que el mensaje de datos recibido corresponde al que quería enviar el iniciador, y podrá actuar 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 había dado lugar a algún error en el mensaje de datos recibido.
- 6) El destinatario tendrá derecho a considerar que cada mensaje de datos recibido es un mensaje de datos separado 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 mensaje de datos era un duplicado.

Artículo 14. Acuse de recibo

1) Los párrafos 2) a 4) del presente artículo serán aplicables cuando, al enviar o antes de enviar un mensaje de datos, el iniciador solicite o acuerde con el destinatario que se acuse recibo del mensaje de datos.

2) Cuando el iniciador no haya acordado con el destinatario que el acuse de recibo se dé en alguna forma determinada o utilizando un método determinado, se podrá acusar recibo mediante:

- a) Toda comunicación del destinatario, automatizada o no, o
- b) Todo acto del destinatario,

que basten para indicar al iniciador que se ha recibido el mensaje de datos.

3) Cuando el iniciador haya indicado que los efectos del mensaje de datos estarán condicionados a la recepción de un acuse de recibo, se considerará que el mensaje de datos no ha sido enviado en tanto que no se haya recibido el acuse de recibo.

4) Cuando el iniciador no haya indicado que los efectos del mensaje de datos estarán condicionados a la recepción de un acuse de recibo, si no ha recibido acuse en el plazo fijado o convenido o no se ha fijado o convenido ningún plazo, en un plazo razonable el iniciador:

a) Podrá dar aviso al destinatario de que no ha recibido acuse de recibo y fijar un plazo razonable para su recepción; y

b) De no recibirse acuse dentro del plazo fijado conforme al inciso a), podrá, dando aviso de ello al destinatario, considerar que el mensaje de datos no ha sido enviado o ejercer cualquier otro derecho que pueda tener.

5) Cuando el iniciador reciba acuse de recibo del destinatario, se presumirá que éste ha recibido el mensaje de datos correspondiente. Esa presunción no implicará que el mensaje de datos corresponda al mensaje recibido.

6) 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 presumirá que ello es así.

7) Salvo en lo que se refiere al envío o recepción del mensaje de datos, el presente artículo no obedece al propósito de regir las consecuencias jurídicas que puedan derivarse de ese mensaje de datos o de su acuse de recibo.

Artículo 15. Tiempo y lugar del envío y la recepción de un mensaje de datos

1) De no convenir otra cosa el iniciador y el destinatario, el mensaje de datos se tendrá por expedido cuando entre en un sistema de información que no esté bajo el control del iniciador o de la persona que envió el mensaje de datos en nombre del iniciador.

2) De no convenir otra cosa el iniciador y el destinatario, el momento de recepción de un mensaje de datos se determinará como sigue:

a) Si el destinatario ha designado un sistema de información para la recepción de mensajes de datos, la recepción tendrá lugar:

- i) En el momento en que entre el mensaje de datos en el sistema de información designado; o

ii) 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;

b) Si el destinatario no ha designado un sistema de información, la recepción tendrá lugar al entrar el mensaje de datos en un sistema de información del destinatario.

3) El párrafo 2) será aplicable aun cuando el sistema de información esté ubicado en un lugar distinto de donde se tenga por recibido el mensaje conforme al párrafo 4).

4) De no convenir otra cosa 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. Para los fines del presente párrafo:

a) Si el iniciador o el 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;

b) Si el iniciador o el destinatario no tienen establecimiento, se tendrá en cuenta su lugar de residencia habitual.

5) Lo dispuesto en el presente artículo no será aplicable a: [...].

Segunda parte. Comercio electrónico en materias específicas

Capítulo I. Transporte de mercancías

Artículo 16. Actos relacionados con los contratos de transporte de mercancías

Sin perjuicio de lo dispuesto en la parte I de la presente Ley, el presente capítulo será aplicable a cualquiera de los siguientes actos que guarde relación con un contrato de transporte de mercancías, o con su cumplimiento, sin que la lista sea exhaustiva:

a) i) indicación de las marcas, el número, la cantidad o el peso de las mercancías;

ii) declaración de la índole o el valor de las mercancías;

iii) emisión de un recibo por las mercancías;

iv) confirmación de haberse completado la carga de las mercancías;

b) i) notificación a alguna persona de las cláusulas y condiciones del contrato;

- ii) comunicación de instrucciones al portador;
- c) i) reclamación de la entrega de las mercancías;
- ii) autorización para proceder a la entrega de las mercancías;
- iii) notificación de la pérdida de las mercancías o de los daños que hayan sufrido;
- d) cualquier otra notificación o declaración relativas al cumplimiento del contrato;
- e) promesa de hacer entrega de las mercancías a la persona designada o a una persona autorizada para reclamar esa entrega;
- f) concesión, adquisición, renuncia, restitución, transferencia o negociación de algún derecho sobre mercancías;
- g) adquisición o transferencia de derechos y obligaciones con arreglo al contrato.

Artículo 17. Documentos de transporte

- 1) Con sujeción a lo dispuesto en el párrafo 3), en los casos en que la ley requiera que alguno de los actos enunciados en el artículo 16 se lleve a cabo por escrito o mediante un documento que conste de papel, ese requisito quedará satisfecho cuando el acto se lleve a cabo por medio de uno o más mensajes de datos.
- 2) El párrafo 1) será aplicable tanto si el requisito en él previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que no se lleve a cabo el acto por escrito o mediante un documento.
- 3) Cuando se conceda algún derecho a una persona determinada y a ninguna otra, o ésta adquiera alguna obligación, y la ley requiera que, para que ese acto surta efecto, el derecho o la obligación hayan de transferirse a esa persona mediante el envío, o la utilización, de un documento, ese requisito quedará satisfecho si el derecho o la obligación se transfieren mediante la utilización de uno o más mensajes de datos, siempre que se emplee un método fiable para garantizar la singularidad de ese mensaje o esos mensajes de datos.
- 4) Para los fines del párrafo 3), el nivel de fiabilidad requerido será determinado a la luz de los fines para los que se transfirió el derecho o la obligación y de todas las circunstancias del caso, incluido cualquier acuerdo pertinente.

- 5) Cuando se utilicen uno o más mensajes de datos para llevar a cabo alguno de los actos enunciados en los incisos f) y g) del artículo 16, no será válido ningún documento utilizado para llevar a cabo cualquiera de esos actos, a menos que se haya puesto fin al uso de mensajes de datos para sustituirlo por el de documentos. Todo documento que se emita en esas circunstancias deberá contener una declaración a tal efecto. La sustitución de mensajes de datos por documentos no afectará a los derechos ni a las obligaciones de las partes.
- 6) Cuando se aplique obligatoriamente una norma jurídica a un contrato de transporte de mercancías que esté consignado, o del que se haya dejado constancia, en un documento, esa norma no dejará de aplicarse a un contrato de transporte de mercancías del que se haya dejado constancia en uno o más mensajes de datos por razón de que el contrato conste en ese mensaje o esos mensajes de datos en lugar de constar en un documento.
- 7) Lo dispuesto en el presente artículo no será aplicable a: [...].

**Guía para la incorporación al derecho interno
de la Ley Modelo de la CNUDMI sobre Comercio
Electrónico**

FINALIDAD DE LA PRESENTE GUÍA

1. Al preparar y dar su aprobación a la Ley Modelo de la CNUDMI sobre Comercio Electrónico (denominada en adelante "la Ley Modelo"), la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) tuvo presente que la Ley Modelo ganaría en eficacia para los Estados que fueran a modernizar su legislación si se facilitaba a los órganos ejecutivos y legislativos de los Estados la debida información de antecedentes y explicativa que les ayudara eventualmente a aplicar la Ley Modelo. La Comisión era además consciente de la probabilidad de que la Ley Modelo fuera aplicada por algunos Estados poco familiarizados con las técnicas de comunicación reguladas en la Ley Modelo. La presente guía, que en gran parte está inspirada en los *trabajos preparatorios* de la Ley Modelo, servirá también para orientar a los usuarios de los medios electrónicos de comunicación en los aspectos jurídicos de su empleo, así como a los estudiosos en la materia. En la preparación de la Ley Modelo se partió del supuesto de que el proyecto de Ley Modelo iría acompañado de una guía. Por ejemplo, se decidió que ciertas cuestiones no serían resueltas en el texto de la Ley Modelo sino en la Guía que había de orientar a los Estados en la incorporación de su régimen al derecho interno. En la información presentada en la Guía se explica cómo las disposiciones incluidas en la Ley Modelo enuncian los rasgos mínimos esenciales de toda norma legal destinada a lograr los objetivos de la Ley Modelo. Esa información puede también ayudar a los Estados a determinar si existe alguna disposición de la Ley Modelo que tal vez convenga modificar en razón de alguna circunstancia nacional particular.

I. INTRODUCCIÓN A LA LEY MODELO

A. Objetivos

2. El recurso a los modernos medios de comunicación, tales como el correo electrónico y el intercambio electrónico de datos (EDI), se ha difundido con notable rapidez en la negociación de las operaciones comerciales internacionales y cabe prever que el empleo de esas vías de comunicación sea cada vez mayor, a medida que se vaya difundiendo el acceso a ciertos soportes técnicos como la INTERNET y otras grandes vías de información transmitida en forma electrónica. No obstante, la comunicación de datos de cierta trascendencia jurídica en forma de mensajes sin soporte de papel pudiera verse obstaculizada por ciertos impedimentos legales al empleo de mensajes electrónicos, o por la incertidumbre que pudiera haber sobre la validez o eficacia jurídica de esos mensajes. La finalidad de la Ley Modelo es la de ofrecer al legislador nacional un conjunto de reglas aceptables en el ámbito internacional que le permitan eliminar algunos de esos obstáculos jurídicos con miras a crear un marco jurídico que permita un desarrollo más seguro de las vías electrónicas de negociación designadas por el nombre de "comercio electrónico". Los principios plasmados en el régimen de la Ley Modelo ayudarán además a los usuarios del comercio electrónico a encontrar las soluciones contractuales requeridas para superar ciertos obstáculos jurídicos que dificulten ese empleo cada vez mayor del comercio electrónico.

3. La decisión de la CNUDMI de formular un régimen legal modelo para el comercio electrónico se debe a que el régimen aplicable en ciertos países a la comunicación y archivo de información era inadecuado o se había quedado anticuado, al no haberse previsto en ese régimen las modalidades propias del comercio electrónico. En algunos casos, la legislación vigente impone o supone restricciones al empleo de los modernos medios de comunicación, por ejemplo, por haberse prescrito el empleo de documentos "originales", "manuscritos" o "firmados". Si bien unos cuantos países han adoptado reglas especiales para regular determinados aspectos del comercio electrónico, se hace sentir en todas partes la ausencia de un régimen general del comercio electrónico. De ello puede resultar incertidumbre acerca de la naturaleza jurídica y la validez de la información presentada en otra forma que no sea la de un documento tradicional sobre papel. Además, la necesidad de un marco legal seguro y de prácticas eficientes se hace sentir no sólo en aquellos países en los que se está difundiendo el empleo del EDI y del correo electrónico sino también en otros muchos países en los que se ha difundido el empleo del fax, el télex y otras técnicas de comunicación parecidas.

4. Además, la Ley Modelo puede ayudar a remediar los inconvenientes que dimanen del hecho de que un régimen legal interno inadecuado puede obstaculizar el comercio internacional, al depender una parte importante de ese comercio de la utilización de las modernas técnicas de comunicación. La diversidad de los regímenes internos aplicables a esas técnicas de comunicación y la incertidumbre a que dará lugar esa disparidad pueden contribuir a limitar el acceso de las empresas a los mercados internacionales.

5. Además, la Ley Modelo puede resultar un valioso instrumento, en el ámbito internacional, para interpretar ciertos convenios y otros instrumentos internacionales existentes que impongan de hecho algunos obstáculos al empleo del comercio

electrónico, al prescribir, por ejemplo, que se han de consignar por escrito ciertos documentos o cláusulas contractuales. Caso de adoptarse la Ley Modelo como regla de interpretación al respecto, los Estados partes en esos instrumentos internacionales dispondrían de un medio para reconocer la validez del comercio electrónico sin necesidad de tener que negociar un protocolo para cada uno de esos instrumentos internacionales en particular.

6. Los objetivos de la Ley Modelo, entre los que figuran el de permitir o facilitar el empleo del comercio electrónico y el de conceder igualdad de trato a los usuarios de mensajes consignados sobre un soporte informático que a los usuarios de la documentación consignada sobre papel, son esenciales para promover la economía y la eficiencia del comercio internacional. Al incorporar a su derecho interno los procedimientos prescritos por la Ley Modelo para todo supuesto en el que las partes opten por emplear medios electrónicos de comunicación, un Estado estará creando un entorno legal neutro para todo medio técnicamente viable de comunicación comercial.

B. Ámbito de aplicación

7. El título de la Ley Modelo habla de "comercio electrónico". Si bien en el artículo 2 se da una definición del "intercambio electrónico de datos (EDI)", la Ley Modelo no especifica lo que se entiende por "comercio electrónico". Al preparar la Ley Modelo, la Comisión decidió que, al ocuparse del tema que tenía ante sí, se atendería a una concepción amplia del EDI que abarcara toda una gama de aplicaciones del mismo relacionadas con el comercio que podrían designarse por el amplio término de "comercio electrónico" (véase A/CN.9/360, párrs. 28 y 29), aunque otros términos descriptivos sirvieran igual de bien. Entre los medios de comunicación recogidos en el concepto de "comercio electrónico" cabe citar las siguientes vías de transmisión basadas en el empleo de técnicas electrónicas: la comunicación por medio del EDI definida en sentido estricto como la transmisión de datos de una terminal informática a otra efectuada en formato normalizado; la transmisión de mensajes electrónicos utilizando normas patentadas o normas de libre acceso; y la transmisión por vía electrónica de textos de formato libre, por ejemplo, a través de la INTERNET. Se señaló también que, en algunos casos, la noción de "comercio electrónico" sería utilizada para referirse al empleo de técnicas como el télex y la telecopia o fax.

8. Conviene destacar que si bien es cierto que al redactarse la Ley Modelo se tuvo siempre presente las técnicas más modernas de comunicación, tales como el EDI y el correo electrónico, los principios en los que se inspira, así como sus disposiciones, son igualmente aplicables a otras técnicas de comunicación menos avanzadas, como el fax. En algunos casos, un mensaje en formato numérico expedido inicialmente en forma de mensaje EDI normalizado será transformado, en algún punto de la cadena de transmisión entre el expedidor y el destinatario, en un mensaje télex expedido a través de una terminal informática o en un fax recibido por la impresora informática del destinatario. Un mensaje de datos puede nacer en forma de una comunicación verbal y ser recibido en

forma de fax, o puede nacer en forma de fax que se entrega al destinatario en forma de mensaje EDI. Una de las características del comercio electrónico es la de que supone el empleo de mensajes programables, cuya programación en una terminal informática constituye el rasgo diferencial básico respecto de los documentos tradicionales consignados sobre papel. Todos estos supuestos están previstos por la Ley Modelo, que responde así a la necesidad en que se encuentran los usuarios del comercio electrónico de poder contar con un régimen coherente que sea aplicable a las diversas técnicas de comunicación que cabe utilizar indistintamente. Cabe señalar que, en principio, no se excluye ninguna técnica de comunicación del ámbito de la Ley Modelo, que debe acoger en su régimen toda eventual innovación técnica en este campo.

9. Los objetivos de la Ley Modelo serán mejor logrados cuanto mayor sea su aplicación. Por ello, aun cuando la Ley Modelo prevé la posibilidad de que se excluyan ciertos supuestos del ámbito de aplicación de los artículos 6, 7, 8, 11, 12, 15 y 17, todo Estado que adopte su régimen podrá decidir no imponer en su derecho interno ninguna restricción importante al ámbito de aplicación de la Ley Modelo.

10. Cabe considerar a la Ley Modelo como un régimen especial bien definido y equilibrado que se recomienda incorporar al derecho interno en forma de norma unitaria de rango legal. Ahora bien, según cuál sea la situación interna de cada Estado, procederá incorporar el régimen de la Ley Modelo en una o en varias normas de rango legal (véase más adelante, el párr. 143).

C. Estructura

11. La Ley Modelo está dividida en dos partes, la primera regula el comercio electrónico en general y la segunda regula el empleo de ese comercio en determinadas ramas de actividad comercial. Cabe señalar que la segunda parte de la Ley Modelo, que se ocupa del comercio electrónico en determinadas esferas consta únicamente del capítulo I dedicado a la utilización del comercio electrónico en el transporte de mercancías. En el futuro tal vez sea preciso regular otras ramas particulares del comercio electrónico, por lo que se ha de considerar a la Ley Modelo como un instrumento abierto destinado a ser complementado por futuras adiciones.

12. La CNUDMI tiene previsto mantenerse al corriente de los avances técnicos, jurídicos y comerciales que se produzcan en el ámbito de aplicación de la Ley Modelo. De juzgarlo aconsejable, la Comisión podría decidir introducir nuevas disposiciones modelo en el texto de la Ley Modelo o modificar alguna de las disposiciones actuales.

D. Una ley "marco" que habrá de ser completada por un reglamento técnico

13. La Ley Modelo tiene por objeto enunciar los procedimientos y principios básicos para facilitar el empleo de las técnicas modernas de comunicación para consignar y comunicar información en diversos tipos de circunstancias. No obstante, se trata de una ley "marco" que no enuncia por sí sola todas las reglas necesarias para aplicar esas técnicas de comunicación en la práctica. Además, la Ley Modelo no tiene por objeto

regular todos los pormenores del empleo del comercio electrónico. Por consiguiente, el Estado promulgante tal vez desee dictar un reglamento para pormenorizar los procedimientos de cada uno de los métodos autorizados por la Ley Modelo a la luz de las circunstancias peculiares y posiblemente variables de ese Estado, pero sin merma de los objetivos de la Ley Modelo. Se recomienda que todo Estado, que decida reglamentar más en detalle el empleo de estas técnicas, procure no perder de vista la necesidad de mantener la encomiable flexibilidad del régimen de la Ley Modelo.

14. Cabe señalar que, además de plantear cuestiones de procedimiento que tal vez hayan de ser resueltas en el reglamento técnico de aplicación de la ley, las técnicas para consignar y comunicar información consideradas en la Ley Modelo pueden plantear ciertas cuestiones jurídicas cuya solución no ha de buscarse en la Ley Modelo, sino más bien en otras normas de derecho interno, como serían las normas eventualmente aplicables de derecho administrativo, contractual, penal o procesal, las cuales quedan fuera del ámbito asignado a la Ley Modelo.

E. Criterio del "equivalente funcional"

15. La Ley Modelo se basa en el reconocimiento de que los requisitos legales que prescriben el empleo de la documentación tradicional con soporte de papel constituyen el principal obstáculo para el desarrollo de medios modernos de comunicación. En la preparación de la Ley Modelo se estudió la posibilidad de abordar los impedimentos al empleo del comercio electrónico creados por esos requisitos ampliando el alcance de conceptos como los de "escrito", "firma" y "original" con miras a dar entrada al empleo de técnicas basadas en la informática. Este criterio se sigue en varios instrumentos legales existentes, como en el artículo 7 de la Ley Modelo de la CNUDMI sobre Arbitraje Comercial Internacional y el artículo 13 de la Convención de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías. Se señaló que la Ley Modelo debería permitir a los Estados adaptar su legislación en función de los avances técnicos de las comunicaciones aplicables al derecho mercantil, sin necesidad de eliminar por completo el requisito de un escrito ni de trastocar los conceptos y planteamientos jurídicos en que se basa dicho requisito. Se dijo, al mismo tiempo, que la observancia de este requisito por medios electrónicos requeriría en algunos casos una reforma de la normativa aplicable al respecto, que tuviera en cuenta una, en particular, de las muchas distinciones entre un documento consignado sobre papel y un mensaje EDI, a saber, que el documento de papel es legible para el ojo humano y el mensaje EDI no lo es, de no ser ese mensaje consignado sobre papel o mostrado en pantalla.

16. Así pues, la Ley Modelo sigue un nuevo criterio, denominado a veces "criterio del equivalente funcional", basado en un análisis de los objetivos y funciones del requisito tradicional de la presentación de un escrito consignado sobre papel con miras a determinar la manera de satisfacer sus objetivos y funciones con técnicas del llamado comercio electrónico. Por ejemplo, ese documento de papel cumple funciones como las siguientes: proporcionar un documento legible para todos; asegurar la inalterabilidad de

un documento a lo largo del tiempo; permitir la reproducción de un documento a fin de que cada una de las partes disponga de un ejemplar del mismo escrito; permitir la autenticación de los datos consignados suscribiéndolos con una firma; y proporcionar una forma aceptable para la presentación de un escrito ante las autoridades públicas y los tribunales. Cabe señalar que, respecto de todas esas funciones, la documentación consignada por medios electrónicos puede ofrecer un grado de seguridad equivalente al del papel y, en la mayoría de los casos, mucha mayor fiabilidad y rapidez, especialmente respecto de la determinación del origen y del contenido de los datos, con tal que se observen ciertos requisitos técnicos y jurídicos. Ahora bien, la adopción de este criterio del equivalente funcional no debe dar lugar a que se impongan normas de seguridad más estrictas a los usuarios del comercio electrónico (con el consiguiente costo) que las aplicables a la documentación consignada sobre papel.

17. Un mensaje de datos no es, de por sí, el equivalente de un documento de papel, ya que es de naturaleza distinta y no cumple necesariamente todas las funciones imaginables de un documento de papel. Por ello se adoptó en la Ley Modelo un criterio flexible que tuviera en cuenta la graduación actual de los requisitos aplicables a la documentación consignada sobre papel: al adoptar el criterio del "equivalente funcional", se prestó atención a esa jerarquía actual de los requisitos de forma, que sirven para dotar a los documentos de papel del grado de fiabilidad, inalterabilidad y rastreabilidad que mejor convenga a la función que les haya sido atribuida. Por ejemplo, el requisito de que los datos se presenten por escrito (que suele constituir un "requisito mínimo") no debe ser confundido con otros requisitos más estrictos como el de "escrito firmado", "original firmado" o "acto jurídico autenticado".

18. La Ley Modelo no pretende definir un equivalente informático para todo tipo de documentos de papel, sino que trata de determinar la función básica de cada uno de los requisitos de forma de la documentación sobre papel, con miras a determinar los criterios que, de ser cumplidos por un mensaje de datos, permitirían la atribución a ese mensaje de un reconocimiento legal equivalente al de un documento de papel que haya de desempeñar idéntica función. Cabe señalar que en los artículos 6 a 8 de la Ley Modelo se ha seguido el criterio del equivalente funcional respecto de las nociones de "escrito", "firma" y "original", pero no respecto de otras nociones jurídicas que en esa Ley se regulan. Por ejemplo, no se ha intentado establecer un equivalente funcional en el artículo 10 de los requisitos actualmente aplicables al archivo de datos.

F. Reglas de derecho supletorio y de derecho imperativo

19. La decisión de emprender la preparación de la Ley Modelo está basada en el reconocimiento de que, en la práctica, la solución de la mayoría de las dificultades jurídicas suscitadas por el empleo de los modernos medios de comunicación suele buscarse por vía contractual. La Ley Modelo enuncia en el artículo 4 el principio de la autonomía de las partes respecto de las disposiciones del capítulo III de la primera parte. El capítulo III incorpora ciertas reglas que aparecen muy a menudo en acuerdos

concertados entre las partes, por ejemplo, en acuerdos de intercambio de comunicaciones o en el "reglamento de un sistema de información" o red de comunicaciones. Conviene tener presente que la noción de "reglamento de un sistema" puede abarcar dos tipos de reglas, a saber, las condiciones generales impuestas por una red de comunicaciones y las reglas especiales que puedan ser incorporadas a esas condiciones generales para regular la relación bilateral entre ciertos iniciadores y destinatarios de mensajes de datos. El artículo 4 (y la noción de "acuerdo" en él mencionada) tiene por objeto abarcar ambos tipos de reglas.

20. Las reglas enunciadas en el capítulo III de la primera parte pueden servir de punto de partida a las partes cuando vayan a concertar esos acuerdos. Pueden también servir para colmar las lagunas u omisiones en las estipulaciones contractuales. Además, cabe considerar que esas reglas fijan una norma de conducta mínima para el intercambio de mensajes de datos en casos en los que no se haya concertado acuerdo alguno para el intercambio de comunicaciones entre las partes, por ejemplo, en el marco de redes de comunicación abiertas.

21. Las disposiciones que figuran en el capítulo II de la primera parte son de distinta naturaleza. Una de las principales finalidades de la Ley Modelo es facilitar el empleo de las técnicas de comunicación modernas, dotando al empleo de dichas técnicas de la certeza requerida por el comercio cuando la normativa por lo demás aplicable cree obstáculos a dicho empleo o sea fuente de incertidumbres que no puedan eliminarse mediante estipulaciones contractuales. Las disposiciones del capítulo II pueden, en cierta medida, considerarse como un conjunto de excepciones al régimen tradicionalmente aplicable a la forma de las operaciones jurídicas. Ese régimen tradicional acostumbra a ser de carácter imperativo, por reflejar, en general, decisiones inspiradas en principios de orden público interno. Debe considerarse que las reglas enunciadas en el capítulo II expresan el "mínimo aceptable" en materia de requisitos de forma para el comercio electrónico, por lo que deberán ser tenidas por imperativas, salvo que en ellas mismas se disponga lo contrario. El hecho de que esos requisitos de forma deban ser considerados como el "mínimo aceptable" no debe, sin embargo, ser entendido como una invitación a establecer requisitos más estrictos que los enunciados en la Ley Modelo.

G. Asistencia de la Secretaría de la CNUDMI

22. En el marco de sus actividades de formación y asistencia, la secretaría de la CNUDMI podrá organizar consultas técnicas para las autoridades públicas que estén preparando alguna norma legal basada en la Ley Modelo de la CNUDMI sobre Comercio Electrónico, o en alguna otra ley modelo de la CNUDMI, o que estén considerando dar su adhesión a algún convenio de derecho mercantil internacional preparado por la CNUDMI.

23. Puede pedirse a la secretaría, cuya dirección se indica a continuación, más información acerca de la Ley Modelo, así como sobre la Guía y sobre otras leyes modelos y convenios preparados por la CNUDMI. La secretaría agradecerá cualquier observación que reciba sobre la Ley Modelo y la Guía, así como sobre la promulgación de cualquier norma legal basada en la Ley Modelo.

Subdivisión de Derecho Mercantil Internacional
Oficina de Asuntos Jurídicos, Naciones Unidas
Centro Internacional de Viena, Apartado Postal 500
A-1400, Viena, Austria
Teléfono: (43-1) 26060-4060 ó 4061
Fax: (43-1) 26060-5813 ó (43-1) 263 3389
Télex: 135612 uno a
Correo-e: uncitral@unov.un.or.at
Dirección de Internet: <http://www.un.or.at/uncitral>

II. OBSERVACIONES ARTÍCULO POR ARTÍCULO

Primera parte. Comercio electrónico en general

Capítulo I. Disposiciones generales

Artículo 1. Ámbito de aplicación

24. La finalidad del artículo 1, que debe leerse conjuntamente con la definición de "mensaje de datos" en el artículo 2 a), es demarcar el ámbito de aplicación de la Ley Modelo. En la Ley Modelo se han querido abarcar, en principio, todas las situaciones de hecho en que se genera, archiva o comunica información, con independencia de cuál sea el soporte en el que se consigne la información. Durante la preparación de la Ley Modelo se consideró que si se excluía alguna forma o algún soporte posible limitando así el alcance de la Ley Modelo, surgirían dificultades prácticas y se incumpliría el objetivo de formular reglas verdaderamente aptas para cualquier soporte electrónico. Ahora bien, el régimen de la Ley Modelo ha sido concebido especialmente para los medios de comunicación cuyo soporte "no sea el papel" y, salvo que su texto disponga expresamente otra cosa, la Ley Modelo no tiene por objeto modificar ninguna regla tradicionalmente aplicable a las comunicaciones sobre soporte de papel.

25. Se opinó, además, que la Ley Modelo debería indicar que estaba concebida para regular los tipos de situaciones que se dan en la esfera comercial y que había sido formulada pensando en las relaciones comerciales. Por esta razón, en el artículo 1 se habla de "actividades comerciales" y en la nota de pie de página **** se explica lo que debe entenderse por ello. Esas indicaciones, que pueden ser particularmente útiles para los países que carecen de un cuerpo especial de derecho mercantil, están inspiradas, por razones de coherencia, en la nota de pie de página correspondiente al artículo 1 de la Ley Modelo de la CNUDMI sobre Arbitraje Comercial Internacional. En ciertos países, el uso de notas de pie de página en un texto legislativo no se consideraría una práctica legislativa aceptable. Así pues, las autoridades nacionales que incorporen la Ley Modelo

podrían estudiar la posible inclusión del texto de las notas de pie de página en el cuerpo de la ley propiamente dicha.

26. La Ley Modelo es aplicable a todos los tipos de mensajes de datos que puedan generarse, archivarse o comunicarse, y nada en la Ley Modelo debería impedir a un Estado que al aplicarla ampliara su alcance a aplicaciones no comerciales del llamado comercio electrónico. Por ejemplo, si bien la Ley Modelo no está especialmente concebida para regular las relaciones entre los usuarios del comercio electrónico y las autoridades públicas, ello no quiere decir que la Ley Modelo no sea aplicable a dichas relaciones. En la nota de pie de página^{***} se sugieren algunas variantes que podrían utilizar los Estados que al incorporar la Ley Modelo estimen apropiado extender su ámbito de aplicación más allá de la esfera comercial.

27. Algunos países disponen de leyes especiales para la protección del consumidor que pueden regular ciertos aspectos del empleo de los sistemas de información. Con respecto a esa legislación protectora del consumidor, al igual que en anteriores instrumentos de la CNUDMI (por ejemplo, la Ley Modelo de la CNUDMI sobre Transferencias Internacionales de Crédito), se estimó que debería indicarse en la Ley Modelo que no se había prestado particular atención en su texto a las cuestiones que podrían suscitarse en el contexto de la protección del consumidor. Se opinó, al mismo tiempo, que no había motivo para excluir del ámbito de aplicación de la Ley Modelo, por medio de una disposición general al efecto, las situaciones que afectaran a consumidores, ya que pudiera estimarse que el régimen de la Ley Modelo resulta adecuado para los fines de la protección del consumidor, al menos en el marco de la normativa aplicable en algunos Estados. En la nota^{**} se reconoce que la legislación protectora del consumidor puede gozar de prelación sobre el régimen de la Ley Modelo. El legislador deberá tal vez considerar si la ley por la que se incorpore la Ley Modelo al derecho interno ha de ser o no aplicable a los consumidores. La determinación de las personas físicas o jurídicas que han de ser tenidas por "consumidores" es una cuestión que se deja al arbitrio de la norma de derecho interno aplicable al efecto.

28. La primera nota de pie de página prevé otra posible limitación del ámbito de aplicación de la Ley Modelo. En principio, la Ley Modelo es aplicable al empleo tanto nacional como internacional de los mensajes de datos. El texto de la nota de pie de página^{*} podrá ser utilizado por todo Estado que desee limitar la aplicabilidad de la Ley Modelo a los casos internacionales. La nota contiene un criterio de internacionalidad al que podrán recurrir dichos Estados para distinguir los casos internacionales de los nacionales. Cabe advertir, sin embargo, que en algunas jurisdicciones, especialmente en Estados federales, podría ser muy difícil distinguir el comercio internacional del comercio nacional. No debe interpretarse esta nota como si alentara a los Estados que incorporen la Ley Modelo a su derecho interno a limitar su aplicabilidad a los casos internacionales.

29. Se recomienda ampliar lo más posible el ámbito de aplicación de la Ley Modelo. Convendría, en particular, que el ámbito de aplicación de la Ley Modelo no quedara reducido a los mensajes de datos internacionales, ya que puede considerarse que esa limitación menoscabaría los objetivos de la Ley Modelo. Además, la diversidad de los

procedimientos previstos en la Ley Modelo (particularmente en los artículos 6 a 8) para limitar el empleo de mensajes de datos si es necesario (por ejemplo, por motivos de orden público) puede hacer innecesario limitar el ámbito de aplicación de la Ley Modelo. Dado que la Ley Modelo contiene diversos artículos (artículos 6, 7, 8, 11, 12, 15 y 17) que otorgan cierto grado de flexibilidad a los Estados que la incorporen a su derecho interno para limitar el ámbito de aplicación de determinados aspectos de dicha Ley, no debería ser necesario restringir el ámbito de aplicación de su régimen al comercio internacional. Cabe señalar asimismo que sería difícil dividir las comunicaciones relacionadas con el comercio internacional en secciones puramente internas o puramente internacionales. La certeza jurídica que se espera obtener de la Ley Modelo es necesaria para el comercio tanto nacional como internacional, y una dualidad de regímenes para la utilización de los medios electrónicos de consignación y comunicación de datos podría crear un grave obstáculo para el empleo de esos medios.

*Referencias:*²

A/50/17, párrs. 213 a 219; A/CN.9/407, párrs. 37 a 40;

A/CN.9/406, párrs. 80 a 85;

A/CN.9/WG.IV/WP.62, artículo 1;

A/CN.9/390, párrs. 21 a 43;

A/CN.9/WG.IV/WP.60, artículo 1;

A/CN.9/387, párrs. 15 a 28;

A/CN.9/WG.IV/WP.57, artículo 1;

A/CN.9/373, párrs. 21 a 25 y 29 a 33;

A/CN.9/WG.IV/WP.55, párrs. 15 a 20.

Artículo 2. Definiciones

"Mensaje de datos"

30. El concepto de "mensaje de datos" no se limita a la comunicación sino que pretende también englobar cualquier información consignada sobre un soporte informático que no esté destinada a ser comunicada. Así pues, el concepto de "mensaje" incluye el de información meramente consignada. No obstante nada impide que, en los ordenamientos jurídicos en que se estime necesario, se añada una definición de "información consignada" que recoja los elementos característicos del "escrito" en el artículo 6.

31. La referencia a "medios similares" pretende reflejar el hecho de que la Ley Modelo no está únicamente destinada a regir las técnicas actuales de comunicación, sino que pretende ser apta para acomodar todos los avances técnicos previsibles. La definición de "mensaje de datos" está formulada en términos por los que se trata de abarcar todo tipo de mensajes generados, archivados o comunicados en alguna forma básicamente distinta del papel. Por ello, al hablar de "medios similares" se trata de abarcar cualquier medio de comunicación y archivo de información que se preste a ser utilizado para alguna de las funciones desempeñadas por los medios enumerados en la definición, aunque, por ejemplo, no cabe decir que un medio "óptico" de comunicación sea estrictamente similar

a un medio "electrónico". Para los fines de la Ley Modelo, el término "similar" denota la noción de "equivalente funcional".

32. La definición de "mensaje de datos" pretende abarcar también el supuesto de la revocación o modificación de un mensaje de datos. Se supone que el contenido de un mensaje de datos es invariable, pero ese mensaje puede ser revocado o modificado por otro mensaje de datos.

"Intercambio electrónico de datos (EDI)"

33. La definición de EDI está tomada de la definición adoptada por el Grupo de Trabajo sobre facilitación de los procedimientos comerciales internacionales (WP.4) de la Comisión Económica para Europa, que es el órgano de las Naciones Unidas que se encarga de elaborar las normas técnicas Naciones Unidas/EDIFACT.

34. La Ley Modelo no resuelve la cuestión de si la definición de EDI supone necesariamente que un mensaje EDI ha de ser comunicado electrónicamente de una terminal informática a otra, o de si esa definición, si bien se refiere básicamente a situaciones en las que se comunica un mensaje de datos a través de un sistema de telecomunicaciones, se refiere también a otros supuestos excepcionales u ocasionales en los que se comunican datos estructurados en forma de un mensaje EDI por algún medio que no suponga el recurso a un sistema de telecomunicaciones, por ejemplo, de enviarse por correo al destinatario un disco magnético que contenga mensajes EDI. Sin embargo, con independencia de que la definición de "EDI" sea o no aplicable a la entrega manual de datos consignados en forma numérica, la definición de "mensaje de datos" de la Ley Modelo sí es aplicable a ese supuesto.

"Iniciador" y "destinatario"

35. En la mayoría de los ordenamientos jurídicos, se utiliza la noción de "persona" para designar a los titulares de derechos y obligaciones y debe ser entendida en el sentido de abarcar tanto a la persona natural como a las sociedades legalmente constituidas o demás personas jurídicas. Se ha previsto que el inciso c) sea aplicable a los mensajes de datos que sean generados automáticamente en una terminal informática o computadora sin intervención humana directa. Ello no debe entenderse, sin embargo en el sentido de que la Ley Modelo autorice la atribución de la titularidad de derechos y obligaciones a una terminal informática. Los mensajes de datos generados automáticamente en una terminal informática sin intervención humana directa deberán ser considerados como "iniciados" por la persona jurídica en cuyo nombre se haya programado la terminal informática. Toda cuestión relativa a la representación o al mandato que se suscite a ese respecto deberá ser resuelta por la normativa aplicable al margen de la Ley Modelo.

36. En el marco de la Ley Modelo, por "destinatario" se ha de entender la persona con la cual el iniciador tiene la intención de comunicarse mediante la transmisión del mensaje de datos, por oposición a cualquier persona que pudiera recibir, retransmitir o copiar el mensaje de datos en el curso de la transmisión. El "iniciador" es la persona que genera el mensaje de datos aun si el mensaje ha sido transmitido por otra persona. La definición de "destinatario" contrasta con la definición de "iniciador", que no hace hincapié en la intención. Cabe señalar que, conforme a estas definiciones de "iniciador" y "destinatario", el iniciador y el destinatario de un determinado mensaje de datos podrían

ser una y la misma persona, por ejemplo en el caso en que el autor del mensaje de datos lo hubiera generado con la intención de archivarlo. Sin embargo, el destinatario que archiva un mensaje transmitido por un iniciador no queda incluido dentro de la definición de "iniciador".

37. La definición de "iniciador" debe tenerse por aplicable no sólo al supuesto en el que se genere información para ser comunicada, sino también al supuesto de que se genere información simplemente para ser archivada. Sin embargo, se ha definido "iniciador" en términos destinados a eliminar la posibilidad de que un destinatario de un mensaje de datos que se limita a archivar ese mensaje pueda ser considerado como iniciador del mismo.

"Intermediario"

38. La Ley Modelo se centra en la relación entre el iniciador y el destinatario, y no en la relación entre el iniciador o el destinatario y uno o más intermediarios. No obstante, la Ley Modelo no desestima la importancia primordial de los intermediarios en las comunicaciones electrónicas. Además, se necesita la noción de "intermediario" en la Ley Modelo para establecer la necesaria distinción entre iniciadores o destinatarios y terceros.

39. La definición de "intermediario" pretende abarcar a los intermediarios profesionales y no profesionales, es decir, a cualquier persona, distinta del iniciador y del destinatario, que desempeñe cualquiera de las funciones de un intermediario. Las principales funciones de un intermediario vienen enunciadas en el inciso e), a saber, la recepción, transmisión y archivo de mensajes de datos por cuenta de otra persona. Los operadores de las redes y otros intermediarios pueden prestar servicios adicionales "con valor añadido" como los de formatear, traducir, consignar, autenticar, certificar y archivar los mensajes de datos y prestar además servicios de seguridad respecto de las operaciones electrónicas. Con arreglo a la Ley Modelo, "intermediario" no se define como categoría genérica sino con respecto a cada mensaje de datos, con lo que se reconoce que la misma persona podría ser el iniciador o el destinatario de un mensaje de datos y ser un intermediario respecto de otro mensaje de datos. La Ley Modelo, que se centra en las relaciones entre iniciadores y destinatarios, no trata en general de los derechos y obligaciones de los intermediarios.

"Sistema de información"

40. La definición de "sistema de información" pretende englobar toda la gama de medios técnicos empleados para transmitir, recibir y archivar información. Por ejemplo, en algunos casos, un "sistema de información" podría referirse a una red de comunicaciones, y en otros casos podría referirse a un buzón electrónico o incluso a una telecopiadora. La Ley Modelo no aborda la cuestión de si el sistema de información está ubicado en un local del destinatario o en algún otro sitio, ya que la ubicación del sistema de información no es un criterio al que se recurra en la Ley Modelo.

Referencias:

A/51/17, párrs. 116 a 138; A/CN.9/407, párrs. 41 a 52;

A/CN.9/406, párrs. 132 a 156;

A/CN.9/WG.IV/WP.62, artículo 2; A/CN.9/390, párrs. 44 a 65;

A/CN.9/WG.IV/WP.60, artículo 2;
A/CN.9/387, párrs. 29 a 52;
A/CN.9/WG.IV/WP.57, artículo 1;
A/CN.9/373, párrs. 11 a 20, 26 a 28 y 35 a 36;
A/CN.9/WG.IV/WP.55, párrs. 23 a 26;
A/CN.9/360, párrs. 29 a 31;
A/CN.9/WG.IV/WP.53, párrs. 25 a 33.

Artículo 3. Interpretación

41. El artículo 3 está inspirado por el artículo 7 de la Convención de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías. Este artículo ofrece orientación a los tribunales y otras autoridades nacionales o locales para la interpretación de la Ley Modelo. El efecto previsto del artículo 3 sería el de limitar la interpretación del régimen uniforme, una vez incorporado a la legislación local, en función únicamente de los conceptos del derecho local.

42. La finalidad del párrafo 1) es señalar a los tribunales y a otras autoridades nacionales que las disposiciones de la Ley Modelo (o las disposiciones de la ley por la que se incorpora su régimen al derecho interno), que si bien se promulgarían como parte de la legislación nacional y, en consecuencia, tendrían carácter interno, deben ser interpretadas con referencia a su origen internacional, a fin de velar por la uniformidad de su interpretación en distintos países.

43. Con respecto a los principios generales en que se basa la Ley Modelo, cabe tener en cuenta la siguiente lista no exhaustiva: 1) facilitar el comercio electrónico en el interior y más allá de las fronteras nacionales; 2) validar las operaciones efectuadas por medio de las nuevas tecnologías de la información; 3) fomentar y estimular la aplicación de nuevas tecnologías de la información; 4) promover la uniformidad del derecho aplicable en la materia; y 5) apoyar las nuevas prácticas comerciales. Si bien la finalidad general de la Ley Modelo es la de facilitar el empleo de los medios electrónicos de comunicación, conviene tener presente que su régimen no trata de imponer en modo alguno el recurso a estos medios de comunicación.

Referencias:

A/50/17, párrs. 220 a 224; A/CN.9/407, párrs. 53 y 54;
A/CN.9/406, párrs. 86 y 87;
A/CN.9/WG.IV/WP.62, artículo 3;
A/CN.9/390, párrs. 66 a 73;
A/CN.9/WG.IV/WP.60, artículo 3;
A/CN.9/387, párrs. 53 a 58;
A/CN.9/WG.IV/WP.57, artículo 3;
A/CN.9/373, párrs. 38 a 42;
A/CN.9/WG.IV/WP.55, párrs. 30 y 31.

Artículo 4. Modificación mediante acuerdo

44. La decisión de preparar una ley modelo partió del reconocimiento de que, en la práctica, se acostumbra a buscar por vía contractual la solución de las dificultades jurídicas planteadas por el empleo de los medios modernos de comunicación. La Ley Modelo apoya, por ello, el principio de la autonomía contractual de las partes. Ahora bien, este principio se enuncia únicamente respecto de las disposiciones que figuran en el capítulo III de la primera parte de la Ley Modelo. Ello se debe a que, las disposiciones del capítulo II de la primera parte constituyen, en cierto modo, un conjunto de excepciones a las reglas tradicionalmente aplicables a la forma de las operaciones jurídicas. Esas reglas suelen ser de derecho imperativo ya que reflejan decisiones inspiradas en motivos de orden público de derecho interno. Por ello, una declaración sin más de la autonomía contractual de las partes respecto de las disposiciones de la Ley Modelo podría ser erróneamente entendida como facultando a las partes para sustraerse por vía contractual a la observancia de reglas de derecho imperativo inspiradas en razones de orden público. Debe considerarse que las disposiciones del capítulo II enuncian el requisito mínimo aceptable en materia de forma de los actos jurídicos, por lo que deberán ser consideradas como de derecho imperativo, salvo que se disponga en ellas expresamente otra cosa. La indicación de que esos requisitos de forma han de ser considerados como el "mínimo aceptable" no deberá ser, sin embargo, entendida como una invitación a establecer requisitos de forma más estrictos en el derecho interno que los enunciados en la Ley Modelo.

45. El artículo 4 ha de ser aplicable no sólo en el contexto de las relaciones entre iniciadores y destinatarios de mensajes de datos sino también en el contexto de las relaciones con intermediarios. Por tanto, las partes podrán sustraerse al régimen peculiar del capítulo III de la primera parte concertando al efecto un acuerdo bilateral o multilateral. No obstante, el texto limita expresamente los efectos de esa autonomía de las partes a los derechos y obligaciones que surjan entre ellas mismas, a fin de no sugerir posibles efectos de su acuerdo sobre los derechos y obligaciones de terceros.

Referencias:

A/51/17, párrs. 68, 90 a 93, 110, 137, 188 y 207 (artículo 10);

A/50/17, párrs. 271 a 274 (artículo 5); A/CN.9/407, párr. 85;

A/CN.9/406, párrs. 88 y 89;

A/CN.9/WG.IV/WP.62, artículo 5;

A/CN.9/390, párrs. 74 a 78;

A/CN.9/WG.IV/WP.60, artículo 5;

A/CN.9/387, párrs. 62 a 65;

A/CN.9/WG.IV/WP.57, artículo 5;

A/CN.9/373, párr. 37;

A/CN.9/WG.IV/WP.55, párrs. 27 a 29.

Capítulo II. Aplicación de los requisitos legales a los mensajes de datos

Artículo 5. Reconocimiento jurídico de los mensajes de datos

46. El artículo 5 enuncia el principio fundamental de que los mensajes de datos no deben ser objeto de discriminación, es decir, de que esos mensajes deberán ser tratados sin disparidad alguna respecto de los documentos consignados sobre papel. Este principio debe ser aplicable aun cuando la ley exija la presentación de un escrito o de un original. Se trata de un principio de aplicación general, por lo que no debe limitarse su alcance a la práctica de la prueba o a otras cuestiones mencionadas en el capítulo II. Conviene recordar, sin embargo, que dicho principio no pretende anular ninguno de los requisitos enunciados en los artículos 6 a 10. Al disponer que "no se negarán efectos jurídicos, validez o fuerza obligatoria (en los textos francés e inglés "fuerza ejecutoria", por ejemplo, del texto de una sentencia) a la información por la sola razón de que esté en forma de mensaje de datos", el artículo 5 se limita a indicar que la forma en que se haya conservado o sea presentada cierta información no podrá ser aducida como única razón para denegar eficacia jurídica, validez o fuerza ejecutoria a esa información. Ahora bien, no debe interpretarse erróneamente el artículo 5 como si fuera un texto por el que se conceda validez jurídica a todo mensaje de datos o a todo dato en él consignado.

Referencias:

A/51/17, párrs. 92 y 97 (artículo 4);

A/50/17, párrs. 225 a 227;

A/CN.9/407, párr. 55;

A/CN.9/406, párrs. 91 a 94;

A/CN.9/WG.IV/WP.62, artículo 5 *bis*;

A/CN.9/390, párrs. 79 a 87;

A/CN.9/WG.IV/WP.60, artículo 5 *bis*;

A/CN.9/387, párrs. 93 y 94.

Artículo 5 bis. Incorporación por remisión

46-1. El artículo 5 *bis* fue aprobado por la Comisión en su 31.º período de sesiones, en junio de 1998. Su finalidad es orientar acerca de la forma en que la legislación cuyo objetivo es facilitar la utilización del comercio electrónico puede regular una situación en la que tal vez sea necesario reconocer determinadas condiciones, aunque no se expresen íntegramente sino que exista una mera remisión a ellos en el mensaje de datos, otorgándoles el mismo grado de validez jurídica que si figurasen íntegramente en el texto del mensaje de datos. Este reconocimiento es aceptable conforme a la legislación de muchos Estados cuando se trata de comunicaciones escritas convencionales, por lo general en el contexto de ciertas normas de derecho que establecen salvaguardias, por ejemplo normas de protección del consumidor. La expresión "incorporación por remisión" se utiliza a menudo como fórmula concisa para describir situaciones en las

que un documento se refiere de manera genérica a disposiciones que se detallan en otro lugar, en vez de reproducirlas íntegramente.

46-2. En el ámbito electrónico, la incorporación por remisión se considera con frecuencia esencial para extender la utilización del intercambio electrónico de datos (EDI), el correo electrónico, los certificados numéricos y otras formas de comercio electrónico. Por ejemplo, las comunicaciones electrónicas están estructuradas normalmente de tal forma que se intercambian grandes cantidades de mensajes, cada uno de ellos con un breve contenido de información, y basándose con mucha mayor frecuencia que los documentos escritos en remisiones a información que puede obtenerse en otro lugar. No debe someterse a los usuarios de las comunicaciones electrónicas a la engorrosa obligación de sobrecargar sus mensajes de datos con abundante texto si pueden aprovechar fuentes externas de información, como bases de datos, glosarios o listas de códigos, y utilizar abreviaturas, códigos y otras remisiones a dicha información.

46-3. Las normas para incorporar por remisión mensajes de datos a otros mensajes de datos pueden ser también fundamentales para la utilización de certificados de clave pública, ya que estos certificados son generalmente anotaciones breves con contenidos estrictamente establecidos y tamaño definido. No obstante, es probable que el tercero de confianza que emite el certificado exija la inclusión de condiciones contractuales pertinentes que limiten su responsabilidad. Por ello, el ámbito, la finalidad y el efecto de un certificado en la práctica comercial serían ambiguos e inciertos de no incorporarse por remisión condiciones externas. Así ocurre especialmente en el marco de comunicaciones internacionales en las que intervienen varias partes que actúan conforme a costumbres y prácticas comerciales diversas.

46-4. El establecimiento de normas para la incorporación por remisión de mensajes de datos a otros mensajes de datos es fundamental para fomentar una infraestructura comercial informatizada. Sin la seguridad jurídica que proporcionan esas normas, existiría un riesgo considerable de que las pruebas tradicionales para determinar la ejecutoriedad de las condiciones que se tratara de incorporar por remisión fueran ineficaces al aplicarse a las condiciones correspondientes al comercio electrónico debido a las diferencias existentes entre los mecanismos del comercio tradicional y del comercio electrónico.

46-5. Si bien el comercio electrónico se basa principalmente en el mecanismo de la incorporación por remisión, el acceso al texto íntegro de la información a la que se remite puede mejorarse notablemente mediante la utilización de comunicaciones electrónicas. Por ejemplo, pueden incluirse en un mensaje localizadores uniformes de recursos, que dirijan al lector al documento de remisión. Dichos localizadores pueden proporcionar hiperenlaces que permitan al lector simplemente situar un mecanismo señalizador (como un ratón) sobre una palabra clave vinculada con un localizador uniforme de recursos. Aparecería entonces el texto de referencia. Al evaluar las posibilidades de acceso al texto de referencia deben tenerse en cuenta, entre otros factores, la disponibilidad (horas de funcionamiento del fondo en el que se encuentra la información y facilidad de acceso a éste); el costo del acceso; la integridad (verificación

del contenido, autenticación del remitente, y mecanismos para la corrección de errores de comunicación), y la posibilidad de que dichas condiciones estén sujetas a posteriores modificaciones (notificación de actualizaciones; notificación de la política de modificaciones).

46-6. Uno de los objetivos del artículo 5 *bis* es facilitar la incorporación por remisión en el ámbito electrónico eliminando la incertidumbre que existe en muchas jurisdicciones con respecto a si las disposiciones que regulan la incorporación por remisión tradicional son aplicables a la incorporación por remisión en el ámbito electrónico. No obstante, al incorporar el artículo 5 *bis* al derecho interno, hay que procurar evitar que los requisitos que regulen la incorporación por remisión en el comercio electrónico sean más restrictivos que los ya existentes para el comercio con soporte de papel.

46-7. Otro de los objetivos de la disposición es reconocer que no debe interferirse en la legislación sobre protección del consumidor ni en otras leyes nacionales o internacionales de carácter imperativo (por ejemplo, las normas para proteger a la parte más débil en los contratos de adhesión). Este resultado puede obtenerse también dando validez a la incorporación por remisión en el ámbito electrónico "en la medida en que lo permita la ley", o enumerando las normas de derecho que no se ven afectadas por el artículo 5 *bis*. No debe interpretarse el artículo 5 *bis* en el sentido de que crea un régimen jurídico específico para la incorporación por remisión en el ámbito electrónico. Conviene más bien entender que el artículo 5 *bis*, al establecer un principio de no discriminación, permite que las reglas internas aplicables a la incorporación por remisión con soporte de papel sean igualmente aplicables a la incorporación por remisión con fines de comercio electrónico. Por ejemplo, en una serie de jurisdicciones, las normas de derecho imperativo existentes sólo reconocen la incorporación por remisión si se cumplen las tres condiciones siguientes: *a*) la cláusula de remisión se inserta en el mensaje de datos; *b*) el documento de referencia, y concretamente sus condiciones generales, son conocidos realmente por la parte contra la que pueda esgrimirse el documento de referencia, y *c*) el documento de referencia es aceptado, además de ser conocido, por dicha parte.

Referencias

A/53/17, párrs. 212 a 221;

A/CN.9/450;

A/CN.9/446, párrs. 14 a 24;

A/CN.9/WG.IV/WP.74;

A/52/17, párrs. 248 a 250;

A/CN.9/437, párrs. 151 a 155;

A/CN.9/WP.71, párrs. 77 a 93;

A/51/17, párrs. 222 y 223;

A/CN.9/421, párrs. 109 y 114;

A/CN.9/WG.IV/WP.69, párrs. 30, 53, 59, 60 y 91;

A/CN.9/407, párrs. 100 a 105 y 117;

A/CN.9/WG.IV/WP.66;

A/CN.9/WG.IV/WP.65;
A/CN.9/406, párrs. 90 y 178 a 179;
A/CN.9/WG.IV/WP.55, párrs. 109 a 113;
A/CN.9/360, párrs. 90 a 95;
A/CN.9/WG.IV/WP.53, párrs. 77 y 78;
A/CN.9/350, párrs. 95 y 96;
A/CN.9/333, párrs. 66 a 68.

Artículo 6. Escrito

47. El artículo 6 tiene la finalidad de definir la norma básica que todo mensaje de datos deberá satisfacer para que pueda considerarse que satisface un requisito (legal, reglamentario o jurisprudencial) de que la información conste o sea presentada por escrito. Conviene señalar que el artículo 6 forma parte de una serie de tres artículos (artículos 6, 7 y 8) que comparten una misma estructura y que deben ser leídos conjuntamente.

48. Durante la preparación de la Ley Modelo se prestó particular atención a las funciones que tradicionalmente desempeñan diversos tipos de "escritos" consignados sobre papel. Por ejemplo, en la siguiente lista no exhaustiva se indican las razones por las cuales el derecho interno acostumbra a requerir la presentación de un "escrito": 1) dejar una prueba tangible de la existencia y la naturaleza de la intención de las partes de comprometerse; 2) alertar a las partes ante la gravedad de las consecuencias de concluir un contrato; 3) proporcionar un documento que sea legible para todos; 4) proporcionar un documento inalterable que permita dejar constancia permanente de la operación; 5) facilitar la reproducción de un documento de manera que cada una de las partes pueda disponer de un ejemplar de un mismo texto; 6) permitir la autenticación mediante la firma del documento de los datos en él consignados; 7) proporcionar un documento presentable ante las autoridades públicas y los tribunales; 8) dar expresión definitiva a la intención del autor del "escrito" y dejar constancia de dicha intención; 9) proporcionar un soporte material que facilite la conservación de los datos en forma visible; 10) facilitar las tareas de control o de verificación ulterior para fines contables, fiscales o reglamentarios; y 11) determinar el nacimiento de todo derecho o de toda obligación jurídica cuya validez dependa de un escrito.

49. Sin embargo, al preparar la Ley Modelo se pensó que sería inadecuado adoptar una noción demasiado genérica de las funciones de un escrito. En los requisitos actuales por los que se requiere la presentación de ciertos datos por escrito, se combina a menudo esa noción de "escrito" con las nociones complementarias, pero distintas, de firma y original. Por ello, al adoptar un criterio funcional, debe prestarse atención al hecho de que el requisito de un "escrito" ha de ser considerado como el nivel inferior en la jerarquía de los requisitos de forma, que proporcionan a los documentos de papel diversos grados de fiabilidad, rastreabilidad e inalterabilidad. El requisito de que los datos se presenten por escrito (lo que constituye un "requisito de forma mínimo") no

debe confundirse con requisitos más estrictos como el de "escrito firmado", "original firmado" o "acto jurídico autenticado". Por ejemplo, en algunos ordenamientos jurídicos un documento escrito que no lleve ni fecha ni firma y cuyo autor no se identifique en el escrito o se identifique mediante un simple membrete, sería considerado como "escrito" pese a su escaso valor probatorio, en ausencia de otra prueba (p.ej., testifical) en lo tocante a la autoría del documento. Además, no debe considerarse que la noción de inalterabilidad sea un requisito absoluto inherente a la noción de escrito, ya que un documento escrito a lápiz podría ser considerado un "escrito" a tenor de algunas definiciones legales. Habida cuenta de cómo se resuelven las cuestiones relativas a la integridad de los datos y a la protección contra el fraude en la documentación consignada sobre un soporte de papel, cabe decir que un documento fraudulento sería no obstante considerado como un "escrito". En general, conviene que las nociones de "valor probatorio" y de "intención (de las partes) de obligarse" sean tratadas en relación a las cuestiones más generales de la fiabilidad y autenticación de los datos, por lo que no deben incluirse en la definición de "escrito".

50. La finalidad del artículo 6 no es establecer el requisito de que, en todos los casos, los mensajes de datos deben cumplir todas las funciones concebibles de un escrito. En vez de concentrarse en funciones específicas de un "escrito", por ejemplo, su función probatoria en el contexto del derecho fiscal o su función de advertencia en el contexto del derecho civil, el artículo 6 se centra en el concepto básico de que la información se reproduce y se lee. En el artículo 5 esta idea se expresa en términos que se consideró que fijaban un criterio objetivo, a saber, que la información de un mensaje de datos debe ser accesible para su ulterior consulta. Al emplear la palabra "accesible" se quiere sugerir que la información en forma de datos informatizados debe ser legible e interpretable y que debe conservarse todo programa informático que sea necesario para hacer legible esa información. En la versión inglesa la palabra "usable" ("disponible"), sobreentendida en la versión española en la noción de accesibilidad no se refiere únicamente al acceso humano sino también a su procesamiento informático. En cuanto a la noción de "ulterior consulta", se prefirió a otras nociones como "durabilidad" o "inalterabilidad", que hubiesen establecido un criterio demasiado estricto, y a nociones como "legibilidad" o "inteligibilidad", que podrían constituir criterios demasiado subjetivos.

51. El principio en que se basan el párrafo 3) de los artículos 6 y 7 y el párrafo 4) del artículo 8 es que todo Estado podrá excluir del ámbito de aplicación de estos artículos ciertas situaciones especificadas en la legislación por la que se incorpore la Ley Modelo al derecho interno. Un Estado tal vez desee excluir expresamente ciertos tipos de situaciones, concretamente en función del propósito del requisito formal de que se trate. Una de estas situaciones podría ser la obligación de notificar por escrito ciertos riesgos de jure o de facto, por ejemplo, las precauciones que se han de observar con ciertos tipos de productos. También cabría excluir específicamente otras situaciones, por ejemplo, en el contexto de las formalidades exigidas en virtud de las obligaciones contraídas por un Estado (por ejemplo, la exigencia de que un cheque se presente por escrito de conformidad con el Convenio que establece una ley uniforme sobre cheques, Ginebra,

1931) y otros tipos de situaciones y normas de su derecho interno que un Estado no pueda modificar por ley.

52. Se incluyó el párrafo 3) con el propósito de dar una mayor aceptabilidad a la Ley Modelo. En él se reconoce que la especificación de exclusiones debe dejarse en manos de cada Estado, a fin de respetar así mejor las diferentes circunstancias nacionales. No obstante, cabe señalar que si se recurre al párrafo 3) para hacer exclusiones generales ello puede minar los objetivos de la Ley Modelo, por lo que debe evitarse el peligro de abusar del párrafo 3) en ese sentido. De multiplicarse las exclusiones del ámbito de aplicación de los artículos 6 a 8, se obstaculizaría innecesariamente el desarrollo de las técnicas modernas de comunicación, ya que la Ley Modelo enuncia principios y criterios de índole básica que debieran ser generalmente aplicables.

Referencias:

A/51/17, párrs. 180 y 181;

A/50/17, párrs. 228 a 241 (artículo 5);

A/CN.9/407, párrs. 56 a 63;

A/CN.9/406, párrs. 95 a 101;

A/CN.9/WG.IV/WP.62, artículo 6;

A/CN.9/390, párrs. 88 a 96;

A/CN.9/WG.IV/WP.60, artículo 6;

A/CN.9/387, párrs. 66 a 80;

A/CN.9/WG.IV/WP.57, artículo 6;

A/CN.9/WG.IV/WP.58, anexo;

A/CN.9/373, párrs. 45 a 62;

A/CN.9/WG.IV/WP.55, párrs. 36 a 49;

A/CN.9/360, párrs. 32 a 43;

A/CN.9/WG.IV/WP.53, párrs. 37 a 45;

A/CN.9/350, párrs. 68 a 78;

A/CN.9/333, párrs. 20 a 28;

A/CN.9/265, párrs. 59 a 72.

Artículo 7. Firma

53. El artículo 7 se basa en el reconocimiento de las funciones que se atribuyen a una firma en las comunicaciones consignadas sobre papel. En la preparación de la Ley Modelo se tomaron en consideración las siguientes funciones de la firma: identificar a una persona; dar certeza a la participación personal de esa persona en el acto de firmar; y asociar a esa persona con el contenido de un documento. Se observó que una firma podía desempeñar además diversas otras funciones, según la naturaleza del documento firmado. Por ejemplo, podía demostrar la intención de una parte contractual de obligarse por el contenido del contrato firmado; la intención de una persona de reivindicar la autoría de un texto; la intención de una persona de asociarse con el contenido de un

documento escrito por otra; y el hecho de que esa persona había estado en un lugar determinado, en un momento dado.

54. Cabe observar que, junto con la firma manuscrita tradicional, existen varios tipos de procedimientos (por ejemplo, estampillado, perforado), a veces denominados también "firmas", que brindan distintos grados de certeza. Por ejemplo, en algunos países existe el requisito general de que los contratos de compraventa de mercaderías por encima de cierto monto estén "firmados" para ser exigibles. Sin embargo, el concepto de la firma adoptado en ese contexto es tal que un sello, un perforado o incluso una firma mecanografiada o un membrete puede considerarse suficiente para satisfacer el requisito de la firma. En el otro extremo del espectro, existen requisitos que combinan la firma manuscrita tradicional con procedimientos de seguridad adicionales como la confirmación de la firma por testigos.

55. Podría ser recomendable desarrollar equivalentes funcionales para los distintos tipos y niveles de firmas requeridas existentes. Ese enfoque aumentaría el nivel de certidumbre en cuanto al grado de reconocimiento legal que podría esperarse del uso de los distintos tipos de autenticación utilizados en la práctica del comercio electrónico como sustitutos de la "firma". Sin embargo, la noción de firma está íntimamente vinculada con el empleo del papel. Además, cualquier esfuerzo por elaborar reglas sobre las normas y procedimientos que deberían utilizarse como sustitutos en casos específicos de "firmas" podría crear el riesgo de vincular irremisiblemente el régimen de la Ley Modelo a una determinada etapa del desarrollo técnico.

56. Para evitar que se niegue validez jurídica a un mensaje que deba autenticarse por el mero hecho de que no está autenticado en la forma característica de los documentos consignados sobre papel, el artículo 7 ofrece una fórmula general. El artículo define las condiciones generales que, de cumplirse, autenticarían un mensaje de datos con suficiente credibilidad para satisfacer los requisitos de firma que actualmente obstaculizan el comercio electrónico. El artículo 7 se centra en las dos funciones básicas de la firma: la identificación del autor y la confirmación de que el autor aprueba el contenido del documento. En el inciso a) del párrafo 1) se enuncia el principio de que, en las comunicaciones electrónicas, esas dos funciones jurídicas básicas de la firma se cumplen al utilizarse un método que identifique al iniciador de un mensaje de datos y confirme que el iniciador aprueba la información en él consignada.

57. El inciso b) del párrafo 1) establece un criterio flexible respecto del grado de seguridad que se ha de alcanzar con la utilización del método de identificación mencionado en el inciso a). El método seleccionado conforme al inciso a) del párrafo 1) deberá ser tan fiable como sea apropiado para los fines para los que se consignó o comunicó el mensaje de datos, a la luz de las circunstancias del caso, así como del acuerdo entre el iniciador y el destinatario del mensaje.

58. Para determinar si el método seleccionado con arreglo al párrafo 1) es apropiado, pueden tenerse en cuenta, entre otros, los siguientes factores jurídicos, técnicos y comerciales: 1) la perfección técnica del equipo utilizado por cada una de las partes; 2) la naturaleza de su actividad comercial; 3) la frecuencia de sus relaciones comerciales; 4) el tipo y la magnitud de la operación; 5) la función de los requisitos de

firma con arreglo a la norma legal o reglamentaria aplicable; 6) la capacidad de los sistemas de comunicación; 7) la observancia de los procedimientos de autenticación establecidos por intermediarios; 8) la gama de procedimientos de autenticación que ofrecen los intermediarios; 9) la observancia de los usos y prácticas comerciales; 10) la existencia de mecanismos de aseguramiento contra el riesgo de mensajes no autorizados; 11) la importancia y el valor de la información contenida en el mensaje de datos; 12) la disponibilidad de otros métodos de identificación y el costo de su aplicación; 13) el grado de aceptación o no aceptación del método de identificación en la industria o esfera pertinente, tanto en el momento cuando se acordó el método como cuando se comunicó el mensaje de datos; y 14) cualquier otro factor pertinente.

59. El inciso b) del párrafo 1) no introduce ninguna distinción entre la situación en que los usuarios del comercio electrónico están vinculados por un acuerdo de comunicaciones y la situación en que las partes no tengan ninguna relación contractual previa relativa al empleo del comercio electrónico. Así pues, puede considerarse que el artículo 7 establece una norma mínima de autenticación para los mensajes de datos intercambiados en ausencia de una relación contractual previa y, al mismo tiempo, da orientación sobre lo que eventualmente podría suplir la firma cuando las partes recurrieran a comunicaciones electrónicas en el contexto de un convenio de comunicaciones. Por consiguiente, la Ley Modelo tiene la finalidad de aportar una orientación útil cuando el derecho interno deje totalmente a la discreción de las partes la cuestión de la autenticación de los mensajes de datos y en un contexto en que los requisitos de firma, normalmente fijados por disposiciones imperativas de derecho interno, no puedan ser alterados mediante acuerdo entre las partes.

60. La noción de "cualquier acuerdo pertinente" debe interpretarse en el sentido de que engloba no sólo los acuerdos bilaterales o multilaterales concertados entre partes que intercambien directamente mensajes de datos (por ejemplo, "acuerdos entre socios comerciales") sino también los acuerdos de comunicaciones (por ejemplo, "contratos de servicios con terceros") en los que participen intermediarios, tales como los acuerdos con redes de comunicación. Los acuerdos entre los usuarios del comercio electrónico y las redes de comunicación puede que remitan a las reglas de la propia red, es decir, a los reglamentos y procedimientos administrativos y técnicos aplicables a la comunicación de mensajes de datos a través de la red. Sin embargo, un acuerdo eventual entre iniciadores y destinatarios de mensajes de datos en cuanto a la utilización de un método de autenticación no constituye de por sí prueba fehaciente de que ese método sea fiable.

61. Cabe señalar que con arreglo a la Ley Modelo, la mera firma de un mensaje de datos mediante el equivalente funcional de una firma manuscrita no basta de por sí para dar validez jurídica al mensaje. La cuestión de la validez jurídica de un mensaje de datos que cumple el requisito de una firma deberá dirimirse con arreglo a la normativa aplicable al margen de la Ley Modelo.

Referencias:

A/51/17, párrs. 180 y 181;

A/50/17, párrs. 242 a 248 (artículo 6);

A/CN.9/407, párrs. 64 a 70;

A/CN.9/406, párrs. 102 a 105;
A/CN.9/WG.IV/WP.62, artículo 7;
A/CN.9/390, párrs. 97 a 109;
A/CN.9/WG.IV/WP.60, artículo 7;
A/CN.9/387, párrs. 81 a 90;
A/CN.9/WG.IV/WP.57, artículo 7;
A/CN.9/WG.IV/WP.58, anexo;
A/CN.9/373, párrs. 63 a 76;
A/CN.9/WG.IV/WP.55, párrs. 50 a 63;
A/CN.9/360, párrs. 71 a 75;
A/CN.9/WG.IV/WP.53, párrs. 61 a 66;
A/CN.9/350, párrs. 86 a 89;
A/CN.9/333, párrs. 50 a 59;
A/CN.9/265, párrs. 49 a 58 y 79 y 80.

Artículo 8. Original

62. Si por "original" se entiende el soporte en el que por primera vez se consigna la información, 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.

63. 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 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 otro. 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.

64. Se debe considerar que el artículo 8 enuncia el requisito de forma mínimo para que un mensaje sea aceptable como el equivalente funcional de un original. Las disposiciones del artículo 8 deben ser consideradas como de derecho imperativo, en la misma medida en que sean consideradas de derecho imperativo las disposiciones actuales relativas a la utilización de documentos originales consignados sobre papel. La indicación de que se han de considerar los requisitos de forma enunciados en el artículo 8 como el "mínimo aceptable" no debe, sin embargo, ser entendido como una invitación a que los Estados establezcan requisitos de forma más severos que los enunciados en la Ley Modelo.

65. El artículo 8 subraya la importancia de la integridad de la información para su originalidad y fija criterios que deberán tenerse en cuenta al evaluar la integridad: la consignación sistemática de la información, garantías de que la información fue consignada sin lagunas y protección de los datos contra toda modificación. El artículo vincula el concepto de originalidad a un método de autenticación y se centra en el método de autenticación que debe utilizarse para cumplir el requisito. El artículo se basa en los siguientes elementos: un criterio sencillo como el de la "integridad" de los datos; una descripción de los elementos que deben tenerse en cuenta al evaluar esa integridad; y un elemento de flexibilidad, como, por ejemplo, una referencia a las circunstancias.

66. En cuanto a las palabras "el momento en que se generó por primera vez en su forma definitiva", empleadas en el párrafo 1) a), cabe señalar que la disposición obedece al propósito de tener en cuenta la situación en que la información se hubiese compuesto primero como documento escrito para ser luego transferida a una terminal informática. En esa situación, el párrafo 1) a) debe interpretarse en el sentido de exigir seguridades de que la información ha permanecido completa e inalterada desde el momento en que se compuso por primera vez como documento escrito y no solamente desde el momento en que se tradujo a formato electrónico. Sin embargo, cuando se creaban y almacenaban diversos borradores antes de componer el mensaje definitivo, no había que interpretar el párrafo 1) a) en el sentido de que exigiera seguridades en cuanto a la integridad de los borradores.

67. En el párrafo 3) a) se enuncian los criterios para evaluar la integridad, teniendo en cuidado de exceptuar las adiciones necesarias al primer mensaje de datos ("original"), como endosos, certificados, notarizaciones, etc. Mientras el contenido de un mensaje de datos sea completo y esté inalterado, las adiciones que sea necesario introducir no afectarán a su calidad de "original". Así, cuando se añade un certificado electrónico al final de un mensaje de datos "original" para certificar que es el "original" o cuando la red informática utilizada inserte automáticamente ciertos datos de transmisión al principio y al final de cada mensaje de datos transmitido, esas adiciones se considerarían

escritos complementarios adjuntados a un escrito "original" o serían asimiladas al sobre y los sellos utilizados para enviar ese escrito "original".

68. Como en otros artículos del capítulo II, debe entenderse el término "la ley", que figura en la frase inicial del artículo 8, como referida no sólo a disposiciones de derecho legislativo o reglamentario, sino también a otras normas de derecho jurisprudencial y de derecho procesal. En algunos países del common law, el término "la ley" sería normalmente interpretado como referido a disposiciones del common law, y no a requisitos de origen propiamente legislativo, por lo que debe tenerse presente que en el marco de la Ley Modelo el término "la ley" abarcaría una y otra fuente del derecho. Ahora bien, la Ley Modelo no utiliza este término para referirse a ramas del derecho que no formen parte del derecho interno y que se designan a veces con cierta imprecisión por términos como el de "*lex mercatoria*" o "derecho mercantil".

69. El párrafo 4), al igual que las disposiciones análogas de los artículos 6 y 7, para facilitar la aceptabilidad de la Ley Modelo. En él se reconoce que la cuestión de especificar exclusiones debería dejarse a discreción de cada Estado, criterio que permitiría tomar debidamente en cuenta las diferentes circunstancias nacionales. No obstante, cabe advertir que los objetivos de la Ley Modelo no se cumplirían si se utilizara el párrafo 4 para establecer excepciones generales. De limitarse el ámbito de aplicación de los artículos 6 a 8 con diversas exclusiones se obstaculizaría innecesariamente el desarrollo de las técnicas de comunicación modernas, puesto que la Ley Modelo brinda una serie de principios y criterios básicos destinados a ser de aplicación general.

Referencias:

A/51/17, párrs. 180 y 181 y 185 a 187;

A/50/17, párrs. 249 a 255 (artículo 7);

A/CN.9/407, párrs. 71 a 79;

A/CN.9/406, párrs. 106 a 110;

A/CN.9/WG.IV/WP.58, anexo;

A/CN.9/373, párrs. 77 a 96;

A/CN.9/WG.IV/WP.55, párrs. 64 a 70;

A/CN.9/360, párrs. 60 a 70;

A/CN.9/WG.IV/WP.62, artículo 8;

A/CN.9/390, párrs. 110 a 133;

A/CN.9/WG.IV/WP.60, artículo 8;

A/CN.9/387, párrs. 91 a 97;

A/CN.9/WG.IV/WP.57, artículo 8;

A/CN.9/WG.IV/WP.53, párrs. 56 a 60;

A/CN.9/350, párrs. 84 y 85;

A/CN.9/265, párrs. 43 a 48.

Artículo 9. Admisibilidad y fuerza probatoria de un mensaje de datos

70. La finalidad del artículo 9 es establecer la admisibilidad de los mensajes de datos como pruebas en actuaciones legales y su fuerza probatoria. Con respecto a la admisibilidad, el párrafo 1), al disponer que no debe negarse la admisibilidad de los

mensajes de datos como pruebas en actuaciones judiciales por la sola razón de que figuran en formato electrónico, hace hincapié en el principio general enunciado en el artículo 4 y es necesario para hacerlo expresamente aplicable a la admisibilidad de la prueba, aspecto en que podrían plantearse cuestiones particularmente complejas en ciertas jurisdicciones. El término "la mejor prueba" expresa un tecnicismo necesario en ciertas jurisdicciones de common law. No obstante, el concepto de "la mejor prueba" puede ser fuente de incertidumbre en los ordenamientos jurídicos que desconocen esa regla. Los Estados en que la expresión carezca de sentido y pueda causar malentendidos tal vez deseen adoptar el régimen modelo sin hacer referencia a la regla de "la mejor prueba", enunciada en el párrafo 1).

71. Por lo que respecta a la fuerza probatoria de un mensaje de datos, el párrafo 2) da orientación útil sobre cómo evaluar la fuerza probatoria de los mensajes de datos (por ejemplo, en función de si han sido consignados, archivados o comunicados de forma fiable).

Referencias:

A/50/17, párrs. 256 a 263;
A/CN.9/407, párrs. 80 y 81 (artículo 8);
A/CN.9/406, párrs. 111 a 113;
A/CN.9/WG.IV/WP.62, artículo 9;
A/CN.9/390, párrs. 134 a 143;
A/CN.9/WG.IV/WP.60, artículo 9;
A/CN.9/387, párrs. 98 a 109;
A/CN.9/WG.IV/WP.57, artículo 9;
A/CN.9/WG.IV/WP.58, anexo;
A/CN.9/373, párrs. 97 a 108;
A/CN.9/WG.IV/WP.55, párrs. 71 a 81;
A/CN.9/360, párrs. 44 a 59;
A/CN.9/WG.IV/WP.53, párrs. 46 a 55;
A/CN.9/350, párrs. 79 a 83 y 90 y 91;
A/CN.9/333, párrs. 29 a 41;
A/CN.9/265, párrs. 27 a 48.

Artículo 10. Conservación de los mensajes de datos

72. El artículo 10 establece un conjunto de nuevas reglas con respecto a los requisitos actuales de conservación de la información (por ejemplo, a efectos contables o fiscales) a fin de evitar que esos requisitos obstaculicen el desarrollo comercial moderno.

73. El párrafo 1) tiene la finalidad de fijar las condiciones en los que se cumpliría la obligación de conservar mensajes de datos que pudiera existir con arreglo a la ley aplicable. En el inciso a) se reproducen las condiciones enunciadas en el artículo 6 para que un mensaje de datos satisfaga la regla que exige la presentación de un escrito. En el inciso b) se pone de relieve que no es preciso conservar el mensaje sin modificaciones, a condición de que la información archivada reproduzca con exactitud el mensaje de datos en la forma recibida. No sería apropiado exigir que la información se conservara sin

modificaciones, ya que por regla general los mensajes son descodificados, comprimidos o convertidos antes de ser archivados.

74. El inciso c) tiene la finalidad de englobar toda la información que debe archivar, que incluye, aparte del mensaje propiamente dicho, cierta información sobre la transmisión que puede resultar necesaria para identificar el mensaje. El inciso c), al imponer la conservación de la información de transmisión relacionada con el mensaje de datos, creaba una norma más exigente que la mayoría de las normas nacionales vigentes respecto de la conservación de comunicaciones consignadas sobre papel. No obstante, no debía interpretarse en el sentido de imponer una obligación de conservar la información relativa a la transmisión que fuese adicional a la contenida en el mensaje de datos al momento de su generación, almacenamiento o transmisión o la información en un mensaje de datos separado, como un acuse de recibo. Además, si bien cierta información sobre la transmisión es importante y debe conservarse, puede exceptuarse otra información relativa a la transmisión sin que ello merme la integridad del mensaje de datos. Esta es la razón por la cual el inciso c) distingue entre los elementos de la información sobre la transmisión que son importantes para la identificación del mensaje y los escasos elementos de dicha información abarcados en el párrafo 2) (como los protocolos de comunicaciones) que carecen totalmente de valor para el mensaje de datos y que normalmente serían separados automáticamente de un mensaje de datos por la terminal receptora antes de que el mensaje de datos entrase efectivamente en el sistema de información del destinatario.

75. En la práctica, la conservación de información, especialmente de la relativa a la transmisión, puede estar a cargo muchas veces de alguien que no sea ni el iniciador ni el destinatario, como un intermediario. En todo caso, la intención consiste en que la persona obligada a conservar cierta información relativa a la transmisión no pueda aducir para no cumplirla que, por ejemplo, el sistema de comunicaciones que utiliza la otra persona no conserva la información necesaria. Con ello se pretende desalentar las malas prácticas o las conductas dolosas. El párrafo 3) dispone que, para cumplir las obligaciones que le incumben con arreglo al párrafo 1), el iniciador o el destinatario puede recurrir a los servicios de cualquier tercero y no solamente de un intermediario.

Referencias:

A/51/17, párrs. 185 a 187;

A/50/17, párrs. 264 a 270 (artículo 9);

A/CN.9/407, párrs. 82 a 84;

A/CN.9/406, párrs. 59 a 72;

A/CN.9/WG.IV/WP.60 artículo 14;

A/CN.9/387, párrs. 164 a 168;

A/CN.9/WG.IV/WP.57, artículo 14;

A/CN.9/373, párrs. 123 a 125;

A/CN.9/WG.IV/WP.55, párr. 94.

CAPÍTULO III. COMUNICACIÓN DE MENSAJES DE DATOS

Artículo 11. Formación y validez de los contratos

76. El artículo 11 no tiene por objeto interferir con el régimen relativo a la formación de los contratos, sino promover el comercio internacional dando mayor certeza jurídica a la celebración de contratos por medios electrónicos. El artículo no trata solamente de la formación del contrato sino también de la forma en que cabría expresar la oferta y la aceptación de la misma. En ciertos países, una disposición enunciada en los términos del párrafo 1) podría considerarse como la mera expresión de algo evidente como que la oferta y la aceptación pueden ser comunicadas por cualquier medio, incluidos los mensajes de datos. No obstante, la disposición es necesaria debido a la incertidumbre que subsiste en numerosos países sobre la posibilidad de que un contrato pueda perfeccionarse válidamente por medios electrónicos. Esa incertidumbre dimana del hecho de que, en ciertos casos, los mensajes de datos en los que se expresaban la oferta y la aceptación bien eran generados por una terminal informática sin que hubiera una intervención humana inmediata, dando así lugar a dudas en cuanto a la expresión de voluntad de las partes. Otra razón de esa incertidumbre era inherente a la modalidad de comunicación y se debe a la ausencia de un documento escrito.

77. Cabe señalar asimismo que el párrafo 1) refuerza, en el contexto de la formación de un contrato, un principio ya enunciado en otros artículos de la Ley Modelo, como los artículos 5, 9 y 13, que reconocen la validez jurídica de los mensajes de datos. Sin embargo, el párrafo 1) es necesario, pues el hecho de que los mensajes electrónicos puedan tener valor probatorio y surtir algún efecto, como los dispuestos en los artículos 9 y 13, no significa necesariamente que puedan ser utilizados para celebrar contratos válidos.

78. El párrafo 1) no sólo ha previsto el caso en que tanto la oferta como la aceptación se comunican por vía electrónica sino también el caso en que sólo se comunica por esa vía la oferta o la aceptación. Respecto del lugar y momento de la formación del contrato cuando la oferta o la aceptación de una oferta se expresan por mensaje de datos, la Ley Modelo no dice nada a fin de no interferir con el derecho interno aplicable a la formación del contrato. Se consideró que una disposición de esa índole podría ir más allá del objetivo de la Ley Modelo, que debería limitarse a dar a las comunicaciones electrónicas un grado de certeza jurídica idéntico al de las comunicaciones consignadas sobre papel. La combinación del régimen aplicable a la formación del contrato con las disposiciones del artículo 15 tiene por objeto disipar la incertidumbre sobre el lugar y momento de la formación del contrato cuando la oferta o la aceptación se intercambien electrónicamente.

79. Las palabras "de no convenir las partes otra cosa", que se limitan a reiterar, en el contexto del artículo relativo a la formación del contrato, el reconocimiento de la autonomía de las partes enunciada en el artículo 4, tienen por objeto dejar en claro que la finalidad de la Ley Modelo no es la de imponer el recurso a los medios electrónicos de comunicación a aquellas partes que acostumbren a concertar sus contratos mediante el recurso a la documentación consignada sobre papel. Por ello, el artículo 11 no deberá ser interpretado como limitando en modo alguno la autonomía de las partes que no recurran para la negociación de su contrato a formas de comunicación electrónica.

80. Durante la preparación del párrafo 1), se consideró que existía el riesgo de que esta disposición prevaleciera sobre ciertas disposiciones de derecho interno, de lo contrario aplicables, que prescribieran ciertas formalidades para la formación de determinados contratos. Entre esas formalidades se incluyen la fe pública notarial y otros requisitos de "escriturización" impuestos por consideraciones de orden público, como la necesidad de proteger a ciertas partes o de advertirlas de ciertos riesgos. Por esta razón, el párrafo 2) dispone que el Estado promulgante puede excluir la aplicación del párrafo 1) en determinados supuestos que se especificarán en la legislación que promulgue la Ley Modelo.

Referencias:

A/51/17, párrs. 89 a 94 (artículo 13);

A/CN.9/407, párr. 93;

A/CN.9/406, párrs. 34 a 41;

A/CN.9/WG.IV/WP.60, artículo 12;

A/CN.9/387, párrs. 145 a 151;

A/CN.9/WG.IV/WP.57, artículo 12;

A/CN.9/373, párrs. 126 a 133;

A/CN.9/WG.IV/WP.55, párrs. 95 a 102;

A/CN.9/360, párrs. 76 a 86;

A/CN.9/WG.IV/WP.53, párrs. 67 a 73;

A/CN.9/350, párrs. 93 a 96;

A/CN.9/333, párrs. 60 a 68.

Artículo 12. Reconocimiento por las partes de los mensajes de datos

81. Se añadió el artículo 12 en una etapa avanzada de la preparación de la Ley Modelo, como reconocimiento del hecho de que el artículo 11 se ocupaba únicamente del empleo de los mensajes de datos para la negociación de un contrato, pero el régimen modelo no enunciaba ninguna regla especial respecto de aquellos mensajes que se utilizaban no para concluir un contrato sino en el cumplimiento de una obligación contractual (por ejemplo, la notificación dada de algún defecto en las mercancías, una oferta de pago, la notificación del lugar en el que se daría cumplimiento al contrato, el reconocimiento de una deuda). Dado que en la mayoría de los países se recurre a los medios modernos de comunicación en un cierto clima de incertidumbre jurídica atribuible a la ausencia de una legislación especial al respecto, se juzgó apropiado que la Ley Modelo no se limitara a enunciar el principio general de que el recurso a los medios electrónicos de comunicación no sería objeto de un trato discriminatorio, expresado en el artículo 5, sino que se regularan además algunos supuestos ilustrativos de la correcta observancia de este principio. La formación de un contrato no es sino uno de los supuestos ilustrativos que pueden ser valiosos a este respecto lo que se juzgó necesario ilustrar también la validez jurídica de expresiones unilaterales de la voluntad, tales como notificaciones o declaraciones unilaterales de voluntad emitidas en forma de mensaje de datos.

82. Al igual que en el caso del artículo 11, la finalidad del artículo 12 no es la de imponer el empleo de los medios electrónicos de comunicación sino la de validar ese

empleo, salvo que las partes convengan otra cosa. Por ello, no debe invocarse el artículo 12 para imponer al destinatario las consecuencias jurídicas de un mensaje que le haya sido enviado, si el recurso a un soporte físico distinto del papel para su transmisión sorprende al destinatario.

Referencias:

A/51/17, párrs. 95 a 99 (nuevo artículo 13 bis)

Artículo 13. Atribución de los mensajes de datos

83. El artículo 13 se inspira en el artículo 5 de la Ley Modelo de la CNUDMI sobre Transferencias Internacionales de Crédito, que define las obligaciones del expedidor de una orden de pago. El artículo 13 debe aplicarse cuando se plantee la cuestión de si un mensaje de datos fue realmente enviado por la persona que consta como iniciador. En el caso de una comunicación consignada sobre papel, el problema surgiría a raíz de una firma presuntamente falsificada del supuesto expedidor. En las comunicaciones electrónicas, puede suceder que una persona no autorizada haya enviado el mensaje, pero que la autenticación mediante clave, criptografía o medio similar sea correcta. La finalidad del artículo 13 no es la de asignar responsabilidad, sino la atribución de los mensajes de datos. Establece una presunción de que en ciertas circunstancias un mensaje de datos se consideraría un mensaje emanado del iniciador, y hace una reserva a esa presunción si el destinatario sabía o debiera haber sabido que el mensaje de datos no emanaba del iniciador.

84. El párrafo 1) recuerda el principio de que el iniciador queda vinculado por todo mensaje de datos que haya efectivamente enviado. El párrafo 2) se refiere al supuesto de que el mensaje haya sido enviado por una persona distinta del iniciador facultada para actuar en nombre del iniciador. El propósito del párrafo 2) no altera en nada el régimen interno de la representación o mandato, y la cuestión de si la otra persona estaba, de hecho y de derecho, facultada para actuar en nombre del iniciador se regirá por la norma de derecho interno por lo demás aplicable.

85. El párrafo 3) se ocupa de dos supuestos en los que el destinatario podría considerar que el mensaje de datos emanaba del iniciador: en primer lugar, el supuesto de que el destinatario haya aplicado adecuadamente un procedimiento de autenticación previamente aceptado por el iniciador y en segundo lugar el supuesto de que el mensaje de datos haya resultado de los actos de una persona cuya relación con el iniciador le haya dado acceso a algún método de autenticación del iniciador. Al estipular que el destinatario "tendrá derecho a considerar que un mensaje de datos proviene del iniciador", el párrafo 3), leído juntamente con el párrafo 4) a), tiene por objeto indicar que el destinatario podrá actuar sobre el supuesto de que el mensaje de datos proviene del iniciador hasta el momento en que el iniciador le informe de que el mensaje de datos no es suyo, o hasta el momento en que sepa o deba saber que el mensaje de datos no es del iniciador.

86. Con arreglo al párrafo 3) a), si el destinatario aplica un procedimiento de autenticación previamente convenido y comprueba debidamente que el iniciador es la fuente del mensaje, se presumirá que el mensaje proviene del iniciador. Esa regla es aplicable no sólo al supuesto de que el iniciador y el destinatario hayan convenido entre

sí el procedimiento de autenticación, sino también a aquellos supuestos en los que un iniciador, unilateralmente o como resultado de un acuerdo concertado con un intermediario, designó un procedimiento y convino en quedar obligado por todo mensaje de datos que cumpliera con los requisitos relativos a ese procedimiento. Por ello, el párrafo 3) a) es aplicable no sólo a un acuerdo que entre en vigor a raíz de un acuerdo directo entre el iniciador y el destinatario sino también a todo acuerdo que entre en vigor gracias a la intervención prevista de un tercero proveedor de servicios. Ahora bien, cabe señalar que el párrafo 3) a) será aplicable únicamente si la comunicación entre el iniciador y el destinatario se apoya en un acuerdo previamente concertado, pero no sería aplicable a un mensaje de datos transmitido a través de una red abierta al público en general.

87. El efecto del párrafo 3) b), leído conjuntamente con el párrafo 4) b), es que el iniciador o el destinatario, según sea el caso, sería responsable de todo mensaje de datos no autorizado que pueda demostrarse que ha sido enviado como resultado de una falta o negligencia de esa parte.

88. El párrafo 4) a) no debe interpretarse como si liberara al iniciador, con efecto retroactivo, de las consecuencias de haber enviado un mensaje de datos con independencia de si el destinatario ha actuado ya o no sobre el supuesto de que el mensaje de datos procedía del iniciador. El párrafo 4) no tenía por objeto disponer que la recepción de una notificación conforme al inciso a) anularía retroactivamente el mensaje original. Conforme al inciso a), el iniciador queda liberado del efecto vinculante del mensaje en el momento de recibirse la notificación conforme al inciso a) y no con anterioridad a ese momento. Además, el párrafo 4) no debe ser interpretado como si permitiera que el iniciador se libere de las consecuencias del mensaje de datos informando al destinatario conforme al inciso a), en casos en los que el mensaje haya sido efectivamente enviado por el iniciador y el destinatario haya aplicado adecuadamente un procedimiento razonable de autenticación. Si el destinatario puede probar que el mensaje es del iniciador, sería aplicable la regla del párrafo 1) y no la del inciso a) del párrafo 4). En cuanto al significado de "un plazo razonable", se deberá informar al destinatario con tiempo suficiente para poder actuar en consonancia, por ejemplo, en el caso de un arreglo de suministro "puntual" en el que deberá darse al destinatario tiempo suficiente para que pueda ajustar su cadena de producción.

89. Con respecto al párrafo 4) b) cabe señalar que la Ley Modelo podría dar lugar al resultado de que el destinatario estaría facultado para fiarse del mensaje de datos de haber aplicado debidamente el método de autenticación convenido, aun cuando supiera que el mensaje de datos no era del destinatario. Cuando se elaboró la Ley Modelo se opinó en general que debería aceptarse el riesgo de que se produjera esa situación, con miras a preservar la fiabilidad de los procedimientos de autenticación.

90. El párrafo 5) tiene la finalidad de impedir que el iniciador desautorice el mensaje una vez enviado, a menos que el destinatario sepa, o deba haber sabido, que el mensaje de datos no es el del iniciador. Además, el párrafo 5) se ocupa del supuesto de que haya errores en el contenido del mensaje derivados de errores en la transmisión.

91. El párrafo 6) aborda la cuestión de la duplicación errónea de los mensajes de datos, que reviste considerable importancia en la práctica. Establece la norma de diligencia con que ha de actuar el destinatario a fin de distinguir entre una duplicación errónea de un mensaje de datos y la transmisión de un mensaje de datos separado.

92. Las primeras versiones del artículo 13 contenían un párrafo adicional en el que se expresaba el principio de que la atribución de la autoría del mensaje al iniciador no regulaba en nada las consecuencias jurídicas del mensaje, que habrían de ser determinadas por la norma por lo demás aplicable de derecho interno. Posteriormente se estimó que no era necesario expresar ese principio en la Ley Modelo, pero que debería mencionarse en la presente Guía.

Referencias:

A/51/17, párrs. 189 a 194;

A/50/17, párrs. 275 a 303 (artículo 11);

A/CN.9/407, párrs. 86 a 89;

A/CN.9/406, párrs. 114 a 131;

A/CN.9/WG.IV/WP.62, artículo 10;

A/CN.9/390, párrs. 144 a 153;

A/CN.9/WG.IV/WP.60, artículo 10;

A/CN.9/387, párrs. 110 a 132;

A/CN.9/WG.IV/WP.57, artículo 10;

A/CN.9/373, párrs. 109 a 115;

A/CN.9/WG.IV/WP.55, párrs. 82 a 86.

Artículo 14. Acuse de recibo

93. El empleo funcional de acuses de recibo es una decisión comercial que deben tomar los usuarios del comercio electrónico; la Ley Modelo no tiene la finalidad de imponer ningún procedimiento de este tipo. No obstante, habida cuenta de la utilidad comercial de un sistema de acuse de recibo y del uso extendido de esos sistemas en el contexto del comercio electrónico, se consideró que la Ley Modelo debía abordar una serie de cuestiones jurídicas derivadas del uso de procedimientos de acuse de recibo. Cabe señalar que la noción de "acuse de recibo" se emplea a menudo para abarcar toda una gama de procedimientos, que van desde el simple acuse de recibo de un mensaje no individualizado a la manifestación de acuerdo con el contenido de un mensaje de datos determinado. En muchos casos, el procedimiento de "acuse de recibo" se utilizaría paralelamente al sistema conocido con el nombre de "petición de acuse de recibo" en las administraciones postales. Los acuses de recibo pueden exigirse en diversos tipos de instrumentos, como en los mensajes de datos propiamente tales, en acuerdos sobre comunicaciones bilaterales o multilaterales, o en "reglas de sistema". Cabe tener presente que la variedad de procedimientos de acuse de recibo supone una variedad de costos correspondientes. Las disposiciones del artículo 14 se basan en el supuesto de que los procedimientos de acuse de recibo han de utilizarse a la discreción del iniciador. El artículo 14 no se propone abordar las consecuencias jurídicas que podrían dimanarse del envío de un acuse de recibo, aparte de determinar que se ha recibido el mensaje de datos. Por ejemplo, cuando el iniciador envía una oferta en un mensaje de datos y pide un

acuse de recibo, ese acuse de recibo sólo constituye prueba de que la oferta se ha recibido. Que enviar o no ese acuse de recibo equivalga a una aceptación de la oferta es materia sobre la cual la Ley Modelo no legisla, pues está regida por el derecho de los contratos que escapa al ámbito de la Ley Modelo.

94. La finalidad del párrafo 2) es validar el acuse de recibo mediante cualquier comunicación o acto del destinatario (por ejemplo, la expedición de las mercancías, como acuse de recibo de un pedido de compra) cuando el iniciador no haya convenido con el destinatario que el acuse de recibo se haga de determinada forma. El artículo 14 no aborda el supuesto de que el iniciador haya solicitado unilateralmente que el acuse de recibo se haga de determinada forma, lo que tal vez dé lugar a que la solicitud unilateral del iniciador relativa a la forma del acuse de recibo no altere en nada el derecho del destinatario a acusar recibo mediante cualquier comunicación o acto que sea tenido por suficiente para indicar al iniciador que el mensaje ha sido recibido. Esa interpretación posible del párrafo 2) hace particularmente necesario que se insista en la Ley Modelo en la distinción que ha de hacerse entre los efectos de un acuse de recibo de un mensaje de datos y de toda otra comunicación por la que se responda al contenido de ese mensaje de datos, razón por la cual se juzgó necesario insertar el párrafo 7).

95. El párrafo 3), que regula la situación en que el iniciador ha afirmado que el mensaje de datos depende de que se reciba un acuse de recibo, es aplicable independientemente de si el iniciador ha especificado o no que el acuse de recibo debe recibirse dentro de cierto plazo.

96. La finalidad del párrafo 4) es prever la situación más frecuente que es la que se da cuando se pide un acuse de recibo, sin que el iniciador haga ninguna declaración en el sentido de que el mensaje de datos no producirá efectos hasta que se reciba un acuse de recibo. Esta disposición es necesaria para fijar el momento a partir del cual el iniciador de un mensaje de datos que haya solicitado acuse de recibo quedará exento de las consecuencias jurídicas del envío de ese mensaje de datos, de no haber recibido el acuse de recibo solicitado. Como ejemplo de una situación en la que resultaría particularmente útil una disposición redactada en los términos del párrafo 4) sería el caso de que un iniciador de una oferta de contrato que no hubiera recibido el acuse de recibo solicitado al destinatario de la oferta necesitara saber el momento a partir del cual tendría libertad para trasladar su oferta a otro cliente o socio comercial eventual. Cabe señalar que la disposición no impone ninguna obligación vinculante al iniciador sino que establece meramente medios que permitan a éste, si lo desea, aclarar su situación en casos en que no haya recibido el acuse de recibo solicitado. Cabe observar también que la disposición no impone ninguna obligación al destinatario del mensaje de datos que, en la mayoría de las circunstancias, tendría libertad para confiar o no en un determinado mensaje de datos, siempre y cuando estuviera dispuesto a asumir el riesgo de que el mensaje de datos no fuera fiable por falta de acuse de recibo. Sin embargo, el destinatario está protegido, ya que el iniciador que no reciba el acuse de recibo solicitado no podrá tratar automáticamente el mensaje de datos como si no se hubiera transmitido nunca, sin notificar al destinatario. El procedimiento descrito en el párrafo 4) del artículo 14 queda librado exclusivamente a la discreción del iniciador. Por ejemplo, caso de enviar el

iniciador un mensaje de datos que, conforme al acuerdo entre las partes se debía recibir en cierta fecha, y solicitar un acuse de recibo, el destinatario no podrá denegar la eficacia jurídica del mensaje con sólo abstenerse de hacer el acuse de recibo solicitado.

97. La presunción rebatible enunciada en el párrafo 5) es necesaria para crear certeza y resultaría particularmente útil en el contexto de una comunicación electrónica entre partes no vinculadas por un acuerdo de socios comerciales. La segunda frase del párrafo 5) debe ser leída conjuntamente con el párrafo 5) del artículo 13, en el que se enuncian las condiciones que, caso de cumplirse, permiten al destinatario considerar como válido el texto recibido, aun cuando existiera cierta divergencia entre ese texto y el texto del mensaje de datos tal como fue expedido.

98. El párrafo 6) corresponde a cierto tipo de acuse de recibo, por ejemplo, un mensaje EDIFACT que establezca que el mensaje de datos recibido es sintácticamente correcto, es decir, que puede ser procesado por la terminal receptora. La referencia a los requisitos técnicos, que ha de ser entendida primordialmente como una referencia a la "sintaxis informática" en el contexto de las comunicaciones EDI, puede ser menos importante en el caso de que se utilicen otros medios de comunicación, como el telegrama o el télex. Además de la coherencia debida con las reglas de la "sintaxis informática", los requisitos técnicos enunciados en las normas aplicables tal vez obliguen, por ejemplo, a utilizar ciertos procedimientos para la verificación de la integridad del contenido del mensaje de datos.

99. El párrafo 7) tiene por finalidad eliminar ciertas incertidumbres que pudiera haber sobre el efecto jurídico de un acuse de recibo, por ejemplo, el párrafo 7) indica que no debe confundirse el acuse de recibo con una comunicación relativa al contenido del mensaje del que se acuse recepción.

Referencias:

A/51/17, párrs. 63 a 88 (artículo 12);

A/CN.9/407, párrs. 90 a 92;

A/CN.9/406, párrs. 15 a 33;

A/CN.9/WG.IV/WP.60, artículo 11;

A/CN.387, párrs. 133 a 144;

A/CN.9/WG.IV/WP.57, artículo 11;

A/CN.9/373, párrs. 116 a 122;

A/CN.9/WG.IV/WP.55, párrs. 87 a 93;

A/CN.9/360, párr. 125;

A/CN.9/WG.IV/WP.53, párrs. 80 y 81;

A/CN.9/350, párr. 92;

A/CN.9/333, párrs. 48 y 49.

Artículo 15. Tiempo y lugar del envío y la recepción de un mensaje de datos

100. El artículo 15 deriva del reconocimiento de que, para la aplicación de muchas normas jurídicas, es importante determinar el tiempo y el lugar del recibo de la información. El empleo de las técnicas de comunicación electrónica dificulta la determinación del tiempo y el lugar. No es desusado que los usuarios del comercio

electrónico y otros medios conexos de comunicación se comuniquen de un Estado a otro sin percatarse de la ubicación de los sistemas de información por medio de los cuales se efectúa la comunicación. Además, la ubicación de ciertos sistemas de comunicación bien puede modificarse sin que ninguna de las partes tenga noticia del cambio. La Ley Modelo, pues, tiene por objeto dejar constancia de que la ubicación de los sistemas de información es indiferente y prevé un criterio más objetivo, a saber, el establecimiento de las partes. A ese respecto, cabe señalar que el artículo 15 no tiene por objeto enunciar una regla de conflicto de leyes.

101. El párrafo 1) dispone que un mensaje de datos se considerará expedido a partir del momento en que entre en un sistema de información que no esté bajo el control del iniciador, que puede ser el sistema de información de un intermediario o un sistema de información del destinatario. El concepto de "expedición" se refiere al comienzo de la transmisión electrónica del mensaje de datos. Cuando el término "expedición" tenga un sentido ya definido, conviene tener presente que el artículo 15 se propone complementar y no sustituir el régimen de derecho interno aplicable en la materia. Si la expedición se produce cuando el mensaje de datos llega al sistema de información del destinatario, la expedición según el párrafo 1) y la recepción según el párrafo 2) son simultáneos, excepto cuando el mensaje de datos se expida a un sistema de información del destinatario que no sea el sistema designado por el destinatario con arreglo al inciso a) del párrafo 2).

102. El párrafo 2), cuya finalidad es definir el momento de recepción de un mensaje de datos, aborda la situación en que el destinatario designa unilateralmente un determinado sistema de información para la recepción de un mensaje (en cuyo caso el sistema designado puede o no ser un sistema de información del destinatario), y el mensaje llega a un sistema de información del destinatario que no es el sistema designado. En este supuesto, la recepción tendrá lugar cuando el destinatario recupere el mensaje de datos. Por "sistema de información designado" la Ley Modelo se refiere al sistema que una parte haya designado específicamente, por ejemplo, en el caso en que una oferta estipule expresamente el domicilio al cual se debe enviar la aceptación. La sola indicación de una dirección de correo electrónico o de un número de fax en el membrete o en otro documento no se debe considerar como designación expresa de uno o más sistemas de información.

103. Conviene detenerse a analizar el concepto de "entrada" en un sistema de información, utilizado para definir tanto la expedición como la recepción de un mensaje de datos. Un mensaje de datos entra en un sistema de información desde el momento en que puede ser procesado en ese sistema de información. La cuestión de si un mensaje de datos que entra en un sistema de información es inteligible o utilizable por el destinatario no entra en el ámbito de la Ley Modelo. La Ley Modelo no pretende invalidar las disposiciones de derecho interno conforme a las cuales la recepción de un mensaje puede producirse en el momento en que el mensaje entra en la esfera del destinatario, prescindiendo de si el mensaje es inteligible o utilizable por el destinatario. La Ley Modelo tampoco se ha concebido para ir en contra de los usos del comercio, según los cuales ciertos mensajes cifrados se consideran recibidos incluso antes de que

sean utilizables por el destinatario o inteligibles para dicha persona. Se estimó que la Ley Modelo no debía crear un requisito más estricto que los actualmente aplicados a las comunicaciones consignadas sobre papel, en que un mensaje puede considerarse recibido aunque no resulte inteligible para el destinatario ni pretenda serlo (por ejemplo, cuando se transmiten datos en forma criptográfica a un depositario con el único propósito de su retención en el contexto de la protección de los derechos de propiedad intelectual).

104. Un mensaje de datos no habría de considerarse expedido si simplemente ha llegado al sistema de información del destinatario, pero sin conseguir entrar en él. Cabe señalar que la Ley Modelo no prevé expresamente el mal funcionamiento de los sistemas de información como base para la responsabilidad. En particular, cuando el sistema de información del destinatario no funciona en absoluto o no funciona en la debida forma, o cuando, aun funcionando debidamente, el mensaje de datos no puede entrar en él (por ejemplo, en el caso de una telecopiadora constantemente ocupada), el mensaje no puede considerarse expedido en el sentido de la Ley Modelo. Durante la preparación de la Ley Modelo, se estimó que no debía imponerse al destinatario, mediante una disposición general, la onerosa obligación de mantener su sistema en constante funcionamiento.

105. El párrafo 4) regula el lugar de recepción de un mensaje de datos. Esta disposición se ha incluido en la Ley Modelo con la principal finalidad de prever una peculiaridad del comercio electrónico que tal vez no esté adecuadamente regulada en la legislación vigente, a saber, que muy a menudo el sistema de información del destinatario en el que se recibe o recupera el mensaje de datos no se halla bajo la misma jurisdicción que el destinatario. El párrafo 4) tiene, pues, la principal finalidad de asegurar que el lugar en que se encuentra el sistema de información no sea el elemento determinante, y que haya un vínculo razonable entre el destinatario y lo que se considere el lugar de recepción, y que el iniciador pueda determinar fácilmente ese lugar. La Ley Modelo no contiene disposiciones concretas sobre el modo de designar un sistema de información ni prevé que puedan efectuarse cambios una vez que el destinatario haya designado el sistema.

106. Cabe observar que el párrafo 4), que contiene una referencia a la "operación subyacente", se refiere en realidad a operaciones subyacentes efectivamente realizadas y previstas. Las referencias a "establecimiento", "establecimiento principal" y "lugar de residencia habitual" se introdujeron en el texto para armonizarlo con el artículo 10 de la Convención de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías.

107. El efecto del párrafo 4) es introducir una distinción entre el lugar considerado de recepción y el lugar al que haya llegado realmente el mensaje de datos en el momento de recepción con arreglo al párrafo 2). Esta distinción no debe interpretarse en el sentido de que reparte los riesgos entre el iniciador y el destinatario en caso de alteración o pérdida de un mensaje de datos entre el momento de su recepción con arreglo al párrafo 2) y el momento en que llegó a su lugar de recepción en el sentido del párrafo 4). El párrafo 4) establece meramente una presunción irrefutable sobre un hecho jurídico a la que deberá recurrirse cuando otro cuerpo de leyes (por ejemplo, sobre la formación de contratos o los conflictos de leyes) requiera que se determine el lugar de recepción de un mensaje de

datos. No obstante, durante la preparación de la Ley Modelo se estimó que introducir la noción de un supuesto lugar de recepción de un mensaje de datos como noción distinta del lugar al que llegue realmente dicho mensaje en el momento de su recepción sería inapropiado fuera del contexto de las transmisiones informatizadas (por ejemplo, en el contexto de un telegrama o de un télex). Así pues, el ámbito de aplicación de la disposición estaba limitado a las transmisiones informáticas de mensajes de datos. El párrafo 5) enuncia una limitación adicional que reproduce la fórmula ya utilizada en los artículos 6, 7, 8, 11 y 12 (véase el anterior párr. 69).

Referencias:

A/51/17, párrs. 100 a 115 (artículo 14);
A/CN.9/407, párrs. 94 a 99;
A/CN.9/406, párrs. 42 a 58;
 A/CN.9/WG.IV/WP.60, artículo 13;
A/CN.9/387, párrs. 152 a 163;
 A/CN.9/WG.IV/WP.57, artículo 13;
A/CN.9/373, párrs. 134 a 146;
 A/CN.9/WG.IV/WP.55, párrs. 103 a 108;
A/CN.9/360, párrs. 87 a 89;
 A/CN.9/WG.IV/WP.53, párrs. 74 a 76;
A/CN.9/350, párrs. 97 a 100;
A/CN.9/333, párrs. 69 a 75.

Segunda parte. Comercio electrónico en materias específicas

108. En contraste con las reglas básicas aplicables al comercio electrónico en general, que figuran en la primera parte de la Ley Modelo, la segunda parte contiene reglas de carácter especial. Al preparar la Ley Modelo, la Comisión convino en que se incluyeron en la Ley Modelo esas reglas especiales relativas a determinadas aplicaciones del comercio electrónico, pero de forma tal que su presentación reflejara a la vez el carácter especial de su régimen y su rango legislativo, en nada distinto del de las disposiciones de carácter general enunciadas en la primera parte de la Ley Modelo. Al aprobar la Ley Modelo, la Comisión se limitó a examinar ciertas disposiciones especiales relativas a los documentos de transporte, por lo que se convino en que esas disposiciones figuraran en la Ley Modelo bajo el epígrafe de capítulo I de la segunda parte. Se opinó que esa estructura dejaba abierta la puerta a la adición de otros grupos de disposiciones especiales en forma de capítulos adicionales de la segunda parte de Ley Modelo, conforme se fuera haciendo sentir la necesidad de esos regímenes especiales.

109. La adopción de un régimen especial para determinadas aplicaciones del comercio electrónico, como pudiera ser para la utilización de mensajes EDI como sucedáneos de ciertos documentos de transporte, no supone en modo alguno que las restantes disposiciones de la Ley Modelo no sean también aplicables a esos sucedáneos de los documentos de transporte. En particular, las disposiciones de la segunda parte, tales como los artículos 16 y 17 relativos a la transferencia de derechos sobre mercancías, parten del supuesto de que las garantías de fiabilidad y autenticidad, enunciadas en los

artículos 6 a 8, son igualmente aplicables a los equivalentes electrónicos de los documentos de transporte. La segunda parte de la Ley Modelo no restringe pues en modo alguno el ámbito de aplicación de las disposiciones generales de la Ley Modelo.

Capítulo I. Transporte de mercancías

110. Al preparar la Ley Modelo, la Comisión tomó nota de que el transporte de mercancías era la rama comercial en la que era más probable que se recurriera a las comunicaciones electrónicas, por lo que era asimismo aquella en la que se necesitaba más urgentemente un marco jurídico que facilitara el empleo de esos medios de comunicación. Los artículos 16 y 17 enuncian ciertas disposiciones que son, por igual, aplicables a los documentos de transporte no negociables y a la transferencia de derechos en las mercancías por medio de un conocimiento de embarque negociable o transferible. Los principios enunciados en los artículo 16 y 17 son aplicables no sólo al transporte marítimo sino también al transporte de mercancías por otros medios, tales como al transporte aéreo y al transporte por carretera y ferrocarril.

Artículo 16. Actos relacionados con los contratos de transporte de mercancías

111. El artículo 16, que enuncia el ámbito de aplicación del capítulo I de la segunda parte de la Ley Modelo, ha sido redactado con amplitud de criterio. Ese capítulo sería aplicable a una amplia gama de documentos que se utilizan en el transporte de mercancías, como, por ejemplo, la póliza de fletamento. En la preparación de la Ley Modelo, la Comisión juzgó que al regular en general los contratos de transporte de mercancías, el artículo 16 respondía a la necesidad de regular todo tipo de documentos de transporte, ya fueran negociables o no negociables, sin excluir ningún documento en particular, como pudiera ser la póliza de fletamento. Se señaló que, de no desear un Estado que el capítulo I de la segunda parte fuera aplicable a determinado tipo de documento o de contrato, por ejemplo, caso de considerarse que la inclusión de la póliza de fletamento en el ámbito de ese capítulo encajaría mal en el derecho interno de ese Estado, entonces ese Estado podría recurrir a la cláusula de exclusión enunciada en el párrafo 7) del artículo 17.

112. El artículo 16 es de índole ilustrativa y los actos en él mencionados, pese a ser más propios del comercio marítimo, no son exclusivos de ningún tipo de comercio ya que son actos que podrían ejecutarse en relación con el transporte aéreo o el transporte multimodal de mercancías.

Referencias:

A/51/17, párrs. 139 a 172 y 198 a 204 (proyecto de artículo x);

A/CN.9/421, párrs. 53 a 103;

A/CN.9/WG.IV/WP.69, párrs. 82 a 95;

A/50/17, párrs. 307 a 309;

A/CN.9/407, párrs. 106 a 118;

A/CN.9/WG.IV/WP.67, anexo;

A/CN.9/WG.IV/WP.66, anexo II;

A/49/17, párrs.178, 179 y 201;

A/CN.9/390, párr. 158.

Artículo 17. Documentos de transporte

113. Los párrafos 1) y 2) dimanar de la regla enunciada en el artículo 6. En el contexto de los documentos de transporte, es preciso establecer no sólo un equivalente funcional de la información consignada por escrito de los actos mencionados en el artículo 16, sino también un equivalente funcional de la modalidad de ejecución de dichos actos que se basa en el empleo de un documento consignado sobre papel. La necesidad de un equivalente funcional se refiere especialmente, en este caso, a la función desempeñada por la transferencia de un escrito en la transferencia de ciertos derechos y obligaciones. Por ejemplo, los párrafos 1) y 2) permiten sustituir no sólo el requisito de que el contrato de transporte conste por escrito sino también los requisitos de endoso y transferencia de la posesión aplicables al conocimiento de embarque. Al prepararse la Ley Modelo, se estimó que la disposición del artículo 17 debía ser referida inequívocamente a los actos enunciados en el artículo 16, particularmente en razón de las dificultades, que pudiera haber en determinados países, para el reconocimiento de la transmisión de un mensaje de datos como equivalente funcional de la entrega material de las mercancías o de la transferencia material de un documento de titularidad sobre las mercancías.

114. La referencia que se hace en los párrafos 1), 3) y 6) a "uno o más mensajes de datos" no debe ser entendida de modo distinto que la referencia que se hace en otras disposiciones de la Ley Modelo a "un mensaje de datos", que debe también entenderse como aplicable indistintamente al supuesto en el que se genere un solo mensaje de datos y al supuesto en el que se generen dos o más mensajes de datos como soporte de un cierto elemento de información. La formulación más detallada de esta idea en el artículo 17 refleja meramente la consideración de que, para la transferencia electrónica de derechos, algunas de las funciones que tradicionalmente se llevan a cabo mediante la entrega de un único conocimiento de embarque consignado sobre papel habrán de efectuarse necesariamente mediante la transmisión de más de un mensaje de datos, sin que ese hecho entrañe, de por sí, ninguna consecuencia negativa para la admisibilidad del comercio electrónico para la ejecución de este acto.

115. La lectura conjunta del párrafo 3) y del párrafo 4) tiene por objeto asegurar que un derecho sólo podrá ser transferido a una sola persona, y que sólo una sola persona podrá en un momento dado invocar ese derecho. Esos dos párrafos introducen, por así decir, un requisito que cabe designar como la "garantía de singularidad". Todo procedimiento por el que sea posible transferir un derecho o una obligación por vía electrónica, en lugar de mediante la entrega de un documento de papel, deberá llevar incorporada la garantía de singularidad como rasgo esencial del mismo. Toda red de comunicaciones debe disponer de un dispositivo técnico de seguridad que ofrezca a la comunidad comercial esa garantía de singularidad y la fiabilidad de ese dispositivo deberá ser demostrada convincentemente. Ahora bien, es además preciso posibilitar el cumplimiento por otros medios de ese requisito legal de que se pruebe la fiabilidad de la garantía de singularidad ofrecida en casos en los que, por ejemplo, se utilice habitualmente un documento del tipo del conocimiento de embarque. Se necesita por ello una norma como la enunciada en el párrafo 3) para que se pueda autorizar el empleo de una comunicación electrónica en lugar de un documento consignado sobre papel.

116. Las palabras "a una determinada persona y a ninguna otra" no deben ser entendidas como excluyendo de su ámbito a aquellos casos en los que dos o más personas gocen conjuntamente de la titularidad sobre las mercancías. Por ejemplo, la referencia a "una persona" no tiene por objeto excluir aquellos casos en los que se haya incorporado a un solo conocimiento de embarque un derecho de copropiedad o más de un derecho sobre las mercancías.

117. Tal vez convenga aclarar algo más la noción de la "singularidad" de un mensaje de datos, ya que de lo contrario pudiera ser interpretada erróneamente. Por una parte, todo mensaje de datos enviado a una persona es necesariamente único, aun cuando su función sea la de duplicar un mensaje anterior, ya que ese mensaje de datos será enviado en un momento necesariamente distinto que el de todo otro mensaje de datos enviado anteriormente a esa misma persona. Si se envía un mensaje de datos a otra persona, ese mensaje es incluso más evidentemente único, aun cuando con él se esté transfiriendo el mismo derecho o la misma obligación. Ahora bien, en ese supuesto es probable que toda transferencia, que no sea la primera, sea fraudulenta. Por el contrario, si por "singularidad" se entiende que un mensaje de datos ha de ser de una categoría singular, es preciso señalar que en ese sentido ningún mensaje de datos puede ser único y ninguna transferencia efectuada por medio de un mensaje de datos puede ser única. Tras haber considerado la posibilidad de ese malentendido, la Comisión decidió retener la referencia a la noción de singularidad del mensaje de datos y de singularidad de la transferencia para los fines del artículo 17, ya que las nociones de la "unicidad" o "singularidad" de los documentos de transporte no son algo desconocido para los profesionales del derecho de transporte o para los usuarios de los documentos de transporte. Se decidió, no obstante, aclarar en la presente Guía que las palabras "se emplee un método fiable para garantizar la singularidad de ese mensaje o esos mensajes de datos" deben ser entendidas como referidas a que se ha de utilizar un método fiable que garantice que los mensajes de datos, por los que se expresa el acto de llevar a cabo la transferencia de cierto derecho o cierta obligación de una persona, no puedan ser utilizados por esa persona, o en su nombre, de forma incoherente con cualesquiera otros mensajes de datos por los que se transfiera ese derecho o esa obligación por esa misma persona o en su nombre.

118. El párrafo 5) es un complemento necesario de la garantía de singularidad enunciada en el párrafo 3. La necesidad de seguridad es una consideración indispensable por lo que se ha de asegurar no sólo que el método utilizado ofrece una seguridad razonable de que un mismo mensaje de datos no será multiplicado, sino también de que no se podrán utilizar simultáneamente dos vías de comunicación para un mismo fin. El párrafo 5) aborda la necesidad básica de que se evite el riesgo de duplicar los documentos de transporte. El empleo de más de una forma de comunicación para diversos fines, por ejemplo, el empleo de documentos de papel para los mensajes auxiliares y de comunicaciones electrónicas para los conocimientos de embarque, no plantea ningún problema. Sin embargo, es indispensable para el buen funcionamiento de cualquier sistema basado en el empleo de un equivalente electrónico del conocimiento de embarque que se excluya la posibilidad de que unos mismos derechos puedan ser

incorporados simultáneamente a un mensaje de datos y a un documento de papel. El párrafo 5) prevé asimismo la situación en la que una parte que haya convenido inicialmente en negociar a través de comunicaciones electrónicas haya de proseguirlas mediante el empleo de comunicaciones consignadas sobre papel, caso de resultarle ulteriormente imposible proseguir esas comunicaciones por vía electrónica.

119. La referencia a la noción de "poner fin" al empleo de mensajes de datos queda abierta a interpretación. En particular, la Ley Modelo no especifica quién ha de ser el que ponga término a ese empleo. De desear algún Estado precisar algo más este punto, tal vez desee indicar, por ejemplo, que puesto que el empleo del comercio electrónico suele estar basado en un acuerdo entre las partes, la decisión de "retornar" a las comunicaciones consignadas sobre papel habrá de ser también objeto de un acuerdo entre todas las partes interesadas. De lo contrario, el iniciador gozaría de la facultad de seleccionar unilateralmente los medios de comunicación. También es posible que el Estado que incorpore el nuevo régimen desee disponer que, dado que el tenedor o titular del conocimiento de embarque ha de ser quien aplique el párrafo 5), será el tenedor de este conocimiento el que decida si prefiere ejercer sus derechos a través de un conocimiento de embarque consignado sobre papel o a través de un equivalente electrónico de ese documento, debiendo ser en ese caso el propio tenedor el que asuma los gastos de su decisión.

120. Si bien el párrafo 5) trata expresamente del supuesto en el que se sustituya la utilización de mensajes de datos por la utilización de documentos de papel, su texto puede ser entendido a la inversa. La sustitución de los mensajes de datos por un documento de papel no afectará a ningún derecho que pueda tenerse a devolver el documento de papel a su emisor y reanudar el empleo, en su lugar, de mensajes de datos.

121. La finalidad del párrafo 6) es la de regular directamente la aplicación de ciertas normas jurídicas al transporte de mercancías por mar. Por ejemplo, con arreglo a las Reglas de La Haya y de La Haya-Visby, un contrato de transporte significa un contrato plasmado en un conocimiento de embarque. El empleo de un conocimiento de embarque o de un documento de titularidad similar hace que las Reglas de La Haya y de La Haya-Visby sean imperativamente aplicables al contrato de transporte incorporado a ese documento. Esas reglas no serían automáticamente aplicables a los contratos concertados por uno o más mensajes de datos. Por ello, se juzgó necesario una disposición como la del párrafo 6) a fin de evitar que se excluyera a un contrato del ámbito de aplicación de esas reglas por el mero hecho de que estuviera consignado mensajes de datos en lugar de en un conocimiento de embarque incorporado a un documento de papel. Si bien el párrafo 1) dispone que un mensaje de datos puede ser un medio eficaz para ejecutar los actos mencionados en el artículo 16, esa disposición no se ocupa de las reglas de derecho sustantivo que pudieran ser aplicables a un contrato que esté consignado, o del que se haya dejado constancia, en mensajes de datos.

122. Respecto al significado de la frase "esa norma no dejará de aplicarse" que figura en el párrafo 6), tal vez hubiera sido más sencillo expresar esa misma idea disponiendo que las reglas aplicables a los contratos de transporte que consten en documentos de papel serán asimismo aplicables a los contratos de transporte que consten en mensajes de

datos. Ahora bien, dada la amplitud del ámbito de aplicación del artículo 17, que regula no sólo el supuesto del conocimiento de embarque sino también el supuesto de una diversidad de otros documentos de transporte, una disposición expresada en esos términos hubiera tenido tal vez el efecto no buscado de extender la aplicación de normas como las Reglas de Hamburgo y las Reglas de La Haya-Visby a contratos a los que nunca se tuvo la intención de que esas normas fueran aplicables. La Comisión opinó que la formulación adoptada era la más adecuada para superar el obstáculo dimanante del derecho de que las Reglas de La Haya-Visby y otras normas imperativamente aplicables al conocimiento de embarque no fueran automáticamente aplicables a contratos de transporte consignados en mensajes de datos, sin ampliar inintencionalmente la aplicación de esas normas a otros tipos de contratos.

Referencias:

A/51/17, párrs. 139 a 172 y 198 a 204 (proyecto de artículo x);

A/CN.9/421, párrs. 53 a 103;

A/CN.9/WG.IV/WP.69, párrs. 82 a 95;

A/50/17, párrs. 307 a 309;

A/CN.9/407, párrs. 106 a 118;

A/CN.9/WG.IV/WP.67, anexo;

A/CN.9/WG.IV/WP.66, anexo II;

A/49/17, párrs. 178, 179 y 201;

A/CN.9/390, párr. 158.

III. HISTORIA Y ANTECEDENTES DE LA LEY MODELO

123. La Ley Modelo de la CNUDMI sobre Comercio Electrónico y otros medios conexos de comunicación de datos, fue aprobada por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) de la Asamblea General de las Naciones Unidas en 1996 en cumplimiento de su mandato de fomentar la armonización y unificación del derecho mercantil internacional, con miras a eliminar los obstáculos innecesarios ocasionados al comercio internacional por las insuficiencias y divergencias del derecho interno que afectan a ese comercio. Durante los últimos 25 años, la CNUDMI, en la que colaboran Estados de todas las regiones situados en todos los niveles de desarrollo económico, ha cumplido su mandato formulando convenios internacionales (convenios y convenciones de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías, sobre la prescripción en materia de compraventa internacional de mercaderías, sobre el Transporte Marítimo de Mercancías, 1978 ("Reglas de Hamburgo"), sobre la responsabilidad de los empresarios de terminales de transporte en el comercio internacional, sobre letras de cambio internacionales y pagarés internacionales, sobre Garantías Independientes y Cartas de Crédito Contingente), leyes modelo (las Leyes Modelo de la CNUDMI sobre arbitraje comercial internacional, sobre transferencias internacionales de crédito y sobre la Contratación Pública de Bienes, de Obras y de Servicios), el Reglamento de Arbitraje de la CNUDMI y el Reglamento de Conciliación de la CNUDMI, así como guías jurídicas (de contratos

de obras, de operaciones de comercio compensatorio y de transferencias electrónicas de fondos).

124. La Ley Modelo fue preparada en respuesta al cambio fundamental que se había operado en las comunicaciones entre las partes (denominadas en ocasiones "socios comerciales") que recurrían a las modernas técnicas informáticas o de otra índole para sus relaciones de negocios. La Ley Modelo ofrece a los países un texto normativo ejemplar para la evaluación y modernización de algunos aspectos de su propia normativa legal y de sus prácticas contractuales relativas al empleo de la informática, y demás técnicas de comunicación modernas, en las relaciones comerciales. El texto de la Ley Modelo, reproducido anteriormente, figura en el anexo I del informe de la CNUDMI sobre la labor de su 29º período de sesiones.³

125. La Comisión, en su 17.º período de sesiones (1984), examinó un informe del Secretario General titulado "Aspectos jurídicos del proceso automático de datos" (A/CN.9/254), donde se describían diversas cuestiones jurídicas relativas al valor jurídico de la documentación informática, así como el requisito de un escrito, la autenticación, las condiciones generales, la responsabilidad y los conocimientos de embarque. La Comisión tomó nota de un informe del Grupo de Trabajo sobre facilitación de los procedimientos comerciales internacionales (WP.4), que está copatrocinado por la Comisión Económica para Europa y la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo, y se ocupa de formular los mensajes normalizados de Naciones Unidas/EDIFACT. En ese informe se sugería que, como estos problemas eran esencialmente de derecho mercantil internacional, la Comisión, en su calidad de principal órgano jurídico en esa esfera, parecía ser el foro de convergencia apropiado para realizar y coordinar las actividades necesarias.⁴ La Comisión decidió inscribir en su programa de trabajo, como tema prioritario, la cuestión de las consecuencias jurídicas del procesamiento automático de datos en las corrientes del comercio internacional.⁵

126. En su 18.º período de sesiones (1985), la Comisión examinó un informe del Secretario General titulado "Valor jurídico de los registros computadorizados" (A/CN.9/265). En ese informe se llegó a la conclusión de que, a nivel mundial, se tropieza con menos problemas de lo que cabría esperar en el empleo de datos almacenados en soportes informáticos como prueba en los litigios. Se señaló que uno de los obstáculos jurídicos más graves para el empleo de la informática y de las telecomunicaciones de terminal a terminal en el comercio internacional radicaba en la exigencia de que los documentos estuviesen firmados o consignados sobre papel. Tras deliberar sobre el informe, la Comisión decidió aprobar la siguiente recomendación en la que se expresan algunos de los principios en que se basa la Ley Modelo:

"La Comisión de las Naciones Unidas para el Derecho Mercantil Internacional,

Observando que el empleo del procesamiento automático de datos (PAD) está próximo a quedar firmemente

arraigado en todo el mundo en muchas fases del comercio nacional e internacional, así como en los servicios administrativos,

Observando también que las normas jurídicas referidas a los medios anteriores al PAD basados en el empleo del papel para documentar el comercio internacional pueden crear un obstáculo al empleo del PAD en cuanto llevan a la inseguridad jurídica o dificultan la eficiente utilización del PAD cuando su uso está por lo demás justificado,

Observando asimismo con reconocimiento los esfuerzos del Consejo de Europa, del Consejo de Cooperación Aduanera y de la Comisión Económica de las Naciones Unidas para Europa tendientes a superar los obstáculos que, como consecuencia de estas normas jurídicas, se oponen a la utilización del PAD en el comercio internacional,

Considerando al mismo tiempo que no es necesaria una unificación de las normas sobre la prueba respecto del empleo de registros de computadora en el comercio internacional, vista la experiencia que muestra que diferencias sustanciales en las normas sobre la prueba aplicadas al sistema de documentación sobre papel no han causado hasta el momento ningún daño apreciable al desarrollo del comercio internacional,

Considerando también que, como consecuencia de las novedades en la utilización del PAD, en diversos sistemas jurídicos se viene experimentando la conveniencia de adaptar las normas jurídicas existentes a estas novedades, teniendo debidamente en cuenta, sin embargo, la necesidad de estimular el empleo de los medios del PAD que proporcionarían la misma o mayor fiabilidad que la documentación sobre papel,

1. Recomienda a los gobiernos que:

a) Examinen las normas jurídicas que afectan la utilización de registros de computadora como prueba en los litigios, a fin de eliminar obstáculos innecesarios a su

admisión, asegurarse de que las normas sean coherentes con las novedades de la tecnología y proporcionar medios apropiados para que los tribunales evalúen el crédito que merezcan los datos contenidos en esos registros;

b) Examinen las exigencias legales de que determinadas operaciones comerciales o documentos relacionados con el comercio consten por escrito, para determinar si la forma escrita es una condición de la eficacia de la validez de la operación o el documento, con miras a permitir, según corresponda, que la operación o el documento se registren y transmitan en forma legible mediante computadora;

c) Examinen los requisitos jurídicos de una firma manuscrita u otro método de autenticación sobre papel en los documentos relacionados con el comercio, con miras a permitir, según corresponda, la utilización de medios electrónicos de autenticación;

d) Examinen los requisitos jurídicos de que, para ser presentados a las autoridades, los documentos deban constar por escrito y estar firmados de puño y letra, con miras a permitir que, cuando corresponda, esos documentos se presenten en forma legible mediante computadora a los servicios administrativos que hayan adquirido el equipo necesario y fijado los procedimientos aplicables.

2. Recomienda a las organizaciones internacionales que elaboran textos jurídicos relacionados con el comercio que tengan en cuenta la presente Recomendación al adoptar esos textos y, según corresponda, estudien la posibilidad de modificar los textos jurídicos vigentes en armonía con la presente Recomendación.⁶

127. Dicha recomendación (denominada en adelante "Recomendación de la CNUDMI de 1985") fue aprobada por la Asamblea General en su resolución 40/71, inciso b) del párrafo 5, de 11 de diciembre de 1985 a saber:

"La Asamblea General,

. . . Pide a los gobiernos y a las organizaciones internacionales que, cuando así convenga, adopten medidas de conformidad con la recomendación de la Comisión 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; . . . ".⁷

128. Como se ha señalado en diversos documentos y reuniones relativas al empleo internacional del comercio electrónico, por ejemplo en las reuniones del grupo de trabajo WP.4, se tiene en general la impresión de que pese a la labor efectuada desde que se aprobó la Recomendación de la CNUDMI de 1985, se ha progresado muy poco en la labor de ir eliminando del derecho interno la obligatoriedad legal del papel y de la firma escrita. El Comité Noruego sobre Procedimientos Comerciales (NORPRO) ha sugerido, en una carta a la Secretaría, que "una de las razones por las que se ha progresado tan poco pudiera ser que la recomendación de la CNUDMI señala la necesidad de una actualización jurídica, pero sin dar ninguna indicación de cómo efectuarla". En este sentido, la Comisión consideró qué medidas de seguimiento a la Recomendación de la CNUDMI de 1985 cabría adoptar a fin de estimular la necesaria modernización de la legislación. La decisión de la CNUDMI de formular legislación modelo sobre aspectos jurídicos del intercambio electrónico de datos y otros medios conexos de comunicación de datos puede considerarse una consecuencia del proceso a raíz del cual la Comisión aprobó la Recomendación de la CNUDMI de 1985.

129. En su 21.º período de sesiones (1988), la Comisión consideró una propuesta de que se examinara la necesidad de elaborar unos principios jurídicos aplicables a la formación de los contratos mercantiles internacionales por medios electrónicos. Se señaló la carencia de un marco jurídico bien definido para esta práctica innovadora y cada vez más difundida, y que la labor futura en esa esfera podría contribuir a colmar esa laguna jurídica y a reducir la incertidumbre y las dificultades con las que se tropezaba en la práctica. La Comisión pidió a la Secretaría que preparase un estudio preliminar sobre este tema.⁸

130. En su 23.º período de sesiones (1990), la Comisión tuvo ante sí un informe titulado "Estudio preliminar de las cuestiones jurídicas relacionadas con el perfeccionamiento de contratos por medios electrónicos" (A/CN.9/333). Ese informe contiene un resumen de los trabajos realizados en las Comunidades Europeas y en los Estados Unidos de América con respecto al requisito de la "forma escrita" y otros problemas observados en relación con el perfeccionamiento de los contratos por medios electrónicos. También se examinaron los esfuerzos realizados para superar algunos de los problemas mediante el recurso a acuerdos modelo en el campo de las comunicaciones.⁹

131. En su 24.º período de sesiones (1991), la Comisión tuvo ante sí el informe titulado "Intercambio electrónico de datos" (A/CN.9/350). En ese informe se describían las

actividades actuales de las diversas organizaciones que se ocupaban de las cuestiones jurídicas relacionadas con el intercambio electrónico de datos (EDI) y se analizaba el contenido de diversos modelos de acuerdos de intercambio de información ya preparados o que se estaban preparando. En él se señalaba que esos documentos variaban considerablemente al variar también las necesidades de las diversas categorías de usuarios a las que iban destinados y que esa diversidad de los arreglos contractuales había sido considerada en ocasiones como un obstáculo para el desarrollo de un marco jurídico satisfactorio para la utilización en los negocios del comercio electrónico. Ese informe sugirió que existía la necesidad de un marco general que permitiera identificar las cuestiones importantes y que proporcionara un cuerpo básico de principios y reglas de derecho aplicables a las comunicaciones canalizadas por vía del comercio electrónico. En él se enuncia la conclusión de que cabía crear ese marco básico, pero hasta cierto punto únicamente, mediante arreglos contractuales entre las partes en una relación mantenida por comercio electrónico y que los marcos contractuales existentes que se ofrecían a la comunidad de usuarios del comercio electrónico eran a menudo incompletos, mutuamente incompatibles e inapropiados para su utilización internacional por depender en gran medida de las estructuras del derecho interno local.

132. Con miras a armonizar las reglas básicas del EDI para facilitar su empleo en el comercio internacional, el informe indicaba que tal vez la Comisión deseara considerar la conveniencia de preparar un acuerdo uniforme de comunicaciones para ser aplicado en el comercio internacional. También señalaba que la labor de la Comisión en esta esfera sería de particular interés porque participarían en ella representantes de todos los ordenamientos jurídicos, así como representantes de países en desarrollo que habían tropezado ya o tropezarían pronto con las cuestiones que suscitaba el comercio electrónico.

133. La Comisión convino en que las cuestiones jurídicas que el comercio electrónico planteaba irían siendo cada vez más importantes a medida que se difundía el empleo del comercio electrónico y en que debería emprender trabajos en esta esfera. Recibió amplio apoyo la propuesta de que la Comisión emprendiera la preparación de una serie de principios jurídicos y reglas de derecho básicas aplicables a las comunicaciones por comercio electrónico.¹⁰ La Comisión llegó a la conclusión de que era prematuro iniciar inmediatamente la preparación de un acuerdo uniforme de comunicaciones y tal vez fuese preferible seguir de cerca las actividades de otras organizaciones, en particular, de la Comisión de las Comunidades Europeas y de la Comisión Económica para Europa. Se señaló que el comercio electrónico de alta velocidad requería un nuevo examen de cuestiones contractuales básicas como la oferta y la aceptación, y que debían examinarse las repercusiones jurídicas del papel de los sistemas de gestión centralizada de datos en el derecho mercantil internacional.

134. Tras haber deliberado al respecto, la Comisión decidió que se dedicara un período de sesiones del Grupo de Trabajo sobre Pagos Internacionales a la identificación de las cuestiones jurídicas planteadas, y al examen de posibles disposiciones legales y que el Grupo de Trabajo informara a la Comisión sobre la conveniencia y viabilidad de

emprender alguna nueva tarea, como la de preparar un acuerdo uniforme de las comunicaciones.¹¹

135. En su 24.º período de sesiones, el Grupo de Trabajo sobre Pagos Internacionales recomendó a la Comisión, que emprendiera la labor de elaborar un régimen jurídico uniforme para el comercio electrónico. Se convino en que esa labor debería tener la finalidad de facilitar la formulación de normas de tipo legislativo aplicables al comercio electrónico y que regularan cuestiones como las siguientes: el perfeccionamiento de los contratos; el riesgo y la responsabilidad de los socios comerciales y de los terceros proveedores de servicios en el marco de relaciones concertadas por comercio electrónico; ampliar el alcance de las definiciones de "escrito" y de "original" para dar cabida en ellas a las aplicaciones del comercio electrónico; y cuestiones relacionadas con la negociabilidad de los títulos negociables y documentos de titularidad (A/CN.9/360).

136. Aunque en general se estimaba conveniente lograr el alto grado de certidumbre y armonización jurídicas que ofrecían las disposiciones detalladas de una ley uniforme, era necesario actuar con cautela para mantener un enfoque flexible respecto de ciertas cuestiones acerca de las cuales sería tal vez prematuro o inapropiado legislar. Como ejemplo de una cuestión de esa índole, se afirmó que sería probablemente prematuro tratar de lograr la unificación legislativa de las reglas sobre el valor probatorio de los mensajes transmitidos por vía del comercio electrónico (*Ibid.*, párr. 130). Se convino en que no se adoptaría ninguna decisión en esta temprana etapa en cuanto a la forma o al contenido definitivos del régimen jurídico que se prepararía. Se observó que, de conformidad con el enfoque flexible que había de adaptarse, podían plantearse situaciones en las cuales la preparación de cláusulas contractuales que sirvieran de modelo se consideraría una manera apropiada de abordar cuestiones concretas (*Ibid.*, párr. 132).

137. La Comisión, en su 25.º período de sesiones (1992), apoyó la recomendación contenida en el informe del Grupo de Trabajo (*Ibid.*, párrs. 129 a 133) y encomendó al Grupo de Trabajo sobre Pagos Internacionales que preparara una reglamentación jurídica del comercio electrónico, dándole, al mismo tiempo, a ese Grupo el nuevo nombre de Grupo de Trabajo sobre Intercambio Electrónico de Datos.¹²

138. El Grupo de Trabajo dedicó sus períodos de sesiones 25.º a 28.º a la preparación de reglas jurídicas aplicables al "intercambio electrónico de datos (EDI) y otros medios de comunicación de datos" (en los documentos A/CN.9/373, 387, 390 y 406 figuran informes sobre esos períodos de sesiones).¹³

139. El Grupo de Trabajo utilizó para su tarea los documentos de trabajo preparados por la Secretaría sobre posibles cuestiones que cabría incluir en la Ley Modelo. Entre esos documentos cabe citar el A/CN.9/WG.IV/WP.53 (Cuestiones que cabría incluir en el programa de futuros trabajos sobre los aspectos jurídicos del intercambio electrónico de datos (EDI)) y el documento A/CN.9/WG.IV/WP.55 (Esbozo de una reglamentación uniforme eventual de ciertos aspectos jurídicos del intercambio electrónico de datos (EDI)). Los proyectos de artículo de la Ley Modelo fueron presentados a la Secretaría en

los documentos A/CN.9/WG.IV/WP.57, 60 y 62. El Grupo de Trabajo tuvo ante sí además una propuesta del Reino Unido de Gran Bretaña e Irlanda del Norte relativa al contenido eventual del proyecto de Ley Modelo (A/CN.9/WG.IV/WP.58).

140. El Grupo de Trabajo observó que si bien era cierto que a menudo se buscaban soluciones prácticas a las dificultades jurídicas que planteaba el empleo del comercio electrónico por la vía contractual (A/CN.9/WG.IV/WP.53, párrs. 35 y 36), esas soluciones contractuales de la problemática jurídica del comercio electrónico se habían ido elaborando no sólo por razón de sus ventajas intrínsecas, como pudiera ser la mayor flexibilidad de una reglamentación contractual, sino también por razón de la falta de un régimen adecuado de carácter legislativo o jurisprudencial. La vía contractual adolece de una limitación intrínseca que es su incapacidad para resolver aquellos obstáculos jurídicos contra el empleo del comercio electrónico que puedan resultar de las normas imperativas del derecho legal o jurisprudencial interno aplicable. A ese respecto, una dificultad inherente al recurso a esta técnica de los acuerdos de comunicaciones sería la incertidumbre sobre el valor que puedan tener ante los tribunales algunas de las estipulaciones contractuales. Otra limitación de la vía contractual resulta de la imposibilidad de que las partes regulen en un contrato los derechos y obligaciones de terceros. Cabe pensar que, al menos, para aquellas partes que sean ajenas al acuerdo contractual de comunicaciones, sería preciso establecer un régimen legal basado en una ley modelo o en un convenio internacional (véase A/CN.9/350, párr. 107).

141. El Grupo de Trabajo examinó la conveniencia de preparar reglas uniformes con miras a eliminar los obstáculos e incertidumbres de índole jurídica que dificultan la utilización de las técnicas modernas de comunicación en aquellos casos en los que su eliminación efectiva sólo sea posible por medio de disposiciones de rango legislativo. Una de las finalidades de esas reglas uniformes sería la de facultar a los posibles usuarios del comercio electrónico para establecer un enlace de comercio electrónico jurídicamente seguro por medio de un acuerdo de comunicaciones en el interior de una red cerrada. La segunda finalidad de ese régimen uniforme sería la de apoyar el empleo del comercio electrónico fuera de esa red cerrada, es decir, en un marco abierto. No obstante, debe recalarse que la finalidad de las reglas uniformes es posibilitar, y no imponer, el empleo del EDI y de otros medios de comunicación conexos. Además, la finalidad del régimen uniforme no es la de regular las relaciones de comercio electrónico desde una perspectiva técnica sino la de crear un marco jurídico lo más seguro posible para facilitar la utilización del comercio electrónico por las partes para sus comunicaciones comerciales.

142. En cuanto al régimen uniforme, el Grupo de Trabajo acordó que debería seguir adelante con su labor, sobre la hipótesis de que el régimen uniforme revestiría la forma de disposiciones de rango legislativo. Si bien se convino en que se impartiría al texto la forma de una ley modelo, en un principio se estimó que, dada la naturaleza especial del texto jurídico que se estaba elaborando, había que encontrar un término más flexible que el de "ley modelo". Se hizo ver que el título debería reflejar que el texto contenía diversas disposiciones relativas a normas vigentes que estarían distribuidas en diversas partes de distintas leyes nacionales en el Estado que diera efecto a esa normativa. Era,

pues, posible que los Estados que dieran efecto a la normativa no incorporaran necesariamente el texto in toto y que las disposiciones de tal "ley modelo" podrían no figurar juntas en un cuerpo normativo discreto del derecho interno. El texto podía calificarse, en la terminología de un ordenamiento jurídico, como "ley de enmienda de diversos otros textos legales". El Grupo de Trabajo convino en que la naturaleza especial del texto se expresaría mejor si se empleaba el término "disposiciones legales modelo". También se opinó que la naturaleza y el propósito de las "disposiciones legales modelo" podrían explicarse en una introducción o en las directrices que acompañaran al texto.

143. No obstante, el Grupo de Trabajo, en su 28.º período de sesiones, reconsideró su decisión anterior de formular un texto jurídico redactado en forma de "disposiciones legales modelo" (A/CN.9/390, párr. 16). Se opinó en general que el empleo del término "disposiciones legales modelo" podía suscitar incertidumbre sobre la índole jurídica del instrumento. Si bien hubo cierto apoyo en favor de que se retuviera el término "disposiciones legales modelo", prevaleció el parecer de que era preferible el término "ley modelo". Se opinó en general que, como resultado de la orientación seguida por el Grupo de Trabajo, a medida que avanzaba su labor hacia la finalización del texto, cabía ahora considerar que las disposiciones legales modelo formaban un régimen equilibrado y bien definido que cabría promulgar conjuntamente como un solo instrumento (A/CN.9/406, párr. 75). Sin embargo, según la situación imperante en cada Estado que le diera efecto, la Ley Modelo podía incorporarse en forma de ley especial o integrarse en diversas partes de la legislación existente.

144. El texto del proyecto de Ley Modelo aprobado por el Grupo de Trabajo en su 28.º período de sesiones fue enviado a todos los gobiernos y organizaciones internacionales interesadas para que presentaran sus observaciones. Las observaciones recibidas fueron reproducidas en el documento A/CN.9/409 y Add.1 a 4. El texto de los proyectos de artículo de la Ley Modelo figura en el anexo del documento A/CN.9/406.

145. En su 28.º período de sesiones (1995) la Comisión aprobó el texto de los artículos 1 y 3 a 11 del proyecto de Ley Modelo y, por falta de tiempo suficiente, no completó su examen del proyecto de Ley Modelo, que fue por ello colocado en el programa del 29.º período de sesiones de la Comisión.¹⁴

146. La Comisión, en su 28.º período de sesiones,¹⁵ recordó que, en su 27.º período de sesiones (1994), había habido apoyo general en favor de una recomendación presentada por el Grupo de Trabajo de que se iniciara alguna labor preliminar sobre el tema de la negociabilidad y transferibilidad de los derechos reales en un entorno informático tan pronto como concluyera la preparación de la Ley Modelo.¹⁶ Se observó que, sobre la base de esa recomendación, se había celebrado un debate preliminar sobre la labor futura en el campo del intercambio electrónico de datos con ocasión del 29.º período de sesiones del Grupo de Trabajo (el informe sobre ese debate figura en el documento A/CN.9/407, párrs. 106 a 118). En ese período de sesiones, el Grupo de Trabajo examinó también propuestas de la Cámara de Comercio Internacional (A/CN.9/WG.IV/WP.65) y del Reino Unido de Gran Bretaña e Irlanda del Norte (A/CN.9/WG.IV/WP.66) de que se incluyeran disposiciones adicionales en el proyecto

de Ley Modelo que reconocieran a ciertas cláusulas y condiciones incorporadas a un mensaje de datos por simple remisión el mismo grado de eficacia jurídica que si hubieran sido enunciadas en su integridad en el texto del mensaje de datos (el informe sobre el debate figura en el documento A/CN.9/407, párrs. 100 a 105). Se convino en que la cuestión de la incorporación por remisión debía considerarse en el contexto de la labor futura sobre negociabilidad y transferibilidad de los derechos reales (A/CN.9/407, párr. 103). La Comisión hizo suya la recomendación del Grupo de Trabajo de que se encomendara a la Secretaría la preparación de un estudio de antecedentes sobre la negociabilidad y transferibilidad por EDI de los documentos de transporte, que se refiriera en particular a la utilización del EDI para los fines de la documentación relativa al transporte marítimo, habida cuenta de las sugerencias y opiniones expresadas en el 29.º período de sesiones del Grupo de Trabajo.¹⁷

147. Sobre la base del estudio preparado por la Secretaría (A/CN.9/WG.IV/WP.69), el Grupo de Trabajo, en su 30.º período de sesiones, examinó las cuestiones de la transferibilidad de derechos en el contexto de los documentos de transporte y aprobó el texto del proyecto de disposiciones legales relativas a las cuestiones específicas de los mensajes de datos relativos a contratos de transporte de mercancías (el informe sobre ese período de sesiones figura en el documento A/CN.9/421). El texto de ese proyecto de disposiciones presentado a la Comisión por el Grupo de Trabajo para su examen final y posible adición como parte II de la Ley Modelo figuraba en el anexo del documento A/CN.9/421.

148. Al preparar la Ley Modelo, el Grupo de Trabajo estimó que convendría proporcionar en un comentario información adicional relativa a la Ley Modelo. En particular, en el 28.º período de sesiones del Grupo de Trabajo, durante el cual se finalizó el texto del proyecto de Ley Modelo para presentarlo a la Comisión, recibió apoyo general la sugerencia de que el proyecto de Ley Modelo fuera acompañado de una guía para ayudar a los Estados en la incorporación del proyecto de Ley Modelo al derecho interno y en su aplicación. La guía, que en gran parte podría basarse en los trabajos preparatorios del proyecto de Ley Modelo, sería también de utilidad para los usuarios de medios electrónicos de comunicación, así como para los estudiosos en la materia. El Grupo de Trabajo observó que, en las deliberaciones celebradas en ese período de sesiones, había partido de la hipótesis de que el proyecto de Ley Modelo iría acompañado de una guía. Por ejemplo, el Grupo de Trabajo había decidido no resolver algunas cuestiones en el proyecto de Ley Modelo sino en la guía, a fin de orientar a los Estados en la incorporación del proyecto de Ley Modelo a su derecho interno. Se pidió a la Secretaría que preparara un proyecto y lo presentara al Grupo de Trabajo en su 29.º período de sesiones para que lo examinara (A/CN.9/406, párr. 177).

149. En su 29.º período de sesiones, el Grupo de Trabajo examinó el proyecto de Guía para la incorporación al derecho interno de la Ley Modelo (en adelante denominado "el proyecto de Guía") que figuraba en una nota preparada por la Secretaría (A/CN.9/WG.IV/WP.64). Se pidió a la Secretaría que preparara una versión revisada del proyecto de Guía en la que se tuvieran en cuenta las decisiones adoptadas por el Grupo

de Trabajo, así como las distintas opiniones, sugerencias y preocupaciones expresadas en ese período de sesiones. En su 28.º período de sesiones, la Comisión colocó el proyecto de Guía para la incorporación al derecho interno en el programa de su 29.º período de sesiones.¹⁸

150. En su 29.º período de sesiones, tras examinar el texto del proyecto de Ley Modelo, con las modificaciones introducidas por el grupo de redacción, la Comisión aprobó la siguiente decisión en su 605a. sesión, celebrada el 12 de junio de 1996:

"La Comisión de las Naciones Unidas para el Derecho Mercantil Internacional,

Recordando que en la resolución 2205 (XXI) de la Asamblea General, de 17 de diciembre de 1996, se le pidió que fomentara la armonización y unificación progresivas del derecho mercantil internacional y tuviera presentes a ese respecto los intereses de todos los pueblos, particularmente los de los países en desarrollo, en el progreso amplio del comercio internacional,

Observando que es cada vez mayor el número de transacciones del comercio internacional que se realizan mediante intercambio electrónico de datos y otros medios de comunicación denominados generalmente comercio electrónico, que entrañan el uso de formas de comunicación y almacenamiento de información distintas del papel,

Recordando la recomendación sobre el valor jurídico de los registros computadorizados que aprobó en su 18.º período de sesiones, celebrado en 1985, y el inciso b) del párrafo 5 de la resolución 40/71 de la Asamblea General, de 11 de diciembre de 1985, en que se pedía a los gobiernos y a las organizaciones internacionales que, cuando así conviniera, adoptasen medidas de conformidad con la recomendación de la Comisión¹⁹ 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,

Considerando que la aprobación de una ley modelo que facilite el uso del comercio electrónico y sea aceptable para Estados con sistemas jurídicos, sociales y económicos

distintos contribuirá al fomento de la armonización de las relaciones económicas internacionales,

Convencida de que la Ley Modelo de la CNUDMI sobre el comercio electrónico será muy útil para que los gobiernos mejoren sus leyes sobre el uso de formas de comunicación y almacenamiento de información distintas del papel y para la elaboración de esas leyes donde no existan actualmente,

1. *Aprueba* la Ley Modelo de la CNUDMI sobre el comercio electrónico tal como figura en el anexo I del informe sobre la labor realizada en el período de sesiones en curso;

2. *Pide* al Secretario General que transmita a los gobiernos y otros órganos interesados el texto de la Ley Modelo de la CNUDMI sobre el comercio electrónico, acompañado de la Guía para la incorporación al derecho interno de la Ley Modelo que ha preparado la Secretaría;

3. *Recomienda* a todos los Estados que den consideración favorable a la Ley Modelo de la CNUDMI sobre el comercio electrónico cuando aprueben o modifiquen sus leyes, en vista de la necesidad de uniformidad en la legislación aplicable a las formas de comunicación y almacenamiento de información distintas del papel."²⁰

1 Véase Documentos Oficiales de la Asamblea General, cuadragésimo período de sesiones, Suplemento No. 17 (A/40/17), cap. VI, sec. B.

2 La documentación de referencia a la que se hace remisión por su signatura en la presente Guía pertenece a las tres categorías siguientes de documentos:

A/50/17 y A/51/17 son las
signaturas de los informes
de la CNUDMI a la
Asamblea General sobre la

labor de sus períodos de sesiones 28° y 29°, celebrados en 1995 y 1996, respectivamente;

Los documentos de la serie A/CN.9/ son los informes y notas examinados por la CNUDMI en sus períodos de sesiones anuales, en particular los informes presentados por el Grupo de Trabajo al examen de la Comisión;

Los documentos de la serie A/CN.9/WG.IV/ son los documentos de trabajo examinados por el Grupo de Trabajo de la CNUDMI sobre comercio electrónico (denominado anteriormente Grupo de Trabajo de la CNUDMI sobre intercambio electrónico de datos) en su labor de preparación de la Ley Modelo.

3 Documentos Oficiales de la Asamblea General, quincuagésimo primer período de sesiones, Suplemento No. 17 (A/51/17), anexo I.

4 "Legal aspects of automatic trade data interchange" (TRADE/WP.4/R.185/Rev.1). El informe presentado al Grupo de Trabajo figura en el anexo del documento A/CN.9/238.

5 Documentos Oficiales de la Asamblea General, trigésimo noveno período de sesiones, Suplemento No. 17 (A/39/17), párr. 136.

6 *Documentos Oficiales de la Asamblea General, cuadragésimo período de sesiones, Suplemento No. 17 (A/40/17)*, párr. 360.

7 La resolución 40/71 fue reproducida en el *Anuario de la Comisión de las Naciones Unidas para el Derecho Internacional*, 1985, vol. XVI, primera parte, D (publicación de las Naciones Unidas, Núm. de venta S.87.V.4).

8 *Documentos Oficiales de la Asamblea General, cuadragésimo tercer período de sesiones, Suplemento No. 17 (A/43/17)*, párrs. 46 y 47, e *ibid.*, *cuadragésimo cuarto período de sesiones, Suplemento No. 17 (A/44/17)*, párr. 289.

9 *Ibid.*, *Cuadragésimo quinto período de sesiones, Suplemento No. 17 (A/45/17)*, párrs. 38 a 40.

10 Cabe observar que la Ley Modelo no está concebida como un régimen completo aplicable a todos los aspectos del comercio electrónico. La finalidad principal de la Ley Modelo es adaptar los requisitos legales existentes para que dejen de constituir obstáculos a la utilización de los medios de comunicación y archivo de información sin soporte de papel.

11 *Ibid.*, *Cuadragésimo sexto período de sesiones, Suplemento No. 17 (A/46/17)*, párrs. 311 a 317.

12 *Ibid.*, *Cuadragésimo séptimo período de sesiones, Suplemento No. 17 (A/47/17)*, párrs. 141 a 148.

13 El concepto "EDI y otros medios conexos de comunicación de datos" no debía interpretarse como una referencia al intercambio electrónico de datos en sentido estricto definido en el artículo 2 b) de la Ley Modelo sino a una variedad de usos de las técnicas de comunicación modernas relacionados con el comercio a los que cabría referirse ampliamente bajo la rúbrica de "comercio electrónico". La Ley Modelo no está destinada únicamente a ser aplicada en el contexto de las técnicas de

comunicación existentes sino más bien como conjunto de reglas flexibles que deberían dar cabida a los adelantos técnicos previsibles. Se debería hacer hincapié en que la Ley Modelo tenía por finalidad no sólo establecer reglas para el movimiento o flujo de información comunicada por medio de mensajes de datos sino también tratar la información archivada en los mensajes de datos que no se pretendía comunicar.

14 Documentos Oficiales de la Asamblea General, quincuagésimo período de sesiones, Suplemento N.º. 17 (A/50/17), párr. 306.

15 Ibid., párr. 307.

16 Ibid., Cuadragésimo noveno período de sesiones, Suplemento N.º. 17 (A/49/17), párr. 201.

17 Ibid., Quincuagésimo período de sesiones, Suplemento N.º. 17 (A/50/17), párr. 309.

18 Ibid., párr. 306.

19 Ibid., cuadragésimo período de sesiones, Suplemento N.º. 17 (A/40/17), párrs. 354 a 360.

20 Ibid., quincuagésimo primer período de sesiones, Suplemento N.º. 17 (A/51/17), párr. 209.

A N E X O 4

**L e y M o d e l o p a r a l a s
F i r m a s E l e c t r ó n i c a s
U N C I T R A L**

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

Proyecto de Ley Modelo y proyecto de guía para la incorporación al derecho interno aprobado por el Grupo de Trabajo en su 38º periodo de Sesiones (Nueva York 12 al 23 de Marzo de 2001) que se presentará a la Comisión para su examen y aprobación en el 34º período de sesiones de ésta, que se celebraría del 25 de junio al 13 de julio de 2001 en Viena.

Ley Modelo de la CNUDMI para las firmas electrónicas (2001)
(aprobada por el Grupo de Trabajo de la CNUDMI sobre Comercio Electrónico en su 37º período de sesiones, celebrado del 18 al 29 de septiembre de 2000 en Viena)

Artículo 1. Ámbito de aplicación

La presente Ley será aplicable en todos los casos en que se utilicen firmas electrónicas en el contexto* de actividades comerciales**. No deroga ninguna norma jurídica destinada a la protección del consumidor.

* 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].”

** 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, sin que esta lista sea taxativa, las operaciones siguientes: toda operación comercial de suministro o intercambio de bienes o servicios; acuerdos de distribución; representación o mandato comercial; facturaje (Factoring@); arrendamiento con opción de compra (Leasing@); 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.

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 contenida 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 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 en nombre propio o 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 habrán de tenerse en cuenta su origen internacional y la necesidad de promover la uniformidad en su aplicación y la observancia de la buena fe.

2) *Las cuestiones relativas a materias que se rijan por la presente Ley y que no estén expresamente resueltas en ella serán dirimidas de conformidad con los principios generales en que se inspira.*

Artículo 5. Modificación mediante acuerdo

Las partes podrán hacer 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 tan fiable como resulte apropiado a los fines para 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 la 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.
- 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) dar aviso sin dilación indebida a cualquier persona que, según pueda razonablemente prever, pueda considerar fiable la firma electrónica o prestar servicios que la apoyen si:
 - i) sabe que los datos de creación de la firma han quedado en entredicho; o
 - ii) las circunstancias de que tiene conocimiento 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 su ciclo vital o que hayan de consignarse en él sean exactas y cabales.
- 2) El firmante incurrirá en responsabilidad por el incumplimiento de 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 sean exactas y cabales;
 - c) proporcionar medios de acceso razonablemente fácil que permitan a la parte que confía en el certificado determinar mediante éste:
 - 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 medios de acceso razonablemente fácil que, según proceda, permitan a la parte que confía en el certificado determinar mediante éste o de otra manera:
 - i) el método utilizado para identificar al firmante;
 - ii) cualquier limitación en los fines o el 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 en cuanto al ámbito o el alcance de la responsabilidad indicada por 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;
 - vi) si se ofrece un servicio de revocación oportuna del 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 y, cuando se ofrezcan servicios en virtud del inciso vi) del apartado d), cerciorarse de que exista un servicio de revocación oportuna del certificado;
 - f) utilizar, al prestar sus servicios, sistemas, procedimientos y recursos humanos fiables.
- 2) El prestador de servicios de certificación incurrirá en responsabilidad por el incumplimiento de 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 un activo;
- 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 confían en éste;
- e) la periodicidad y el alcance de la auditoría 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; y
- 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 y firmas electrónicas extranjeros

1) Al determinar si un certificado o una firma electrónica produce efectos jurídicos, o en qué medida los produce, 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 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 y certificados, se reconocerá que ese acuerdo es suficiente a efectos del reconocimiento transfronterizo, salvo que ese acuerdo no sea válido o eficaz conforme al derecho aplicable.

A N E X O 5

**L e y 5 9 / 2 0 0 3 d e 1 9 d e
d i c i e m b r e d e F i r m a
E l e c t r ó n i c a d e E s p a ñ a**

LEY 59/2003, de 19 de diciembre, de firma electrónica.

Sumario:

TITULO 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.

TITULO 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 los 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.

TITULO III Prestación de servicios de certificación

CAPÍTULO I Disposiciones generales

Artículo 17. Protección de 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.

TITULO 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.

TITULO V Supervisión y control

Artículo 29. Supervisión y control.

Artículo 30. Deber de información y colaboración.

TITULO VI Infracciones y sanciones

<u>Artículo 31.</u>	<u>Infracciones.</u>	<u>Artículo</u>	<u>32.</u>	<u>Sanciones.</u>
<u>Artículo</u>	<u>33.</u>	<u>Graduación</u>	<u>de la cuantía</u>	<u>de las sanciones.</u>
<u>Artículo</u>	<u>34.</u>	<u>Medidas</u>		<u>provisionales.</u>
<u>Artículo</u>	<u>35.</u>	<u>Multa</u>		<u>coercitiva.</u>
<u>Artículo 36.</u>	<u>Competencia y procedimiento sancionador.</u>			

Disposición adicional primera. Fe publica 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 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.

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 recalarse 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.

TITULO 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 el redactado en soporte electrónico que incorpore datos que estén firmados electrónicamente.

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 por el prestador de servicios de certificación, que expide los certificados electrónicos, se cumplen todos los requisitos establecidos en la ley en cuanto a la garantía de los servicios que presta en la comprobación de la eficacia de la firma electrónica, y en especial, las obligaciones de garantizar la confidencialidad del proceso así como la autenticidad, conservación e integridad de la información generada y la identidad de los firmantes. 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 con arreglo a los principios de objetividad, transparencia y no discriminación.

TITULO II
Certificados electrónicos
CAPITULO 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.

CAPITULO 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, bien mediante consulta en el registro público en el que estén inscritos los documentos de constitución y de apoderamiento, bien mediante los documentos públicos que sirvan para acreditar los extremos citados de manera fehaciente, cuando aquellos no sean de inscripción obligatoria.

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, bien mediante consulta en el registro público en el que estén inscritas, bien mediante los documentos públicos que sirvan para acreditar los extremos citados de manera fehaciente, cuando aquellos no sean de inscripción obligatoria. 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.

CAPITULO 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 las 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.

TITULO III

Prestación de servicios de certificación

CAPITULO 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.º 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.º Los mecanismos para garantizar la fiabilidad de la firma electrónica de un documento a lo largo del tiempo.

3.º El método utilizado por el prestador para comprobar la identidad del firmante u otros datos que figuren en el certificado.

4.º Las condiciones precisas de utilización del certificado, sus posibles límites de uso y la forma en que el prestador garantiza su responsabilidad patrimonial.

5.º 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.º 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.

CAPITULO 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. En caso de que dichos datos deban figurar inscritos en un registro público, el prestador de servicios de certificación deberá comprobarlos en el citado registro en el momento inmediato anterior a la expedición del certificado, pudiendo emplear, en su caso, medios telemáticos.

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.

TITULO 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.

TITULO 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.

TITULO 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 señaladas en el artículo 18 y las restantes de esta ley, cuando no constituya infracción grave o muy grave, excepto las 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 15/1 999, 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 adecue a sus características particulares, el documento nacional de identidad electrónico se registrará 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 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.^a, 18.^a, 21.^a y 29.^a 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 MARIA AZNAR LOPEZ

A N E X O 6

**L e y 2 5 . 5 0 6 d e F i r m a
D i g i t a l d e A r g e n t i n a**

FIRMA DIGITAL

Ley 25.506

Consideraciones generales. Certificados digitales. Certificador licenciado. Titular de un certificado digital. Organización institucional. Autoridad de aplicación. Sistema de auditoría. Comisión Asesora para la Infraestructura de Firma Digital. Responsabilidad. Sanciones. Disposiciones Complementarias.

Sancionada: Noviembre 14 de 2001.

Promulgada de Hecho: Diciembre 11 de 2001.

El Senado y Cámara de Diputados de la Nación Argentina reunidos en Congreso, etc. sancionan con fuerza de Ley:

LEY DE FIRMA DIGITAL

CAPITULO I

Consideraciones generales

ARTICULO 1° — Objeto. Se reconoce el empleo de la firma electrónica y de la firma digital y su eficacia jurídica en las condiciones que establece la presente ley.

ARTICULO 2° — Firma Digital. Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma.

Los procedimientos de firma y verificación a ser utilizados para tales fines serán los determinados por la Autoridad de Aplicación en consonancia con estándares tecnológicos internacionales vigentes.

ARTICULO 3° — Del requerimiento de firma. Cuando la ley requiera una firma manuscrita, esa exigencia también queda satisfecha por una firma digital. Este principio es aplicable a los casos en que la ley establece la obligación de firmar o prescribe consecuencias para su ausencia.

ARTICULO 4° — Exclusiones. Las disposiciones de esta ley no son aplicables:

- a) A las disposiciones por causa de muerte;
- b) A los actos jurídicos del derecho de familia;
- c) A los actos personalísimos en general;
- d) A los actos que deban ser instrumentados bajo exigencias o formalidades incompatibles con la utilización de la firma digital, ya sea como consecuencia de disposiciones legales o acuerdo de partes.

ARTICULO 5° — Firma electrónica. Se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez.

ARTICULO 6° — Documento digital. Se entiende por documento digital a la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo. Un documento digital también satisface el requerimiento de escritura.

ARTICULO 7º — Presunción de autoría. Se presume, salvo prueba en contrario, que toda firma digital pertenece al titular del certificado digital que permite la verificación de dicha firma.

ARTICULO 8º — Presunción de integridad. Si el resultado de un procedimiento de verificación de una firma digital aplicado a un documento digital es verdadero, se presume, salvo prueba en contrario, que este documento digital no ha sido modificado desde el momento de su firma.

ARTICULO 9º — Validez. Una firma digital es válida si cumple con los siguientes requisitos:

- a) Haber sido creada durante el período de vigencia del certificado digital válido del firmante;
- b) Ser debidamente verificada por la referencia a los datos de verificación de firma digital indicados en dicho certificado según el procedimiento de verificación correspondiente;
- c) Que dicho certificado haya sido emitido o reconocido, según el artículo 16 de la presente, por un certificador licenciado.

ARTICULO 10. — Remitente. Presunción. Cuando un documento digital sea enviado en forma automática por un dispositivo programado y lleve la firma digital del remitente se presumirá, salvo prueba en contrario, que el documento firmado proviene del remitente.

ARTICULO 11. — Original. Los documentos electrónicos firmados digitalmente y los reproducidos en formato digital firmados digitalmente a partir de originales de primera generación en cualquier otro soporte, también serán considerados originales y poseen, como consecuencia de ello, valor probatorio como tales, según los procedimientos que determine la reglamentación.

ARTICULO 12. — Conservación. La exigencia legal de conservar documentos, registros o datos, también queda satisfecha con la conservación de los correspondientes documentos digitales firmados digitalmente, según los procedimientos que determine la reglamentación, siempre que sean accesibles para su posterior consulta y permitan determinar fehacientemente el origen, destino, fecha y hora de su generación, envío y/o recepción.

CAPITULO II

De los certificados digitales

ARTICULO 13. — Certificado digital. Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular.

ARTICULO 14. — Requisitos de validez de los certificados digitales. Los certificados digitales para ser válidos deben:

- a) Ser emitidos por un certificador licenciado por el ente licenciante;
- b) Responder a formatos estándares reconocidos internacionalmente, fijados por la autoridad de aplicación, y contener, como mínimo, los datos que permitan:
 1. Identificar indubitablemente a su titular y al certificador licenciado que lo emitió, indicando su período de vigencia y los datos que permitan su identificación única;
 2. Ser susceptible de verificación respecto de su estado de revocación;
 3. Diferenciar claramente la información verificada de la no verificada incluidas en el certificado;
 4. Contemplar la información necesaria para la verificación de la firma;
 5. Identificar la política de certificación bajo la cual fue emitido.

ARTICULO 15. — Período de vigencia del certificado digital. A los efectos de esta ley, el certificado digital es válido únicamente dentro del período de vigencia, que comienza en la fecha de inicio y finaliza en su fecha de vencimiento, debiendo ambas ser indicadas en el certificado digital, o su revocación si fuere revocado.

La fecha de vencimiento del certificado digital referido en el párrafo anterior en ningún caso puede ser posterior a la del vencimiento del certificado digital del certificador licenciado que lo emitió.

La Autoridad de Aplicación podrá establecer mayores exigencias respecto de la determinación exacta del momento de emisión, revocación y vencimiento de los certificados digitales.

ARTICULO 16. — Reconocimiento de certificados extranjeros. Los certificados digitales emitidos por certificadores extranjeros podrán ser reconocidos en los mismos términos y condiciones exigidos en la ley y sus normas reglamentarias cuando:

a) Reúnan las condiciones que establece la presente ley y la reglamentación correspondiente para los certificados emitidos por certificadores nacionales y se encuentre vigente un acuerdo de reciprocidad firmado por la República Argentina y el país de origen del certificador extranjero, o

b) Tales certificados sean reconocidos por un certificador licenciado en el país, que garantice su validez y vigencia conforme a la presente ley. A fin de tener efectos, este reconocimiento deberá ser validado por la autoridad de aplicación.

CAPITULO III

Del certificador licenciado

ARTICULO 17. — Del certificador licenciado. Se entiende por certificador licenciado a toda persona de existencia ideal, registro público de contratos u organismo público que expide certificados, presta otros servicios en relación con la firma digital y cuenta con una licencia para ello, otorgada por el ente licenciante.

La actividad de los certificadores licenciados no pertenecientes al sector público se prestará en régimen de competencia. El arancel de los servicios prestados por los certificadores licenciados será establecido libremente por éstos.

ARTICULO 18. — Certificados por profesión. Las entidades que controlan la matrícula, en relación a la prestación de servicios profesionales, podrán emitir certificados digitales en lo referido a esta función, con igual validez y alcance jurídico que las firmas efectuadas en forma manuscrita. A ese efecto deberán cumplir los requisitos para ser certificador licenciado.

ARTICULO 19. — Funciones. El certificador licenciado tiene las siguientes funciones:

a) Recibir una solicitud de emisión de certificado digital, firmada digitalmente con los correspondientes datos de verificación de firma digital del solicitante;

b) Emitir certificados digitales de acuerdo a lo establecido en sus políticas de certificación, y a las condiciones que la autoridad de aplicación indique en la reglamentación de la presente ley;

c) Identificar inequívocamente los certificados digitales emitidos;

d) Mantener copia de todos los certificados digitales emitidos, consignando su fecha de emisión y de vencimiento si correspondiere, y de sus correspondientes solicitudes de emisión;

e) Revocar los certificados digitales por él emitidos en los siguientes casos, entre otros que serán determinados por la reglamentación:

1) A solicitud del titular del certificado digital.

2) Si determinara que un certificado digital fue emitido en [base](#) a una información falsa, que en el momento de la emisión hubiera sido objeto de verificación.

3) Si determinara que los procedimientos de emisión y/o verificación han dejado de ser seguros.

4) Por condiciones especiales definidas en su política de certificación.

5) Por resolución judicial o de la autoridad de aplicación.

f) Informar públicamente el estado de los certificados digitales por él emitidos. Los certificados digitales revocados deben ser incluidos en una lista de certificados revocados indicando fecha y hora de la revocación. La validez y autoría de dicha lista de certificados revocados deben ser garantizadas.

ARTICULO 20. — Licencia. Para obtener una licencia el certificador debe cumplir con los requisitos establecidos por la ley y tramitar la solicitud respectiva ante el ente licenciante, el que otorgará la licencia previo dictamen legal y técnico que acredite la aptitud para cumplir con sus funciones y obligaciones. Estas licencias son intransferibles.

ARTICULO 21. — Obligaciones. Son obligaciones del certificador licenciado:

a) Informar a quien solicita un certificado con carácter previo a su emisión y utilizando un medio de comunicación las condiciones precisas de utilización del certificado digital, sus características y efectos, la existencia de un sistema de licenciamiento y los procedimientos, forma que garantiza su posible responsabilidad patrimonial y los efectos de la revocación de su propio certificado digital y de la licencia que le otorga el ente licenciante. Esa información deberá estar libremente accesible en lenguaje fácilmente comprensible. La parte pertinente de dicha información estará también disponible para terceros;

b) Abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder bajo ninguna circunstancia, a los datos de creación de firma digital de los titulares de certificados digitales por él emitidos;

c) Mantener el control exclusivo de sus propios datos de creación de firma digital e impedir su divulgación;

d) Operar utilizando un sistema técnicamente confiable de acuerdo con lo que determine la autoridad de aplicación;

e) Notificar al solicitante las medidas que está obligado a adoptar para crear firmas digitales seguras y para su verificación confiable, y las obligaciones que asume por el solo hecho de ser titular de un certificado digital;

f) Recabar únicamente aquellos datos personales del titular del certificado digital que sean necesarios para su emisión, quedando el solicitante en libertad de proveer información adicional;

g) Mantener la confidencialidad de toda información que no figure en el certificado digital;

h) Poner a disposición del solicitante de un certificado digital toda la información relativa a su tramitación;

i) Mantener la documentación respaldatoria de los certificados digitales emitidos, por diez (10) años a partir de su fecha de vencimiento o revocación;

j) Incorporar en su política de certificación los efectos de la revocación de su propio certificado digital y/o de la licencia que le otorgara la autoridad de aplicación;

k) Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, la lista de certificados digitales revocados, las políticas de certificación, la información relevante de los informes de la última auditoría de que hubiera sido objeto, su manual de procedimientos y toda información que determine la autoridad de aplicación;

l) Publicar en el Boletín Oficial aquellos datos que la autoridad de aplicación determine;

m) Registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas;

- n) Informar en las políticas de certificación si los certificados digitales por él emitidos requieren la verificación de la identidad del titular;
- o) Verificar, de acuerdo con lo dispuesto en su manual de procedimientos, toda otra información que deba ser objeto de verificación, la que debe figurar en las políticas de certificación y en los certificados digitales;
- p) Solicitar inmediatamente al ente licenciante la revocación de su certificado, o informarle la revocación del mismo, cuando existieren indicios de que los datos de creación de firma digital que utiliza hubiesen sido comprometidos o cuando el uso de los procedimientos de aplicación de los datos de verificación de firma digital en él contenidos hayan dejado de ser seguros;
- q) Informar inmediatamente al ente licenciante sobre cualquier cambio en los datos relativos a su licencia;
- r) Permitir el ingreso de los funcionarios autorizados de la autoridad de aplicación, del ente licenciante o de los auditores a su local operativo, poner a su disposición toda la información necesaria y proveer la asistencia del caso;
- s) Emplear personal idóneo que tenga los conocimientos específicos, la experiencia necesaria para proveer los servicios ofrecidos y en particular, competencia en materia de gestión, conocimientos técnicos en el ámbito de la firma digital y experiencia adecuada en los procedimientos de seguridad pertinentes;
- t) Someter a aprobación del ente licenciante el manual de procedimientos, el plan de seguridad y el de cese de actividades, así como el detalle de los componentes técnicos a utilizar;
- u) Constituir domicilio legal en la República Argentina;
- v) Disponer de recursos humanos y tecnológicos suficientes para operar de acuerdo a las exigencias establecidas en la presente ley y su reglamentación;
- w) Cumplir con toda otra obligación emergente de su calidad de titular de la licencia adjudicada por el ente licenciante.

ARTICULO 22. — Cese del certificador. El certificador licenciado cesa en tal calidad:

- a) Por decisión unilateral comunicada al ente licenciante;
- b) Por cancelación de su personería jurídica;
- c) Por cancelación de su licencia dispuesta por el ente licenciante.

La autoridad de aplicación determinará los procedimientos de revocación aplicables en estos casos.

ARTICULO 23. — Desconocimiento de la validez de un certificado digital. Un certificado digital no es válido si es utilizado:

- a) Para alguna finalidad diferente a los fines para los cuales fue extendido;
- b) Para operaciones que superen el valor máximo autorizado cuando corresponda;
- c) Una vez revocado.

CAPITULO IV

Del titular de un certificado digital

ARTICULO 24. — Derechos del titular de un certificado digital. El titular de un certificado digital tiene los siguientes derechos:

- a) A ser informado por el certificador licenciado, con carácter previo a la emisión del certificado digital, y utilizando un medio de comunicación sobre las condiciones precisas de utilización del certificado digital, sus características y efectos, la existencia de este sistema de licenciamiento y los procedimientos asociados. Esa información deberá darse por escrito en un lenguaje fácilmente comprensible. La parte pertinente de dicha información estará también disponible para terceros;
- b) A que el certificador licenciado emplee los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por él, y a ser informado sobre ello;
- c) A ser informado, previamente a la emisión del certificado, del precio de los servicios de certificación, incluyendo cargos adicionales y formas de pago;
- d) A que el certificador licenciado le informe sobre su domicilio en la República Argentina, y sobre los medios a los que puede acudir para solicitar aclaraciones, dar cuenta del mal funcionamiento del sistema, o presentar sus reclamos;
- e) A que el certificador licenciado proporcione los servicios pactados, y a no recibir publicidad comercial de ningún tipo por intermedio del certificador licenciado.

ARTICULO 25. — Obligaciones del titular del certificado digital. Son obligaciones del titular de un certificado digital:

- a) Mantener el control exclusivo de sus datos de creación de firma digital, no compartirlos, e impedir su divulgación;
- b) Utilizar un dispositivo de creación de firma digital técnicamente confiable;
- c) Solicitar la revocación de su certificado al certificador licenciado ante cualquier circunstancia que pueda haber comprometido la privacidad de sus datos de creación de firma;
- d) Informar sin demora al certificador licenciado el cambio de alguno de los datos contenidos en el certificado digital que hubiera sido objeto de verificación.

CAPITULO V

De la organización institucional

ARTICULO 26. — Infraestructura de Firma Digital. Los certificados digitales regulados por esta ley deben ser emitidos o reconocidos, según lo establecido por el artículo 16, por un certificador licenciado.

ARTICULO 27. — Sistema de Auditoría. La autoridad de aplicación, con el concurso de la Comisión Asesora para la Infraestructura de Firma Digital, diseñará un sistema de auditoría para evaluar la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y disponibilidad de los datos, así como también el cumplimiento de las especificaciones del manual de procedimientos y los planes de seguridad y de contingencia aprobados por el ente licenciante.

ARTICULO 28. — Comisión Asesora para la Infraestructura de Firma Digital. Créase en el ámbito jurisdiccional de la Autoridad de Aplicación, la Comisión Asesora para la Infraestructura de Firma Digital.

(Nota Infoleg: Por art. 8° del [Decreto N° 624/2003](#) B.O. 22/8/2003 se establece que la Comisión creada por el presente artículo actuará en la órbita de la SUBSECRETARIA DE LA GESTION PUBLICA de la JEFATURA DE GABINETE DE MINISTROS.)

CAPITULO VI

De la autoridad de aplicación

ARTICULO 29. — Autoridad de Aplicación. La autoridad de aplicación de la presente ley será la Jefatura de Gabinete de Ministros.

ARTICULO 30. — Funciones. La autoridad de aplicación tiene las siguientes funciones:

- a) Dictar las normas reglamentarias y de aplicación de la presente;
- b) Establecer, previa recomendación de la Comisión Asesora para la Infraestructura de la Firma Digital, los estándares tecnológicos y operativos de la Infraestructura de Firma Digital;
- c) Determinar los efectos de la revocación de los certificados de los certificadores licenciados o del ente licenciante;
- d) Instrumentar acuerdos nacionales e internacionales a fin de otorgar validez jurídica a las firmas digitales creadas sobre la [base](#) de certificados emitidos por certificadores de otros países;
- e) Determinar las pautas de auditoría, incluyendo los dictámenes tipo que deban emitirse como conclusión de las revisiones;
- f) Actualizar los valores monetarios previstos en el régimen de sanciones de la presente ley;
- g) Determinar los niveles de licenciamiento;
- h) Otorgar o revocar las licencias a los certificadores licenciados y supervisar su actividad, según las exigencias instituidas por la reglamentación;
- i) Fiscalizar el cumplimiento de las normas legales y reglamentarias en lo referente a la actividad de los certificadores licenciados;
- j) Homologar los dispositivos de creación y verificación de firmas digitales, con ajuste a las normas y procedimientos establecidos por la reglamentación;
- k) Aplicar las sanciones previstas en la presente ley.

ARTICULO 31. — Obligaciones. En su calidad de titular de certificado digital, la autoridad de aplicación tiene las mismas obligaciones que los titulares de certificados y que los certificadores licenciados. En especial y en particular debe:

- a) Abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder, bajo ninguna circunstancia, a los datos utilizados para generar la firma digital de los certificadores licenciados;
- b) Mantener el control exclusivo de los datos utilizados para generar su propia firma digital e impedir su divulgación;
- c) Revocar su propio certificado frente al compromiso de la privacidad de los datos de creación de firma digital;
- d) Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, los domicilios, números telefónicos y direcciones de Internet tanto de los certificadores licenciados como los propios y su certificado digital;
- e) Supervisar la ejecución del plan de cese de actividades de los certificadores licenciados que discontinúan sus funciones.

ARTICULO 32. — Arancelamiento. La autoridad de aplicación podrá cobrar un arancel de licenciamiento para cubrir su costo operativo y el de las auditorías realizadas por sí o por terceros contratados a tal efecto.

CAPITULO VII

Del sistema de auditoría

ARTICULO 33. — Sujetos a auditar. El ente licenciante y los certificadores licenciados, deben ser auditados periódicamente, de acuerdo al sistema de auditoría que diseñe y apruebe la autoridad de aplicación.

La autoridad de aplicación podrá implementar el sistema de auditoría por sí o por terceros habilitados a tal efecto. Las auditorías deben como mínimo evaluar la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y, disponibilidad de los datos, así como también el cumplimiento de las especificaciones del manual de procedimientos y los planes de seguridad y, de contingencia aprobados por el ente licenciante.

ARTICULO 34. — Requisitos de habilitación. Podrán ser terceros habilitados para efectuar las auditorías las Universidades y organismos científicos y/o tecnológicos nacionales o provinciales, los Colegios y Consejos profesionales que acrediten experiencia profesional acorde en la materia.

CAPITULO VIII

De la Comisión Asesora para la Infraestructura de Firma Digital

ARTICULO 35.— Integración y funcionamiento. La Comisión Asesora para la Infraestructura de Firma Digital estará integrada multidisciplinariamente por un máximo de 7 (siete) profesionales de carreras afines a la actividad de reconocida trayectoria y experiencia, provenientes de Organismos del Estado nacional, Universidades Nacionales y Provinciales, Cámaras, Colegios u otros entes representativos de profesionales.

Los integrantes serán designados por el Poder Ejecutivo por un período de cinco (5) años renovables por única vez.

Se reunirá como mínimo trimestralmente. Deberá expedirse prontamente a solicitud de la autoridad de aplicación y sus recomendaciones y disidencias se incluirán en las actas de la Comisión.

Consultará periódicamente mediante audiencias públicas con las cámaras empresarias, los usuarios y las asociaciones de consumidores y mantendrá a la autoridad de aplicación regularmente informada de los resultados de dichas consultas.

ARTICULO 36. — Funciones. La Comisión debe emitir recomendaciones por iniciativa propia o a solicitud de la autoridad de aplicación, sobre los siguientes aspectos:

- a) Estándares tecnológicos;
- b) Sistema de registro de toda la información relativa a la emisión de certificados digitales;
- c) Requisitos mínimos de información que se debe suministrar a los potenciales titulares de certificados digitales de los términos de las políticas de certificación;
- d) Metodología y requerimiento del resguardo físico de la información;
- e) Otros que le sean requeridos por la autoridad de aplicación.

CAPITULO IX

Responsabilidad

ARTICULO 37. — Convenio de partes. La relación entre el certificador licenciado que emita un certificado digital y el titular de ese certificado se rige por el contrato que celebren entre ellos, sin perjuicio de las previsiones de la presente ley, y demás legislación vigente.

ARTICULO 38. — Responsabilidad de los certificadores licenciados ante terceros.

El certificador que emita un certificado digital o lo reconozca en los términos del artículo 16 de la presente ley, es responsable por los daños y perjuicios que provoque, por los incumplimientos a las previsiones de ésta, por los errores u omisiones que presenten los certificados digitales que expida, por no revocarlos, en legal tiempo y forma cuando así correspondiere y por las consecuencias imputables a la inobservancia de procedimientos de certificación exigibles. Corresponderá al prestador del servicio demostrar que actuó con la debida diligencia.

ARTICULO 39. — Limitaciones de responsabilidad. Los certificadores licenciados no son responsables en los siguientes casos:

- a) Por los casos que se excluyan taxativamente en las condiciones de emisión y utilización de sus certificados y que no estén expresamente previstos en la ley;
- b) Por los daños y perjuicios que resulten del uso no autorizado de un certificado digital, si en las correspondientes condiciones de emisión y utilización de sus certificados constan las restricciones de su utilización;
- c) Por eventuales inexactitudes en el certificado que resulten de la información facilitada por el titular que, según lo dispuesto en las normas y en los manuales de procedimientos respectivos, deba ser objeto de verificación, siempre que el certificador pueda demostrar que ha tomado todas las medidas razonables.

CAPITULO X

Sanciones

ARTICULO 40. — Procedimiento. La instrucción sumarial y la aplicación de sanciones por violación a disposiciones de la presente ley serán realizadas por el ente licenciante. Es aplicable la Ley de Procedimientos Administrativos 19.549 y sus normas reglamentarias.

ARTICULO 41. — Sanciones. El incumplimiento de las obligaciones establecidas en la presente ley para los certificadores licenciados dará lugar a la aplicación de las siguientes sanciones:

- a) Apercibimiento;
- b) Multa de pesos diez mil (\$ 10.000) a pesos quinientos mil (\$ 500.000);
- c) Caducidad de la licencia.

Su gradación según reincidencia y/u oportunidad serán establecidas por la reglamentación.

El pago de la sanción que aplique el ente licenciante no relevará al certificador licenciado de eventuales reclamos por daños y perjuicios causados a terceros y/o bienes de propiedad de éstos, como consecuencia de la ejecución del contrato que celebren y/o por el incumplimiento de las obligaciones asumidas conforme al mismo y/o la prestación del servicio.

ARTICULO 42. — Apercibimiento. Podrá aplicarse sanción de apercibimiento en los siguientes casos:

- a) Emisión de certificados sin contar con la totalidad de los datos requeridos, cuando su omisión no invalidare el certificado;
- b) No facilitar los datos requeridos por el ente licenciante en ejercicio de sus funciones;
- c) Cualquier otra infracción a la presente ley que no tenga una sanción mayor.

ARTICULO 43. — Multa. Podrá aplicarse sanción de multa en los siguientes casos:

- a) Incumplimiento de las obligaciones previstas en el artículo 21;
- b) Si la emisión de certificados se realizare sin cumplimentar las políticas de certificación comprometida y causare perjuicios a los usuarios, signatarios o terceros, o se afectare gravemente la seguridad de los servicios de certificación;
- c) Omisión de llevar el registro de los certificados expedidos;
- d) Omisión de revocar en forma o tiempo oportuno un certificado cuando así correspondiere;

- e) Cualquier impedimento u obstrucción a la realización de inspecciones o auditorías por parte de la autoridad de aplicación y del ente licenciante;
- f) Incumplimiento de las normas dictadas por la autoridad de aplicación;
- g) Reincidencia en la comisión de infracciones que dieran lugar a la sanción de apercibimiento.

ARTICULO 44. — Caducidad. Podrá aplicarse la sanción de caducidad de la licencia en caso de:

- a) No tomar los debidos recaudos de seguridad en los servicios de certificación;
- b) Expedición de certificados falsos;
- c) Transferencia no autorizada o fraude en la titularidad de la licencia;
- d) Reincidencia en la comisión de infracciones que dieran lugar a la sanción de multa;
- e) Quiebra del titular.

La sanción de caducidad inhabilita a la titular sancionada y a los integrantes de órganos directivos por el término de 10 años para ser titular de licencias.

ARTICULO 45. — Recurribilidad. Las sanciones aplicadas podrán ser recurridas ante los Tribunales Federales con competencia en lo Contencioso Administrativo correspondientes al domicilio de la entidad, una vez agotada la vía administrativa pertinente.

La interposición de los recursos previstos en este capítulo tendrá efecto devolutivo.

ARTICULO 46. — Jurisdicción. En los conflictos entre particulares y certificadores licenciados es competente la Justicia en lo Civil y Comercial Federal. En los conflictos en que sea parte un organismo público certificador licenciado, es competente la Justicia en lo Contencioso-administrativo Federal.

CAPITULO XI

Disposiciones Complementarias

ARTICULO 47. — Utilización por el Estado Nacional. El Estado nacional utilizará las tecnologías y previsiones de la presente ley en su ámbito interno y en relación con los administrados de acuerdo con las condiciones que se fijen reglamentariamente en cada uno de sus poderes.

ARTICULO 48. — Implementación. El Estado nacional, dentro de las jurisdicciones y entidades comprendidas en el artículo 8° de la Ley 24.156, promoverá el uso masivo de la firma digital de tal forma que posibilite el trámite de los expedientes por vías simultáneas, búsquedas automáticas de la información y seguimiento y control por parte del interesado, propendiendo a la progresiva despapelización.

En un plazo máximo de 5 (cinco) años contados a partir de la entrada en vigencia de la presente ley, se aplicará la tecnología de firma digital a la totalidad de las leyes, decretos, decisiones administrativas, resoluciones y sentencias emanados de las jurisdicciones y entidades comprendidas en el artículo 8° de la Ley 24.156.

ARTICULO 49. — Reglamentación. El Poder Ejecutivo deberá reglamentar esta ley en un plazo no mayor a los 180 (ciento ochenta) días de su publicación en el Boletín Oficial de la Nación.

ARTICULO 50. — Invitación. Invítase a las jurisdicciones provinciales a dictar los instrumentos legales pertinentes para adherir a la presente ley.

ARTICULO 51. — Equiparación a los efectos del derecho penal. Incorporáse el siguiente texto como artículo 78 (bis) del Código Penal:

Los términos firma y suscripción comprenden la firma digital, la creación de una firma digital o firmar digitalmente. Los términos documento, instrumento privado y certificado comprenden el documento digital firmado digitalmente.

ARTICULO 52. — Autorización al Poder Ejecutivo. Autorízase al Poder Ejecutivo para que por la vía del artículo 99, inciso 2, de la Constitución Nacional actualice los contenidos del Anexo de la presente ley a fin de evitar su obsolescencia.

ARTICULO 53. — Comuníquese al Poder Ejecutivo.

DADA EN LA SALA DE SESIONES DEL CONGRESO ARGENTINO, EN BUENOS AIRES, A LOS CATORCE DIAS DEL MES DE NOVIEMBRE DEL AÑO DOS MIL UNO.

— REGISTRADA BAJO EL N° 25.506 —

RAFAEL PASCUAL. — EDUARDO MENEM. — Guillermo Aramburu. — Juan C. Oyarzún.

ANEXO

Información: conocimiento adquirido acerca de algo o alguien.

Procedimiento de verificación: proceso utilizado para determinar la validez de una firma digital. Dicho proceso debe considerar al menos:

- a) que dicha firma digital ha sido creada durante el período de validez del certificado digital del firmante;
- b) que dicha firma digital ha sido creada utilizando los datos de creación de firma digital correspondientes a los datos de verificación de firma digital indicados en el certificado del firmante;
- c) la verificación de la autenticidad y la validez de los certificados involucrados.

Datos de creación de firma digital: datos únicos, tales como códigos o claves criptográficas privadas, que el firmante utiliza para crear su firma digital.

Datos de verificación de firma digital: datos únicos, tales como códigos o claves criptográficas públicas, que se utilizan para verificar la firma digital, la integridad del documento digital y la identidad del firmante.

Dispositivo de creación de firma digital: dispositivo de hardware o software técnicamente confiable que permite firmar digitalmente.

Dispositivo de verificación de firma digital: dispositivo de hardware o software técnicamente confiable que permite verificar la integridad del documento digital y la identidad del firmante.

Políticas de certificación: reglas en las que se establecen los criterios de emisión y utilización de los certificados digitales.

Técnicamente confiable: cualidad del conjunto de equipos de computación, software, protocolos de comunicación y de seguridad y procedimientos administrativos relacionados que cumplan los siguientes requisitos:

1. Resguardar contra la posibilidad de intrusión y/o uso no autorizado;

2. Asegurar la disponibilidad, confiabilidad, confidencialidad y correcto funcionamiento;
3. Ser apto para el desempeño de sus funciones específicas;
4. Cumplir las normas de seguridad apropiadas, acordes a estándares internacionales en la materia;
5. Cumplir con los estándares técnicos y de auditoría que establezca la Autoridad de Aplicación.

Clave criptográfica privada: En un criptosistema asimétrico es aquella que se utiliza para firmar digitalmente.

Clave criptográfica pública: En un criptosistema asimétrico es aquella que se utiliza para verificar una firma digital.

Integridad: Condición que permite verificar que una información no ha sido alterada por medios desconocidos o no autorizados.

Criptosistema asimétrico: Algoritmo que utiliza un par de claves, una clave privada para firmar digitalmente y su correspondiente clave pública para verificar dicha firma digital.

A N E X O 7

**R e g l a m e n t o d e l a L e y
2 5 . 5 0 6 d e A r g e n t i n a**

FIRMA DIGITAL

Decreto 2628/2002

Reglamentación de la Ley N° 25.506. Consideraciones Generales. Autoridad de Aplicación. Comisión Asesora para la Infraestructura de Firma Digital. Ente Administrador de Firma Digital. Sistema de Auditoría. Estándares Tecnológicos. Revocación de Certificados Digitales. Certificadores Licenciados. Autoridades de Registro. Disposiciones para la Administración Pública Nacional.

Bs. As., 19/12/2002

VISTO la Ley N° 25.506, el Decreto N° 427 del 16 de abril de 1998, el Decreto N° 78 del 10 de enero de 2002, el Decreto N° 333 del 19 de febrero de 1985 y sus modificatorios y la Resolución N° 194 del 27 de noviembre de 1998 de la ex SECRETARIA DE LA FUNCION PUBLICA, y

CONSIDERANDO:

Que la sanción de la Ley N° 25.506 de firma digital representa un avance significativo para la inserción, de nuestro país en la sociedad de la información y en la economía digital, brindando una oportunidad para el desarrollo del sector productivo vinculado a las nuevas tecnologías.

Que otros países ya han normado sobre la materia, con positiva repercusión tanto en el ámbito privado como público.

Que con la sanción de la citada Ley N° 25.506, de firma digital se reconoce el empleo de la firma, digital y de la firma electrónica y su eficacia jurídica en las condiciones que la misma ley establece.

Que dicho reconocimiento constituye un elemento esencial para otorgar seguridad a las transacciones electrónicas, promoviendo el comercio electrónico seguro, de modo de permitir la identificación en forma fehaciente de las personas que realicen transacciones electrónicas.

Que asimismo, la sanción de la Ley N° 25.506 otorga un decisivo impulso para la progresiva despapelización del Estado, contribuyendo a mejorar su gestión, facilitar el acceso de la comunidad a la información pública y posibilitar la realización de trámites por Internet en forma segura.

Que la reglamentación de la Ley N° 25.506 permitirá establecer una Infraestructura de Firma Digital que ofrezca autenticación, y garantía de integridad para los documentos digitales o electrónicos y constituir la base tecnológica que permita otorgarles validez jurídica.

Que debe regularse el funcionamiento de los certificadores licenciados de manera de garantizar la adecuada prestación de los servicios de certificación.

Que resulta necesario crear un Ente Administrador de Firma Digital, encargado de otorgar las licencias a los certificadores, supervisar su actividad y dictar las normas tendientes a asegurar el régimen de libre competencia en el mercado de los prestadores y protección de los usuarios de Firma Digital.

Que la citada Ley contempla la creación de una Comisión Asesora para la Infraestructura de Firma Digital, conformada por un equipo multidisciplinario de especialistas en la materia, con el fin de asesorar y recomendar a la Autoridad de Aplicación estándares tecnológicos, y otros aspectos que hacen al funcionamiento de la mencionada Infraestructura, por lo cual deben establecerse las bases para su formación y adecuado funcionamiento.

Que el Decreto N° 427 del 16 de abril de 1998 ha sido una de las normas pioneras a nivel nacional e internacional en reconocer la validez jurídica de la firma digital, para lo cual creó una Infraestructura de Firma Digital para el Sector Público Nacional bajo la dependencia de la JEFATURA DE GABINETE DE MINISTROS.

Que esta experiencia ha sido un antecedente fundamental para la incorporación de la tecnología en la gestión pública, constituyendo una fuente de consulta para distintas jurisdicciones nacionales y provinciales.

Que dado que la Ley N° 25.506 establece una Infraestructura de Firma Digital de alcance federal, a fin de optimizar el aprovechamiento de los recursos y las experiencias desarrolladas, resulta conveniente subsumir la mencionada Infraestructura del Sector Público Nacional dentro de la creada a nivel federal por la Ley citada.

Que a tal fin, corresponde derogar el Decreto N° 427/98, por el cual se reconoce el empleo de la firma digital en el ámbito de la Administración Pública Nacional, ya que la Ley N° 25.506 cubre los objetivos y el alcance del mencionado Decreto.

Que ha tomado intervención el servicio jurídico competente.

Que la presente medida se dicta en virtud lo dispuesto por el artículo 49 de la Ley N° 25.506, y por el artículo 99, inciso 2, de la Constitución de la Nación Argentina.

Por ello,

EL PRESIDENTE DE LA NACION ARGENTINA

DECRETA:

CAPITULO I

CONSIDERACIONES GENERALES

Artículo 1° — Objeto. La presente reglamentación regula el empleo de la firma electrónica y de la firma digital y su eficacia jurídica.

En los casos contemplados por los artículos 3°, 4° y 5° de la Ley N° 25.506 podrán utilizarse los siguientes sistemas de comprobación de autoría e integridad:

- a) Firma electrónica,
- b) Firma digital basada en certificados digitales emitidos por certificadores no licenciados en el marco de la presente reglamentación,
- c) Firma digital basada en certificados digitales emitidos por certificadores licenciados en el marco de la presente reglamentación,
- d) Firma digital basada en certificados digitales emitidos por certificadores extranjeros que hayan sido reconocidos en los siguientes casos:
 1. En virtud de la existencia de acuerdos de reciprocidad entre la República Argentina y el país de origen del certificador extranjero.
 2. Por un certificador licenciado en el país en el marco de la presente reglamentación y validado por la Autoridad de Aplicación.

Art. 2° — Validez de los certificados, digitales emitidos por certificadores no licenciados. Los certificados digitales emitidos por certificadores no licenciados serán válidos para producir los efectos jurídicos que la ley otorga a la firma electrónica.

Art. 3° — Certificados digitales emitidos por certificadores licenciados. Los certificados digitales contemplados, en el artículo 13 de la Ley N° 25.506 son aquellos cuya

utilización permite disponer de una firma digital amparada por las presunciones de autoría e integridad establecidas en los artículos 7° y 8° de la ley citada.

CAPITULO II

DE LA AUTORIDAD DE APLICACION

Art. 4° — Normas técnicas. Facúltase a la JEFATURA DE GABINETE DE MINISTROS, a determinar las normas y los procedimientos técnicos para la generación, comunicación, archivo y conservación del documento digital o electrónico, según lo previsto en los artículos 11 y 12 de la Ley N° 25.506.

Art. 5° — Conservación. El cumplimiento de la exigencia legal de conservar documentos, registros o datos, conforme a la legislación vigente a la materia, podrá quedar satisfecha con la conservación de los correspondientes, documentos digitales firmados digitalmente. Los documentos, registros o datos electrónicos, deberán ser almacenados por los intervinientes o por terceros confiables aceptados por los intervinientes, durante los plazos establecidos en las normas específicas.

Se podrán obtener copias autenticadas a partir de los originales en formato digital firmado digitalmente. La certificación de autenticidad se hará de conformidad a los procedimientos legales, vigentes para el acto de que se trate, identificando el soporte que procede la copia.

Art. 6° — Regulación. Facúltase a la JEFATURA DE GABINETE DE MINISTROS a establecer:

- a) Los estándares tecnológicos y de seguridad aplicables en consonancia con estándares internacionales.
- b) Los procedimientos de firma y verificación en consonancia con los estándares tecnológicos definidos conforme el inciso precedente.
- c) Las condiciones mínimas de emisión de certificados digitales.
- d) Los casos en los cuales deben revocarse los certificados digitales.
- e) Los datos considerados públicos contenidos en los certificados digitales.
- f) Los mecanismos que garantizarán la validez y autoría de las listas de certificados revocados.

- g) La información que los certificadores licenciados deberán publicar por internet.
- h) La información que los certificadores licenciados deberán publicar en el Boletín Oficial.
- i) Los procedimientos mínimos de revocación de certificados digitales cualquiera que sea la fuente de emisión, y los procedimientos mínimos de conservación de la documentación de respaldo de la operatoria de los certificadores licenciados, en el caso que éstos cesen su actividad.

- j) El sistema de auditoría, incluyendo las modalidades de difusión de los informes de auditoría y los requisitos de habilitación para efectuar auditorías.
- k) Las condiciones y procedimientos para el otorgamiento y revocación de las licencias.
- l) Las normas y procedimientos para la homologación de los dispositivos de creación y verificación de firmas digitales.
- m) El reglamento de funcionamiento de la Comisión Asesora para la Infraestructura de Firma Digital.
- n) El procedimiento de instrucción sumarial y lagradación de sanciones previstas en la Ley N° 25.506, en virtud de reincidencia y/u oportunidad.
- o) Los procedimientos aplicables para el reconocimiento de certificados extranjeros.
- p) Las condiciones de aplicación de la presente ley en el Sector Público Nacional, incluyendo la autorización para prestar servicios de certificación digital para las entidades y jurisdicciones de la Administración Pública Nacional.
- q) Los contenidos mínimos de las políticas de certificación de acuerdo con los estándares nacionales e internacionales y las condiciones mínimas que deberán cumplirse en el caso de cese de actividades de un certificador licenciado.
- r) Los niveles de licenciamiento.

- s) Reglamentar el uso y los alcances de los certificados de firma digital emitidos por los Registros Públicos de Contratos.
- t) Exigir las garantías y seguros necesarios para prestar el servicio previsto.
- u) Las condiciones de prestación de otros servicios en relación con la firma digital y otros temas cubiertos en la ley.

CAPITULO III

DE LA COMISION ASESORA PARA LA INFRAESTRUCTURA DE FIRMA DIGITAL

Art. 7° — Comisión Asesora para la Infraestructura de Firma Digital. En el ámbito de la JEFATURA DE GABINETE DE MINISTROS funcionará la Comisión Asesora para la Infraestructura de Firma Digital, que se constituirá de acuerdo a lo dispuesto por el artículo 35 de la Ley N° 25.506.

Art. 8° — Integración. La Comisión Asesora para la Infraestructura de Firma Digital estará integrada multidisciplinariamente por profesionales de carreras afines a la actividad, de reconocida trayectoria y experiencia, provenientes de organismos del Estado Nacional, Universidades, Cámaras, Colegios u otros entes representativos profesionales. Para integrar la Comisión Asesora para la Infraestructura de Firma Digital se deberán reunir los siguientes requisitos:

- a) Poseer título universitario, expedido por Universidad Nacional o privada reconocida por el Estado, correspondiente a carrera profesional de duración no inferior a CUATRO (4) años, con incumbencias relacionadas con la materia.
- b) Antecedentes académicos y/o profesionales o laborales en la materia.

Art. 9° — Ejercicio de funciones. El ejercicio de las funciones como miembro de la Comisión Asesora para la Infraestructura de Firma Digital será ad honorem.

Art. 10. — Consulta Pública. La Comisión Asesora para la Infraestructura de Firma Digital establecerá los mecanismos que permitan mantener un intercambio de información fluido con organismos públicos, Cámaras, usuarios y asociaciones de consumidores sobre los temas que se está tratando los efectos de recibir aportes y opiniones. Para cumplir con este cometido podrá implementar consultas públicas presenciales, por escrito o mediante foros virtuales, abiertos e indiscriminados, o cualquier otro medio que la Comisión considere conveniente o necesario.

CAPITULO IV

DEL ENTE ADMINISTRADOR DE FIRMA DIGITAL

Art. 11. — Ente Administrador de Firma Digital. Créase el Ente Administrador de Firma Digital dependiente de la JEFATURA DE GABINETE DE MINISTROS, como órgano técnico, administrativo encargado de otorgar las licencias a los certificadores y de supervisar su actividad, según las exigencias instituidas por el presente decreto y las normas reglamentarias, modificatorias o de aplicación que se dicten en el futuro y de dictar las normas tendientes a asegurar el régimen de libre competencia, equilibrio de participación en el mercado de los prestadores y protección de los usuarios.

(Nota Infoleg: Por art. 1° del [Decreto N° 1028/2003](#) B.O. 10/11/2003 se disuelve el Ente Administrador de Firma Digital creado por el presente artículo).

Art. 12. — Autoridades del Ente Administrador de Firma Digital. El Ente Administrador de Firma Digital será conducido por un Directorio integrado por TRES (3) miembros, designados

por el JEFE DE GABINETE DE MINISTROS, previo concurso. Hasta tanto, sea realizado el concurso el JEFE DE GABINETE DE MINISTROS designará a los integrantes del Directorio, uno de los cuales ocupará el cargo de Presidente del Ente. El gerenciamiento del Ente estará a cargo del Coordinador Ejecutivo designado por el JEFE DE GABINETE DE MINISTROS.

Art. 13. — Funciones del Ente Administrador.

Son funciones del Ente Administrador:

- a) Otorgar las licencias habilitantes para acreditar a los certificadores en las condiciones que fijen el presente decreto y las normas reglamentarias, modificatorias o de aplicación que se dicten en el futuro.
- b) Fiscalizar el cumplimiento de las normas legales y reglamentarias en lo referente a la actividad de los certificadores licenciados.
- c) Denegar las solicitudes de licencia a los prestadores de servicios de certificación que no cumplan con los requisitos establecidos, para su licenciamiento.

- d) Revocar las licencias otorgadas a los Certificadores licenciados que dejen de cumplir con los requisitos establecidos para su licenciamiento.
- e) Aprobar las políticas de certificación, el manual de procedimiento, el plan de seguridad, de cese de actividades y el plan de contingencia, presentado por los certificadores solicitantes de la licencia o licenciados.
- f) Solicitar los informes de auditoría en los casos que correspondiere.
- g) Realizar inspecciones a los certificadores licenciados por sí o por terceros.
- h) Homologar los dispositivos de creación y verificación de firmas digitales, con ajuste a las normas y procedimientos establecidos por la presente reglamentación.
- i) Disponer la instrucción sumarial, la aplicación de sanciones e inhabilitar en forma temporal o permanente a todo certificador o licenciado que no respetare o incumpliere los requerimientos y disposiciones de la Ley N° 25.506, el presente decreto y las normas complementarias.
- j) Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, los domicilios, números telefónicos, direcciones de internet y certificados digitales de los certificadores licenciados.
- k) Publicar en internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, los domicilios, los números telefónicos, direcciones de internet y certificados digitales de los certificadores cuyas licencias han sido revocadas.
- l) Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, el domicilio, números telefónicos, direcciones de internet y certificados digitales del Ente Administrador.
- m) Administrar los recursos generados de acuerdo con lo dispuesto por el artículo 16 de la presente reglamentación, provenientes de las distintas fuentes de financiamiento.
- n) Fijar el concepto y los importes de todo tipo de aranceles y multas previstos en la Ley N° 25.506 y en el artículo 16 de la presente reglamentación.
- o) Solicitar la ampliación o aclaración sobre la documentación presentada por el certificador.

p) Dictar las normas tendientes a asegurar el régimen de libre competencia, equilibrio de participación en el mercado de los prestadores y protección de los usuarios.

Art. 14. — Obligaciones del Ente Administrador.

El Ente Administrador tiene idénticas obligaciones que los titulares, de certificados y que los Certificadores Licenciados, en su caso, y además debe:

a) Permitir el acceso público permanente a la nómina actualizada de certificadores licenciados con los datos correspondientes.

b) Supervisar la ejecución del plan de cese de actividades de los Certificadores licenciados que discontinúan sus funciones;

c) Registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas.

d) Supervisar la ejecución de planes de contingencia de los certificadores licenciados.

e) Efectuar las tareas de control del cumplimiento de las recomendaciones formuladas por el Ente Administrador para determinar si se han tomado las acciones correctivas correspondientes.

f) Recibir, evaluar y resolver los reclamos de los usuarios de certificados digitales relativos a la prestación del servicio por parte de certificadores licenciados.

Art. 15. — Organización del Ente Administrador. Dentro del plazo de SESENTA (60) días corridos de la fecha de constitución del Directorio, el ENTE ADMINISTRADOR DE FIRMA DIGITAL elevará para su consideración al JEFE DE GABINETE DE MINISTROS la propuesta de su estructura organizativa y de su reglamento de funcionamiento.

Art. 16. — Recursos del Ente Administrador. El Ente Administrador podrá arancelar los servicios que preste para cubrir total o parcialmente sus costos. Los recursos propios del Ente Administrador se integrarán con:

a) Los importes provenientes de los aranceles que se abonen por la provisión de los siguientes servicios:

- 1.- Servicios de certificación digital,
- 2.- Servicios de certificación digital de fecha y hora,
- 3.- Servicios de almacenamiento seguro de documentos electrónicos,
- 4.- Servicios prestados por autoridades de registro,
5. - Servicios prestados por terceras partes confiables,
6. - Servicios de certificación de documentos electrónicos firmados digitalmente
- 7.- Otros servicios o actividades relacionados a la firma digital.

b) Los importes provenientes de los aranceles de homologación de dispositivos de creación y verificación de firmas digitales.

c) Los importes provenientes de los aranceles de certificación de sistemas que utilizan firma digital.

d) Los importes provenientes de los aranceles de administración del sistema de auditoría y las auditorías que el organismo realice por sí o por terceros.

e) Los subsidios, herencias, legados, donaciones o transferencias bajo cualquier título que reciba.

f) El producido de multas.

g) Los importes que se le asignen en el cálculo de recursos de la respectiva ley de presupuesto para la administración nacional.

h) Los demás fondos, bienes, o recursos que puedan serle asignados en virtud de las leyes y reglamentaciones aplicables.

Art. 17. — Financiamiento del Ente Administrador. Instrúyese a la JEFATURA DE GABINETE DE MINISTROS para que proceda a incluir en su presupuesto los fondos necesarios para que el Ente Administrador pueda cumplir adecuadamente sus funciones.

Transitoriamente, desde la entrada en vigencia de la presente reglamentación y hasta que se incluyan las partidas necesarias en el Presupuesto Nacional los costos de financiamiento del Ente Administrador serán afrontados con el crédito presupuestario correspondiente a la JEFATURA DE GABINETE DE MINISTROS.

CAPITULO V

DEL SISTEMA DE AUDITORIA

Art. 18. — Precalificación de entidades de auditoría. La JEFATURA DE GABINETE DE MINISTROS convocará a concurso público para la precalificación de entidades de auditoría entre las universidades y organismos científicos y/o tecnológicos nacionales o provinciales, los Colegios y Consejos profesionales, que acrediten experiencia profesional acorde en la materia, interesadas en prestar el servicio de auditoría de entidades prestadoras de servicios de certificación digital. A tal fin, elaborará un Pliego Estándar de Precalificación de Entidades de Auditoría, y determinará la periodicidad de la convocatoria.

Art. 19. — Informe de auditoría. El informe de auditoría evaluará los sistemas utilizados por el certificador de acuerdo con los requerimientos de la Ley N° 25.506, el presente decreto y las normas complementarias.

Art. 20. — Conflicto de intereses. Para garantizar la objetividad e imparcialidad de la actividad de auditoría no podrán desempeñarse en la prestación de servicios de auditoría aquellas entidades o personas vinculadas con prestadores de servicios de certificación, lo que será establecido en el Pliego Estándar de Precalificación de Entidades de Auditoría previsto en el artículo 18 del presente decreto.

Art. 21. — Deber de confidencialidad. Las entidades auditantes y las personas que efectúen las auditorías deben mantener la confidencialidad sobre la información considerada amparada bajo normas de confidencialidad por el Certificado Licenciado.

CAPITULO VI

DE LOS ESTANDARES TECNOLOGICOS

Art. 22. — Aplicación provisoria de los estándares vigentes. Hasta tanto la JEFATURA DE GABINETE DE MINISTROS apruebe los Estándares Tecnológicos de Infraestructura de Firma Digital en consonancia con estándares tecnológicos internacionales, mantendrán su vigencia los establecidos en la Resolución N° 194/98 de la ex Secretaría de la Función Publica.

CAPITULO VII

DE LA REVOCACION DE CERTIFICADOS DIGITALES

Art. 23. — Revocación de certificados. Se deberán revocar los certificados digitales emitidos en los siguientes casos:

- a) A solicitud del titular del certificado digital
- b) Si se determina que un certificado digital fue emitido en base a una información falsa que en el momento de la emisión hubiera sido objeto de verificación.
- c) Si se determina que los procedimientos de emisión y/o verificación han dejado de ser seguros.
- d) Por condiciones especiales definidas en las Políticas de Certificación.
- e) Por Resolución Judicial o de la Autoridad de Aplicación debidamente fundada.
- f) Por fallecimiento del titular.
- g) Por declaración judicial de ausencia con presunción de fallecimiento del titular.
- h) Por declaración judicial de incapacidad del titular.
- i) Si se determina que la información contenida en el certificado ha dejado de ser válida.
- j) Por el cese de la relación de representación respecto de una persona.

CAPITULO VIII

DE LOS CERTIFICADORES LICENCIADOS

Art. 24. — Obtención de la licencia. Para obtener una licencia, los proveedores de servicios de certificación deberán particularizar las actividades para las cuales requieren la licencia y acreditar por los medios que este determine ante el Ente Administrador de Firma Digital:

- a) Documentación que demuestre:
 - 1.- En el caso de personas jurídicas, su personería.

2.- En el caso de registro público de contratos, tal condición

3.- En el caso de organización pública, la autorización de su máxima autoridad para iniciar el proceso de licenciamiento y la correspondiente aprobación de la JEFATURA DE GABINETE DE MINISTROS, de acuerdo con lo dispuesto en el artículo 41 de la presente reglamentación.

b) El cumplimiento de las condiciones establecidas en la ley; este decreto y las normas complementarias.

c) Las políticas de certificación para las cuales solicita licencia que respaldan la emisión de sus certificados, Manual de Procedimientos, Plan de Seguridad, Plan de Cese de Actividades y Plan de Contingencia satisfactorias de acuerdo con las normas reglamentarias.

d) Toda aquella información o requerimiento, que demande la Autoridad de Aplicación.

Art. 25. — Efectos del licenciamiento. El otorgamiento de la licencia no implica que el Ente Administrador de la Infraestructura de Firma Digital, la JEFATURA DE GABINETE DE MINISTROS, las entidades auditantes o cualquier organismo del Estado garantice la provisión de los servicios de certificación o los productos provistos por el Certificador Licenciado.

Art. 26. — Duración de la licencia. Las licencias tendrán un plazo de duración de CINCO (5) años y podrán ser renovadas.

Los certificadores licenciados deberán efectuar anualmente una declaración jurada en la cual conste el cumplimiento de las normas establecidas en la Ley N° 25.506, en el presente decreto y en las normas complementarias.

Los certificadores licenciados serán sometidos a auditorías anuales.

Art. 27. — Causales de caducidad de la licencia. El Ente Administrador podrá disponer de oficio, y en forma preventiva la caducidad de la licencia en los siguientes casos:

a) Falta de presentación de la declaración jurada anual.

b) Falsedad de los datos contenidos en la declaración jurada anual.

- c) Dictamen desfavorable de auditoría basado en causales graves.
- d) Informe de la inspección dispuesta por el Ente Administrador desfavorable basado, en causales graves.
- e) Cuando el certificador licenciado no permita la realización de auditorías o inspecciones dispuestas por el Ente Administrador.

Art. 28. — Reconocimiento de certificados extranjeros. De acuerdo a lo establecido en el artículo 6° de la presente reglamentación, facúltase a la JEFATURA DE GABINETE DE MINISTROS a elaborar y firmar acuerdos de reciprocidad con gobiernos de países extranjeros, a fin de otorgar validez, en sus respectivos territorios, a los certificados digitales emitidos por certificadores de ambos países, en tanto se verifique el cumplimiento de las condiciones establecidas por la Ley N° 25.506 y su reglamentación para los certificados emitidos por certificadores nacionales.

Los certificadores licenciados no podrán reconocer certificaciones emitidas por certificadores extranjeros correspondientes a personas con domicilio o residencia en la República Argentina. El Ente Administrador de Firma Digital establecerá las relaciones que los certificadores licenciados deberán guardar entre los certificados emitidos en la República Argentina y los certificados reconocidos de certificadores extranjeros.

Art. 29. — Políticas de Certificación. La JEFATURA DE GABINETE DE MINISTROS definirá el contenido, mínimo de las políticas de certificación de acuerdo con los estándares nacionales e internacionales vigentes, las que deberán contener al menos la siguiente información:

- a) Identificación del certificador licenciado.
- b) Política de administración de los certificados y detalles de los servicios arancelados.
- c) Obligaciones de la entidad y de los suscriptores de los certificados.
- d) Tratamiento de la información suministrada por los suscriptores, y resguardo de la confidencialidad en su caso.
- e) Garantías que ofrece para el cumplimiento de las obligaciones que se deriven de sus actividades.

Art. 30. — Seguros. El certificador licenciado debe contar con seguros vigentes acordes con las responsabilidades asumidas, que cumplan con los siguientes requisitos.

a) Ser expedidos por una entidad aseguradora autorizada para operar en la República Argentina.

b) Establecer la obligación de la entidad aseguradora de informar previamente al Ente Administrador de la Infraestructura de Firma Digital la terminación del contrato o las modificaciones que reduzcan el alcance o monto de la cobertura.

Los certificadores licenciados pertenecientes a entidades y jurisdicciones del sector público quedarán exentos de la obligación de constituir el seguro previsto en el presente artículo.

Art. 31. — Responsabilidad de los certificadores licenciados. En ningún caso, la responsabilidad que pueda emanar de una certificación efectuada por un certificador licenciado, público o privado, comprometerá la responsabilidad pecuniaria del Estado en su calidad de Ente Administrador de la Infraestructura de Firma Digital.

Art. 32. — Recursos de los certificadores licenciados. Para el desarrollo adecuado de las actividades de certificación, el certificador deberá acreditar que cuenta con un equipo de profesionales, infraestructura física tecnológica y recursos financieros, como así también procedimientos y sistemas de seguridad que permitan:

a) Generar en un ambiente seguro las firmas digitales propias y todos los servicios para los cuales solicite licencia.

b) Cumplir con lo previsto en sus políticas y procedimientos de certificación.

c) Garantizar la confiabilidad de los sistemas de acuerdo con los estándares aprobados por la Autoridad de Aplicación.

d) Expedir certificados que cumplan con:

1.- Lo previsto en los artículos 13 y 14 de la Ley N° 25.506.

2.- Los estándares tecnológicos aprobados por la JEFATURA DE GABINETE DE MINISTROS.

e) Garantizar la existencia de sistemas de seguridad física y lógica que cumplan las normativas vigentes.

- f) Proteger el manejo de la clave privada de la entidad mediante un procedimiento de seguridad que impida el acceso a la misma a personal no autorizado.
- g) Proteger el acceso y el uso de la clave privada mediante procedimientos que exijan la participación de más de una persona.
- h) Registrar las transacciones realizadas, a fin de identificar el autor y el momento de cada una de las operaciones.
- i) Utilizar con exclusividad los sistemas que cumplan las funciones de certificación con ese propósito, sin que se les asigne ninguna otra función.
- j) Proteger a todos los sistemas utilizados directa o indirectamente en la función de certificación con procedimientos de autenticación y seguridad de alto nivel de protección, que deban ser actualizados de acuerdo a los avances tecnológicos para garantizar la correcta prestación de los servicios de certificación.
- k) Garantizar la continuidad de las operaciones mediante un Plan de Contingencia actualizado y aprobado.
- l) Disponer de los recursos financieros adecuados al tipo de actividad de certificación que desarrolla, acorde con los niveles de responsabilidad derivados de la misma.

Art. 33. — Servicios de Terceros. En los casos en que el certificador licenciado requiera o utilice los servicios de infraestructura tecnológicos prestados por un tercero, deberá prever dentro de su Plan de Contingencia los procedimientos a seguir en caso de interrupción de estos servicios, de modo tal que permita continuar prestando sus servicios de certificación sin ningún perjuicio para los suscriptores.

Los contratos entre el certificador licenciado y los proveedores de servicios o infraestructura deberán garantizar la ejecución de los procedimientos contemplados en el Plan de Cese de actividades aprobado por el Ente Licenciante. El certificador licenciado o en proceso de licenciamiento deberá facilitar al Ente Licenciante toda aquella información obrante en los contratos vinculada a la prestación de servicios de certificación y a la implementación del Plan de Cese de actividades y el Plan de Contingencia.

La contratación de servicios o infraestructura no exime al prestador de la presentación de los informes de auditoría, los cuales deberán incluir los sistemas y seguridades del prestador contratado.

Art. 34. — Obligaciones del certificador licenciado. Además de lo previsto en el artículo 21 de la Ley N° 25.506, los certificadores licenciados deberán:

- a) Comprobar por sí o por medio de una Autoridad de Registro que actúe en nombre y por cuenta suya, la identidad y cualquier otro dato de los solicitantes considerado relevante para los procedimientos de verificación de identidad previos a la emisión del certificado digital, según la Política de Certificación bajo la cual se solicita.
- b) Mantener a disposición permanente del público las Políticas de Certificación y el Manual de Procedimientos correspondiente.
- c) Cumplir cabalmente con las políticas de certificación acordadas con el titular y con su Manual de Procedimientos.
- d) Garantizar la prestación establecida según los niveles definidos en el acuerdo de servicios pactados con sus usuarios, relativo a los servicios para los cuales solicitó el licenciamiento.
- e) Informar al solicitante de un certificado digital, en un lenguaje claro y accesible, en idioma nacional, respecto de las características del certificado solicitado, las limitaciones a la responsabilidad, si las hubiere, los precios de los servicios de certificación, uso, administración y otros asociados, incluyendo cargos adicionales y formas de pago, los niveles de servicio al proveer, las obligaciones que el suscriptor asume como usuario del servicio de certificación, su domicilio en la República Argentina y los medios a los que el suscriptor puede acudir para solicitar aclaraciones, dar cuenta del mal funcionamiento del sistema o presentar sus reclamos.
- f) Disponer de un servicio de atención a titulares y terceros, que permita evacuar las consultas y la pronta solicitud de revocación de certificados.
- g) Garantizar el acceso permanente, eficiente y gratuito de los titulares y terceros al repositorio de certificados revocados.
- h) Mantener actualizados los repositorios de certificados revocados por el período establecido por el Ente Administrador.
- i) Abstenerse de generar, exigir, tomar conocimiento o acceder bajo ninguna circunstancia a la clave privada del suscriptor.
- j) Informar al Ente Administrador de modo inmediato la ocurrencia de cualquier evento que comprometa la correcta prestación del servicio.

k) Respetar el derecho del titular del certificado digital a no recibir publicidad de ningún tipo por su intermedio, salvo consentimiento expreso de éste.

l) Publicar en el Boletín Oficial durante UN (1) día, el certificado de clave pública correspondiente a la política para la cual obtuvo licenciamiento;

m) Cumplir las normas y recaudos establecidos para la protección de datos personales.

n) En los casos de revocación de certificados contemplados en el apartado 3 del inciso e) del artículo 19 de la Ley N° 25.506, deberá sustituir en forma gratuita aquel certificado digital que ha dejado de ser seguro por otro que sí cumpla con estos requisitos.

El Ente Administrador deberá establecer el proceso de reemplazo de certificados en estos casos. En los casos en los que un certificado digital haya dejado de ser seguro por razones atribuibles a su titular, el certificador licenciado no estará obligado a sustituir el certificado digital.

o) Enviar periódicamente al Ente Administrador, informes de estado de operaciones con carácter de declaración jurada.

p) Contar con personal idóneo y confiable, con antecedentes profesionales acordes a la función desempeñada.

q) Responder a los pedidos de informes por parte de un tercero respecto de la validez y alcance de un certificado digital emitido por él.

CAPITULO IX

DE LAS AUTORIDADES DE REGISTRO

Art. 35. — Funciones de las Autoridades de Registro. Los Certificadores Licenciados podrán delegar en Autoridades de Registro las funciones de validación de identidad y otros datos de los suscriptores de certificados y de registro de las presentaciones y trámites que les sean formuladas, bajo la responsabilidad del Certificador Licenciado, cumpliendo las normas y procedimientos establecidos por la presente reglamentación.

Una autoridad de Registro es una entidad responsable de las siguientes funciones:

- a) La recepción de las solicitudes de emisión de certificados.
- b) La validación de la identidad y autenticación de los datos de los titulares de certificados.
- c) La validación de otros datos de los titulares de certificados que se presenten ante ella cuya verificación delegue el Certificador Licenciado.
- d) La remisión de las solicitudes aprobadas al Certificador Licenciado con la que se encuentre operativamente vinculada.
- e) La recepción y validación de las solicitudes de revocación de certificados; y su direccionamiento al Certificador Licenciado con el que se vinculen.
- f) La identificación y autenticación de los solicitantes de revocación de certificados.
- g) El archivo y la conservación de toda la documentación respaldatoria del proceso de validación de identidad, de acuerdo con los procedimientos establecidos por el certificador licenciado.
- h) El cumplimiento de las normas y recaudos establecidos para la protección de datos personales.
- i) El cumplimiento de las disposiciones que establezca la Política de Certificación y el Manual de Procedimientos del Certificador Licenciado con el que se encuentre vinculada, en la parte que resulte aplicable.

Art. 36. — Responsabilidad del certificador licenciado respecto de la Autoridad de Registro. Una Autoridad de Registro puede constituirse como una única unidad o con varias unidades dependientes jerárquicamente entre sí, pudiendo, delegar su operatoria en otras autoridades de registro, siempre que medie la aprobación del Certificador Licenciado. El Certificador, Licenciado es responsable con los alcances establecidos en la Ley N° 25.506, aún en el caso de que delegue parte de su operatoria en Autoridades de Registro, sin perjuicio del derecho del certificador de reclamar a la Autoridad de Registro las indemnizaciones por los daños y perjuicios que aquél sufriera como consecuencia de los actos y/u omisiones de ésta.

CAPITULO X

DISPOSICIONES PARA LA ADMINISTRACION PUBLICA NACIONAL

Art. 37. — Despapelización del Estado. Sin perjuicio de la aplicación directa de la ley en lo relativo a la validez jurídica de la firma electrónica, de la firma digital y de los documentos digitales, la implementación de las disposiciones de la ley y del presente decreto para la digitalización de procedimientos y trámites internos de la Administración Pública Nacional, de las Administraciones Públicas Provinciales, y de los Poderes Legislativos y Judiciales del orden nacional y provincial, así como los vinculados a la relación de las mencionadas jurisdicciones y entidades con los administrados, se hará de acuerdo a lo que fijen reglamentariamente cada uno de los Poderes y Administraciones.

Art. 38. — Aplicaciones en organismos de la Administración Pública Nacional. Los organismos de la Administración Pública Nacional que para la tramitación de documentos digitales o la implementación de aplicaciones requieran firma digital, solamente aceptarán certificados digitales emitidos por Certificadores, Licenciados, o certificados digitales emitidos por certificadores extranjeros reconocidos por acuerdos internacionales o por certificadores licenciados del país.

Las entidades y jurisdicciones pertenecientes al sector público podrán ser certificadores licenciados y emitir certificados para agentes y funcionarios públicos destinados a las aplicaciones de gestión interna de los organismos públicos a que éstos pertenecieran. Cuando razones de orden público o de interés social lo ameriten y cuenten con la autorización de la JEFATURA DE GABINETE DE MINISTROS podrán emitir certificados a particulares.

En aquellas aplicaciones en las que el Estado interactúe con la comunidad, se deberá admitir la recepción de documentos digitales firmados digitalmente utilizando certificados digitales emitidos por certificadores licenciados privados o públicos, indistintamente.

Art. 39. — Autoridades de Registro pertenecientes a la Administración Pública Nacional. En las entidades y jurisdicciones pertenecientes a la Administración Pública Nacional, las áreas de recursos humanos cumplirán las funciones de Autoridades de Registro para los agentes y funcionarios de su jurisdicción. En el caso, y si las aplicaciones de que se trate lo requieren, la máxima autoridad del organismo podrá asignar, adicionalmente, a otra unidad las funciones de Autoridad de Registro.

Art. 40. — Agentes y funcionarios. La Autoridad de Aplicación podrá requerir para el cumplimiento de lo establecido en la presente reglamentación la adscripción de agentes y funcionarios pertenecientes a las entidades y jurisdicciones comprendidas en el artículo 8° de la Ley N° 24.156 y sus modificatorias.

Art. 41. — Utilización por las entidades y jurisdicciones de la Administración Pública Nacional. La JEFATURA DE GABINETE DE MINISTROS, establecerá las normas de aplicación de la presente reglamentación en la Administración Pública Nacional, que deberán contemplar:

a) Las acciones tendientes a promover el uso masivo de la firma digital con el fin de posibilitar el trámite de los expedientes en forma simultánea, búsquedas automáticas de información, seguimiento y control por parte de los interesados.

b) Las acciones tendientes a implementar la progresiva despapelización del Estado, a fin de contar en un plazo de CINCO (5) años con la totalidad de la documentación administrativa en formato digital.

c) La interoperabilidad entre aplicaciones.

d) La autorización para solicitar el licenciamiento como certificador ante el Ente Administrador de la Infraestructura de Firma Digital para las entidades y jurisdicciones de la Administración Pública Nacional.

e) La participación del Cuerpo de Administradores Gubernamentales a los fines de difundir el uso de la firma digital y facilitar los procesos de despapelización.

Art. 42. — Presentación de documentos electrónicos. Los organismos de la Administración Pública Nacional deberán establecer mecanismos que garanticen la opción de remisión, recepción, mantenimiento y publicación de información electrónica, siempre que esto sea aplicable, tanto para la gestión de documentos entre organismos como para con los ciudadanos.

Art. 43. — Normas para la elaboración y redacción de la documentación administrativa. Lo dispuesto en la presente reglamentación constituye una alternativa a lo establecido por el Decreto N° 333/85 y sus modificatorios.

Art. 44. — Glosario. Apruébase el glosario que obra como Anexo I del presente Decreto.

Art. 45. — Derogación. Derógase el Decreto N° 427/98.

Art. 46. — Comuníquese, publíquese, dése a la Dirección Nacional del Registro Oficial y archívese. — DUHALDE. — Alfredo N. Atanasof. — Juan J. Alvarez.

GLOSARIO

1.- Firma Electrónica: Se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizados por el signatario como su medio de identificación, que carezca de algunos de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez (artículo 5°, Ley N° 25.506).

2.- Firma digital: Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital, posterior a su firma.

Los procedimientos de firma y verificación a ser utilizados para tales fines serán los determinados por la Autoridad de Aplicación en consonancia con estándares tecnológicos internacionales vigentes (artículo 2°, Ley N° 25.506).

3.- Documento Digital o Electrónico: Se entiende por documento digital a la representación digital de actos o hechos, con independencia del soporte: utilizado para su fijación, almacenamiento archivo. Un documento digital también satisface el requerimiento de escritura (artículo 6°, Ley N° 25.506).

4.- Certificado Digital: Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular (artículo 13, Ley N° 25.506).

5.- Certificador Licenciado: Se entiende por certificador licenciado a toda persona de existencia ideal, registro público de contratos u organismo público que expide certificados, presta otros servicios en relación con la firma digital y cuenta con una licencia para ello, otorgada por el ente licenciante.

La actividad de los certificadores licenciados no pertenecientes al sector público se prestará en régimen de competencia. El arancel de los servicios prestados por los certificadores licenciados será establecido libremente por éstos (artículo 17, Ley N° 25.506).

6.- Política de Certificación: Conjunto de criterios que indican la aplicabilidad de un certificado a un grupo de usuarios en particular o a un conjunto de aplicaciones con similares requerimientos de seguridad. En inglés Certification Policy (CP).

7.- Manual de Procedimientos: Conjunto de prácticas utilizadas por el certificador licenciado en la remisión y administración de los certificados. En inglés Certification Practice Statement (CPS).

8.- Plan de Seguridad: Conjunto de políticas, prácticas y procedimientos destinados a la protección; de los recursos del certificador licenciado.

9.- Plan de Cese de Actividades: conjunto de actividades a desarrollar por el certificador licenciado en caso de finalizar la prestación de sus servicios.

10.- Plan de Contingencias: Conjunto de procedimientos a seguir por el certificador licenciado ante situaciones de ocurrencia no previstas que comprometan la continuidad de sus operaciones.

11.- Lista de certificados revocados: Lista de certificados que han sido dejados sin efecto en forma permanente por el Certificador Licenciado, la cual ha sido firmada digitalmente y publicada por el mismo. En inglés Certificate Revocation List (CRL).

12.- Certificación digital de fecha y hora: Indicación de la fecha y hora cierta, asignada a un documento o registro electrónico por una tercera parte confiable y firmada digitalmente por ella.

13.- Terceras partes confiables: Entidades independientes que otorgan seguridad y confiabilidad al manejo de la información.

14.- Proveedor de servicios de certificación digital: Entidad que provee el servicio de emisión y administración de certificados digitales.

15.- Homologación de dispositivos de creación y verificación de firmas digitales: Proceso de comprobación efectuado para establecer la adecuación de los dispositivos a requerimientos mínimos establecidos.

16.- Certificación de sistemas que utilizan firma digital: Proceso de comprobación efectuado para establecer la adecuación de un sistema o aplicación a requerimientos mínimos establecidos.

17.- Suscriptor o Titular de certificado digital: Persona a cuyo nombre se emite un certificado y posee una clave privada que se corresponde con la clave pública contenida en el mismo.

A N E X O 8

**L e y 5 2 7 d e C o l o m b i a y
L e y d e F i r m a y
C e t i f i c a d o s D i g i t a l e s
d e l P e r ú**

Ley de Firmas y Certificados Digitales del Perú

LEY NO. 27269

EL PRESIDENTE DE LA REPUBLICA

POR CUANTO:

El Congreso de la República ha dado la Ley siguiente:

EL CONGRESO DE LA REPÚBLICA;

Ha dado la Ley siguiente

LEY DE FIRMAS Y CERTIFICADOS DIGITALES

Artículo 1.- Objeto de la ley

La presente ley tiene por objeto regular la utilización de la firma electrónica otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad.

Entiéndase por firma electrónica a cualquier símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención precisa de vincularse o autenticar un documento cumpliendo todas o algunas de las funciones características de la firma manuscrita.

Artículo 2.-Ambito de aplicación

La presente ley se aplica a aquellas firmas electrónicas que, puestas sobre un mensaje de datos o añadidas o asociadas lógicamente a los mismos, puedan vincular e identificar al firmante, así como garantizar la autenticación e integridad de los documentos electrónicos.

DE LA FIRMA DIGITAL

Artículo 3. Firma digital

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

DEL TITULAR DE LA FIRMA DIGITAL

Artículo 4.- Titular de la firma digital

El titular de la firma digitales la persona a la que se le atribuye de manera exclusiva un certificado digital que contiene una firma digital, identificándolo objetivamente en relación con el mensaje de datos.

Artículo 5.- Obligaciones del titular de la firma digital

El titular de la firma digital tiene la obligación de brindar a las entidades de certificación ya los terceros con quienes se relacione a través de la utilización de la firma digital, declaraciones o manifestaciones materiales exactas y completas.

DE LOS CERTIFICADOS DIGITALES

Artículo 6.- Certificado digital

El certificado digital es el documento electrónico generado y firmado digitalmente por una entidad de certificación, la cual vincula una parte claves con una persona determinada confirmando su identidad.

Artículo 7. Contenido del certificado digital

Los certificados digitales emitidos por las entidades de certificación deben contener al menos:

1. Datos que identifiquen indubitablemente al suscriptor.
2. Datos que identifiquen a la Entidad de Certificación.
3. La clave pública.
4. La metodología para verificar la firma digital del suscriptor impuesta a un mensaje de datos.
5. Número de serie del certificado.
6. Vigencia del certificado.
7. Firma digital de la Entidad de Certificación

Artículo 8.- Confidencialidad de la información

La entidad de registro recabará los datos personales del solicitante de la firma digital directamente de éste y para los fines señalados en la presente ley.

Asimismo la información relativa a las claves privadas y datos que no sean materia de certificación se mantiene bajo la reserva correspondiente. Sólo puede ser levantada por orden judicial o pedido expreso del suscriptor de la firma digital.

Artículo 9. Cancelación del certificado digital

La cancelación del certificado digital puede darse:

1. A solicitud del titular de la firma digital,
2. Por revocatoria de la entidad certificante o
3. Por expiración del plazo de vigencia
4. Por cese de operaciones de la Entidad de Certificación.

Artículo 10.- Revocación del certificado digital

La Entidad de Certificación revocará el certificado digital en los siguientes casos:

1. Se determine que la información contenida en el certificado digital sea inexacta o haya sido modificada.
2. Por muerte del titular de la firma digital.
3. Por incumplimiento derivado de la relación contractual con la Entidad de certificación.

Artículo 11.-Reconocimiento del certificados emitidos por entidades extranjeras

Los Certificados de Firmas Digitales emitidos por entidades extranjeras tendrán la misma validez y eficacia jurídica reconocida en la presente ley, siempre y cuando tales certificados sean reconocidos por una entidad de certificación nacional que garantice, en la misma forma que lo hace con sus propios certificados, el cumplimiento de los requisitos, del procedimiento, así como la validez y la vigencia del certificado.

DE LAS ENTIDADES DE CERTIFICACIÓN Y DE REGISTRO

Artículo 12.- Entidad de Certificación

La Entidad de Certificación cumple con la función de emitir o cancelar certificados digitales, así como brindar otros servicios inherentes al propio certificado o aquellos que brinden seguridad al sistema de certificados en particular o del comercio electrónico en general.

Artículo 13.- Entidad de Registro o Verificación

La Entidad de Registro o Verificación cumple con la función de levantamiento de datos y comprobación de la información de un solicitante de certificado digital; identificación y autenticación del suscriptor de firma digital; aceptación y autorización de solicitudes de emisión de certificados digitales; aceptación y autorización de las solicitudes de cancelación de certificados digitales.

Artículo 14- Depósito de los Certificados Digitales

Cada Entidad de Certificación debe contar con un Registro disponible en forma permanente, que servirá para constatar la clave pública de determinado certificado y no podrá ser usado para fines distintos a los estipulados en la presente ley.

El Registro contará con una sección referida a los certificados digitales que hayan sido emitidos y figurarán las circunstancias que afecten la cancelación o vigencia de los mismos, debiendo constar la fecha y hora de inicio y fecha y hora de finalización.

A dicho Registro podrá accederse por medios telemáticos y su contenido estará a disposición de las personas que lo soliciten.

Artículo 15. Inscripción de Entidades de Certificación y de Registro o Verificación

El Poder Ejecutivo, por Decreto Supremo, determinará la autoridad administrativa competente y señalará sus funciones y facultades.

La autoridad competente se encargará del Registro de Entidades de Certificación y Entidades de Registro o Verificación, las mismas que deberán cumplir con los estándares técnicos internacionales.

Los datos que contendrá el referido Registro deben cumplir principalmente con la función de identificar a las Entidades de Certificación y Entidades de Registro o Verificación.

Artículo 16. Reglamentación

DISPOSICIONES COMPLEMENTARIAS, TRANSITORIAS Y FINALES

PRIMERA.- Mientras se cree el Registro señalado en el Artículo 150, la validez de los actos celebrados por Entidades de Certificación y Entidades de Registro o Verificación, en el ámbito de la presente ley, está condicionada a la inscripción respectiva dentro de los 45 (cuarenta y cinco) días siguientes a la creación el referido Registro.

SEGUNDA.- El Reglamento de la presente ley incluirá un glosario de términos referidos a esta ley y a las firmas electrónicas en general, observando las definiciones establecidas por los organismos internacionales de los que el Perú es parte.

TERCERA.- La autoridad competente podrá aprobar la utilización de otras tecnologías de firmas electrónicas siempre que cumplan con los requisitos establecidos en la presente ley, debiendo establecer el Reglamento las disposiciones que sean necesarias para su adecuación.

Comuníquese al señor Presidente de la República para su promulgación.

En Lima, a los ocho días del mes de mayo del dos mil.

MARTHA HILDEBRANDT PÉREZ TRE VINO
Presidenta del Congreso de la República

RICARDO MARCENARO FRERS
Primer Vicepresidente del Congreso de la República

AL SEÑOR PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA

POR TANTO:

Mando se publique y cumpla.

Dado en la Casa de Gobierno, en Lima, a los veintiséis días del mes de mayo del año dos mil.

ALBERTO FUJIMORI FUJIMORI
Presidente Constitucional de la República

ALBERTO BUSTAMANTE BELAUNDE
Presidente del Consejo de Ministros y
Ministro de Justicia

A N E X O 9

**L e y d e F i r m a D i g i t a l
y C e r t i f i c a d o s
D i g i t a l e s d e C o s t a
R i c a**

LA ASAMBLEA LEGISLATIVA DE LA REPUBLICA DE COSTA RICA

DECRETA:

LEY DE FIRMA DIGITAL Y CERTIFICADOS DIGITALES

TÍTULO I PRINCIPIOS Y NORMAS GENERALES

CAPÍTULO PRIMERO DISPOSICIONES GENERALES

ARTÍCULO 1.- La presente Ley tiene por objetivo regular el uso y el reconocimiento jurídico de la Firma Digital, otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad, así como el autorizar al Estado para su utilización.

ARTÍCULO 2.- Para los propósitos de la presente Ley se establecen las siguientes definiciones:

1.- **Acreditación:** La acreditación es el procedimiento mediante el cual un organismo autorizado reconoce formalmente que una entidad o empresa es competente para realizar tareas específicas.

2.- **Acreditación voluntaria del prestador de servicios de certificación:** Resolución que establece los derechos y obligaciones específicos para la prestación de servicios de certificación y que se emite, a petición del interesado, por el Órgano Rector y la Autoridad Competente de acreditación, de conformidad con lo previsto en esta Ley, su reglamento y la normativa intencional aplicable.

3.- **Certificado Digital:** Es la certificación digital que vincula unos datos de verificación de firma a un signatario y confirma su identidad.

4.- **Certificado Digital Reconocido:** Es el certificado que cumple con los requisitos establecidos en la presente Ley y su reglamento, y que vincula un documento digital con determinada persona como su signatario, mediante un proceso seguro de certificación y es expedido por un prestador de servicios de certificación acreditado por el Órgano Rector y la autoridad competente de acreditación.

5.- Datos de creación de firma: Son los datos únicos, como códigos o claves criptográficas privadas, que el signatario utiliza para crear la Firma Digital.

6.- Datos de verificación de firma: Son los datos como códigos o claves criptográficas públicas, que se utilizan para verificar la Firma Digital.

7.- Dispositivo de creación de firma: Es un mecanismo que sirve para aplicar los datos de creación de firma.

8.- Dispositivo de verificación de firma: Es un mecanismo que sirve para aplicar los datos de verificación de firma.

9.- Dispositivo seguro de creación de firma: Es el mecanismo de creación de firma que cumple adicionalmente con los requisitos establecidos en la presente Ley y su reglamento.

10.- Documento: Significa información que se encuentra almacenada en un medio tangible, o que se guarda en un medio electrónico o de cualquier otra naturaleza, y que se puede recuperar o reproducir en una forma perceptible e inteligible.

11.- Firma Digital: Es el conjunto de datos, anexos a otros datos o datos asociados funcionalmente, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge.

12.- Firma Digital Avanzada: Es la Firma Digital Certificada por un prestador de servicios de certificación debidamente acreditado ante la autoridad competente de acreditación.

13.- Información: Es aquel mensaje comunicado mediante datos, textos, imágenes, sonidos, códigos, programas, información almacenada en bases de datos, aplicaciones, o similares.

14.- Iniciador: Es quien envía un mensaje de datos, esté o no suscrito digitalmente.

15.- Información Íntegra: Se entenderá por íntegra aquella información que haya permanecido completa e inalterada, sin menoscabo de cualquier adición o cambio, inherente al proceso de comunicación, almacenamiento, archivo o presentación. El grado de fiabilidad requerido será determinado a la luz de los fines para los que se generó la información y de todas las circunstancias del caso.

16.- Intermediario: Es aquella persona, física o jurídica, que actuando por cuenta de otra, envíe, reciba, almacene dicho mensaje o preste algún otro servicio con respecto a él.

17.- Mensaje de datos: Es la información generada, enviada, recibida, almacenada, o comunicada por medios digitales, electrónicos, ópticos o similares.

18.- Prestador de servicios de certificación o entidad certificadora: Es la persona física o jurídica que expide certificados.

19.- Procedimiento seguro: Es el procedimiento empleado con el propósito de verificar que una Firma Digital es atribuible a determinada persona como su signatario, o para detectar cambios y errores en un documento digital, incluyendo cualquier proceso que implique el uso de algoritmos matemáticos, códigos, sistemas de encriptamiento, y cualquier otro medio o tecnología de identificación o reconocimiento.

20.- Producto de Firma Digital: Es el instrumento y sus componentes específicos, destinados a la prestación de servicios de Firma Digital por el prestador de servicios de certificación o para la creación o verificación de Firma Digital.

21.- Receptor: Es la persona a quien el signatario dirige el mensaje o documento electrónico.

22.- Signatario: Es la persona física o jurídica que cuenta con un mecanismo de creación de firma, que actúa en nombre propio o con poderes de representación de otra persona física o jurídica.

23.- Sistema: Es el conjunto de elementos independientes pero interrelacionados entre sí para conseguir un propósito común.

24.- Sistema de información: Es un conjunto de elementos ordenado utilizado para generar, enviar, recibir, almacenar o procesar de alguna forma mensajes de datos.

ARTÍCULO 3.- En la presente Ley se utilizará el término digital entendido como cualquier información codificada en dígitos, la cual resulta más precisa que el término electrónico, que se refiere al medio físico de procesamiento, almacenamiento o transmisión, el cual es uno de los medios para generar, transmitir y almacenar información digital.

CAPÍTULO II RECONOCIMIENTO JURÍDICO DE LA FIRMA DIGITAL

ARTÍCULO 4.- La Firma Digital Avanzada, deberá crearse mediante un dispositivo seguro de creación de firma.

ARTÍCULO 5.- La Firma Digital Avanzada, siempre que esté basada en un certificado digital reconocido y que haya sido producida por un dispositivo seguro de creación de firma, tendrá respecto de los datos consignados en forma digital, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel. Cuando la ley exija la presentación o existencia de un documento escrito debidamente firmado, tal requisito será plenamente satisfecho por un documento digital, si el mismo ha sido firmado mediante una Firma Digital Avanzada, creada por un dispositivo seguro de creación de firma. Se presumirá que la Firma Digital Avanzada y el medio de creación de firma con el que ésta se produzca, reúnen las condiciones necesarias para producir los efectos indicados en este apartado cuando el certificado reconocido es emitido por un prestador de servicios de certificación acreditado.

ARTÍCULO 6.- Cuando una ley requiere que un documento o firma esté certificado o autenticado notarialmente por un abogado, o de cualquier otra forma reconocido, verificado o certificado, tal requisito se tendrá por cumplido si una firma electrónica avanzada de un notario público, abogado, funcionario público, o cualquier otra persona autorizada y competente para efectuar tales actos, es puesta o vinculada al documento o firma digital o Firma Digital avanzada.

CAPÍTULO III USO DE LA FIRMA DIGITAL Y LOS DOCUMENTOS ELECTRÓNICOS POR EL ESTADO

ARTÍCULO 7.- Se autoriza a los Poderes Legislativo, Ejecutivo y Judicial, al Tribunal Supremo de Elecciones, Contraloría General de la República, Defensoría de los Habitantes, así como a todas las instituciones públicas descentralizadas, y entes públicos no estatales para la utilización de la Firma Digital avanzada y los documentos electrónicos firmados digitalmente en sus relaciones internas, entre ellos y con los particulares, de conformidad con las previsiones de esta Ley y su reglamento.

TÍTULO II DE LOS SERVICIOS DE CERTIFICACIÓN DIGITAL

CAPÍTULO I DEL ÓRGANO RECTOR

ARTÍCULO 8.- El Ministerio de Ciencia y Tecnología será el Órgano Rector en todo lo concerniente a esta Ley.

8.1 Toda interpretación técnica estará bajo el mejor criterio del Órgano Rector tomando en cuenta el estado de arte en la tecnología, así como los requerimientos y realidades del país.

ARTÍCULO 9.- El Poder Ejecutivo, a través del Ministerio de Ciencia y Tecnología, utilizará un sistema de acreditación voluntario, en el ámbito de los prestadores de servicios de certificación de Firma Digital Avanzada, coordinando para ello con la Autoridad de Acreditación, la cual será un ente con participación activa y equilibrada de los sectores involucrados. La autoridad de acreditación mediante la función de acreditación, reconoce formalmente que una organización es competente para llevar a cabo tareas específicas de acuerdo a los requisitos de normas nacionales e internacionales, que permitan lograr un adecuado grado de seguridad y confianza que proteja debidamente, los derechos de los usuarios, para lo cual deberá llevar a cabo el proceso de evaluación correspondiente, un registro de las entidades acreditadas y velar por que se cumplan los requisitos establecidos por esta Ley y su reglamento.

CAPÍTULO II CERTIFICADOS DIGITALES

ARTÍCULO 10.- Los certificados digitales se vinculan con una persona confirmando su identidad, los cuales deberán contener al menos:

- 1.- Los datos que identifiquen individualmente al firmante.
- 2.- Los datos que identifiquen a la entidad de certificación.
- 3.- Número de serie del certificado.
- 4.- Fecha de emisión y plazo de vigencia.
- 5.- Los demás que el reglamento establezca.

ARTÍCULO 11.- Los certificados digitales se podrán cancelar y revocar en los siguientes casos:

- 1.- A solicitud del titular de la firma.
- 2.- Por expiración del plazo.
- 3.- Por cese de operaciones de la entidad de certificación.
- 4.- Por muerte del titular de la Firma Digital.
- 5.- Por incumplimiento contractual con la entidad de certificación.
- 6.- Las demás que el reglamento establezca.

ARTÍCULO 12.- Los certificados de Firma Digital que sean emitidos por entidades no establecidas en Costa Rica, serán equivalentes a los otorgados por prestadores establecidos en el país, cuando hayan sido homologados por estos últimos, bajo su responsabilidad, y reconocidos por la autoridad de acreditación competente y cumpliendo con los requisitos fijados en esta Ley, su reglamento y normas internacionales correspondientes.

CAPÍTULO III DE LA ACREDITACIÓN E INSPECCIÓN DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN DIGITAL

ARTÍCULO 13.- Mediante la autoridad competente de acreditación, la cual estará adscrita al Ministerio Rector, las empresas que emitan certificados de Firma Digital, deberán someterse al proceso de acreditación que se defina al respecto para estar debidamente acreditados. Las funciones de las empresas certificadoras serán entre otras las de emitir o cancelar certificados digitales, así como brindar otros servicios inherentes al propio certificado.

ARTÍCULO 14.- Con el fin de comprobar el cumplimiento de las obligaciones de los prestadores acreditados, la Autoridad de Acreditación ejercerá la facultad de inspección sobre los prestadores acreditados y podrá, a tal efecto, requerir información, ordenar evaluaciones anunciadas o no anunciadas a sus instalaciones al menos una vez al año y solicitar las modificaciones necesarias para que se mantenga actualizado el sistema y el servicio, con personal que para tal efecto se seleccione de conformidad al reglamento, la Autoridad de Acreditación y del Órgano Rector. Así como suspender las acreditaciones en caso de incumplimiento.

ARTÍCULO 15.- La Autoridad de Acreditación así como el personal que actúe bajo su dependencia o por cuenta de ella, deberá guardar la confidencialidad y

custodia de los documentos y la información que le entreguen las empresas certificadoras.

ARTÍCULO 16.- El Órgano Rector deberá observar en sus actuaciones y regulaciones total neutralidad respecto de las diversas tecnologías de Firma Digital existentes, procurando la mayor adaptabilidad a los avances científicos y tecnológicos en tal área.

TÍTULO III LOS DISPOSITIVOS DE FIRMA DIGITAL AVANZADA Y LA EVALUACIÓN DE SU CONFORMIDAD CON LA NORMATIVA APLICABLE

CAPÍTULO ÚNICO

ARTÍCULO 17.- Los dispositivos seguros de creación de Firma Digital para considerarse como tales deberán cumplir con:

- 1.- Garantizar que los datos utilizados para la generación de firma puedan producirse sólo una vez y asegurar, razonablemente, su secreto, dentro de las posibilidades o limitaciones tecnológicas.
- 2.- Que exista seguridad razonable de que dichos datos no puedan ser alterados o falsificados con la tecnología existente en un momento dado.
- 3.- Que los datos de creación de firma puedan ser protegidos con fiabilidad por el signatario contra la utilización por otros.
- 4.- Que el dispositivo utilizado no altere los datos o el documento que deba firmarse, ni impida que éste se muestre al signatario antes del proceso de firma.

ARTÍCULO 18.- Los dispositivos de verificación de Firma Digital Avanzada deben garantizar al menos lo siguiente:

- 1.- Que la firma se verifique de forma fiable y el resultado de la verificación figure correctamente.
- 2.- Que el verificador pueda, en caso necesario, establecer de forma fiable la integridad de los datos firmados y detectar si han sido modificados.
- 3.- Que aparezca correctamente la identidad del signatario.
- 4.- Que se verifique de forma fiable el certificado.

5.- Que pueda detectarse cualquier cambio relativo a su seguridad e integridad.

ARTÍCULO 19.- Las disposiciones de esta Ley no deberán entenderse en el sentido de prohibir la existencia de sistemas de Firma Digital basados en convenios expresos entre las partes, las que podrán a través de un contrato fijar sus derechos y obligaciones, y las condiciones técnicas y de cualquier otra clase, bajo las cuales reconocerán su autoría sobre un documento digital o mensaje de datos que envíen, o la recepción de un mensaje de datos de su contraparte.

TÍTULO IV DISPOSICIONES FINALES

ARTÍCULO 20.- El Poder Ejecutivo deberá emitir el reglamento a la presente Ley dentro del plazo máximo de tres meses siguientes a su publicación.

Rige a partir de su publicación.

A N E X O 10

**A n t e p r o y e c t o d e L e y
d e C o m e r c i o
E l e c t r ó n i c o d e E l
S a l v a d o r (M i n i s t e r i o
d e E c o n o m í a)**



DECRETO No. _____

LA ASAMBLEA LEGISLATIVA DE LA REPUBLICA DE EL SALVADOR,

CONSIDERANDO:

I.- Que 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 transformándola a pasos acelerados, abriendo nuevas alternativas de acceso a la información, la cultura, el comercio y el entretenimiento, marcando estándares más exigentes, cualitativamente y cuantitativamente, en cada uno de estos campos. Siendo este fenómeno una tendencia mundial;

II.- Que nuestra sociedad esta siendo objeto de estas transformaciones tecnológicas y avances informáticos, a través de lo que conocemos como Internet; que es un medio 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 económico. Es decir, en una herramienta útil para el ejercicio de múltiples actividades financieras, administrativas, y educativas;

III.- Que en el caso de las transacciones comerciales, esta red informática es una plataforma ideal. Lo que abre las puertas a nuevas oportunidades para el desarrollo económico mas eficientemente tanto del comercio de sus productos o servicios en el mercado local como regional e internacional, así como la creación de nuevas fuentes de empleo, de la cual pueden beneficiarse las empresas y el comercio en general;

IV.- Que al no haber regularización en dicha materia se crea incertidumbre, obstaculizando el desarrollo de nuevos productos y servicios, y disuadiendo la inversión, pues, las normas vigentes no contemplaron esta nueva realidad, de ahí que se haga necesario su regulación, adecuándola a sus características propias dinamizándola y modernizándola a fin de adaptarla a los mercados internacionales cada vez mas globalizados;

V.- Que 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 esta red informática, así como el uso de medios innovadores que busquen dar celeridad a distintos tipos de



transacciones comerciales, que le permitirán a las organizaciones de nuestro país, aumentar su productividad, competitividad y al mismo tiempo reducir sus tiempos y costos;

VI.- Que es indispensable una ley que establezca reglas claras que faciliten el desarrollo del comercio electrónico en nuestro país, brindando la confianza necesaria a todos los actores participantes de esta nueva forma de hacer comercio, estableciendo garantías claras que den seguridad a los usuarios y dinamizar nuestro tejido empresarial; y

VII.- Que el artículo 101 de la Constitución manda al Estado a promover el desarrollo económico y tecnológico en aras del beneficio social.

POR TANTO,

En uso de sus facultades constitucionales y a iniciativa del Presidente de la República, por medio del Ministro de Economía,

DECRETA la siguiente:

LEY DE COMERCIO ELECTRÓNICO

CAPITULO I DISPOSICIONES GENERALES

Art. 1 Objeto de la Ley

La presente ley tiene por objeto normar la utilización de mensajes de datos y comunicaciones electrónicas, cualquiera sea la forma utilizada, en el contexto de actividades comerciales en el ámbito nacional e internacional, de tal manera que ellas puedan ser acreditadas válidamente, mediante procedimientos de seguridad electrónicos ya existentes y que a su vez permitan dar claridad, seguridad, autoría y autenticidad de las mismas.

Art. 2 Ambito de Aplicación

La presente Ley será aplicable a todo tipo de comunicación o información transmitida en forma de mensaje de datos, salvo en los siguientes casos y materias:

1. Derecho sucesoral
2. Derecho de familia



3. 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.
4. 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.
5. 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 Digital

Es la certificación electrónica que vincula unos datos de verificación de firma a un iniciador y confirma su identidad vinculándola con su firma electrónica;

Clave Publica

Es aquella que se utiliza para verificar una firma digital;

Clave privada

Es aquella que se utiliza para firmar digitalmente, mediante un dispositivo de creación de firma digital, en un sistema seguro;

Comercio Electrónico

Toda acción comercial, financiera, tributaria o cualquier tipo de transacción, que se efectúe a través del intercambio de mensajes de datos o medios similares;

Contratos Informáticos

Es 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 o jurídica que en las comunicaciones electrónicas contempladas en esta Ley actúa circunstancial y no permanentemente en esta modalidad comercial;



Comunicación

Cualquier mensaje de datos conteniendo información;

Criptografía

Es la codificación 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 devuelta a su forma original y legible;

Destinatario de un mensaje de datos

Es la persona designada por el iniciador para recibir el mensaje, siempre y cuando no esté actuando como intermediario de este;

Documento Electrónico

Es el que está dado en formato electrónico conteniendo información electrónica que se almacena, envía, comunica, recibe, archive o genere por cualquier medio electrónico;

Medio electrónico

Es todo medio que utilice tecnología eléctrica, digital, magnética, inalámbrica, alámbrica, óptica, electromagnética o alguna otra similar conocida para enviar o recibir información;

Entidad Reguladora

Es aquella entidad pública que se encarga de supervisar las actividades de las entidades de certificación;

Entidad de Certificación

Es aquella persona o entidad que legalmente está facultada para emitir certificados digitales, con el objeto de dar certeza sobre la identidad y firmas electrónicas 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 electrónicas;

Firma Electrónica

Es cualquier medio, método, símbolo o proceso electrónico que sustituye la firma manuscrita y se adhiere o se asocia lógicamente con un mensaje de datos aceptado y aprobado por una persona dándolo por auténtico, impidiendo que el signatario pretenda desconocer la autoría de la misma posteriormente;



Información

Son los datos, textos, imágenes, sonidos, códigos, programas computacionales, operaciones informáticas, bases de datos, voz o similares;

Iniciador de un mensaje de datos

Es toda persona que, a tenor del mensaje, haya actuado por su voluntad para enviarlo o generarlo, siempre y cuando no haya actuado a título de intermediario.

Intercambio Electrónico de Datos

Es la transmisión electrónica de datos de una computadora a otra, estando estructurada la información conforme alguna norma técnica convenida por las partes al efecto;

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 al representado;

Mensaje de Datos

Es toda información generada, enviada, recibida, almacenada o comunicada, e intercambiada por métodos o medios de comunicación electrónicos, ópticos o cualquier otra tecnología conocida, tales como el intercambio electrónico de datos, los sitios de Internet, el correo electrónico, el telegrama y fax.

Persona

Es toda persona natural o jurídica de carácter público o privado susceptibles de contraer derechos y obligaciones, conforme a la ley;

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 oneroso a distancia por medio de la vía electrónica a petición del destinatario;

Procedimiento de Seguridad

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 no concensuados o errores en un documento electrónico. Se incluye también 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 criptografico asimétrico seguro

Es un método que utiliza un par de claves en donde una es privada, que se utiliza a su vez para firmar digitalmente su correspondiente clave pública, verificando así la firma digital, de forma tal, que con las longitudes de claves utilizadas, sea computacionalmente imposible obtener, inferir o descifrar la clave privada a partir de la correspondiente clave pública;

Sistema de Información

Es cualquier medio informatizado o 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 de forma total o parcialmente, y en la cual, los actos de al menos una de las partes no son revisados por nadie al momento de pactar o realizar el contrato;

Art. 4 Principios.

En la interpretación y aplicación de la presente Ley habrán de tenerse en cuenta los siguientes principios:

- a) El de validez y factibilidad de las transacciones por medio de mensajes de datos;
- b) El de promover la confianza del público en la validez, integridad, claridad y confiabilidad de los mensajes de datos y las firmas contenidas en ellos.
- c) El de su carácter internacional.
- d) El de la promoción de la uniformidad de su aplicación;
- e) El de la buena fe de las partes;
- f) El de libre contratación;
- g) El de armonización con las prácticas comunes y razonables en esta área;
- h) El desarrollo prioritario de los aspectos técnicos y las nuevas tecnologías;
- i) El de desmaterializar el sistema de soporte papel;
- j) Los que faciliten el archivo electrónico con autoridades locales y agencias gubernamentales promoviendo un eficiente sistema de servicios gubernamentales; y
- k) Otros, que aseguren la agilidad, certeza y legalidad de las comunicaciones que sean objeto de la presente Ley.

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 de la legislación vigente.



Art. 5 Autonomía de las Partes

Las partes tendrán la libertad en sus relaciones contractuales de establecer el alcance de sus derechos y obligaciones permitidas por la ley, no se podrá 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, no esta obligado a realizar futuras transacciones por esos medios. La parte que se opone a realizar futuras transacciones por estos medios debe dar aviso a las partes que pudiesen ser afectadas, debiendo establecer un nuevo acuerdo entre ellas. Este aviso deberá comunicarse por cualquier medio de comunicación con acuse de recibo.

La presente Ley habilita el empleo de la firma electrónica dentro del principio de libertad de contratación.

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, siempre que no atente contra la moral y las buenas costumbres; el acuerdo debe ser expreso. En caso de controversias se someterán a la jurisdicción estipulada en el contrato, a lo establecido en las leyes vigentes o a las normas de arbitraje y mediación si las hubiere. La selección de un foro, no implica la selección de la ley aplicable. ? quizas por 330

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.

Los contratos deberán contener una cláusula compromisoria, que indique la forma en que se van a resolver los conflictos en caso de controversia.

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.

Tendrán efectos jurídicos, validez y fuerza obligatoria la información que aunque no esté contenida en el mensaje de datos o en una firma electrónica se supone ha de dar lugar a estos efectos, siempre y cuando figure en el mensaje de datos en forma de remisión.

CAPITULO II

DE LA APLICACIÓN E INTEGRACIÓN DE LAS REGLAS CONCERNIENTES A LOS MENSAJES DE DATOS CON OTRAS NORMAS.

Art. 8 Reconocimiento y Consecuencias Jurídicas de los Mensajes de Datos

Un mensaje de datos tendrá efecto, validez y fuerza obligatoria como cualquier otro acto o contrato en forma material.

Los documentos que resulten de la transmisión a distancia vía líneas telefónicas o similares que emanen de un facsimil receptor tendrán legalmente el mismo valor que el documento 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 Información escrita

Cuando alguna disposición legal requiera que una información deba constar por escrito y estar formada materialmente, o bien establezca la existencia de consecuencias jurídicas por falta de elaboración de esa forma, se entenderá que un mensaje de datos cumple con el requisito de escrituralidad 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 tal cual es desde el momento en



que fue generada, salvo los cambios que sean hallados como consecuencia del archivo, recuperación y 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 que el mismo no pueda ser recuperado posteriormente por cualquier medio técnico.

Lo dispuesto en el presente artículo no será aplicable respecto a las exclusiones previstas en el 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 cuando se den las siguientes circunstancias:

- a) Que exista alguna garantía confiable de que la información generada o comunicada con un mensaje de datos ha sido dada por medios electrónicos, ópticos o de cualquier otra tecnología.
- b) Que la información generada se ha mantenido íntegra e inalterada a partir del momento en que se generó por primera vez, al margen de los cambios que se den en forma de endoso o cambio normal de la comunicación, así mismo como el archivo o presentación y que permanece accesible para su ulterior consulta.
- c) Que se requiera 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 como original cuando toda aquella información consignada en un mensaje de datos es íntegra, es decir que 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 mismo.

Art. 11 Firma de Documentos

Cuando la ley exija la existencia de una firma manuscrita en un documento en forma material, se entenderá satisfecho dicho requerimiento en relación con un mensaje de datos, cuando:



- a) Se ha utilizado un método que permita identificar al iniciador de ese mensaje de datos e indicar que el contenido es de su conocimiento y consecuentemente de su aprobación.
- b) Que el método informático utilizado sea tanto confiable como apropiado de acuerdo al propósito para el cual el mensaje fue generado o comunicado, o el mensaje de datos ha sido firmado con una firma electrónica de acuerdo a los requisitos dispuestos en la presente Ley.
- c)

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 por la presente Ley.

Este medio y fuerza probatoria que da admisión a un mensaje de datos prevalecerá sobre cualquier otro que lo contrarie sin perjuicio de cualquier otra forma de prueba establecida en nuestra legislación común.

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:

- a) La confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje de datos;
- b) La confiabilidad en la forma en que se haya conservado la integridad de la información;
- c) La forma confiable con la cual se identifique al iniciador;
- d) El tipo de procedimientos que se hayan utilizado para mantener la seguridad; y
- e) Cualquier otro factor pertinente.

Para la valoración de las pruebas, el juez, arbitro o mediador que juzgue el caso deberá designar los peritos que considere necesarios pues en base a su conocimiento técnico e interpretación de las pruebas presentadas le servirán para su análisis y calificación.

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:

- a) Que el mensaje de datos este accesible para su posterior consulta;
- b) Que el mensaje de datos sea conservado en el formato en que se haya generado, enviado o recibido o en cualquier otro formato que permita garantizar y demostrar la integridad del mensaje de datos originalmente enviado;
- c) Que se conserve toda la información que permita determinar el origen, el destino del mensaje, la fecha y la hora en que fue enviado o recibido el mensaje o producido el documento.

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.

CAPITULO III COMUNICACIÓN DE LOS MENSAJES DE DATOS

Art. 15 Reconocimiento de los Mensajes de Datos entre las partes

Las relaciones entre el iniciador y el destinatario de un mensaje de datos, tendrán efectos jurídicos, validez y fuerza obligatoria, por mantener en el mismo una manifestación de voluntad u otra declaración.

Las normas contenidas en la presente Ley serán aplicables a las personas que han acordado expresa o tácitamente, utilizar mensajes de datos para comunicarse. Cuando no sea expreso el acuerdo de las partes respecto del reconocimiento de los mensajes, se presumirá haberlo por el contexto, las circunstancias y de acuerdo a los principios contenidos en el art. 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 en cualquiera de las siguientes circunstancias:

- a) Por el iniciador mismo;
- b) Por alguna persona facultada para actuar en nombre del iniciador respecto de ese mensaje;
- c) Por mandatario o representante legal con suficiente representación para ello; y
- d) Por un sistema de información programado por el iniciador o en su nombre para que opere automáticamente.

En el caso del mandatario o representante legal, se deberá relacionar clara y suficientemente en el mensaje de datos el poder que le otorga dicha calidad.

Art. 17 Presunción del Origen de un Mensaje de Datos

Se presume que un mensaje de datos ha sido enviado por el iniciador, cuando:

- 1) Éste haya aplicado en forma adecuada el procedimiento acordado con el destinatario, en el sentido de que el mensaje de datos provenía efectivamente del primero; y
- 2) El mensaje de datos que reciba el destinatario, resulte de los actos de algún mandatario del iniciador. y

La presunción contenida en este artículo no operará:

- 1) A partir del momento en que el destinatario haya sido informado por el iniciador que el mensaje de datos no proviene de él, disponiendo de un plazo razonable para actuar en consecuencia; y
- 2) En el caso del numeral dos del inciso anterior de este artículo, desde que el destinatario sepa, o que sabiéndolo hubiera actuado con la debida diligencia o que de haber aplicado algún método convenido hubiera sabido que el mensaje de datos no provenía del iniciador.

Art. 18 Concordancia del Mensaje de Datos Enviado con el Mensaje de Datos Recibido



Siempre que en base a las relaciones entre el iniciador y destinatario, 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 esta presunción, éste último tendrá derecho a considerar que el mensaje de datos recibido corresponde al que quería enviar su 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, aunque no se haya acordado entre éstos una forma o método determinado para efectuarlo, se podrá dar uno mediante:

- a) Toda comunicación del destinatario, sea por medio de agente electrónico o no; y
- b) 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 dé el acuse de recibo 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 tendrá por realizado, 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 o acordado, 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 por ellos o no se ha fijado o convenido ninguno, se entenderá por un plazo razonable por parte del iniciador cuando éste:

- a) Dé aviso al destinatario de que no ha recibido acuse de recibo, fijando uno nuevo en su caso para su recepción; y
- b) A pesar de la circunstancia regulada en el literal anterior sigue sin recibir el acuse de recibo requerido, éste podrá previo aviso de tal situación al destinatario, considerar que el mensaje de datos original no ha sido enviado o ejercer en su caso cualquier otro derecho que pueda tener.

Art. 23 Efectos Jurídicos del Acuse de Recibo

Las consecuencias jurídicas del contenido de un mensaje de datos se registrarán conforme al artículo 8 de la presente Ley.

La confirmación de la recepción de un mensaje, indicando que este ha cumplido con los requisitos técnicamente reconocidos o acordados, no implicará 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:

- A) Si el destinatario ha designado un sistema de información para la recepción del mensaje de datos, la recepción tendrá lugar:
 - 1. En el momento en que ingrese el mensaje de datos en el sistema de información designado; o cuando
 - 2. De enviarse el mensaje de datos a un sistema de información del destinatario que no sea el sistema de información designado, será en el momento en que el destinatario recupere el mensaje de datos;
- B) 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 aun cuando el sistema de información esté ubicado en lugar distinto de donde se tenga por recibido el mensaje de datos conforme a las reglas del artículo 26 de esta Ley.

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 electrónica el mensaje de datos se tendrá por expedido en el domicilio que conste en el certificado de firma electrónica del iniciador y por recibido en el que conste en el certificado de firma electrónica 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 forma material.

Las mismas reglas se aplicaran a la entrega por medios electrónicos o digitales de programas informáticos, música y videos digitalizados y cualquier otro 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 en la comunicación de un mensaje de datos, las partes 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 dicho procedimiento, la persona que si lo siguió tendrá derecho, a hacer valer el mensaje de datos en su forma inalterada o sin errores contra la parte que no lo siguió, salvo prueba en contrario.

CAPITULO 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.

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 forma material.



Art. 30 Condiciones Generales de Contratación

Cuando en una transacción electrónica, alguna de las partes se obligue bajo condiciones generales de contratación previamente establecidas, estas deben estar redactadas con claridad, concreción y sencillez y que se encuentren siempre disponibles a la hora de contratar.

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 castellano siempre y cuando este idioma haya sido uno de los de contratación originalmente acordados.

Art. 32 Agentes Electrónicos

Un contrato podrá darse por medio de un intercambio de mensajes de datos entre agentes electrónicos entre sí o con otro particular, aunque no se revisen las acciones del agente electrónico o el resultado de las mismas. Un contrato electrónico hecho por una persona y un agente electrónico de otra distinta no tendrá efectos legales y no será ejecutable en los siguientes casos:

- a) Cuando alguno de los contratantes cometió un error material en el documento y el agente electrónico no le dio oportunidad de corregirlo o prevenirlo; y
- b) Cuando un contratante notifica a la otra parte sobre el error tan pronto como sea posible, y este último no haga nada por corregir el error notificado.

Art. 33 Contratos de Adhesión

Es aquel cuyas cláusulas han sido establecidas por una de las partes, a través de contratos impresos o electrónicos o en formularios sin que la otra parte, para celebrarlo, haya discutido o participado sustancialmente su contenido.

En este tipo de contrato se estará a lo dispuesto conforme a la ley.



Art. 34 Tiempo de validez de la oferta

Cuando el ofertante no establezca un tiempo de validez para su oferta, esta tendrá un tiempo de validez de tres días, contados a partir de la notificación del acuse de recibo..

En el caso de que hubiere aceptación de la oferta, las obligaciones entre las partes se generarán de inmediato.

Art. 35 Nulidad de los contratos

Se consideraran nulos los contratos informáticos cuando estos adolezcan de alguna causa de nulidad o vicio regulado con la legislación vigente.

CAPITULO V

DE LAS FIRMAS ELECTRÓNICAS Y LOS SUSCRIPTORES DE LAS MISMAS

Art. 36 Reconocimiento y Efectos Jurídicos de una Firma Electrónica

Una firma electrónica, siempre y cuando reúna los requisitos determinados en esta Ley y la legislación vigente 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 electrónica para todos aquellos propósitos para los cuales la ley permite o requiere una firma manuscrita, salvo en los casos en que la firma manuscrita es obligatoria.

Cuando una firma electrónica 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 Electrónica

Se reconocerán las firmas electrónicas que incorporen los siguientes requisitos:

- a) Aquellas que garantizan la confidencialidad del mensaje de datos;
- b) Las que son susceptible de verificación en la autoría e identidad del emisor;
- c) Las que están bajo el control exclusivo de la persona que la usa, del mandatario o representante legal;



- d) Las que están ligadas a la información o mensaje de datos, de tal manera que si éstos son cambiados, la firma electrónica es invalidada;
- e) Las que ofrecen seguridad suficiente de que no pueda ser falsificada con la tecnología existente;
- f) Las que no alteran la integridad del mensaje; y
- g) Las que están conforme al Reglamento de esta Ley.

La firma electrónica, debidamente certificada por una Entidad de Certificación conforme a lo establecido en el capítulo VI de esta ley, se considerará que cumple con los requisitos señalados en este artículo.

Art. 38 Deberes y Responsabilidad de los Suscriptores de Firmas Electrónicas

Son deberes de los suscriptores de firmas electrónicas:

- a) Recibir la firma electrónica de la entidad de certificación o generarla utilizando un método autorizado por esta;
- b) Actuar con la debida diligencia y tomar las medidas de seguridad necesarias para mantener la firma electrónica bajo su estricto control y evitar toda utilización no autorizada de su firma;
- c) Suministrar la información que requiera la entidad de certificación;
- d) Solicitar oportunamente la revocación de los certificados conforme al Reglamento de esta Ley que al efecto se dictaren; y
- e) 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 se pruebe que el destinatario aún conociendo 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 electrónica

Mientras el certificado no sea revocado, suspendido o cancelado conforme al Reglamento de esta Ley, la firma electrónica, 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 electrónica 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. 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:

- a) Nombre, dirección y domicilio del suscriptor;
- b) Nombre, dirección y lugar donde realiza sus actividades la entidad de certificación;
- c) La clave pública del usuario, o cualquier otro método que se pudiese utilizar para identificar al suscriptor;
- d) La metodología para verificar la firma electrónica del suscriptor impresa en el mensaje de datos;
- e) El número de serie del certificado;
- f) Fecha de emisión y expiración del certificado;
- h) La limitación del valor hasta donde pueda utilizarse el certificado, así como la responsabilidad del titular de la entidad certificadora;
- i) En los casos de representación, la relación del poder que acredite al representante; y
- j) Cualquier otro requisito que se considere esencial según el Reglamento de la presente Ley.

Artículo 44 Obligaciones de las Entidades de Certificación

Son obligaciones de la Entidades de Certificación:

- a) Estar legalmente constituidas y registradas en el órgano de control correspondiente;
- b) Justificar su capacidad tecnológica de acuerdo al Reglamento de la presente Ley, que garantice 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) Que sus representantes legales y administradores no sean 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 y capacitado en la materia;



- i) Utilizar sistemas y productos confiables que estén protegidos de toda alteración, que garanticen 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, donde 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 electrónica 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, que garanticen la seguridad y confidencialidad durante el proceso de generación de dichas claves;
- n) Almacenar toda la información relativa a un Certificado para efectos de prueba en procedimientos judiciales. El almacenamiento podrá hacerse de forma electrónica;
- o) No almacenar ni copiar las claves privadas de firma electrónica de los usuarios a menos que éstos lo soliciten expresamente.
- p) Mantener informados 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;
- q) 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;
- r) 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 por las entidades administrativas competentes o judiciales en relación con las firmas electrónicas y certificados emitidos; y, en general sobre cualquier mensaje de datos que se encuentre bajo su custodia y administración;
- s) La Entidad de Certificación, 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;
- t) Elaborar los instructivos que definan las relaciones con el suscriptor y la forma de prestación del servicio;
- u) Mantener y publicar oportunamente en Internet un listado de fácil y rápido acceso de los certificados de firmas electrónicas suspendidas, canceladas o revocadas;



- v) Proporcionar a los titulares de certificados de firmas electrónicas un medio efectivo y rápido para dar aviso general que una firma electrónica tiene riesgo de uso indebido, en cuyo caso el titular deberá solicitar la suspensión del mismo;
- w) 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;
- x) Asegurar que el titular del certificado tuvo, en el momento de creación del mismo, el instrumento de generación y verificación de la firma en cuestión, identificados en el certificado.

Las entidades certificadoras están obligadas a aplicar la tecnología informática necesaria para mantener y actualizar los registros antes mencionados.

Artículo 45 Protección de Datos por parte de las Entidades de Certificación

Las Entidades de Certificación garantizarán el archivo de datos obtenidos en función de su trabajo y su buen uso y manejo, para lograr los siguientes propósitos:

- a) La reserva, privacidad, protección y confidencialidad de la información y datos que manejen;
- b) Obtener información únicamente con el consentimiento y voluntad de la persona relacionada con dicha información; y
- c) Otros requisitos establecidos en las leyes y reglamentos que regulen la materia.

Las Entidades de Certificación, recopilán 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 para fines distintos de la prestación de servicios de certificación, sin el consentimiento expreso del titular.

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 protección de datos personales.

Art. 46 Cese de actividades

La Entidad de Certificación cesa de tal calidad en los siguientes casos:

- a) Por decisión unilateral comunicada a la entidad reguladora;
- b) Por revocación de su personalidad jurídica o por cualquier otra causal legal de disolución;



- c) 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 consecutivos, la fecha y la hora de cese de actividades, la cual no puede ser anterior a los noventa 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.

CAPITULO VII DE LA ENTIDAD REGULADORA

Art. 47 Funciones de la Entidad Reguladora

La Entidad Reguladora ejercerá las facultades que legalmente le han sido asignadas respecto de las Entidades de Certificación y adicionalmente tendrá las siguientes funciones:

- a) Autorizar la actividad de las Entidades de Certificación constituidas legalmente en el territorio nacional otorgando licencias de operación;
- b) Velar por el buen funcionamiento de las Entidades de Certificación;
- c) Realizar visitas de auditoría a las Entidades de Certificación de acuerdo a lo dispuesto en el Reglamento de la presente Ley;
- d) Solicitar la información pertinente a las Entidades de Certificación para el ejercicio de sus funciones;
- e) Imponer sanciones a las Entidades de Certificación en caso de incumplimiento de las obligaciones derivadas de la prestación del servicio;
- f) Ordenar la revocación de certificados cuando la Entidad de Certificación los emita sin el cumplimiento de las formalidades legales;
- g) Velar porque las Entidades de Certificación emitan conforme a la ley certificados de Firma electrónica;
- h) Impartir instrucciones sobre el adecuado cumplimiento de las normas a las cuales deben sujetarse las Entidades de Certificación;



- i) Revocar o suspender la acreditación otorgada cuando se incumplan las condiciones, requisitos y obligaciones que se establecen en la presente Ley;
- j) Mantener, procesar, clasificar, resguardar y custodiar el Registro de las Entidades de Certificación de acuerdo a lo dispuesto en el Reglamento de esta Ley.
- k) Recaudar multas de acuerdo a lo dispuesto en el Reglamento de esta Ley; y
- l) 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 al consumidor y el usuario, conforme a esta Ley y su Reglamento.

El Reglamento de esta Ley establecerá las demás regulaciones que gobernarán las actividades y requerimientos, proceso de mediación, creación de registros, aranceles, supervisión, cumplimiento de obligaciones, medidas cautelares, sanciones y otras normas necesarias para la aplicación de la presente Ley.

Art. 48 Sanciones

La Entidad Reguladora en base al debido proceso y al derecho de 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:

- a) Amonestación escrita;
- b) Multa de hasta \$100,000.00 tanto para las Entidades de Certificación como para los administradores y representantes legales de las mismas;
- c) Suspender de inmediato todas o algunas de las actividades de la Entidad infractora;
- d) Una vez probada su infracción, prohibir a la Entidad de Certificación prestar directa o indirectamente los servicios de entidad de certificación hasta por el término de cinco años; y
- e) Revocar definitivamente la autorización para operar como entidad de certificación.

CAPITULO 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.

**CAPITULO IX
DISPOSICIONES VARIAS**

Art. 50 De las infracciones y sus sanciones.

Para efectos de la presente Ley se aplicarán las infracciones, delitos y sanciones establecidas en la legislación común correspondiente.

Art. 51 Reconocimiento de Certificados, Documentos Electrónicos y Firmas Electrónicas Extranjeras

Cuando se requiera determinar la validez de un certificado, documento electrónico o firma electrónica 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, deberán estar emitidos previamente por una Entidad de Certificación autorizada en su país de origen.

Art.52 Reglamentos y Facultad del Organo Ejecutivo para reglamentar la Ley

El Organo Ejecutivo por medio del Ministerio de Economía contará con un plazo de doce 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 el Reglamento que desarrolle el contenido de la presente Ley.

Art. 53 Derogatorias

Quedan derogadas todas aquellas disposiciones contenidas en la legislación vigente que contraríen las de esta Ley.

A N E X O 11

**L e y G e n e r a l M a r í t i m o
y P o r t u a r i a d e E l
S a l v a d o r**

ASAMBLEA LEGISLATIVA --- INDICE LEGISLATIVO

=====

=====

REPUBLICA DE EL SALVADOR --- AMERICA CENTRAL

DECRETO No. 994.-

LA ASAMBLEA LEGISLATIVA DE LA REPUBLICA DE EL SALVADOR,

CONSIDERANDO:

I.- Que la Constitución de la República establece que el territorio nacional es irreductible, estando comprendido dentro del mismo el espacio marítimo, el cual estará su

II.- Que es necesario regular con amplitud, todo lo relacionado con los servicios de navegación marítima y con los servicios de los puertos nacionales en general, a efecto de normar con efectividad la explotación de ambos servicios;

III.- Que para lograr una efectiva regulación técnica y económica del subsector de transporte marítimo portuario, es necesario contar con una entidad reguladora que posea personalidad jurídica, autonomía administrativa, técnica y financiera, a efecto de garantizar su continuo desarrollo institucional y con una capacidad técnica efectiva para el cumplimiento de sus competencias;

IV.- Que es necesario delimitar las competencias del ente rector del sector transporte a la formulación de la política subsectorial marítima portuaria, a la planificación indicativa de ésta y a la normativa legal que permita la implementación de éstas;

V.- Que para que la función reguladora se realice bajo reglas claras y exenta de conflictos de intereses, se requiere que el ente rector posea una relación exclusivamente funcional con respecto al ente regulador, y que el recurso humano que participe en las unidades de dirección y administrativas superiores de ambas entidades, estén plenamente desvinculadas de los sectores usuarios del subsector de transporte marítimo portuario;

VI.- Que para evitar al máximo el abuso en la discrecionalidad de los funcionarios, se hace necesario crear una Autoridad Marítima Portuaria, en calidad de organismo de decisión colegiada;

VII.- Que el ordenamiento del subsector marítimo portuario requiere de una ley general para ese subsector, moderna e integrada, que responda al derecho marítimo internacional con apropiadas disposiciones en concepto de seguridad de la navegación marítima y de la seguridad operacional portuaria, así como de una normativa portuaria efectiva en materia de desarrollo, administración, mantenimiento, conservación y explotación de la infraestructura y superestructura portuaria, y comprenda además el respectivo régimen de infracciones y sanciones;

POR TANTO,

en uso de sus facultades constitucionales y a iniciativa del Presidente de la República, por medio del Ministro de Obras Públicas, Transporte y de Vivienda y Desarrollo Urbano,

DECRETA la siguiente:

LEY GENERAL MARÍTIMO PORTUARIA

TÍTULO I
DE LOS ASPECTOS INSTITUCIONALES
Capítulo I
DISPOSICIONES GENERALES

OBJETO

Artículo 1

La presente Ley tiene por objeto regular todas las actividades relacionadas a la promoción, desarrollo y defensa de los intereses marítimos, al control y vigilancia de los asuntos relativos al mar y al ejercicio de la soberanía y jurisdicción en el territorio marítimo y aguas continentales de El Salvador, así como regular el uso de los espacios marítimos nacionales, incluyendo los acuáticos continentales, respecto a la prestación y desarrollo de los servicios de transporte acuático; igualmente establece las regulaciones relacionadas con la construcción, rehabilitación, administración, operación y mantenimiento de los puertos nacionales en general.

Los espacios marítimos y acuáticos continentales situados en el territorio salvadoreño estarán sujetos a la jurisdicción y soberanía nacional, de conformidad a lo establecido en el Artículo 84 de la Constitución de la República.

AMBITO DE APLICACIÓN Y COMPETENCIA

Artículo 2

Quedan comprendidos en las disposiciones de esta ley y sus reglamentos, todas las relaciones jurídicas vinculadas a la actividad marítima y portuaria. A falta de disposiciones de derecho marítimo portuario en la presente Ley y en cuanto no se pudiese recurrir a la analogía, se aplicará el derecho común.

En especial, estarán comprendidas dentro del ámbito de aplicación y competencia de esta Ley, las siguientes personas y actividades:

- a) La entidad que ejerza la competencia de autoridad marítima portuaria; incluyendo instituciones y entidades estatales que ejerzan competencias relacionadas con dicha autoridad, incluyendo dentro de ese contexto el desarrollo de actividades de apoyo, vinculantes o conexas con la referida autoridad;
- b) Todas las personas naturales y jurídicas, nacionales y extranjeras, que desarrollen actividades marítimas portuarias;
- c) Los actos relacionados a las actividades marítimas portuarias de los buques en razón de la propiedad de éstos, sean nacionales o extranjeros, en cuanto a la ley aplicable;
- d) El conocimiento de las causas que versen sobre los hechos ocurridos, los actos jurídicos realizados y los delitos cometidos a bordo de los buques navales ocurridos en las aguas jurisdiccionales del territorio salvadoreño o donde ningún Estado ejerza su soberanía. Igualmente, quedan sometidos, los hechos ocurridos, los actos jurídicos y los delitos cometidos a bordo de las naves o artefactos navales de bandera nacional durante su travesía en aguas jurisdiccionales de territorio extranjero, a menos que aquellos atenten contra la seguridad del Estado y el orden público del Estado extranjero subyacente. Asimismo, quedan sometidos a la jurisdicción y leyes salvadoreñas, los hechos, actos y los delitos cometidos a bordo de buques y artefactos navales de bandera extranjera que naveguen en las aguas jurisdiccionales salvadoreñas, ya sea con derecho de paso inocente o que ingresen y salgan de puerto salvadoreño, cuando atenten contra la seguridad del Estado o el orden público del Estado Salvadoreño y de las personas domiciliadas en éste, o cuando infrinjan normas de seguridad de navegación marítima, de conformidad a la ley aplicable;

e) Las actividades vinculadas a los puertos, terminales marinas e instalaciones portuarias, su construcción, uso, aprovechamiento, explotación, operación y administración, así como la prestación de servicios a los buques y a las cargas;

f) La planeación, programación y ejecución de las acciones correspondientes a la promoción, operación y desarrollo de los puertos y terminales; y

g) La administración de la zona de desarrollo portuario;

La navegación en los puertos y sus canales de acceso se rige por las disposiciones de la presente Ley, y por las regulaciones de la Autoridad Marítima Portuaria en materia de navegación, atraque y desatraque de buques, de acuerdo a las características hidrográficas de los distintos puertos.

Corresponderá a los tribunales comunes del país conocer de las controversias que se susciten entre particulares con motivo de la aplicación de esta Ley, sin perjuicio que las partes decidan someterlo a arbitraje, de conformidad a las leyes aplicables.

SUJETOS DE LA LEY

Artículo 3

Quedan comprendidos como sujetos a esta Ley, además de las personas jurídicas estatales, las personas naturales o jurídicas cuando negocien y utilicen los servicios de las instalaciones de puertos en el territorio nacional, especialmente los armadores, líneas navieras, agentes marítimos, operadores portuarios y sus usuarios.

EXCLUSION

Artículo 4

Se excluye de la presente Ley a la Fuerza Naval, rama permanente de la Fuerza Armada, que se rige por sus propias Leyes, Reglamentos y disposiciones especiales, de conformidad a lo que le ordena la Constitución de la República.

Se excluye también de la presente Ley, la normativa legal vigente en materia de ordenación y promoción de las actividades de pesca y acuicultura, conservación y desarrollo de los recursos hidrobiológicos; exceptuando el registro del buque o artefacto naval autorizado para estas actividades, el cual queda regulado por esta normativa, conjuntamente con las actividades de navegación para pesca.

DEFINICIONES

Artículo 5

Para los efectos de la presente ley, se entenderá por:

ABANDERAMIENTO: Acción de inscribir una nave en el Registro de Matrículas de Naves para enarbolar el Pabellón Nacional.

ABALIZAMIENTO: Sistema para señalar por medio de dispositivos internacionalmente aceptados, sectores de aguas navegables.

ACCIDENTE MARITIMO: Acontecimiento que ha sido causado, o está relacionado con las operaciones de un buque, por las cuales el buque o cualquier persona se expone a peligro o cuyo resultado puede causar

serios daños a las personas, al buque, estructuras o medio ambiente.

ACTIVIDADES MARITIMAS: Se consideran todas aquellas actividades que se efectúan en el Mar Territorial, Zona Contigua, Zona Económica Exclusiva, Suelo y Subsuelo pertenecientes a la Plataforma Continental, y en las costas y puertos de la República, relacionadas con la navegación de altura, de cabotaje, de pesca y científica, con buques nacionales y extranjeros, o con la investigación y extracción de los recursos del mar y de la plataforma.

AMP o ENTE REGULADOR: Autoridad Marítima Portuaria, institución autónoma de servicio público, sin fines de lucro, responsable de ejercer la regulación técnica y económica de las actividades marítimas y portuarias.

AMPL: Autoridad Marítima Portuaria Local; pueden ser las agencias estatales propietarias de infraestructura y superestructura portuaria propiedad del Estado, o ser los operadores portuarios designados por éstas, o ser los operadores de puertos de uso público de propiedad privada.

ÁREA DE JURISDICCIÓN PORTUARIA: Es la zona donde se realizan las operaciones portuarias.

ARTEFACTO NAVAL: Es todo aquel que no estando constituido para navegar, cumple en el agua funciones de apoyo y complemento a las actividades marítimas, fluviales, lacustres o de extracción de recursos, tales como diques, grúas, plataformas fijas o flotantes, balsas u otros similares. No se incluyen en este concepto las obras portuarias aunque se internen en el agua.

ARMADOR: Es la persona que explota comercialmente o no un buque o un artefacto naval, y que resulta responsable de la navegación del mismo. En términos de propiedad, el armador puede o no ser el propietario del buque.

AUTORIZACIONES: Documentos extendidos por la AMP, mediante los cuales da fe que personas naturales o jurídicas en general, cumplen con los requisitos legales, reglamentarios y de regulaciones establecidas por dicha entidad, para desarrollar una determinada actividad marítima portuaria.

BUQUE: es toda construcción flotante destinada a navegar por agua, cualquiera que sea la finalidad para la cual fue construido, así como cualquiera sea la propulsión que lo haga navegar. Este concepto incluye buques de transporte de carga y de pasajeros, lanchas recreativas y de pesca, barcasas, veleros, transbordadores, remolcadores, y cualquier otro tipo de vehículo acuático. La expresión buque, comprende además de su casco, arboladuras, máquinas principales o auxiliares, y las demás pertenencias fijas o no, que son necesarias para sus servicios de maniobra, navegación y equipamiento, aunque se hallen separadas.

BUQUES EN CONSTRUCCIÓN: Son todos los buques o artefactos navales considerados como tales desde el inicio de su construcción hasta el término de la misma.

BUQUES MILITARES NACIONALES: Son aquellos que están al servicio de la Fuerza Armada de El Salvador, en la rama permanente de la Fuerza Naval.

BUQUES MILITARES EXTRANJEROS: Son aquellos que están al servicio de las fuerzas armadas de otros países.

BUQUES POLICÍA: Son aquellos que independientemente de su propiedad, se encuentran afectados al servicio de los organismos de la Policía Nacional Civil, Aduanas o cualquier otro organismo estatal que ejerza las funciones de policía.

BUQUES PRIVADOS: Se entienden como tales los afectados a actividades de carácter privado o comercial,

ya sea en el transporte de pasajeros o de carga.

BUQUES PÚBLICOS: Son los afectados al servicio del poder público, independientemente del carácter de su propietario, entendiéndose como tal al destino, prestaciones y afectación que éstos tienen, tales como los buques de guerra, policía, aduanas, sanitarios o humanitarios.

BUQUES REGISTRABLES: Son aquellos que conforme a las disposiciones y reglamentaciones de la AMP deben estar registrados ante los registros creados por esta ley.

CARGADOR: Es la persona a quien se le suministra la carga para el transporte, sea o no fletador.

CEPA: Comisión Ejecutiva Portuaria Autónoma.

CONSIGNATARIO O DESTINATARIO: Es la persona facultada para recibir la mercancía en destino.

CDAMP: Consejo Directivo de la Autoridad Marítima Portuaria.

CONCESIONARIO PORTUARIO: Persona natural o jurídica a quien se le entrega mediante un contrato de concesión parcial o total, por un tiempo determinado y a cambio de un canon anual, obra pública portuaria y sus correspondientes servicios, o bien se le entrega solamente la explotación de los servicios portuarios de manera total o parcial. El concesionario podrá operar los servicios portuarios o en su defecto contratar personas naturales o jurídicas que ejecuten los servicios portuarios en calidad de operadores.

CONTRATO DE AJUSTE: Es el valor a pagar al dueño de la carga, por el armador de un buque o por el transportador de un buque, o por el armador o transportador de un buque que colisiona a otro, cuando la carga ha sido sujeta de avería. El valor a pagar lo determina un perito especializado designado por las partes para esos efectos.

CONTRATO DE CARGA GENERAL: Es aquel por el cual una de las partes, el transportador, se obliga, a cambio de un precio o flete, llevar una cosa a un lugar determinado, designado por la otra, el cargador. Cuando el transportador acepte efectos de cuantos cargadores se presenten, el transporte se regirá por las disposiciones de la presente Ley en lo que se haya previsto en el contrato respectivo o en las condiciones del conocimiento o manifiesto de carga.

CONTRATO DE FLETAMENTO: Se denomina a aquel contrato mediante el cual el armador de un buque determinado, conservando su tenencia y mediante el pago de un flete, se compromete a ponerlo a disposición de otra persona, y a realizar los viajes que ésta disponga dentro del término o por los trayectos o viajes y en las condiciones previstas en el contrato, o en las que los usos establezcan. En este contrato el armador se denomina fletante y la otra parte fletador. Los contratos de fletamento se clasifican en fletamentos por viaje o fletamentos a tiempo.

CONTRATO DE FLETAMENTO A TIEMPO: Es aquel contrato mediante el cual el fletante de un buque determinado, lo pone a disposición del fletador, y a realizar los viajes que éste disponga dentro de un lapso determinado de tiempo, suscribiendo el respectivo contrato o póliza de fletamento.

CONTRATO DE FLETAMENTO PARCIAL: Es el contrato mediante el cual el fletador solamente dispondrá de uno o más espacios determinados. Dentro de este contrato, el fletante debe emplear la diligencia razonable para poner el buque en condiciones de navegabilidad, en el tiempo y lugar convenidos y cumplir con las prestaciones comprometidas frente al fletador.

CONTRATO DE FLETAMENTO TOTAL: Es el contrato mediante el cual el fletante pone a disposición del fletador, todos los espacios útiles o todo el porte que posee un buque determinado, el que puede sustituirse por otro, si así se hubiese pactado. Dentro de este contrato, el fletante debe emplear la

diligencia razonable para poner el buque en condiciones de navegabilidad, en el tiempo y lugar convenidos y cumplir con las prestaciones comprometidas frente al fletador.

CONTRATO DE LOCACIÓN DE BUQUE: Es el contrato mediante el cual una parte se obliga, mediante el pago de un precio, a conceder a la otra el uso y goce de un buque por un tiempo determinado, transfiriéndole la tenencia.

CONTRATO DE REMOLQUE: Es el contrato por el cual un buque remolcador presta su fuerza de tracción a favor de otro remolcado para su traslación desde un punto a otro del espacio acuático, o para cooperar con el remolcado en sus maniobras de desplazamiento a cambio de un flete de remolque.

CONTRATO DE FLETAMENTO POR VIAJE: Es aquel por el cual el fletante de un buque determinado, lo pone a disposición del fletador, para realizar una travesía o viaje determinado indicando el puerto de salida y llegada del buque, mediante la suscripción del respectivo contrato o póliza de fletamento. A los demás efectos le son aplicables las normas relativas al fletamento a tiempo.

CREDITOS PRIVILEGIADOS: Persona que tiene prelación para que sus créditos le sean cancelados frente a otra u otras personas, con los bienes del deudor común.

DÁRSENA: Zona o área portuaria, comprendida por un espejo de agua, en donde los buques efectúan maniobras para atracar o fondear.

DERECHO ESPECIAL DE GIRO: Unidad de cuenta establecida por el Fondo Monetario Internacional (FMI), que se empleará para determinar la responsabilidad del armador y de los operadores y concesionarios portuarios; así como para cuantificar las infracciones y sanciones establecidas en la presente ley. El valor del Derecho Especial de Giro, para los efectos de determinar el monto de las responsabilidades, será el fijado por el FMI al momento en que ocurra la pérdida o daño; para la determinación del monto de las infracciones, será el fijado al momento que quede firme la resolución que aplica la multa respectiva.

ENTE RECTOR: Es el Ministerio de Obras Públicas, Transporte, y de Vivienda y Desarrollo Urbano, quien a través del Viceministerio de Transporte, es la entidad estatal responsable de formular, impulsar y vigilar el cumplimiento de la política sectorial de transporte, así como la planificación nacional indicativa de éste, y el establecimiento de la normativa legal para hacer efectiva dicha política y planificación.

INFRAESTRUCTURA PORTUARIA: Está constituida por los canales de acceso al puerto, el área de maniobras de los buques o dársena o rada, las obras de abrigo como rompeolas y esclusas, los elementos de señalización para la navegación de los buques en los canales de acceso y rada, los muelles y diques, áreas abiertas de almacenamiento, y vías de transporte internas del puerto.

INSTALACIONES PORTUARIAS: Son todas aquellas obras de infraestructura y superestructura portuarias, necesarias para el funcionamiento de un puerto.

INTERESES MARÍTIMOS: Son las funciones político-económicas que se materializan en el transporte marítimo, las comunicaciones marítimas comerciales, las estaciones de transferencias como puertos o terminales marítimas, fluviales y lacustre, la pesca, los deportes náuticos, la industria naval, el desarrollo y control del personal marítimo, los recursos marinos renovables y no renovables; abarcando con ello todo su universo.

MERCANCÍA: Es todo objeto o efecto cargado a bordo.

OPERADOR PORTUARIO: Es la persona natural o jurídica, con experiencia específica en actividades de explotación portuaria, que ejecuta dichas actividades en un puerto.

PRÁCTICO: Es la persona que se desempeña a bordo de un buque y que no pertenece a la tripulación de

éste, en calidad de consejero del Capitán del mismo en el curso y maniobra en los canales de acceso y del atraque y desatraque en los puertos, así como también en zonas de navegación que por razones de seguridad requieran de sus servicios y sus conocimientos-

PUERTO: Ámbito acuático y terrestre, natural o artificial, e instalaciones fijas, que por sus condiciones físicas y de organización resulta apto para realizar maniobras de fondeo, atraque y desatraque y estadía de buques o cualquier otro artefacto naval; para efectuar operaciones de transferencia de cargas entre los modos de transporte acuático y terrestre, embarque y desembarque de pasajeros, y demás servicios que puedan ser prestados a los buques, artefactos navales, pasajeros y cargas, y plataformas fijas o flotantes para alijo o comportamiento de cargas y cualquier otra operación considerada portuaria por la Autoridad Portuaria.

RECINTO ADUANERO DEL PUERTO: Área ubicada dentro del recinto portuario sometida al control aduanero.

RECINTO PORTUARIO: Área terrestre de un puerto en donde se realizan actividades operacionales de éste.

SERVICIOS PORTUARIOS: Son todos los servicios que se prestan dentro de un puerto a los buques, a las cargas, y a los pasajeros.

SINIESTRO: Significa todo acontecimiento o serie de acontecimientos cuyo origen sea el mismo, que causa daños por contaminación o de otro tipo.

SUPERESTRUCTURA PORTUARIA: Está constituida por todos los equipos portuarios en general, por las bodegas de mercaderías en general, bodegas de carga a granel sólido, tanques para almacenamiento de gráneles líquidos, almacenes en general, instalaciones administrativas en general, talleres, y toda otra obra construida dentro del recinto portuario.

TARIFA PORTUARIA: Precio que los operadores, permisionarios o prestadores de servicios portuarios, percibirán de los usuarios, como contraprestación por los servicios que brinden a éstos.

TERMINALES PORTUARIAS: Territorio portuario que comprende un conjunto de infraestructura y superestructura, con los equipos y servicios necesarios para atender la demanda de buques de carga y de pasajeros.

TRANSPORTADOR: Es la persona que contrata con el cargador el transporte de mercancías; sea propietario, armador o fletador o quien tenga la disponibilidad del buque. Esta expresión no comprende al agente marítimo o intermediario.

TRANSPORTE MULTIMODAL: Es aquel que se realiza utilizando dos o más medios de transporte, sean éstos marítimos, aéreos o terrestres, realizando el viaje bajo la responsabilidad de un único transportador, denominado transportista multimodal, y amparado bajo un único documento de transporte.

TRIPULACIÓN: Se denomina al conjunto de personas embarcadas conforme a las respectivas autorizaciones o habilitaciones, destinadas a atender todos los servicios del buque.

ZARPE: Documento de autorización de salida de una embarcación procedente de un puerto hacia el mar u otro puerto.

ZONA DE INFLUENCIA PORTUARIA DE LOS PUERTOS (HINTERLAND): Zona adyacente a una zona de jurisdicción portuaria, en la que se desarrollan instalaciones industriales y actividades económicas conexas o vinculadas a las actividades que se efectúan en un puerto.

CAPITULO II
ENTIDAD REGULADORA Y REGIMEN ADMINISTRATIVO

CREACION DEL ENTE REGULADOR

Artículo 6

Créase la Autoridad Marítima Portuaria, la que en lo sucesivo se denominará por sus siglas AMP, con carácter de institución autónoma de servicio público y sin fines de lucro. Dicha autonomía comprende lo administrativo, lo técnico y lo financiero, además tendrá personalidad jurídica y patrimonio propio.

La AMP se relacionará funcionalmente con el ente rector del sector transporte, que tendrá bajo su responsabilidad la definición, difusión, supervisión y control de la política sectorial, la planificación nacional indicativa del desarrollo del sector transporte, y la normativa legal que permita la operativización de dicha política y planificación.

COMPETENCIAS INSTITUCIONALES DE LA AMP

Artículo 7

Son competencias Institucionales de la Autoridad Marítima Portuaria, las siguientes:

1. Fomentar el desarrollo de las actividades marítimas y portuarias de El Salvador, de conformidad a la normativa establecida en la presente Ley, y elaborar y proponer ante las autoridades superiores, propuestas de políticas públicas relacionadas con las actividades marítimo portuarias;
2. Fiscalizar, supervisar y controlar todas las actividades de transporte marítimo y portuarias de El Salvador;
3. Establecer reglas y procedimientos técnicos alternos, para garantizar la seguridad de la navegación de los buques y de todo tipo de artefacto naval, cuando no sea práctico cumplir con algún requerimiento técnico sobre la materia;
4. Ejecutar todas las competencias y funciones relacionadas con el registro marítimo portuario de El Salvador;
5. Ejercer la función de Autoridad Marítima Portuaria Nacional, con competencia para regular en lo técnico y en lo económico, a las Autoridades Portuarias Locales, sean éstas agencias estatales propietarias de la infraestructura y superestructura portuaria de propiedad del Estado, o en su defecto a los operadores portuarios designados por éstas; dicha regulación se ejercerá a su vez a los operadores de puertos de uso público de propiedad privada. La Autoridad Marítima Portuaria, regulará además en lo técnico, a los puertos privados de uso privado, así como todas las actividades de transporte marítimo y de transporte acuático en tierra continental;
6. Establecer las normas que regulen la construcción, remodelación, rehabilitación, mantenimiento y conservación de obras marítimas, inclusive el dragado de puertos y de canales de acceso, con observancia de las normas aplicables en medio ambiente y las normas técnicas que rigen sobre la materia; asimismo, deberá velar por su cumplimiento;
7. Representar al país ante organismos internacionales e intervenir en las negociaciones de tratados y convenios internacionales en materia de puertos y de temáticas marítimas, en coordinación con las dependencias competentes;
8. Supervisar y controlar los procesos de otorgamiento y de cumplimiento de los contratos de concesión de los puertos nacionales, de conformidad a lo establecido en el Artículo 120 de la Constitución de la República; y declarar la caducidad de dichos

contratos de acuerdo a lo que norma sobre la materia la Ley de Adquisiciones y Contrataciones de la Administración Pública;

9. Aprobar todos los actos legales relacionados con la cesión, prórroga, caducidad, y rescate de las concesiones, de acuerdo a la presente ley y a lo establecido en la Ley de Adquisiciones y Contrataciones de la Administración Pública;

10. Regular tarifas portuarias y establecer los mecanismos de ajuste de las mismas, de conformidad a lo establecido en la presente ley;

11. Supervisar las actividades operacionales que se desarrollen en los puertos, incluyendo el mantenimiento de las instalaciones portuarias, y todos los aspectos que inciden en la conservación y mejoramiento de los lugares comunes y vías de acceso; de conformidad a los reglamentos de la presente Ley y de las regulaciones técnicas sobre la materia;

12. Dirimir conflictos marítimos portuarios que se presenten entre los diferentes agentes económicos que intervienen en la actividad económica marítima portuaria, de acuerdo a los procedimientos y criterios que serán establecidos en el reglamento respectivo;

13. Fiscalizar el cumplimiento de requerimientos técnicos relativos a las obras que se construyan en los puertos;

14. Verificar que los usuarios de los puertos nacionales sean sujetos de un trato eficiente, equitativo y universal;

15. Ejercer los derechos que le correspondan al Estado, en relación al cumplimiento de las obligaciones asumidas por los operadores de los puertos y de la actividad marítima;

16. Supervisar el buen funcionamiento de los servicios marítimos que se presten a la navegación de los buques, en especial los servicios de remolque, maniobra, practica y comunicaciones para la seguridad de la navegación;

17. Obtener de los operadores de los servicios informes periódicos que permitan establecer el grado de cumplimiento de los planes de mantenimiento de la infraestructura y superestructura portuaria;

18. Supervisar a los operadores y prestadores de servicios públicos, en lo que respecta al cumplimiento efectivo de las tarifas aprobadas, exigiendo la pública exhibición de las mismas;

19. Atender los reclamos de todos los usuarios de los servicios marítimos y portuarios prestados en el ámbito de la República de El Salvador;

20. Prevenir conductas anticompetitivas y discriminatorias entre los usuarios de los servicios marítimos y portuarios, de acuerdo a lo establecido en la presente ley y su reglamento;

21. Organizar y llevar todos los registros creados por la legislación vigente en materia marítima y portuaria;

22. Supervisar y controlar el cumplimiento efectivo de las normas marítimas portuarias, relativas a la protección y conservación del medio ambiente;

23. Normar la seguridad operacional marítima portuaria en situaciones de riesgos para la seguridad operacional de las instalaciones portuarias; en tales casos, la AMP estará facultada para suspender temporalmente las operaciones portuarias;

24. Establecer las regulaciones técnicas relacionadas con la recepción y zarpe de los buques que utilicen los puertos del país, así como los que navegan en nuestras aguas territoriales con derecho de paso inocente;

25. Establecer la normativa técnica que corresponda a cada una de las áreas funcionales de la Administración Marítima;

26. Establecer las normas que regulen la construcción, mantenimiento, conservación y funcionamiento de las fábricas ensambladoras de buques y todo tipo de artefacto naval, motores o partes de éstas;

27. Aprobar los itinerarios y frecuencias de todo servicio de transporte marítimo en el territorio nacional;
28. Tomar las acciones y medidas que permitan asegurar que los buques y artefactos navales en general que operen en el territorio salvadoreño, o que estando con matrícula salvadoreña operen en el extranjero, cumplan con las disposiciones de la presente Ley, sus reglamentos, y convenios internacionales marítimos portuarios suscritos y ratificados por El Salvador;
29. Prohibir la navegación de buques, artefactos navales e hidroaviones, en los puertos nacionales y en sus canales de acceso, cuando las condiciones meteorológicas o hidrográficas resulten peligrosas, o existan obstáculos para la navegación, o por razones de orden público. Se exceptúa de esta norma a la Unidades Navales de la Fuerza Armada;
30. Dictar sanciones por incumplimiento a la presente Ley, sus reglamentos y regulaciones, de conformidad a las disposiciones legales pertinentes; y
31. Ejercer las demás atribuciones que expresamente le fija esta ley y sus reglamentos.

AUTORIDAD SUPERIOR DE DIRECCIÓN DE LA AMP

Artículo 8

La autoridad superior de la AMP será el Consejo Directivo de la Autoridad Marítima Portuaria, cuyas siglas serán CDAMP, el cual estará integrado de la siguiente forma:

1. Un Director Presidente nombrado por el Presidente de la República.
2. Un Director Propietario nombrado por el Ente Rector.
3. Dos Directores Propietarios del sector privado, elegidos por el Presidente de la República de dos ternas propuestas por la Asociación Nacional de la Empresa Privada, y
4. Un Director Titular, designado por las facultades de ingeniería de las universidades legalmente acreditadas en el país.

De la misma forma, se deberán nombrar los Directores Suplentes, los cuales podrán participar en las reuniones con voz pero sin derecho a voto, salvo en el caso de sustitución del propietario.

El Consejo Directivo se reunirá al menos cada quince días o cuando las circunstancias lo hagan necesario, previa convocatoria del Presidente o de quien haga sus veces.

Las reuniones se establecerán con un quórum de tres miembros, siendo éstos los siguientes: El Director Presidente o quién los sustituya en su ausencia; Un Director del Ente Rector; y uno de los restantes directores de ANEP o de las universidades legalmente acreditadas.

Solamente los Directores Propietarios o los Directores Suplentes que actúen en representación de éstos, incluyendo el Presidente, gozarán de dieta, cuyo monto y mecanismos de ajuste se establecerán reglamentariamente.

REQUISITOS PARA LOS MIEMBROS DEL CONSEJO DIRECTIVO

Artículo 9

Para ser miembro del Consejo Directivo de la AMP se requiere:

1. Ser salvadoreño por nacimiento;
 2. Ser mayor de treinta años de edad;
 3. Ser de reconocida honorabilidad y probidad;
 4. Poseer título universitario y no tener conflicto de intereses con el cargo;
 5. Poseer competencia notoria en las materias relacionadas con sus atribuciones;
 6. Obtener el finiquito de sus cuentas si hubiese administrado fondos públicos;
 7. Hallarse libre de reclamaciones de toda clase, en caso de haber sido contratista de obras públicas ejecutadas con fondos del Estado y de Municipios;
 8. Hallarse solvente con la Hacienda Pública y con el Municipio de su residencia; y
9. No haber desempeñado dentro de los dos últimos años, funciones en empresas privadas vinculadas con el sector marítimo y portuario.

ATRIBUCIONES DEL CDAMP

Artículo 10

El Presidente del CDAMP ejercerá la representación legal de la AMP, con facultad para firmar todos los actos públicos y privados que sean necesarios para el debido cumplimiento de sus funciones; asimismo, convocará a las reuniones del Consejo Directivo y las presidirá; y en su ausencia actuará en su representación el Director designado por el Ente Rector.

El CDAMP, en su calidad de entidad colegiada dirigida por su Presidente, tendrá bajo su responsabilidad las atribuciones siguientes:

1. Designar y remover al Director Ejecutivo de la AMP y a todo el personal ejecutivo necesario para cumplir y ejecutar las funciones asignadas por Ley;
2. Dictar al Director Ejecutivo las políticas, las directrices y los lineamientos para el efectivo cumplimiento de las competencias institucionales especificadas en el Artículo 7 de esta Ley;
3. Aprobar los reglamentos internos de funcionamiento, normativas, disposiciones administrativas internas de la institución, regulaciones, directrices, controles internos, manuales, publicaciones de información marítima portuaria, normas técnicas de operación y modificaciones a todos éstos, de conformidad a la presente Ley, para garantizar el efectivo cumplimiento y desarrollo de la actividad marítima portuaria, incluyendo la aprobación de la aplicación del régimen sancionatorio;
4. Establecer reglas y procedimientos técnicos alternos, para garantizar la seguridad marítima y portuaria, cuando sea impracticable cumplir algún requerimiento técnico sobre la materia; de conformidad a la presente ley;
5. Establecer todas las medidas o acciones necesarias para garantizar que las actividades marítimas y portuarias sean realizadas de manera segura;
6. Aprobar normas, procedimientos y métodos aplicables a los servicios de tránsito de navegación marítima, incluyendo el abalanzamiento de los puertos y vías navegables, instalaciones meteorológicas, oceanográficas y toda otra actividad complementaria de ayuda a la navegación;
7. Aprobar normas, procedimientos y métodos aplicables para la prestación de los servicios de practicaje, entrada y salida de buques y su permanencia en los puertos;

8. Aprobar normas, procedimientos y métodos aplicables relacionados a la correcta recepción, entrega y almacenaje de mercancías;
9. Asegurar la competencia dentro de las actividades marítimas y portuarias, impidiendo prácticas monopólicas, de conformidad con la presente ley;
10. Someter a la consideración y aprobación del Ente Rector, el anteproyecto del presupuesto especial de la AMP, y las modificaciones al mismo, para su presentación a la Asamblea Legislativa, de conformidad con la legislación aplicable;
11. Presentar la Memoria Anual de Labores al Ente Rector para su posterior presentación a la Asamblea Legislativa;
12. Contratar las auditorías técnica y financiera de la institución, especialmente la auditoría técnica y legal; y conocer y aprobar los informes correspondientes;
13. Nombrar los apoderados legales que estime necesario;
14. Aprobar políticas y metodologías de regulación y ajuste de tarifas de servicios portuarios, tarifas de tránsito de navegación acuática y de protección de éste, de acuerdo a lo establecido en la presente ley;
15. Solicitar ante la autoridad gubernamental que tenga la responsabilidad de velar por la libre y sana competencia, dictámenes sobre situaciones de servicios de transporte marítimo que presenten características monopólicas y de posición dominante, así como de competencia desleal entre operadores de transporte marítimo; y, con base a dichos dictámenes, aprobar la regulación efectiva para la corrección de las respectivas situaciones;
16. Conocer en segunda instancia de las resoluciones tomadas por el responsable de la administración ejecutiva de la AMP;
17. Aprobar la estructura orgánica de la AMP, sus modificaciones, actualizaciones y reestructuraciones;
18. Aprobar la política salarial de la AMP y su correspondiente régimen salarial;
19. Asesorar a las áreas de gobierno competentes sobre las modalidades y formas de contratación y trabajo del personal relacionado con los puertos;
20. Autorizar todos los actos jurídicos y contratos relacionados a comprar, permutar, gravar y vender bienes;

21. Aprobar la normativa que regule la construcción, administración, operación, explotación, mantenimiento, rehabilitación y ampliación de la infraestructura y superestructura portuaria;
22. Disponer el cierre parcial o total de los puertos cuando no reúnan las condiciones de seguridad apropiadas para su funcionamiento, de acuerdo con las disposiciones de la presente ley y el reglamento de la misma;
23. Aprobar disposiciones administrativas y regulaciones para garantizar el efectivo cumplimiento y desarrollo de la actividad marítima portuaria;
24. Adquirir y disponer a cualquier título y de conformidad con las normas aplicables, los bienes necesarios para el cumplimiento de sus objetivos;
25. Evaluar la labor desarrollada por el Director Ejecutivo, fundamentalmente con base a los dictámenes de auditorías técnicas y financieras, y a los informes semestrales y extraordinarios que presente dicho funcionario;
26. Llevar a cabo todas las actividades que en la presente ley no se hayan atribuido al Director Ejecutivo o a su Presidente; y

27. Proponer reformas a la presente Ley y sus reglamentos, ante las instancias internas competentes.

RESPONSABLE DE LA ADMINISTRACIÓN

Artículo 11

La administración de la AMP estará a cargo de un Director Ejecutivo, a quien le corresponderá ejercer las funciones que esta ley le atribuye, así como todas aquellas que el Presidente del Consejo Directivo le delegue. Este cargo será a tiempo completo.

El Director Ejecutivo, dentro de las atribuciones que esta ley le otorga, podrá efectuar delegación de las mismas en los gerentes de área, específicamente en la firma de documentos y otros actos administrativos, todo lo cual será establecido y regulado en el reglamento interno de la AMP.

REQUISITOS PARA EL DIRECTOR EJECUTIVO

Artículo 12

Para ser designado Director Ejecutivo de la AMP se requieren los mismos requisitos establecidos para los Directores del CDAMP, en el Artículo 9 de la presente Ley.

ATRIBUCIONES DEL DIRECTOR EJECUTIVO

Artículo 13

Son atribuciones del Director Ejecutivo de la AMP, las siguientes:

1. Ejecutar las decisiones y resoluciones del Consejo Directivo de la AMP;
2. Administrar la institución y cumplir con las atribuciones que la presente Ley le otorgue a la AMP;
3. Asistir a las reuniones del Consejo Directivo, con voz pero sin derecho a voto;
4. Por delegación del Presidente del CDAMP, representar judicial y extrajudicialmente a la AMP, conforme las instrucciones que reciba de ese Consejo Directivo;
5. Administrar todas las actividades relacionadas con el Registro Marítimo Portuario (REMS);
6. Ejercer todas las gestiones que fueran pertinentes para la promoción del sector marítimo y portuario;
7. Por delegación del Presidente del CDAMP, realizar los actos y celebrar los contratos que sean necesarios para el cumplimiento de los objetivos de la AMP;
8. Designar al personal administrativo y operacional de la AMP; y remover y promover al personal de la AMP dentro de la política que establezca el Consejo Directivo;
9. Representar a la AMP ante los organismos internacionales relacionados a la actividad marítima y portuaria, conforme lo disponga el Consejo Directivo;
10. Establecer, mantener y fomentar relaciones de cooperación con instituciones u organismos extranjeros y multilaterales, vinculados al sector;
11. Fijar los estándares de seguridad, operación y servicios en el sector marítimo y portuario en el país, conforme las normas internacionales correspondientes;
12. Emitir circulares internas que contengan directrices organizacionales, reportes, normas y controles administrativos, que faciliten a los empleados la efectiva ejecución de sus funciones;

13. Intercambiar información con otras autoridades o instituciones vinculadas a la actividad marítima y portuaria y del comercio exterior;
 14. Supervisar el funcionamiento de los puertos, de sus operadores, permisionarios y empresas que ahí operen o presten servicios;
 15. En lo administrativo, ejercer la coordinación de todas las acciones necesarias e inherentes a la investigación efectiva de accidentes y de incidentes de la navegación marítima y de las operaciones portuarias;
 16. Conceder y modificar los permisos a empresas operadoras de servicios en los puertos, de acuerdo con lo establecido en la ley y el reglamento respectivo;
 17. Otorgar, revalidar o convalidar licencias al personal afectado a la actividad marítima y portuaria, previa demostración de cumplimiento por parte del solicitante de los requisitos establecidos en la presente ley y sus reglamento, así como también las demás regulaciones emitidas por la AMP; así mismo la suspensión o cancelación de las mismas;
 18. Ejercer el adecuado control y supervisión sobre el personal técnico marítimo y portuario e imponer las sanciones disciplinarias;
 19. Mediar en conflictos entre operadores del sector portuario y marítimo, de conformidad a lo dispuesto en las normas y reglamentos aplicables;
 20. Resolver sobre reclamos de usuarios de los servicios portuarios;
 21. Mantener la más estrecha relación de coordinación con las autoridades en materia de medio ambiente;
 22. Informar a la autoridad respectiva del CDAMP, de la existencia de prácticas que atenten contra la libre competencia;
 23. Desarrollar acciones para recopilar y divulgar la información estadística del sector marítimo y portuario;
 24. Elaborar el proyecto de su presupuesto y sus modificaciones, y presentarlo al Consejo Directivo para su aprobación;
 25. Proponer, para la aprobación del Consejo Directivo, el régimen de remuneraciones de los funcionarios de la AMP;
 26. Realizar todos los actos, contratos y operaciones que sean necesarios para cumplir con los objetivos que le impone la presente Ley y su reglamento;
 27. Aplicar, previo el debido proceso, las sanciones correspondientes a los incumplimientos de lo establecido en la presente ley, reglamentos, regulaciones, tratados y convenios internacionales vigentes; y
 28. Presentar al Consejo Directivo cualquier informe que le sea solicitado, y además dentro de los dos meses siguientes a la terminación de cada año, presentar al CDAMP el informe de labores y de la situación del sector bajo su regulación.
- DURACIÓN EN LOS CARGOS**

Artículo 14

Los Directores del Consejo Directivo de la AMP durarán en sus funciones cuatro años y podrán ser reelectos en sus cargos.

El Director ejecutivo durará en su cargo un período de cinco años y podrá ser reelecto en su cargo.

CESACIÓN EN LOS CARGOS DE DIRECTORES DEL CONSEJO DIRECTIVO

Artículo 15

Los miembros del Consejo Directivo, cesarán en el cargo por las siguientes causas:

1. Por renuncia;
2. Por expiración del plazo para el cual fueron nombrados;
3. Por sentencia judicial condenatoria definitiva en la comisión de un delito;
4. Por incapacidad física o mental que impida el ejercicio en el cargo;
5. Por sobrevenir alguna incompatibilidad de las previstas en esta ley; y
6. Por pérdida de confianza.

Cuando exista o sobrevenga alguna de las causales de cesación mencionadas, debidamente comprobadas, caducará la gestión del director y se procederá a su reemplazo inmediato.

INCOMPATIBILIDADES

Artículo 16

El cargo de miembro del Consejo Directivo o de Director Ejecutivo de la AMP será incompatible con:

1. El ejercicio de cualquier cargo de elección popular, de elección de segundo grado, o de Ministro y Viceministro de Estado, excepto el ejercicio de la docencia;
2. El ejercicio remunerado de cualquier empleo o profesión, para el caso exclusivo del director ejecutivo;
3. El desempeño de funciones de dirección en cualquier partido político, organización sindical, o asociaciones gremiales;
4. La participación directa o indirecta en cualquier sociedad que opere concesiones o mantenga contratos vinculados a los sectores marítimo y portuario o usuario de las mismas; y,
5. El ejercicio de cualquier cargo o función dentro de la Administración Pública.

INHABILIDADES PARA SER MIEMBRO DEL CDAMP Y DIRECTOR EJECUTIVO DE LA AMP

Artículo 17

No podrán ser miembros del CDAMP, ni Director Ejecutivo de la AMP, los titulares que gocen de concesiones en los ramos de transporte acuático y actividades portuarias en general; ni los socios, accionistas, representantes, directores, administradores o apoderados de las sociedades que tengan esas cualidades, o que desarrollen cualquier actividad en el subsector que regula la presente ley, así como los directores de otras instituciones autónomas, el cónyuge y los parientes dentro del cuarto grado de consanguinidad y segundo de afinidad de los Presidentes de los tres Órganos del Estado, ni los que hayan administrado fondos públicos y no hayan obtenido el finiquito de sus cuentas.

Quien se haya desempeñado como miembro del CDAMP o Director Ejecutivo de la AMP, no podrá representar ante ésta a ningún operador o concesionario en el ramo del transporte marítimo portuario,

durante los cuatro años posteriores a la fecha en que haya cesado en sus funciones.

PATRIMONIO Y RECURSOS

Artículo 18

El patrimonio de la AMP estará constituido por los bienes muebles e inmuebles, fondos, valores líquidos que posea o se le transfiera para el cumplimiento de sus fines y los que en el futuro se incorporen por transferencia, donación o legado o los que adquiera con el producto de sus ingresos.

Los recursos de la AMP se integrarán además con:

- a) Un porcentaje no mayor del 6% de los ingresos derivados de las tarifas de los servicios portuarios prestados a las naves y a la carga, en los diferentes puertos de uso público o privados que presten servicios en El Salvador;
- b) Las tarifas por servicios que preste la AMP y que se fijen en el reglamento de la presente ley;
- c) Los derechos que perciban los distintos registros que lleve la AMP y que serán fijados en el reglamento de la presente ley;
- d) El producto de las multas o sanciones económicas que determine la AMP;
- e) El producto de ingresos extraordinarios provenientes de asignaciones especiales del Estado, de organismos internacionales o privados; y
- f) Cualquier otro ingreso que se obtenga a título legal.

El presupuesto de la AMP será anual, debiéndose liquidar anualmente. En caso de excedentes financieros al final de cada año, éstos serán utilizados para cubrir el presupuesto aprobado del año siguiente; y si dichos excedentes fueran inferiores al mencionado presupuesto aprobado, para complementarlo, el porcentaje de contribución para el ente regulador no deberá exceder del 6% de los ingresos derivados de las tarifas de los servicios portuarios prestados a las naves y a la carga, en los diferentes puertos de uso público o privados que presten servicios en El Salvador.

COMPETENCIAS DE OTROS ORGANISMOS ESTATALES

Artículo 19

Las entidades del Estado que brindan soporte a las actividades portuarias, tales como la Policía Nacional Civil (PNC), autoridades aduanales, sanitarias, migratorias o cualquier otra entidad que ejerza funciones en dichos puertos, deberán ejercer las respectivas funciones operacionales, en coordinación con la AMP.

PLANIFICACION TERRITORIAL Y PORTUARIA

Artículo 20

En los Departamentos del país en los cuales la AMP haya autorizado la construcción de un existapuerto que se vaya a construir o se haya reservado y el uso del respectivo borde, una parte del borde costero o litoral para estos fines, el Ministerio de Obras Públicas, Transporte, Vivienda y Desarrollo Urbano, a través del Viceministerio de Transporte, deberá velar porque las vías de acceso a dichos puertos e interconexión con la red nacional de transporte del país se encuentren consideradas en los proyectos viales y urbanos nacionales.

AUDITORIA TÉCNICA Y FINANCIERA EXTERNA

Artículo 21

La AMP, a instancia del Consejo Directivo deberá contratar un servicio de auditoría externa, en lo técnico y en lo financiero, de manera integral.

SERVICIO DE DRAGADO Y TRASVASE DE ARENAS DE LOS PUERTOS NACIONALES

Artículo 22

El ente rector de las obras públicas podrá establecer un servicio de dragado y de trasvase de arenas de los puertos nacionales, que podría ser gestionado en cualquiera de las modalidades directas o indirectas que establece la legislación vigente. Los operadores que resulten beneficiarios del servicio mencionado tienen la consideración de sujetos pasivos obligados a satisfacer las tarifas correspondientes. Esta actividad estará sujeta a las normas, correspondientes del Ministerio de Medio Ambiente y de Recursos Naturales (MARN).

AUTORIZACIONES ADMINISTRATIVAS

Artículo 23

La AMP mantiene las competencias plenas sobre las autorizaciones administrativas existentes en la zona costera mientras se mantengan los usos autorizados.

EJERCICIO DE PODER DE VIGILANCIA

Artículo 24

La AMP y las autoridades responsables de las operaciones en los puertos salvadoreños, podrán coordinar con la Fuerza Naval la vigilancia marítima, en cumplimiento de la función constitucional de ésta, relativa a velar por la Soberanía del Estado.

La Fuerza Naval contribuirá con la AMP a aplicar y fiscalizar en el borde costero y en los espacios acuáticos nacionales fuera de los puertos, especialmente para la salvaguarda de la vida humana en la mar, la protección de los intereses marítimos y la seguridad de la navegación. Para tal efecto, un Reglamento establecerá la forma de implementar estas relaciones entre el Ministerio de la Defensa Nacional y la AMP.

TITULO II
DE LO MARITIMO
Capítulo I
DEL BUQUE Y ARTEFACTOS NAVALES

BIENES REGISTRABLES

Artículo 25

Los buques y los artefactos navales, conforme a su naturaleza, se consideran bienes registrables y se encuentran sometidos al régimen jurídico de la presente ley y de las demás leyes que regulan a los bienes de estas características.

Todos los buques o artefactos navales se consideran como tales desde el inicio de su construcción y la

actividad estará regulada y supervisada por la AMP, quién llevará un registro de todos aquellos que se construyan o reparen en territorio salvadoreño.

Los propietarios de buques o artefactos navales en construcción tienen la obligación de registrarlos desde el inicio de la misma.

PROPIEDAD Y CONDOMINIO NAVAL

Artículo 26

La propiedad de un buque o artefacto naval será atribuida a aquella persona natural o jurídica que efectúe ante el registro correspondiente la inscripción a su nombre, acreditando haberlo adquirido o construido, pudiéndose realizar dicha inscripción aún en la etapa de construcción.

La propiedad de un buque o artefacto naval será admitida bajo el régimen de condominio.

INSCRIPCIÓN

Artículo 27

Todos los actos constitutivos, traslativos o extintivos de la propiedad o de derechos reales sobre un buque que por sus características deba ser registrado, o sobre una o más partes en copropiedad naval, deben registrarse ante la autoridad de registro competente, y producirán efectos frente a terceros desde la fecha de su inscripción.

HIPOTECA NAVAL

Artículo 28

Sobre todo buque o artefacto naval de matrícula salvadoreña, que por sus características deba ser inscrito en el registro previsto en esta ley, incluyendo aquellos en construcción, su propietario podrá constituir sobre el mismo, derecho de hipoteca mediante instrumento público.

PREFERENCIA

Artículo 29

El orden de inscripción de la hipoteca determina la preferencia del título y su orden de privilegio.

Capítulo II DE LOS BUQUES EN PUERTO

LÍMITES DE LAS ZONAS PORTUARIAS

Artículo 30

Los límites de las zonas portuarias se establecen de acuerdo a las determinaciones de la Autoridad Marítima Portuaria. Cuando las zonas portuarias no estén expresamente delimitadas, se reconocerán como tales las establecidas por la práctica y el uso, en concordancia con los criterios y definiciones dados en esta ley.

SEGURIDAD DE LA NAVEGACIÓN

Artículo 31

El arribo, atraque y desatraque, y zarpe de los buques, artefactos navales e hidroaviones serán actividades reguladas por la AMP, la cual tendrá en cuenta a tales fines la seguridad en la navegación. A tal efecto la AMP dictará las reglamentaciones pertinentes mediante las cuales se determinarán las normas y requisitos de seguridad que deberán seguir los buques para su arribo, permanencia y zarpe de los puertos.

AUTORIZACIÓN PARA ENTRAR Y SALIR DE PUERTO

Artículo 32

La autorización para entrar y salir de puerto se concede por la Autoridad Marítima Portuaria Local, a solicitud de los armadores, explotadores o de sus agentes, o del capitán del buque, o encargado del artefacto naval. La autorización se supedita al cumplimiento previo de las disposiciones sobre seguridad de la navegación, sanitarias, aduaneras, migratorias y portuarias vigentes.

ARRIBADA FORZOSA

Artículo 33

En caso de arribada forzosa, el cumplimiento de las disposiciones sobre entrada y salida de puerto, se ajustará a las circunstancias particulares de cada caso, pudiéndose eximir al buque de ciertas normas a criterio de la AMP.

Son considerados casos de arribada forzosa, aquellos que encuadren peligro para las personas transportadas, el propio buque y la carga que se encuentre en sus bodegas, o la preservación del medio ambiente, que requieran prioridad en cuanto a la autorización de entrada al puerto. La arribada forzosa se podrá presentar a su vez en los casos de desperfectos de buques.

Quedará a criterio de la AMP, de acuerdo a las circunstancias especiales de cada caso, determinar los requisitos y exigencias que le demandará al buque que solicita la arribada forzosa, teniendo facultades para rechazarla.

El buque que haga una arribada forzosa será responsable de los gastos que haya demandado a todas aquellas personas que hayan contribuido en su auxilio.

IZAR BANDERA Y EMPAVESADO

Artículo 34

Todo buque amarrado o fondeado en un puerto salvadoreño debe izar la bandera de su nacionalidad. Los buques extranjeros deben izar también la bandera salvadoreña.

RESPONSABLES DE LAS OPERACIONES DE LOS BUQUES EN PUERTOS SALVADOREÑOS

Artículo 35

Los buques anclados en puerto están obligados a facilitar las respectivas operaciones de carga y descarga, en cuanto las mismas no los perjudiquen o les causen averías. Pero ningún otro buque podrá interrumpir las operaciones de otro, salvo en los casos de estar listo para zarpar o por caso fortuito o fuerza mayor.

BUQUES Y ARTEFACTOS NAVALES SALVADOREÑOS

Artículo 36

Los buques y artefactos navales salvadoreños deberán ser registrados en el orden interno y a todos los efectos legales, por su nombre, número, matrícula, tonelaje de desplazamiento y puerto de registro.

NOMBRE DEL BUQUE

Artículo 37

El nombre de un buque salvadoreño no puede ser igual al de otro buque. A tal efecto la reglamentación regulará la imposición, uso y cese de dicho elemento de individualización.

MATRÍCULA

Artículo 38

El número de matrícula del buque o artefacto naval es el de inscripción en el registro correspondiente.

DEBER DE EXHIBICIÓN

Artículo 39

Todo buque debe exhibir en lugar visible la bandera nacional, su nombre, puerto y número de matrícula.

Capítulo III DEL REGISTRO MARITIMO SALVADOREÑO

ESTABLECIMIENTO DEL REGISTRO

Artículo 40

Se establece el Registro Marítimo Salvadoreño, que en adelante se denominará REMS, el cual será una dependencia orgánica de la AMP.

En el registro se inscribirá:

1. Los buques y artefactos navales, acreditando el nombre y demás datos de su propietario;
2. Características técnicas y detalles de su equipamiento;
3. Derechos que graven a los buques o artefactos navales;
4. Hipotecas y demás privilegios;
5. Embargos e Interdicciones;
6. Contratos de Compraventa, Construcción, Fletamento y Locación;
7. Resoluciones Judiciales que afecten, modifiquen o transfieran derechos; y
8. Todo dato o información de interés para el registro.

Para su efectivo funcionamiento, el registro deberá contar con las áreas organizacionales básicas, para lo cual deberá de considerarse por ejemplo, área de registro de buques y artefactos navales, área de aspectos administrativos, área de aspectos portuarios.

Ninguna inscripción se hará en el REMS, si no consta en él, que la persona que constituye o enajena el derecho que pretende inscribir es el titular del mismo.

El REMS está destinado a garantizar la propiedad o posesión de los buques y artefactos navales, la publicidad formal de los contratos y documentos que se relacionen con la operación portuaria; tales como: concesiones, autorizaciones y permisos.

El REMS deberá contar para su efectivo funcionamiento con un reglamento de registro, en el cual se desarrolle su organización funcional, los procedimientos relacionados con los documentos a inscribirse, los requisitos a que deberán sujetarse las inscripciones, las cancelaciones y las certificaciones que deban expedirse.

EFECTOS DE LA INSCRIPCIÓN

Artículo 41

El otorgamiento de la matrícula nacional confiere al buque o artefacto naval la nacionalidad salvadoreña y el derecho de enarbolar el pabellón nacional.

REQUISITOS

Artículo 42

Para inscribir un buque o artefacto naval en el REMS, deberá acreditarse:

1. Haber dado cumplimiento de las exigencias reglamentarias sobre construcción y condiciones de navegabilidad e idoneidad del buque o artefacto naval, conforme lo determinado por su constructor;
2. Que su propietario esté domiciliado en el país; y
3. Si fuere titular de la propiedad una sociedad, que ésta se haya constituido de acuerdo con las leyes del país, o que habiéndose constituido en el extranjero, tenga en El Salvador sucursal, asiento o cualquier otra especie de representación permanente, de acuerdo con lo dispuesto en la ley respectiva.

Los buques extranjeros podrán ser registrados en el REMS, siempre que hayan cancelado previamente su matrícula en el país expeditor. Para ello deberán solicitar su inscripción por escrito, adjuntando a la solicitud el certificado de matrícula cancelado, el pasavante de navegación, los seguros de protección e indemnización o responsabilidad civil, y el contrato o documento que acredite la compraventa, junto con la documentación aduanera que acredite la importación.

CERTIFICADO DE MATRÍCULA

Artículo 43

La AMP otorgará a todo buque o artefacto naval que se inscriba en el REMS, un certificado de matrícula en el que conste el nombre del buque o artefacto naval y el de su propietario, el número de matrícula y la medida de los arcos total y neto, cuando se trate de buque, así como los demás datos contenidos en el folio de su inscripción. Dicho certificado identifica y determina la nacionalidad del buque o del artefacto naval.

CANCELACIÓN DE LA MATRÍCULA NACIONAL

Artículo 44

La cancelación de la matrícula de un buque o artefacto naval en el REMS, procederá en los siguientes casos:

1. Por comprobada innavegabilidad absoluta;

2. Por pérdida total comprobada y declarada por la autoridad marítima;
3. Por presunción fundada de pérdida, después de transcurrido un año desde la última noticia del buque o artefacto naval;
4. Por desguace;
5. Por cancelación de la inscripción a solicitud de su propietario;
6. Por declaración de abandono por parte del REMS;
7. Por estar registrada en otro Estado; y
8. Por orden judicial de la autoridad competente.

REGLAMENTACIÓN

Artículo 45

El régimen de registro y cancelación de la inscripción de los buques y artefactos navales, en todo cuanto no esté previsto en esta ley, será fijado por la reglamentación a dictarse al efecto por la AMP, en orden a su competencia.

Capítulo IV RIESGOS DE LA NAVEGACIÓN

ABORDAJE

Artículo 46

Se entiende por abordaje el choque o la colisión de dos o más buques o entre un buque y un artefacto naval. Cuando un abordaje entre dos o más buques o entre un buque y un artefacto naval se origine por causa de fuerza mayor o caso fortuito, o cuando existan dudas sobre sus causas, los daños deberán ser soportados por quienes los hubieren sufrido.

Si el abordaje es causado por culpa exclusiva de uno de los buques o artefacto naval involucrados, el declarado culpable deberá indemnizar todos los daños producidos. En caso de culpa concurrente, cada buque o artefacto será responsable en proporción a la gravedad de su culpa. Si ésta no pudiese establecerse, la responsabilidad será soportada en partes iguales por cada uno de los siniestrados.

Las responsabilidades subsistirán aún en caso que las mismas sean imputables al práctico, aunque su servicio pueda ser obligatorio. En caso de abordaje, el convoy constituido por el buque remolcado y su remolcador será considerado a los efectos de la responsabilidad hacia terceros, como un solo buque, sin perjuicio del derecho de repetición entre sí, de acuerdo con la culpa de cada uno.

Serán aplicables los principios sobre abordaje, cuando un buque cause a otro o a las personas u objetos que se encuentren sobre éste, daños indemnizables, aunque no haya existido contacto efectivo o material entre éstos.

ASISTENCIA Y SALVAMENTO

Artículo 47

Se entiende por asistencia y salvamento, a la ayuda prestada por un buque a otro que se encuentre en peligro o con riesgo de perderse, y que se haya dado con la anuencia del capitán del buque en peligro y siempre que la ayuda recibida produzca el salvamento previsto. En tal caso, el buque asistente tiene derecho a percibir una equitativa remuneración denominada salario de asistencia o de salvamento, la cual no podrá exceder los valores de los bienes salvados.

El auxilio a las personas no da derecho a indemnización de ningún tipo, salvo que exista responsabilidad del propietario o armador del buque auxiliado, o de un tercero en la creación del peligro que lo motivó.

La tripulación del buque auxiliar tienen derecho a una parte equitativa del salario de asistencia o de salvamento acordado a los que hayan salvado bienes en la misma operación, previa deducción de los gastos y daños causados en la operación.

NAUFRAGIOS Y HALLAZGOS

Artículo 48

Se entiende por naufragios, aquellos restos náuticos de buques que se han perdido en el mar o en aguas interiores a consecuencia de un siniestro de la navegación, o que sin perderse se encuentren abandonados y perdido su condición o habilidad para navegar.

Todo interesado en reflotar, extraer o demoler un buque o artefacto naval o restos náuticos en aguas jurisdiccionales salvadoreñas, deberá solicitar autorización a la AMP, quién notificará el pedido a los titulares del buque o publicará el pedido en caso desconocerse su identidad.

Producido el reflotamiento o extracción del buque o artefacto naval, quien haya realizado la operación tendrá derecho a ser reembolsado por los titulares del buque o con cargo a los restos que rescate, de los gastos realizados y de los daños sufridos y a percibir una remuneración que se calculará de acuerdo con el valor de lo recuperado.

En caso de que se trate de recuperar bienes con valor histórico o arqueológico, situados en el mar territorial salvadoreño y sus aguas interiores, en la zona contigua, y en la plataforma continental; la AMP emitirá la respectiva autorización de conformidad a los procedimientos establecidos por la entidad nacional responsable sobre la materia.

RECUPERACIÓN DE OBJETOS

Artículo 49

Todo el que recupere de las aguas o en las playas de mares, ríos o lagos navegables, accesorios o cargas de buques que hayan sido arrojados por necesidad del buque o como consecuencia de un accidente, deberán entregarlas a la AMP, teniendo derecho a ser reembolsado por su propietario de los gastos incurridos en su recuperación. En caso de no poder identificarse al propietario responsable, podrán reembolsarse los gastos del valor de las mercancías recuperadas.

AVERÍA

Artículo 50

Se entiende por avería en general, todo daño o pérdida que pueda sobrevenir en el curso de una expedición marítima sobre el buque o los efectos transportados, o gastos de carácter excepcional o anormal realizados durante ella, con la finalidad de salvar la expedición. Quedan al margen de este concepto todos los gastos comunes u ordinarios a toda travesía marítima, tales como, derechos de puerto, costo de prácticos, remolque y en general todo gasto razonablemente previsible para el armador.

CLASIFICACIÓN DE LAS AVERÍAS

Artículo 51

1. Avería Simple: Son aquellas que en caso de ocurrencia deben ser soportadas por el dueño de la cosa que ocasionare o sufre el gasto extraordinario.

2. Avería Gruesa: Son aquellas que en caso de ocurrencia deben ser soportadas por el conjunto de los intereses vinculados a la expedición, debido a que las mismas han sido causadas o producidas en beneficio común de todos los interesados.

DESIGNACIÓN DE LIQUIDADOR

Artículo 52

Todos los interesados en la expedición que hayan declarado avería gruesa deberán firmar un compromiso de avería y a depositar o extender una fianza a satisfacción del transportador, para responder al pago de su respectiva contribución y a remitir al Liquidador que se designe, la documentación que justifique el valor de los bienes afectados a la avería, a fin de que éste realice la liquidación y determine el valor de contribución de cada afectado.

Los actos y contribuciones en concepto de avería gruesa se registrarán, salvo convención especial celebrada por las partes interesadas, por las Reglas de York - Amberes.

Capítulo V DEL PERSONAL DE NAVEGACIÓN

AUTORIZACIÓN E INSCRIPCIÓN DEL PERSONAL

Artículo 53

Ninguna persona puede formar parte de la tripulación de los buques o artefactos navales inscritos en el REMS, o ejercer profesión, oficio u ocupación alguna en la jurisdicción portuaria, o en actividad regulada o controlada por la Autoridad Marítima Portuaria, si no es autorizada por ésta e inscrita en la sección respectiva del REMS.

REQUISITOS TÉCNICOS, ACADÉMICOS Y DE IDONEIDAD DEL PERSONAL

Artículo 54

La AMP reglamentará los requisitos mínimos de idoneidad profesional que deberán cumplir y consecuentemente acreditar todo el personal que desempeñe funciones en el ámbito de la industria marítima.

AGRUPAMIENTO DEL PERSONAL

Artículo 55

El personal de los buques, y artefactos navales, y el integrado por quienes ejercen profesiones, oficios y ocupaciones conexas con las actividades marítimas, fluviales, lacustres, que se desempeñen en tierra, se agrupa en:

1. Personal embarcado: el que ejerce profesión, oficio u ocupación a bordo de buques y artefactos navales.
2. Personal terrestre de la navegación: el dedicado a ejercer profesión, oficio u ocupación en jurisdicción portuaria, pero en conexión con la actividad marítima, fluvial y lacustre, tales como la de remolcadores o embarcaciones menores auxiliares del puerto.

La AMP, reglamentariamente deberá establecer los requisitos de idoneidad y capacidad que deberá poseer toda persona que integre las tripulaciones de los buques y artefactos navales, de acuerdo con la normativa técnica sobre la materia.

EMBARQUE Y DESEMBARQUE DE PERSONAL

Artículo 56

El embarque o desembarque del personal en puerto salvadoreño, a que se refiere el artículo anterior, se efectuará mediante la coordinación de la Autoridad Marítima Portuaria Local, con las autoridades de Migración designadas en el respectivo puerto. La AMP deberá asentar constancias respectivas en el REMS.

FORMA ORGÁNICA DEL PERSONAL DEL BUQUE

Artículo 57

Conforme con su función específica, el personal embarcado estará clasificado y asignado según su especialidad en las áreas operacionales siguientes:

1. Cubierta;
2. Máquinas;
3. Comunicaciones;
4. Administración; y
5. Practicaje.

La autorización que otorgue la AMP facultará a sus titulares a ejercer los cargos máximos que se determinen en el reglamento respectivo.

Cuando no se disponga de personal habilitado en un nivel determinado para cubrir algún servicio, las autoridades competentes, a pedido del armador o capitán, pueden autorizar temporalmente a personal de un nivel inferior de habilitación, hasta tanto haya personal disponible y siempre que ello no afecte la seguridad de la navegación, ni la de la vida humana en el mar.

Capítulo VI DEL CAPITAN

DEL COMANDANTE DEL BUQUE

Artículo 58

Todo buque deberá contar con el mando de un comandante o capitán, quien será la máxima autoridad a bordo y la encargada de la dirección y gobierno del buque, ejerciendo la representación del armador o del propietario según sea el caso. El Capitán, a bordo, representa al Estado de Pabellón del buque.

ATRIBUCIONES

Artículo 59

Compete especialmente al Capitán:

1. Resolver todas las cuestiones que se susciten en navegación, entre tripulantes o pasajeros, o entre unos y otros;
2. Autorizar licencias a la tripulación para bajar a tierra o permanecer fuera del buque, de acuerdo con las exigencias del servicio;
3. Disponer sobre la organización de los servicios del buque, de acuerdo con las normas legales o reglamentarias vigentes;
4. Disponer el abandono del buque en peligro cuando sea razonablemente imposible su salvamento; y

5. Toda otra facultad que le otorguen las leyes o reglamentos vigentes.

RESPONSABILIDAD

Artículo 60

El Capitán, aun cuando estará obligado a utilizar los servicios de un práctico, será directamente el responsable de la conducción, maniobra y gobierno del buque, sin perjuicio de la responsabilidad que corresponde al práctico por su defectuoso asesoramiento. La autoridad del Capitán no se subroga a la del práctico.

DEBER DE SERVICIO

Artículo 61

El Capitán, desde el momento que formaliza su embarco ante la Autoridad Marítima, estará al servicio permanente del buque.

DELEGACIÓN DE LA AUTORIDAD PÚBLICA

Artículo 62

El capitán es delegado de la autoridad pública para la conservación del orden, seguridad y salvamento del buque; y para su seguridad y salvación, así como la de los pasajeros, tripulantes y carga. Los tripulantes y pasajeros le deben respeto y obediencia al capitán o quien haga sus veces, en todo cuanto concierne a las referidas funciones.

OBLIGACIONES

Artículo 63

En su carácter de delegado de la autoridad pública, para la seguridad y salvación de las personas, la carga o el buque, el Capitán estará especialmente obligado a:

1. Verificar que el buque sea idóneo para el viaje a emprender y que esté armado y tripulado reglamentariamente;
2. Verificar el buen arrumaje y distribución de los pesos a bordo y el cumplimiento de las normas sobre seguridad de la carga y estabilidad del buque;
3. Rechazar la carga que considere peligrosa para la seguridad del buque u otras cargas que, teniendo tal característica, no estén acondicionadas de acuerdo con las reglamentaciones nacionales o internacionales, y arrojar al agua la que se vuelva peligrosa durante el viaje;
4. Efectuar las inspecciones destinadas a verificar el cumplimiento de los servicios y el estado material del buque;
5. Disponer la ejecución de zafarranchos y la instrucción del personal del buque y de los pasajeros, en todo lo relativo a servicios de emergencia, de acuerdo con lo establecido en leyes y reglamentos vigentes;
6. Adoptar, en caso de peligro, todas las medidas que estén a su alcance para la salvación de las personas, el buque y la carga que se encuentren a bordo, realizando, si fuere necesario, una arribada forzosa o pidiendo auxilio;
7. Tomar los prácticos necesarios en los lugares en que los reglamentos o la prudencia lo exijan;

8. Encontrarse en el puente de mando, en las entradas y en las salidas de los puertos, en los pasajes por canales balizados, estrechos o lugares de navegación restringida, en caso de niebla, en navegación por zonas de intenso tránsito y, en general, en toda otra circunstancia en que los riesgos sean mayores;
9. Todas las maniobras de arribo, amarre y desamarre, y zarpe de puerto, se efectuarán bajo la responsabilidad directa del capitán del buque, a cuyo efecto todos los que colaboren en ello deben obedecer sus órdenes e instrucciones;
10. Velar por el cumplimiento de las disposiciones legales y reglamentarias referentes al alojamiento y alimentación de la tripulación y de los pasajeros y por el buen estado sanitario e higiénico del buque;
11. No abandonar el buque en peligro, sino después de haber agotado todos los medios de salvación, y luego de emplear la mayor diligencia para salvar personas, cargas y documentos de a bordo, correspondiéndole, en todos los casos, ser el último en dejar el buque;
12. Acudir en auxilio de las vidas humanas, aun de enemigos que se encuentren en peligro en el mar, de acuerdo con lo establecido en las convenciones internacionales incorporadas al ordenamiento jurídico nacional. Cesará esta obligación cuando ella signifique un serio peligro para el buque o las personas en él embarcadas, o cuando tenga conocimiento de que el auxilio estará asegurado en mejores o iguales condiciones que las que él podría ofrecer, o cuando tenga motivos razonables para prever que su auxilio es inútil. De estas causas deberá dejar constancia en el diario de navegación;
13. Después de un abordaje, y siempre que pueda hacerlo sin peligro para su buque, tripulación y pasajeros, prestará auxilio al otro buque, a su tripulación y pasajeros, y comunicará a este último buque, en la medida de lo posible, el nombre del suyo y su puerto de matrícula, así como los puertos de donde procede y a donde se dirige;
14. En caso de siniestro, agotará los recaudos o actuaciones tendientes a encontrar a los desaparecidos, siempre que a su juicio ello no implique riesgos graves para la seguridad de las personas, buque y carga;
15. Presentarse en forma inmediata a su llegada a puerto salvadoreño, ante la Autoridad Marítima o ante la Autoridad Marítima de puerto extranjero, para levantar una exposición sobre los hechos extraordinarios ocurridos durante el viaje y de interés para la Autoridad Marítima, con transcripción de la parte pertinente del diario de navegación; y
16. Cumplir y hacer cumplir toda obligación legal o reglamentaria que le sea impuesta en consideración a sus funciones de delegado de la autoridad pública, o como representante del armador, en lo que se refiere a las relaciones de éste con las autoridades.

FUNCIONES DEL CAPITÁN COMO DELEGADO DE LA AUTORIDAD PÚBLICA

Artículo 64

En su carácter de delegado de la autoridad pública, el Capitán ejercerá funciones de policía, y en tal carácter le compete:

1. Mantener el orden interior del buque, e imponer las sanciones establecidas por las leyes y reglamentos respectivos, por las faltas cometidas por tripulantes o pasajeros a bordo;
2. En caso de delito, ordenar e instruir la investigación prevención correspondiente con apego arreglo a lo dispuesto por la legislación penal salvadoreña. Cesa su intervención al llegar a puerto, donde en un plazo no mayor de veinticuatro horas deberá comunicar de los acontecimientos con las correspondientes pruebas, a la Autoridad Marítima si se trata de puerto salvadoreño, o a la Autoridad Marítima del país extranjero si se trata de puerto no salvadoreño;

3. Comunicar de inmediato y por el medio más rápido a la autoridad marítima o consular salvadoreña más cercana, todo accidente de navegación ocurrido al buque o causado por él, y cualquier otra novedad de importancia observada en la ruta que afecte a la navegación; y

4. Aprobar todo embarque o desembarque de personas o cosas, teniendo la facultad de rechazar su embarque o desembarque cuando existan causas que así lo justifiquen y que puedan poner en peligro la expedición.

ACTAS DE REGISTRO CIVIL

Artículo 65

En su carácter de oficial de registro civil y de conformidad a las Leyes de la República vigentes sobre la materia, el Capitán de un buque a bordo de éste, está facultado para efectuar matrimonios y asentar las actas respectivas en el Diario de Navegación. El Capitán deberá asentar a su vez en este diario las actas de los nacimientos y defunciones que ocurran a bordo.

En caso de desaparición o fallecimiento de personas, instruirá la información sumaria pertinente, y consignará en el Diario de Navegación las circunstancias principales de la desaparición, y las medidas adoptadas para la búsqueda y salvamento.

De todos estos actos, el Capitán deberá presentar la documentación correspondiente a las autoridades civiles salvadoreñas en su próxima arribada a puerto nacional, e informar de dichos actos oficialmente a la AMP, de conformidad a reglamento que ésta establezca para esos efectos.

TESTAMENTO

Artículo 66

El capitán estará facultado para otorgar testamentos marítimos, de forma pública o cerrada, de conformidad a los procedimientos siguientes.

En caso de testamento público el Capitán recibirá la manifestación de voluntad del testador, la cual deberá ser extendida por escrito y suscrita por el interesado, el capitán y un oficial del buque, quienes acreditarán la veracidad y existencia del acto.

Para el caso de testamento cerrado, el Capitán recibirá la manifestación del testador por escrito y en sobre cerrado, procediendo a lacrar su contenido en presencia del interesado y de un oficial del buque.

El Capitán deberá dar a conocer de estos actos oficialmente a las autoridades marítimas del puerto de próximo arribo, dejando constancia de todo ello en el diario de navegación.

MUERTE O IMPEDIMENTO DEL CAPITÁN

Artículo 67

En caso de muerte o impedimento del capitán, asumirá el mando del buque, el oficial de cubierta de mayor jerarquía, quien a su vez será reemplazado por el oficial del mismo cuerpo que le sigue en orden de cargo. En última instancia, el mando del buque será asumido por el hombre de la tripulación que ejerza las funciones de conmaestre.

La persona que asumirá el mando del buque lo hará con todas las prerrogativas, facultades, obligaciones y

responsabilidades inherentes a la función del Capitán, hasta que se disponga su sustitución por el armador o la Autoridad Marítima o consular.

RECHAZO DE TRIPULANTE

Artículo 68

En ningún caso el Capitán estará obligado a aceptar tripulantes con cuya permanencia a bordo no esté de acuerdo.

Si el tripulante no aceptado hubiere sido destacado por el organismo encargado de la colocación de la gente de mar, el Capitán deberá expresar las razones del rechazo en un acta en que se dejará constancia del descargo que formule el interesado. El levantamiento y registro de dicho procedimiento no impedirá la salida del buque.

DEBER DE OBEDIENCIA

Artículo 69

El Capitán deberá obedecer toda orden o instrucción impartida por un buque militar o policial salvadoreño, en mar libre y en aguas territoriales salvadoreñas.

APLICACIÓN EXTENSIVA

Artículo 70

Las funciones, facultades, obligaciones y responsabilidades que emergen de los artículos precedentes del presente Capítulo, serán aplicables a toda persona autorizada o habilitada para mandar un buque o embarcación, con las limitaciones que determine el título profesional del cual se trate y la navegación que se efectúe.

Capítulo VII DE LA TRIPULACIÓN

CATEGORÍA DEL PERSONAL

Artículo 71

Las categorías básicas del personal de la navegación, por orden de jerarquía, son las siguientes:

- 1) Capitán;
- 2) Oficiales;
- 3) Habilitados con título no superior;
- 4) Maestranza; y
- 5) Marinería.

La reglamentación fijará dentro de cada categoría los niveles de capacidad.

OBLIGACIONES DE LOS TRIPULANTES

Artículo 72

Los tripulantes estarán obligados de conformidad con lo establecido por la norma legal laboral específica, las convenciones colectivas de trabajo y las estipulaciones especiales del contrato individual; a:

1. Encontrarse a bordo el día y hora señalados por el Capitán;
2. No ausentarse del buque ni de su puesto, en caso de encontrarse de servicio, sin expresa autorización de su superior jerárquico;
3. Colaborar con el capitán en cualquier acontecimiento de la navegación que afecte la seguridad o salvación de los pasajeros, del buque, o de la carga;
4. Velar por el mantenimiento de la regularidad del servicio y del material a su cargo, y por la conservación del orden interno del buque; y
5. Prestar auxilio al Capitán u oficial que actúe en su nombre, cuando éste se vea obligado a usar la coerción para mantener su autoridad y, restablecer el orden, en el ejercicio de sus funciones o con motivo de ellas.

DOTACIÓN MÍNIMA

Artículo 73

La AMP, mediante reglamento respectivo, establecerá el número de tripulantes que todo buque o artefacto naval deberá asignar para asegurar su efectiva navegación y servicio en puerto, con sus elementos fundamentales de seguridad y salvamento, así como para que operen normal y eficientemente en las actividades que el armador o explotador los destine.

Capítulo VIII DE LOS PRÁCTICOS

OBLIGACIONES DE LOS PRÁCTICOS

Artículo 74

Son obligaciones del práctico:

1. Embarcarse a bordo del buque que debe pilotear y permanecer en él hasta la salida de su zona de practica, o hasta que sea amarrado o fondeado en el lugar asignado;
2. Sugerir la ruta y las maniobras necesarias para la debida y segura conducción del buque;
3. Asesorar al Capitán en todo cuanto le sea requerido a los efectos de la navegación, ruta, gobierno, maniobra y seguridad del buque en su zona;
4. Dar directamente órdenes referentes a la conducción y maniobra, cuando sea autorizado por el Capitán y bajo su inmediata vigilancia o la de su reemplazante reglamentario;
5. Informar a los capitanes de buques extranjeros acerca de las reglamentaciones especiales sobre navegación en la zona;
6. Vigilar y exigir en los buques extranjeros el cumplimiento de las leyes y reglamentos vigentes; y
7. Dar cuenta de inmediato y por el conducto más rápido a la Autoridad Marítima más cercana, de todo acontecimiento extraordinario y de toda infracción a las leyes y reglamentos vigentes que se cometan a bordo del buque que pilotea o por otros que naveguen en la zona.

PRACTICAJE OBLIGATORIO

Artículo 75

El practicaje en aguas jurisdiccionales salvadoreñas constituye un servicio público regulado y controlado por la AMP, quién determinará la obligación de utilizar el servicio para todos los buques salvadoreños o extranjeros.

La reglamentación que la AMP dicte al respecto fijará la forma y modalidad de su uso, así como también las disposiciones regulatorias con las tarifas correspondientes.

Capítulo IX DEL ARMADOR

DEBER DE INSCRIPCIÓN

Artículo 76

La persona o entidad que desempeñe las funciones de armador de un buque de matrícula salvadoreña deberá inscribirse como tal en el REMS. Las inscripciones deberán ser cumplidas también por el propietario, cuando el armador las omita.

En defecto de inscripción, responderán frente a terceros el armador y el propietario solidariamente, pero este último estará exento de responsabilidad en el caso de que aquél haya dispuesto del uso del buque en virtud de un hecho ilícito con conocimiento del acreedor.

REQUISITOS DE INSCRIPCIÓN

Artículo 77

La inscripción de armador de un buque deberá hacerse con la transcripción del título o contrato en virtud del cual adquiere ese carácter. La misma se anotará también en el certificado de matrícula del buque.

RESPONSABILIDAD DEL ARMADOR

Artículo 78

El armador es responsable de las indemnizaciones a favor de terceros, a que haya dado lugar por hecho suyo o de los tripulantes, con motivo de las obligaciones contractuales contraídas por el Capitán, en todo lo relativo al buque o artefacto naval y a la expedición.

No responde el armador, en el caso de que el Capitán habiendo sido advertido no haya procedido como corresponde o se haya prestado a hechos ilícitos cometidos por los cargadores, salvo la responsabilidad personal del Capitán.

En el caso del inciso anterior, los responsables quedan sujetos a las leyes del Estado Rector.

LIMITACIÓN DE LA RESPONSABILIDAD DEL ARMADOR

Artículo 79

El armador podrá limitar su responsabilidad, establecida en el artículo anterior, salvo que: exista culpa de su parte con relación a los hechos que den origen al crédito reclamado; al valor que tenga el buque al final del viaje en que tales hechos hayan ocurrido, más el de los fletes brutos; el de los pasajes percibidos o a percibir por ese viaje; y el de los créditos a su favor que hayan nacido durante el mismo.

CRÉDITOS ALCANZADOS

Artículo 80

Los créditos frente a los cuales el armador podrá invocar la limitación autorizada, son los originados en las siguientes causas:

1. Muerte o lesiones corporales de cualquier persona;
2. Pérdida de bienes o de derechos, o daños sufridos en ellos; y
3. Responsabilidad u obligación emergente de la remoción de restos náufragos, o de reflotamiento de un buque hundido o varado, o de daños causados a obras de arte de un puerto o vías navegables.

El beneficio podrá ser invocado aun en el caso de que la responsabilidad del armador derive de la propiedad, posesión, custodia o control del buque, si no se prueba su culpa o la de sus dependientes de la empresa terrestre.

CRÉDITOS EXCLUIDOS

Artículo 81

La limitación de responsabilidad no puede ser invocada frente a créditos provenientes de asistencia y salvamento, contribución de avería gruesa, los del capitán o de sus tripulantes o de los respectivos causahabientes que tengan su origen en el contrato de ajuste, y de los otros dependientes del armador, cuyas funciones se relacionan con el servicio del buque.

PERSONAS COMPRENDIDAS DENTRO DE LA LIMITACIÓN

Artículo 82

La limitación de responsabilidad establecida en los artículos precedentes, podrá ser invocada también por el propietario del buque o por el transportador, cuando sea una persona o entidad distinta del armador, o por sus representantes o por los del armador o por el Capitán y miembros de la tripulación en las acciones ejercidas contra ellos. Si se demanda a dos o más personas, la indemnización total no podrá exceder la referida limitación.

CAPITULO X REGIMEN DE RESPONSABILIDAD DE LOS ARMADORES

RESPONSABILIDAD DEL ARMADOR

Artículo 83

El armador o transportador de mercancías por agua, debe asegurar al dueño de la carga la entrega de las mercancías en destino en la misma forma, peso, cantidad y estado en que la recibió. La responsabilidad del armador o transportista comienza cuando la carga le es entregada bajo su custodia, haya sido o no cargada sobre el buque, y cesa cuando la misma es entregada a su consignatario en el puerto de destino y haya transferido la órbita de su responsabilidad y custodia.

El armador o transportador procederá en forma conveniente y apropiada a la carga, manipuleo, estiba, transporte, custodia y descarga de la mercancía transportada.

LIMITE DE RESPONSABILIDAD

Artículo 84

La responsabilidad del armador o transportador del buque por las pérdidas o daños que sufran las mercancías transportadas, podrá limitarse a dos Derechos Especiales de Giro por kilogramo de peso bruto de las mercancías perdidas o dañadas; de igual manera, si se trata de mercancías cargadas por bulto o pieza, por cada unidad de flete, excepto por aquellas mercancías en las cuales el cargador haya declarado el valor antes del embarque.

Cuando el transporte se realice en contenedores o artefacto unitario de carga, todo bulto o unidad enumerado en el conocimiento de embarque como unidad o bulto, será considerado a los fines de la limitación anterior.

En ningún caso el monto a indemnizar excederá el valor según factura de la mercancía perdida o dañada.

PERIODO DE RESPONSABILIDAD

Artículo 85

El Armador o Transportador será responsable de los perjuicios resultantes de la pérdida o daño de las mercancías, si el hecho que causa la pérdida o el daño se produjo durante el período en que las mercancías se encontraban bajo su custodia, salvo que pruebe que él, sus empleados, representantes u otras personas a quien haya encomendado la prestación del servicio, adoptaron las medidas que razonablemente podían exigirse para evitar el hecho y sus consecuencias.

CONCURRENCIA DE OTRAS CAUSAS

Artículo 86

Cuando el armador o transportador marítimo, sus empleados, mandatarios u otras personas a cuyo cuidado se haya encomendado la prestación del servicio, no hubieran adoptado las medidas a que se refiere el artículo anterior, y ese incumplimiento concorra con otra causa para ocasionar la pérdida o el daño, el armador o transportador será responsable sólo en la medida en que los perjuicios resultantes puedan atribuirse a tal incumplimiento y siempre que pueda probar el monto de los perjuicios que no le pueden ser atribuidos personalmente.

RESPONSABILIDAD OBJETIVA

Artículo 87

El Armador o Transportador Marítimo no podrá limitar su responsabilidad, si se prueba que la pérdida, el daño o el retraso provinieron de una acción u omisión del propio Armador o Transportador marítimo o de sus empleados o mandatarios, realizada con intención de causar tal pérdida o daño, o intencionalmente y a sabiendas que sobrevendrían dicha pérdida o daño.

Esta disposición será igualmente aplicable al empleado o mandatario del Armador o Transportador Marítimo, u otra persona a cuyos servicios éste haya encomendado la prestación de sus servicios, a quien se exija directamente su responsabilidad, si se prueba que la pérdida, el daño o el retraso provinieron de una acción u omisión de ese empleado, mandatario o persona, realizada con intención de causar tal pérdida o daño, o intencionalmente y a sabiendas que sobrevendrían dicha pérdida o daño.

RECEPCION DE MERCANCIAS

Artículo 88

Al momento de recibir las mercancías, el Armador o transportador marítimo deberá emitir por escrito los documentos necesarios en los que se identifiquen las mercancías y se acuse recibo de su recepción, indicando fecha en que fueron recibidas, y se haga constar su estado y cantidad, dicho documento podrá incorporar las condiciones generales de los conocimientos de embarque utilizados por los porteadores.

PRESUNCION DE RECIBO DE MERCANCIAS EN BUEN ESTADO

Artículo 89

Si el armador o transportador no emite los documentos a que se refiere el artículo anterior, se presumirá, salvo prueba en contrario, que ha recibido las mercancías en buen estado.

INTERCAMBIO ELECTRONICO DE DATOS

Artículo 90

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

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

PLAZO PARA DAR AVISO

Artículo 91

El operador portuario, el consignatario o cualquier otra persona facultada para recibir las mercancías de manos del armador o transportador marítimo, dispondrá de un lapso de tres días hábiles contados desde la fecha en que haya recibido dichas mercancías, para dar aviso ante el armador o transportador marítimo de pérdida o daño, especificando la naturaleza del perjuicio sufrido.

Se presume, salvo prueba en contrario, que el armador o transportador marítimo ha entregado las mercancías en buen estado, si no se hubiere dado el aviso señalado en el inciso anterior.

INSPECCIONES

Artículo 92

Cuando se hubiere dado el aviso de pérdida o daño conforme al artículo anterior, el operador portuario, el consignatario o la persona facultada para recibir las mercancías y el armador o transportador, darán todas las facilidades razonables para la inspección de las mercancías y la comprobación del número de bultos.

No obstante, si el operador portuario, el consignatario o la persona facultada para recibir las mercancías hubieren participado en un examen o una inspección de las mismas, documentada mediante acta suscrita por ambas partes en el momento que fueron puestas en su poder por el armador o transportador, se omitirá el régimen de avisos y presunciones establecidas en el artículo precedente.

RESPONSABILIDAD CONTRACTUAL Y EXTRA CONTRACTUAL

Artículo 93

Las exoneraciones y límites de responsabilidad establecidas en este Capítulo, serán aplicables a toda acción contra el operador o administrador portuario respecto de la pérdida o el daño de la mercancía, o daños a los buques, independientemente que la acción se fundamente en la responsabilidad contractual, la responsabilidad extracontractual o en otra causa.

MERCANCIAS PELIGROSAS

Artículo 94

Cuando fueren puestas en poder del armador o transportador marítimo mercancías peligrosas que no estén marcadas, etiquetadas, embaladas o documentadas como tales, o si en el momento de hacerse cargo de ellas, no ha tenido conocimiento por otro medio de su carácter peligroso, aquel tendrá derecho a adoptar cualquiera de las siguientes medidas o conjunto de éstas:

1. Adoptar todas las precauciones que exijan las circunstancias del caso, y en particular, cuando las mercancías constituyan un peligro inminente a las personas o los bienes, para destruir dichas mercancías, a transformarlas en inofensivas o a deshacerse de ellas por otros medios lícitos, sin que haya lugar al pago de una indemnización por el daño o la destrucción de éstas, ocasionadas por la adopción de estas medidas, para lo cual, en todo caso, deberá seguir los procedimientos fijados en el reglamento respectivo de manejo de mercancías peligrosas;
2. A ser reembolsado de todos los gastos en que hubiere incurrido por la adopción de las medidas a que se refiere el numeral anterior, de parte de la persona que no haya cumplido la obligación de hacer notar la peligrosidad de tales mercancías; y
3. A adoptar todas las precauciones especificadas en el Código Marítimo Internacional de Mercancías Peligrosas (IMDG), de Naciones Unidas, del año 1965.

Capítulo XI DEL AGENTE MARÍTIMO

AGENTE MARÍTIMO

Artículo 95

El Agente Marítimo es la persona designada por el propietario, armador o Capitán para realizar ante las Autoridades Marítimas, Portuarias y Aduaneras, las gestiones relacionadas con la atención de un buque en puerto salvadoreño. Dicho agente marítimo tiene la representación activa y pasiva, judicial y extrajudicial, conjunta o separadamente, de su Capitán, propietario o armador, ante los entes públicos y privados, a todos los efectos y responsabilidades del viaje que el buque realice a dicho puerto o desde el mismo y hasta tanto se designe a otro en su reemplazo. No tiene la representación del propietario ni del armador que estuviere domiciliado en el lugar.

El Agente Marítimo, por el solo hecho de solicitar la atención de una nave, se entenderá investido de representación suficiente para todos los efectos subsecuentes, sin perjuicio de tener que acreditar su nombramiento con posterioridad.

REPRESENTACIÓN

Artículo 96

La representación ante los entes privados y públicos prevista en el artículo anterior, subsiste aun en el caso de renuncia, hasta tanto el propietario, armador o capitán designen al reemplazante. La sustitución podrá hacerse aunque el buque haya zarpado de puertos salvadoreños.

DENUNCIA DEL DOMICILIO DEL ARMADOR

Artículo 97

El Agente Marítimo de un buque, en su primera gestión, denunciará ante la AMP el domicilio correspondiente al Armador del buque que se encuentra representando.

En el respectivo reglamento se establecerá todo lo atinente a las designaciones de los agentes marítimos, que se registren en la AMP.

RESPONSABILIDAD

Artículo 98

El Agente Marítimo, en cualquiera de sus designaciones, no responderá por las obligaciones de su representado, salvo la responsabilidad que le corresponde por sus hechos personales o los que surjan de las leyes y reglamentos fiscales y administrativos.

Capítulo XII DEL EJERCICIO DE LA NAVEGACIÓN

REPRESENTACIÓN LEGAL DEL CAPITÁN

Artículo 99

El capitán es representante legal del propietario y del armador del buque no domiciliado en el lugar, en todo lo referente al buque y a la expedición, sin perjuicio del mandato especial que pueda conferírsele.

REPRESENTACIÓN

Artículo 100

En los puertos donde el armador o el propietario no tengan su domicilio, el capitán ejercerá la representación judicial activa y pasiva de aquellos en todos los asuntos relacionados con la expedición. En las mismas circunstancias, y siempre que el puerto no sea el lugar del domicilio del fletador o del respectivo cargador, tendrá también la representación de éstos a fin de salvaguardar los intereses de la carga.

RECIBO DE LA CARGA

Artículo 101

De los efectos que se carguen a bordo, el Capitán o quien lo represente hará constar en los recibos provisionales el estado y condición aparente de la mercancía. En los recibos provisionales de los efectos que se carguen a bordo, el Capitán o quien lo represente hará constar el estado y condición aparente de la mercancía.

RESPONSABILIDAD POR LA CARGA

Artículo 102

El Capitán tendrá, el carácter de depositario de la carga y de cualquier efecto que reciba a bordo, en representación del armador; y como tal, estará obligado a cuidar de su apropiado manipuleo en las operaciones de carga y descarga, de su buen arrumaje y estiba, de su custodia y conservación, y de su pronta entrega en el puerto de destino.

Salvo pacto en contrario, la responsabilidad del Capitán respecto de la carga, comenzará desde que la recibe y termina con el acto de la entrega en el lugar en que se haya pactado, o en el que sea de uso en el puerto de descarga.

DEBER DE COMUNICACIÓN

Artículo 103

El Capitán, dentro de sus posibilidades, deberá mantenerse durante el viaje en continuo contacto con la AMP, para tenerla al corriente de todos los acontecimientos relativos a la expedición, y requerirle instrucciones en los casos que sean necesarios. Los correspondientes mecanismos se establecerán reglamentariamente.

REGISTRO DE AVERÍA GRUESA

Artículo 104

El Capitán, cuando se vea en la necesidad de realizar un acto de avería gruesa, deberá asentar en el diario de navegación, con toda minuciosidad, sus causas, las circunstancias que mediaron en ella y el detalle del sacrificio realizado.

TÍTULO III DE LOS CONTRATOS DE UTILIZACIÓN DE LOS BUQUES Capítulo I DEL CONTRATO DE LOCACIÓN

INSCRIPCIÓN DEL CONTRATO DE BUQUE LOCADO

Artículo 105

El contrato de locación de buque deberá otorgarse por escrito, y para ser invocado frente a terceros, debe estar inscrito en el REMS.

SUBLOCACIÓN

Artículo 106

El locatario no podrá sublocar el buque, ni ceder el contrato sin autorización escrita del locador. Ambos actos deberán satisfacer los requisitos establecidos en el artículo precedente.

ENTREGA Y DEVOLUCIÓN DE BUQUE

Artículo 107

El locador deberá entregar el buque al locatario, en el lugar y tiempo convenidos y con la documentación

necesaria para el viaje, y salvo pacto en contrario, en estado de navegabilidad, en la medida en que con el empleo de una diligencia razonable pueda hacerlo. El locatario deberá devolverlo a la expiración del término estipulado, en el mismo estado, salvo los daños originados por caso fortuito o fuerza mayor o por su uso normal y convenido, libre de tripulación, si así lo hubiere recibido, y de todo crédito privilegiado ocasionado por su explotación o uso.

OBLIGACIÓN DEL LOCADOR

Artículo 108

Es obligación del locador, durante todo el tiempo de la locación, ejercer una diligencia razonable para mantener el buque en el mismo estado de navegabilidad en que fue entregado. El locador será responsable de los daños ocasionados por incumplimiento de esa obligación, salvo que pruebe que se trata de un vicio oculto, que no pudo ser descubierto empleando una diligencia razonable.

USO DEL BUQUE

Artículo 109

El locatario estará obligado a utilizar el buque de acuerdo con sus características técnicas y las modalidades convenidas en el contrato.

LUGAR Y TIEMPO DE RESTITUCIÓN DEL BUQUE

Artículo 110

El locatario deberá restituir el buque a la expiración del término de la locación en el lugar convenido y, en su defecto, en el puerto del domicilio del locador.

PRESCRIPCIÓN

Artículo 111

Todas las acciones derivadas del contrato de locación de buques, prescribirán por el transcurso de un año, contado desde la fecha del vencimiento, rescisión o resolución del contrato, o de la entrega del buque, si fuere posterior y, en caso de pérdida, desde la fecha en que debía ser devuelto.

CAPITULO II DEL CONTRATO DE FLETAMENTO

Obligaciones Genéricas del Fletante

Artículo 112

Son obligaciones del Fletante:

1. Poner el buque fletado a disposición del Fletador en el lugar y tiempo convenidos contractualmente;
2. Ejercer la debida diligencia para colocar al buque fletado en estado de navegabilidad y mantenerlo durante toda la vigencia del contrato en idénticas condiciones;
3. Disponer de todos los elementos necesarios para la operación y funcionamiento del buque fletado, con

su tripulación debidamente embarcada;

4. Disponer de toda la documentación que habilite al buque fletado a navegar hacia los destinos que se le indiquen;
5. Pagar los salarios y gastos de manutención de la tripulación y elementos de cubierta y máquinas;
6. Contratar los seguros necesarios para la navegación; y,
7. Disponer la navegación del buque.

OBLIGACIONES GENÉRICAS DEL FLETADOR

Artículo 113

Son obligaciones genéricas del fletador:

1. Recibir el buque en el lugar y fecha convenidos contractualmente;
2. Pagar todos los costos derivados de la utilización comercial del buque, derechos de puerto y navegación de canales;
3. Utilizar convenientemente el buque fletado, dentro de los límites de seguridad del propio buque fletado;
4. Pagar el flete convenido contractualmente;
5. Reintegrar el buque al fletante en el lugar y tiempo convenido; y
6. Pagar el flete pactado contractualmente y a indicar al fletante en debida forma, los trayectos o rutas que deberá realizar en cumplimiento del contrato.

DERECHOS GENÉRICOS DEL FLETANTE

Artículo 114

Son derechos genéricos del fletante:

1. Abstenerse de navegar el buque fletado cuando pueda quedar expuesto a peligros no previstos en el momento de la celebración del contrato, pudiendo disolver el contrato por imposibilidad de su ejecución;
2. No iniciar el viaje que previsiblemente no vaya a concluir alrededor de la fecha de vencimiento del contrato;
3. Exigir al fletador las indemnizaciones que correspondan a consecuencia de perjuicios experimentados por acciones iniciadas por terceros y derivados de la explotación comercial del buque y que puedan hacerse efectivas sobre el mismo; y,
4. Exigir al fletador el pago del flete, bajo pena de resolución del contrato.

DERECHOS GENÉRICOS DEL FLETADOR

Artículo 115

Son derechos genéricos del fletador:

1. Disponer de las bodegas del buque para el transporte de mercancías;
2. Ordenar al capitán los viajes a realizar;
3. Disponer e instruir al capitán en todo lo referente a la carga, transporte y entrega de la mercancía o personas en destino y documentación;

4. Embarcar un representante para que imparta al capitán las órdenes referentes a la utilización comercial del buque; y,
5. Suspender el pago del flete por causas que no le sean imputables, mientras el buque permanezca innavegable.

RESOLUCIÓN

Artículo 116

El Fletador tiene derecho a resolver el contrato, notificando por escrito al fletante, cuando el buque no sea puesto a su disposición en la época y lugar convenidos. El resarcimiento de los daños y perjuicios queda librado a las circunstancias de cada caso.

GASTOS A CARGO DEL FLETANTE Y DEL FLETADOR

Artículo 117

Son a cargo del fletante el pago de los salarios y los gastos de manutención de la tripulación, seguro del buque y repuestos de artículos de cubierta y de máquinas. Corresponden al fletador todos los gastos de combustible, agua y lubricantes necesarios para el funcionamiento de las máquinas principales y auxiliares, los inherentes a la utilización comercial del buque, y los derechos, tasas y salarios relacionados con la navegación en canales y con los puertos.

NAVEGACIÓN NO PREVISTA EN EL CONTRATO

Artículo 118

El fletante no estará obligado a hacer navegar el buque fuera de los límites geográficos convenidos en el contrato, o en condiciones o lugares que lo expusieren a peligros no previstos en el momento de su celebración. En estos últimos casos, el contrato quedará resuelto si su ejecución resulta imposible por causas no imputables al fletador.

VIAJE QUE EXCEDA EL PLAZO DEL CONTRATO

Artículo 119

Tampoco estará obligado el fletante a iniciar con su buque un viaje que no termine, previsiblemente, alrededor de la fecha del vencimiento del plazo del contrato. Por los días que excedan de dicha fecha, el fletador debe pagar el flete del mercado internacional para este tipo de fletamento, siempre que sea superior al contractual.

DEPENDENCIA DEL CAPITAN

Artículo 120

A los efectos de la gestión náutica del buque, el capitán depende del fletante. También recibirá órdenes del fletador, dentro de lo estipulado en el contrato respecto del uso que haga del buque, especialmente en todo lo referente a la carga, transporte y entrega de efectos en destino, o al transporte de personas, en su caso, y a la respectiva documentación.

RESPONSABILIDAD DEL FLETANTE

Artículo 121

Salvo su responsabilidad en la gestión náutica del buque, el fletante no responde frente al fletador por las obligaciones asumidas por el Capitán en la gestión del transporte, o en el uso que el fletador haga del buque, o por las culpas en que podrían incurrir tanto el capitán como los tripulantes, en lo que respecta al giro o negocio asumido por el fletador.

PAGO DEL FLETE

Artículo 122

Salvo estipulación o uso distinto, el flete deberá pagarse por períodos mensuales y por anticipado, a falta de lo cual el fletante con notificación del fletador, podrá resolver el contrato y retirar el buque de su disposición con una simple orden al capitán. En ese caso, quedará obligado a entregar en destino la carga que tenía a bordo y podrá retener el flete pagadero en dicho lugar.

NO EXIGIBILIDAD DEL FLETE

Artículo 123

El flete no es exigible cuando el fletador, por causas que no le sean imputables, no pueda usar el buque, y, especialmente, cuando éste tenga que inmovilizarse por más de veinticuatro horas para que el fletante cumpla con sus obligaciones relativas a la conservación de su navegabilidad.

Si la inmovilización es ocasionada por una arribada forzosa provocada por peligros del mar, varaduras, averías sufridas por la carga o acto de autoridad nacional o extranjera, el flete se causará durante todo el tiempo que dure la inmovilización, descontando el que corresponda a reparaciones y con deducción de los gastos que su inmovilización haya ahorrado al armador.

En caso de avería común, contribuye el flete de la carga y no el del fletador del buque.

PÉRDIDA DEL BUQUE

Artículo 124

Si el buque se pierde, el flete se deberá hasta el día de su pérdida. Si esta fecha es desconocida, el flete debido se calculará hasta la mitad del plazo transcurrido entre el día de la última noticia que se tuvo del buque y aquel en que debió llegar a destino.

SALARIO DE LA ASISTENCIA O SALVAMENTO

Artículo 125

En el caso de asistencia o de salvamento prestado por el buque, el salario correspondiente se adquirirá por mitades entre el fletante y el fletador, deducidos los gastos, indemnizaciones, participaciones del Capitán y tripulantes, y el importe del flete por los días que durare la operación.

PRESCRIPCIÓN

Artículo 126

Las acciones que se derivan del contrato de fletamento a tiempo, prescribirán por el transcurso de un año, contado desde la fecha de su vencimiento, o desde la fecha en que se rescindió o resolvió el contrato, o desde el día de terminación del último viaje, si es posterior.

PÓLIZA DE FLETAMENTO

Artículo 127

El fletamento total o parcial se prueba mediante la póliza de fletamento, que deberá contener las siguientes menciones:

1. Nombre del Armador;
2. Nombres del Fletante y Fletador con los respectivos domicilios;
3. Nombre del buque, puerto de matrícula, nacionalidad y tonelaje de registro;
4. La designación del viaje o viajes a realizar;
5. Si el fletamento es total o parcial, en este último caso, la individualización de los espacios a disposición del fletador;
6. Si el fletamento corresponde a mercancías, la clase y cantidad, la forma de computarlas, los días convenidos para estadías y sobreestadías;
7. Si es un fletamento con fines específicos o para el transporte de personas; y,
8. El flete y su forma y tiempo de pago

VENTA DEL BUQUE

Artículo 128

Firmada la póliza de fletamento, el contrato subsistirá aunque el buque fuere vendido, teniendo los nuevos propietarios obligación de cumplirlo.

LUGAR PARA CARGA O DESCARGA

Artículo 129

Si la póliza no establece el lugar del puerto donde el buque debe colocarse para cargar o descargar, su designación corresponderá al fletador, salvo disposiciones portuarias en contrario. El lugar deberá ser seguro y permitir al buque permanecer siempre a flote. Si el fletador omitiere hacer la designación del lugar de carga o descarga o si siendo varios los fletadores no se ponen de acuerdo sobre el particular, el fletante, previo requerimiento, podrá elegir dicho lugar.

RESOLUCIÓN

Artículo 130

Salvo estipulación distinta, si el fletante no pusiere el buque a la carga en la época y puerto establecidos en el contrato, el fletador, mediante notificación por escrito a aquél, podrá resolver el contrato, quedando librado del resarcimiento de los daños y perjuicios a las circunstancias del caso.

OBLIGACIONES DE LAS PARTES

Artículo 131

El fletante estará obligado a hacer saber por escrito al fletador que el buque se encuentra en condiciones de recibir o entregar la carga. El fletador deberá efectuar la carga o descarga en el plazo de estadías estipulado en la póliza de fletamento.

ESTADÍAS Y SOBREESTADÍAS

Artículo 132

A falta de estipulación expresa en la póliza de fletamento, la estadía comprenderá únicamente los días de trabajo. Los usos del puerto determinan su duración y el momento a partir del cual deben computarse, así como la duración, monto, época y forma de pago de las sobreestadías. Si al respecto no existieren usos del puerto, se fijarán judicialmente, y la duración de las sobreestadías será la mitad de los días de trabajo correspondientes a las estadías y se computarán por días corridos.

FALTA DE CARGA, VENCIDAS LAS ESTADÍAS

Artículo 133

Si vencidas las estadías pactadas o de las que sean de uso, y que el fletador no cargare efecto alguno, el fletante tendrá derecho a resolver el contrato, exigiendo la mitad del flete bruto estipulado y las sobreestadías, o a emprender viaje sin carga y, finalizado el mismo, a exigir el flete por entero con las contribuciones que se debían y las sobreestadías; salvo explicación expresa contenida en la póliza del fletamento.

CARGA INCOMPLETA

Artículo 134

Cuando el fletador sólo embarque durante las estadías una parte de la carga, vencido el plazo respectivo y el de las sobreestadías, y salvo convenio expreso en la póliza de fletamento, el fletante tendrá la opción de proceder a la descarga, por cuenta del fletador, exigiendo el pago de la mitad del flete bruto, o de emprender el viaje con la carga que tenga a bordo y reclamar el flete íntegro en el puerto de destino, con los demás gastos mencionados en el artículo precedente. La decisión que adopte el fletante, tanto en estos casos como en los del artículo anterior, se deberá asentar en la protesta que será notificada al fletador.

AVERÍA GRUESA

Artículo 135

Cuando en los casos previstos en los dos artículos anteriores, se produzca durante el viaje una avería gruesa, la contribución de la carga será por los dos tercios del valor de lo no cargado, además de la que corresponde, en su caso, a lo cargado.

RESOLUCIÓN POR EL FLETADOR

Artículo 136

El fletador, antes del vencimiento de las estadías, tiene derecho a resolver el contrato, pagando si no mediare estipulación contraria, la mitad del flete bruto y, en su caso, los gastos de descarga y las sobreestadías. Si el fletamento es por viaje redondo, debe pagar la mitad del flete de ida.

CARGA SUFICIENTE

Artículo 137

Cuando el fletamento es total, el fletador podrá obligar al fletante a emprender el viaje si el buque tiene a bordo carga suficiente para el pago del flete, sobreestadías y demás obligaciones contractuales y para los gastos suplementarios que le ocasione el cargamento incompleto, o si diese fianza suficiente para dicho pago. En tal caso, el fletante no puede recibir carga de terceros, sin consentimiento por escrito del fletador.

CARGA DE TERCEROS

Artículo 138

En los casos en que el fletante tiene derecho a emprender viaje sin carga o con sólo una parte de ella, podrá por su sola voluntad, tomar carga de terceros a los efectos de la seguridad del flete y de las otras indemnizaciones a que haya lugar. Si de esta nueva carga resultare una pérdida de flete, el fletador será deudor por la diferencia. Si por el contrario, con dicha carga se produjere ganancia, ésta pertenecerá al fletador, sin perjuicio de los pagos a que esté obligado por los artículos precedentes.

COMISIÓN DE LA DESCARGA

Artículo 139

Si transcurrida la mitad de las estadías contractuales o de las que sean de uso, el fletador o los tenedores de los respectivos conocimientos o manifiestos de carga no hubiere empezado la descarga, o si habiéndola iniciado no estuviere terminada al vencimiento de aquéllas, salvo convenio expreso en la póliza de fletamento, el fletante podrá descargar a tierra o a lanchas por cuenta y riesgo del fletador o consignatario. Si éstos tuvieren domicilio conocido en el lugar, deberá notificárseles.

BLOQUEO DEL PUERTO DE DESTINO

Artículo 140

Si después de iniciado el viaje se declara el bloqueo del puerto de destino, el fletante deberá intimar al fletador para que indique, dentro de las cuarenta y ocho horas, el puerto de descarga de la mercancía. Éste deberá estar en el trayecto que el buque debería seguir para llegar a su primitivo destino. Si dichas instrucciones no llegan a tiempo, el fletante o el capitán determinarán el puerto de descarga.

SUBFLETAMENTO

Artículo 141

Salvo autorización expresa del fletante, el fletador no podrá ceder total o parcialmente el contrato. Pero, en caso de fletamento total, y a falta de prohibición expresa en el contrato, podrá subfletar a uno o más subfletadores, subsistiendo su responsabilidad frente al fletante por el cumplimiento de las obligaciones

contractuales.

PRESCRIPCIÓN

Artículo 142

Las acciones que se derivan del contrato de fletamento total o parcial prescriben por el transcurso de un año contado desde la terminación del viaje, o desde la fecha en que se rescindió o resolvió el contrato, si ello se produjo antes de comenzado el viaje o en el curso del mismo.

Capítulo III DEL CONTRATO DE CARGA GENERAL

SUSTITUCIÓN DEL BUQUE

Artículo 143

Salvo estipulación expresa en contrario, el transportador tendrá derecho a sustituir el buque designado para el transporte de la carga, por otro igualmente apto para cumplir sin retardo, el contrato de transporte convenido.

TARIFAS Y CONDICIONES

Artículo 144

Si el transportador ha publicado tarifas y condiciones del transporte, deberá ajustarse a ellas, salvo convenio por escrito en contrario.

OBLIGACIÓN DEL CARGADOR

Artículo 145

El cargador deberá entregar los efectos en el tiempo y forma fijados por el transportador y, en su defecto, de conformidad con lo que establezcan los usos y costumbres sobre la materia. A falta de éstos, el buque puede zarpar quedando obligado el cargador al pago íntegro del flete estipulado, siempre que su importe no haya sido pagado por otra mercancía que ocupó el lugar de aquella.

RESOLUCIÓN POR EL CARGADOR

Artículo 146

Después de cargada la mercancía, el cargador podrá resolver el contrato dentro del término de la permanencia del buque en puerto, cuando ello no ocasionare retardo en la partida del buque, pagando el flete y los gastos de descarga.

ENTREGA DE LA CARGA POR EL TRANSPORTADOR

Artículo 147

El transportador deberá entregar la carga en el puerto de destino de acuerdo con lo que disponen el

conocimiento o manifiesto de carga, las reglamentaciones aduaneras y portuarias y los usos y costumbres sobre la materia. Si en virtud de dichas disposiciones las mercancías debieran entrar a depósito fiscal, la entrega quedará cumplida con la descarga al depósito correspondiente o a lanchas cuando por causas no imputables al buque no pudiere efectuarse la descarga a depósito.

ENTREGA A LANCHAS EN INTERÉS DEL TRANSPORTADOR

Artículo 148

Cuando la carga se entregare a lanchas como prolongación de bodega, en interés del transportador, su responsabilidad subsistirá como si continuara en el buque, hasta su posterior descarga en la forma prevista en el artículo precedente.

CESACIÓN DE RESPONSABILIDAD DEL TRANSPORTADOR

Artículo 149

Cesará toda responsabilidad del transportador respecto de la carga, a partir del momento en que sea entregada a depósitos fiscales, patios, o en lugares situados dentro de la jurisdicción aduanera, o cuando hubiere sido descargada a lanchas u otro lugar por cuenta y riesgo del titular de la mercancía.

ÁMBITO DE APLICACIÓN

Artículo 150

Las disposiciones del presente capítulo se aplicarán durante el tiempo transcurrido, desde la carga hasta la descarga, al transporte de cosas que se haya realizado en virtud de un contrato de fletamento total o parcial; al efectuado en buques de carga general; al de bultos aislados en cualquier buque; y a todo otro en que el transportador asuma la obligación de entregar la carga en destino.

CONTENEDORES

Artículo 151

Se aplicarán al transporte de cajas de carga o contenedores, las normas convencionales sobre la materia; las normas de las leyes especiales; y las normas de esta ley en lo aplicable; teniendo en cuenta las características y condiciones de los mismos.

EMBARGO DE LA CARGA

Artículo 152

El armador, sea éste fletante o transportador efectivo, podrá solicitar a la autoridad judicial competente el embargo de los efectos transportados, en garantía de sus créditos correspondientes al flete, sobreestadías, avería gruesa u otros gastos relacionados con el transporte de la carga.

RESPONSABILIDAD

Artículo 153

El transportista multimodal será el único responsable frente a los titulares de la carga por todos los tramos

de la cadena de transporte, sin perjuicio del derecho de éste a reclamar a los distintos factores de la cadena de transporte y responderá en los mismos términos que esta ley señala para el transportador marítimo, durante todo el período en que las cargas se encuentren bajo su custodia, cualquiera que sea el medio de transporte que se esté empleando.

DOCUMENTO DE TRANSPORTE MULTIMODAL

Artículo 154

El transportista multimodal, con la recepción de la carga, emitirá un único documento que cubrirá a la mercancía en todo el trayecto del transporte, independiente del tipo de transporte utilizado durante el trayecto parcial.

Capítulo IV DEL TRANSPORTE DE PERSONAS

TRANSPORTE DE PERSONAS

Artículo 155

El armador del buque de pasajeros es responsable de trasladar a las personas que contratan sus servicios de un lugar a otro, mediante el empleo de un buque y, mediante el pago de un boleto o pasaje. El transportador deberá ejercer una razonable diligencia para poner el buque en estado de navegabilidad, armándolo y equipándolo convenientemente y mantenerlo en el mismo estado durante el curso del transporte, a efectos de que el viaje se realice en condiciones de seguridad para los pasajeros. El transportador de personas será responsable de todo daño originado por la muerte o lesiones del pasajero, siempre que el daño ocurra durante el transporte por su culpa o negligencia, o por la de sus dependientes.

EQUIPAJE

Artículo 156

En el precio del pasaje estará comprendido el del transporte del equipaje del pasajero, dentro de los pesos y volúmenes establecidos por el transportador o por los usos y costumbres, entendiéndose como tales los efectos de uso personal del pasajero. El transportador será responsable por la pérdida o daños que sufra el equipaje del pasajero que sea guardado en bodega del buque, si no prueba que la causa de los mismos no le es imputable. Se fija en cuatrocientos cincuenta Derechos Especiales de Giro, el límite de responsabilidad del transportador de pasajeros por cada bulto o pieza de equipaje.

Capítulo V CONTRATO DE REMOLQUE

CLASES DE REMOLQUE

Artículo 157

El contrato de remolque puede ser por su clase, de la manera siguiente:

Remolque Maniobra: Es el que se realiza con el propósito de facilitar la operación de un buque o cooperar con ella, ya sea en su salida de puertos o entrada a ellos, travesías en aguas restringidas donde los buques de cierto tonelaje y calado, destinados a navegar específicamente en aguas abiertas requieren el concurso de una energía motriz de más fácil manejo. El mando de la operación estará a cargo del buque remolcado.

Remolque Transporte: Es la operación que tiene por objeto el traslado de unidades remolcadas carentes de propulsión, de un punto a otro del espacio acuático, bajo la dirección de un capitán de remolcador.

OBLIGACIÓN IMPLÍCITA

Artículo 158

Es obligación implícita en el contrato de remolque maniobra, tanto por parte del remolcado como del remolcador, observar durante el curso de la operación, todas las precauciones indispensables para no poner en peligro al otro buque. La responsabilidad por los daños que resulten del incumplimiento de esta obligación no podrá ser motivo de una cláusula de exoneración o de limitación.

Capítulo VI DISPOSICIONES COMUNES DE LOS CONTRATOS

CONOCIMIENTOS O MANIFIESTO DE EMBARQUE

Artículo 159

Antes de comenzar la carga, el cargador deberá suministrar por escrito al transportador una declaración de embarque que contenga un detalle de la naturaleza y calidad de la mercancía que será objeto del transporte, con indicación del número de bultos o piezas, cantidad o peso, según los casos y las marcas principales de identificación.

DEBER DE VERACIDAD

Artículo 160

El cargador garantizará al transportador la exactitud del contenido de la declaración de embarque, y deberá indemnizarlo, de conformidad a lo indicado en el capítulo correspondiente de esta ley, de todos los daños y perjuicios que sufra con motivo de alguna mención inexacta. El derecho a esta indemnización no modificará en forma alguna la responsabilidad y obligaciones del transportador frente a toda persona que no sea el cargador.

ENTREGA DE LA ORDEN DE EMBARQUE

Artículo 161

El transportador o agente marítimo, aceptada la declaración de embarque y formalizado el contrato, deberá entregar al cargador una orden de embarque para el capitán, en la que se transcribirá el contenido de la declaración. Embarcada la mercancía el capitán deberá entregar al cargador los recibos provisorios. La entrega de la carga se acreditará con los recibos provisorios y los demás medios de prueba admisibles en materia comercial.

INSERCIÓN DE RESERVAS

Artículo 162

El transportador, capitán o agente podrá insertar reservas en el conocimiento con respecto a las marcas, números, cantidades o pesos de las mercancías, cuando sospechare razonablemente que tales especificaciones no correspondieren a la mercancía recibida, o cuando no tuviera medios normales para verificarlo. En defecto de estas reservas, se presume salvo prueba en contrario, que las mercancías fueron embarcadas conforme a las menciones del conocimiento. Esta prueba no será admitida cuando el conocimiento haya sido transferido a un tercer portador de buena fe.

VALIDEZ Y NULIDAD DE LAS CARTAS DE GARANTÍA

Artículo 163

Son válidas las cartas de garantía entre cargador y transportador, y no podrán ser opuestas al consignatario ni a terceros. Serán nulas las cartas de garantía que se hubiesen emitido para perjudicar los derechos de un tercero o que contengan estipulaciones prohibidas por la ley.

NÚMERO DE EJEMPLARES DEL CONOCIMIENTO O MANIFIESTO DE CARGA

Artículo 164

El cargador puede exigir al transportador, agente o capitán, hasta tres originales de cada conocimiento. Las demás copias que solicitare, deberán llevar la mención no negociable. Con esta misma mención, una de las copias firmada por el cargador deberá quedar en poder del transportador. Entregada la mercancía en destino con uno de los originales, los demás carecerán de valor.

ENTREGA DE LA MERCANCIA ANTES DE LA LLEGADA A DESTINO

Artículo 165

Antes de la llegada a destino, el transportador no podrá entregar la mercancía sino contra la devolución de todos los conocimientos originales o, en su defecto, otorgándosele fianza suficiente por los perjuicios que pueda sufrir por la falta de restitución de uno de ellos.

CATEGORÍAS DE CONOCIMIENTO

Artículo 166

El conocimiento de embarque podrá ser a la orden, al portador o nominativos, y son transferibles con las formalidades y efectos que establezca el Código de Comercio. El tenedor legítimo del conocimiento tiene derecho a disponer de la mercancía respectiva durante el viaje y a exigir su entrega en destino.

PREVALENCIA DE LA PÓLIZA DE FLETAMENTO

Artículo 167

Las cláusulas de la póliza de fletamento prevalecen entre las partes, sobre las del conocimiento de embarque, salvo pacto en contrario. Contra terceros, dichas cláusulas prevalecerán cuando en el conocimiento se inserte la mención según póliza de fletamento.

INTERVENCIÓN DE DISTINTOS MEDIOS DE TRANSPORTE

Artículo 168

Cuando se otorgare un conocimiento directo destinado a cubrir el transporte de mercancías en trayectos servidos por distintos medios de transporte, serán aplicables las disposiciones de esta ley.

Sus cláusulas regirán durante todo el transporte hasta la entrega de la mercancía en destino, sin que puedan ser alteradas por los conocimientos que se otorguen por trayectos parciales, los cuales deberán mencionar que la mercancía se transporta bajo un conocimiento directo.

ÓRDENES DE ENTREGA FRACCIONADA

Artículo 169

A pedido del tenedor legítimo del conocimiento, cuando así se conviniere en el contrato de transporte, el transportador o su agente marítimo, deberán librar órdenes de entrega contra el capitán o agente marítimo del buque en el puerto de descarga, por fracciones de la carga respectiva.

Al expedir tales órdenes de entrega, el transportador o su agente marítimo deberán anotar en los originales del conocimiento, la calidad y cantidad de mercancía correspondiente a cada orden, con su firma y con la del tenedor, y retener el documento si el fraccionamiento comprende la totalidad de la carga que ampara. Las órdenes de entrega podrán ser nominativas, a la orden o al portador. La utilización de estos documentos en puertos salvadoreños quedará supeditada al cumplimiento de las disposiciones aduaneras.

Capítulo VII SEGUROS MARÍTIMOS

DISPOSICIONES APLICABLES

Artículo 170

El contrato de seguro vinculado con la actividad marítima se rige por las disposiciones de los seguros generales.

Son considerados asegurables, los siguientes bienes y personas:

1. El buque o artefacto naval;
2. Todo elemento utilizado para equipar al buque;
3. Todos los efectos que se transporten sobre el buque;
4. El flete o precio del pasaje;
5. La Avería;
6. El salario de asistencia y salvamento; y
7. Las tripulaciones y pasajeros transportados.

SEGURO OBLIGATORIO

Artículo 171

Todo buque que ingrese, transite o permanezca en aguas jurisdiccionales salvadoreñas deberá tener en forma obligatoria los siguientes seguros:

1. De Casco y Maquinarias;
2. De Protección e Indemnización;
3. De Protección a la Contaminación de las Aguas; y
4. De Vida sobre las Personas Transportadas.

Capítulo VIII TRIBUNALES COMPETENTES

TRIBUNALES COMPETENTES

Artículo 172

Los tribunales salvadoreños son competentes en todos aquellos hechos producidos dentro de sus aguas jurisdiccionales, salvo convención expresa de las partes involucradas, que sometan su controversia a conocimiento de un tribunal extranjero, a excepción de los delitos.

COMPETENCIA EN AGUAS NO JURISDICCIONALES

Artículo 173

En los casos de accidentes o abordajes ocurridos en aguas no jurisdiccionales, los tribunales salvadoreños serán competentes para conocer de las acciones penales o administrativas que correspondan contra los responsables del buque, cuando éstos sean de bandera salvadoreña.

COMPETENCIA SOBRE CONTRATOS Y HECHOS DEL BUQUE

Artículo 174

Los tribunales salvadoreños serán competentes para conocer de entender las acciones derivadas de los contratos sobre buque, tales como fletamento, locación, transporte, remolque y sus actividades conexas, cuando las obligaciones que nacen de los mismos deban cumplirse o ejecutarse en territorio salvadoreño. Asimismo, serán competentes los tribunales salvadoreños, en todos los asuntos derivados de averías, asistencia y salvamento, abordajes o seguros, cuando, aunque no hayan ocurrido en aguas jurisdiccionales salvadoreñas, el buque fuere de bandera salvadoreña, o las consecuencias de dichos hechos finalicen en los puertos de El Salvador.

Capítulo IX DEL EMBARGO DE BUQUES

BUQUES SALVADOREÑOS

Artículo 175

Los buques de bandera salvadoreña, podrán ser embargados preventivamente en cualquier punto del país, por créditos privilegiados y por otros créditos en el puerto donde su propietario tenga su domicilio o establecimiento principal. El embargo por crédito ajeno al buque, a su explotación o a la navegación, deberá reunir, para su procedencia, los requisitos exigidos por la ley común.

BUQUES EXTRANJEROS

Artículo 176

Los buques extranjeros anclados en puertos de El Salvador, podrán ser embargados preventivamente en los siguientes casos:

1. Por créditos privilegiados;
2. Por deudas contraídas en territorio salvadoreño en utilidad del mismo buque, o de otro buque que pertenezca o haya pertenecido, cuando se originó el crédito, al mismo propietario;
3. Por deudas originadas en la actividad del buque, o por otros créditos ajenos a ésta, cuando sean

exigibles ante los tribunales del país; y

4. Por accidentes marítimos o por daños causados a las instalaciones portuarias.

BUQUE LOCADO

Artículo 177

Si el buque que originó el crédito se encontrare sujeto a un contrato de locación, explotado por un armador-locatario, o existiere un fletador a tiempo, únicos responsables de la deuda respectiva, procederá el embargo de otro buque de propiedad del armador-locatario o del fletador a tiempo, pero no el embargo de otro buque que pertenezca al propietario de aquél.

EMBARGO EJECUTIVO

Artículo 178

El embargo por ejecución de sentencia procederá contra cualquier buque del deudor, sea de matrícula nacional o extranjera, sin las restricciones impuestas por los artículos anteriores.

TRABA DEL EMBARGO

Artículo 179

El embargo se practicará mediante comunicación que ante la autoridad marítima, deberá librar el juez embargante, a los efectos de su anotación en los respectivos registros. Si se trata de un buque de matrícula salvadoreña, su zarpe debe ser impedido si se dispone la prohibición de navegar. Esta última medida se encontrará implícita en el embargo que se dicte contra un buque de bandera extranjera. A pedido de parte, el tribunal podrá ordenar que se levante un inventario de las pertenencias del buque.

CESACIÓN DEL EMBARGO

Artículo 180

Todo embargo o prohibición de zarpe cesará si cualquier interesado en el zarpe otorga fianza o garantía suficiente para el pago de la deuda reclamada en cuanto sea legítima, o cuando se garantizare el límite de la responsabilidad.

RESPONSABILIDAD DEL EMBARGANTE

Artículo 181

La responsabilidad de quien, sin actuar maliciosamente, obtenga el embargo del buque y no exija en definitiva el derecho pretendido, se limitará a los perjuicios que cause la inmovilización del buque hasta el momento en que su armador sustituya dicho embargo por otra garantía, y a los gastos que ésta le ocasionare.

INEMBARGABILIDAD

Artículo 182

No pueden ser objeto de embargo ni de prohibición de zarpe:

1. Los buques de guerra nacionales o extranjeros y los buques en construcción destinados a incorporarse a los efectivos militares de un Estado; y
2. Todo otro buque afectado al servicio del poder público del Estado. Tampoco pueden ser embargados los buques afectados al servicio del poder público de un Estado extranjero.

TÍTULO IV
DE LOS PUERTOS
Capítulo I
CLASIFICACION DE LOS PUERTOS

CLASIFICACIÓN

Artículo 183

La naturaleza de los puertos de El Salvador se define según la titularidad, uso, finalidad y grado de intervención de la AMPL.

Según su titularidad, son:

1. Puertos Estatales: son aquellos de propiedad del Estado, los cuales pueden ser administrados por entidades del Gobierno Nacional, por los Gobiernos locales o por entidades del sector privado a través de contratos de concesión de obra pública o de servicios, total o parcial.
2. Puertos Particulares o Privados: son aquellos de propiedad privada, que contando con las correspondientes autorizaciones son administrados y operados por entidades del sector privado.
3. Puertos Mixtos: Son puertos cuyo capital accionario es parte privado y el remanente del sector estatal.

Según su uso, son:

1. Públicos: los que por sus características operacionales prestan servicios obligatorios a todo usuario que lo requiera.
2. Privados: los que ofrecen y prestan servicios a buques, armadores, cargadores y recibidores de mercancía en forma restringida a las propias necesidades de los particulares o terceros vinculados contractualmente con ellos. Dichos puertos se desarrollarán dentro del sistema de libre competencia.

Por su actividad económica, son:

1. Puertos Comerciales: aquellos cuya os destinos finalidad es la prestación de servicios a buques y a cargas, cobrando un precio por tales servicios.
2. Puertos Industriales: aquellos cuya finalidad es la de operar exclusivamente cargas específicas de sus procesos industriales, extractivos o de captura, debiendo existir una integración operativa entre la actividad principal de la industria y el puerto.
3. Puertos Recreativos: aquellos destinados a actividades deportivas o turísticas locales.
4. Puertos Artesanales: aquellos cuyas actividades se desarrollan mediante procesos no industriales.
5. Puertos Mixtos: aquellos puertos que por su actividad económica pueden tener dos o más de las finalidades expresadas para esta actividad en los literales anteriores.

Por el grado de intervención de la Autoridad Portuaria Local, los puertos se clasifican en:

1. Puertos Lanlord: Son aquellos cuya infraestructura es propiedad de la Autoridad Portuaria Local, la cual se ocupa de su gestión. En estos el resto de los servicios portuarios son prestados mediante contratos de concesión parcial o total por empresas privadas propietarias de los activos que conforman la superestructura y de todos aquellos otros activos necesarios para la producción de servicios.
2. Puertos Tool: Son aquellos puertos en los cuales la Autoridad Portuaria Local es propietaria de la infraestructura y de la superestructura, y el sector privado se encarga de la provisión de los servicios portuarios mediante contratos de concesión parcial o total o licencias.
3. Puertos Services: Son aquellos puertos en los cuales la Autoridad Portuaria Local es responsable del puerto en su conjunto, como propietaria de la infraestructura y de la superestructura y se encarga totalmente de la provisión de los servicios portuarios.

La finalidad de los puertos podrá ser modificada por la Autoridad Portuaria Local y autorizada por la Autoridad Marítimo Portuaria. Asimismo, los puertos estatales serán siempre de uso público y estarán administrados por la autoridad portuaria respectiva.

Capítulo II DE LA NAVEGACIÓN Y DEL TRAFICO MARÍTIMO

NAVEGACIÓN Y TRÁFICO

Artículo 184

Los puertos salvadoreños en tiempo de paz estarán abiertos a la navegación y tráfico a las embarcaciones de todos los países. La AMP podrá negar la entrada cuando no exista reciprocidad con el país de matrícula de la embarcación o cuando lo exija el interés público, o por razones de seguridad o de estrategia de Estado.

PUERTOS EN FUNCIONAMIENTO

Artículo 185

Los puertos que se encuentran actualmente en funcionamiento, ya sean públicos o privados, a la fecha de la vigencia de la presente ley, deberán someterse al régimen regulatorio de la Autoridad Marítima Portuaria, en lo aplicable.

Capítulo III ADMINISTRACIÓN Y OPERACIÓN DE LOS PUERTOS

PUERTOS ESTATALES

Artículo 186

Los puertos estatales o municipales de carácter público existentes o a crearse, serán administrados por la entidad del Estado que ejerza la respectiva propiedad o titularidad; administración que podrá ser ejercida directamente u otorgada por contrato de concesión a terceros, de conformidad al Artículo 120 de la Constitución Política y a la respectiva normativa que ordena la Ley de Adquisiciones y Contrataciones de la Administración Pública y bajo el control y regulación de la AMP.

Dependiendo de la naturaleza del contrato, la entidad concedente podrá convenir la explotación, reparación, mantenimiento, conservación y modificación de las instalaciones existentes, inclusive la construcción de nuevas instalaciones para la prestación de servicios.

PUERTOS PRIVADOS

Artículo 187

De conformidad con la presente Ley y al reglamento que la AMP establezca sobre la materia, ésta podrá autorizar la construcción de puertos privados, de uso privado o de uso público, a fin de que en ellos se ejecuten una o más de las actividades económicas especificadas en el Artículo 183 de esta Ley.

SERVICIOS PORTUARIOS

Artículo 188

En los puertos de uso público, el operador portuario establecerá los servicios esenciales que deberán ser prestados a los buques y a las cargas según el Reglamento respectivo; y de aquellas instalaciones que deberán facilitar a los organismos del Estado que estarán a cargo de los controles policiales y aduaneros.

MANTENIMIENTO DE PUERTOS

Artículo 189

El titular del puerto será responsable del mantenimiento y mejoras de las obras esenciales, tales como dragado, señalización de accesos y dársenas, instalaciones de amarre, remolque y practicable, equipos e instalaciones en tierra, de conformidad a las regulaciones establecidas en la presente ley. Dichas actividades podrán ser realizadas a través de sus propios medios o por terceros.

SUSPENSIÓN DE OPERACIONES EN CASOS DE SEGURIDAD NACIONAL

Artículo 190

Será facultad del Presidente de la República, intervenir en las operaciones de un puerto en particular, mediante Decreto Ejecutivo correspondiente, cuando la seguridad nacional o la defensa nacional lo requieran.

CAPITULO IV REGIMEN ECONÓMICO DE LOS SERVICIOS PORTUARIOS

REGIMEN ECONOMICO

Artículo 191

Se entiende por régimen económico, las estructuras de tarifas o precios, que de acuerdo a lo establecido en la presente ley deban ser aprobados por la Autoridad Marítima Portuaria, a través de normativa de su competencia, para ser cumplida por todo operador o prestador de servicios de todo puerto público o privado de uso público y para ser aplicadas a los usuarios, en concepto de contraprestación por los servicios portuarios que se les brinden a los buques y a las cargas.

COMPETENCIA TARIFARIA

Artículo 192

La política tarifaria o de precios de los servicios portuarios que presten los puertos públicos o los puertos privados de uso público que operen en El Salvador, será emitida por la AMP a través del Reglamento Especial para la Aplicación de Tarifas de Servicios Portuarios, de conformidad con los criterios, procedimientos y métodos de cálculo establecidos en la presente ley. Asimismo, será la AMP la entidad

competente para verificar y aplicar su cumplimiento.

La política tarifaria, tendrá como propósito determinar para cada tipo de puerto, el método tarifario que más se ajuste a su naturaleza, operación y condición de mercado.

PROCEDIMIENTO PARA DETERMINAR LAS TARIFAS

Artículo 193

De acuerdo al Reglamento Especial para la Aplicación de Tarifas de Servicios Portuarios, los operadores de puertos deberán presentar a la AMP, para su aprobación, el Pliego Tarifario que ellos pretendan cobrar a los usuarios, incluyendo los valores tarifarios o precios de los servicios portuarios, la metodología que se ha utilizado para calcularlos y la forma en que dichas tarifas o precios serán ajustados en el futuro.

La solicitud de aprobación de un Pliego Tarifario presentado a la AMP por un operador portuario potencial o activo, deberá presentarse de conformidad con esta ley y los respectivos procedimientos que se establezcan en el reglamento correspondiente.

Presentada la referida solicitud y siempre que ésta llene los requisitos y formalidades legales y reglamentarios establecidos para esos efectos, la AMP en un plazo no mayor de cinco días hábiles, mandará a publicar en un diario de circulación nacional, a costa del peticionario, un edicto conteniendo la solicitud.

En el edicto se señalará lugar, día y hora para la celebración de la audiencia pública, la cual deberá efectuarse dentro de un plazo no mayor de los siete días hábiles subsiguientes a la publicación, con el objeto que la AMP conozca documentalmente de parte de los sectores interesados vinculados con los servicios portuarios, su posición respecto a las tarifas de los servicios portuarios sujetos de regulación tarifaria comprendidos dentro del Pliego Tarifario propuesto.

En dicha audiencia se escuchará al peticionario y a los interesados, quienes previamente deberán acreditar legalmente la calidad con la que actúan, así como presentar y ofrecer las pruebas y alegatos por escrito.

Con base al análisis de los argumentos de las partes, la resolución definitiva sobre la aprobación del Pliego Tarifario de tarifas portuarias propuestas, la AMP deberá emitirla dentro de un plazo que no exceda de siete días hábiles posteriores a la fecha en que haya efectuado la audiencia pública. Si no mediare rechazo expreso en el término de ese plazo, el Pliego Tarifario propuesto entrará en vigencia a los quince días posteriores a dicha fecha, entendiéndose como aprobado y automáticamente aceptado por la AMP. El Pliego Tarifario propuesto solo podrá ser desaprobado por la AMP con la debida justificación, si el mismo no cumple con los criterios y requisitos establecidos en la presente ley y en el Reglamento Especial para la Aplicación de Tarifas de Servicios Portuarios.

CONDICIONES ESENCIALES PARA DETERMINAR LAS TARIFAS

Artículo 194

Con el fin de evitar subsidios cruzados, los operadores de servicios portuarios deberán llevar un sistema de contabilidad de costos por actividad.

La AMP también definirá los servicios portuarios que serán desregulados en aquellos casos en que exista suficiente competencia en el mercado. Sin embargo, en caso que las tarifas de los servicios portuarios desregulados presenten desequilibrios entre la oferta y la demanda, o se evidencie la existencia de prácticas anticompetitivas que alteren el funcionamiento normal del mercado, la AMP deberá consultar a la

entidad responsable de velar por la libre y sana competencia, el dictamen sobre la existencia de dichas prácticas o viceversa y en caso de que el dictamen confirme prácticas anticompetitivas, la AMP deberá fijar tarifas máximas y mínimas para los servicios, las cuales deberán permanecer vigentes durante el tiempo que permanezcan las distorsiones del mercado.

METODOS DE CALCULO DE TARIFAS PORTUARIAS

Artículo 195

La AMP en atención a su política tarifaria, determinará de entre los métodos que se describen en el presente artículo, el que se aplicará con más razonabilidad técnica y económica a cada puerto en particular.

Dichos métodos son los siguientes:

1. Tarifas Ajustadas en base a Índices de Inflación y Mejoras Operativas: Método por medio del cual los servicios portuarios sujetos de regulación económica, se tarifican mediante formulación que pondera parámetros de inflación, e insumos utilizados en la prestación de dichos servicios.
2. Tarifas por Comparación con otros Puertos de su Área Competitiva: Método mediante el cual los servicios portuarios sujetos de regulación económica, se tarifican mediante formulación comparativa entre el valor de tarifa actual, con las tarifas de los puertos competitivos del área de influencia.
3. Tarifas en base al Cálculo de la Rentabilidad de la Inversión: Método mediante se fijan tarifas máximas para los servicios portuarios sujetos de regulación económica, en función de una tasa de retorno de la inversión (TIR) previamente determinada.
4. Mercado Libre: Método mediante el cual las tarifas de los servicios portuarios se determinan en función de la libre oferta y demanda de los servicios portuarios por parte de los operadores portuarios y los usuarios del puerto.

MODIFICACION DE TARIFAS

Artículo 196

Toda modificación de tarifas portuarias reguladas por la AMP, deberá solicitarse por el operador interesado en atención a las normas que se establezcan en el Reglamento Especial para la Aplicación de Tarifas de Servicios Portuarios.

Asimismo, dicho reglamento establecerá el procedimiento para solicitar la aprobación de tarifas de nuevos servicios portuarios que no hayan sido considerados en el Pliego Tarifario original, en caso que éstos no sean desregulados.

Toda solicitud de modificación de tarifas portuarias, así como de aprobación de tarifas de nuevos servicios, deberá estar fundada en análisis debidamente sustentados ante la Autoridad Marítima Portuaria, la cual dispondrá de un plazo de sesenta días calendario para resolver sobre la petición de los ajustes tarifarios o de las nuevas tarifas. Si no mediare rechazo expreso en el término de ese plazo, las tarifas solicitadas entrarán en vigencia a los quince días calendario posteriores a dicha fecha, entendiéndose la petición de los ajustes tarifarios o de las nuevas tarifas, automáticamente aceptadas. La sustentación de esas solicitudes deberá ser debidamente justificada, con análisis en informes técnicos, económicos, financieros y legales previos, así como en la prueba de hechos, actos y sus consecuencias, que hayan dado lugar a las mismas. Las modificaciones tarifarias no podrán ser utilizadas como forma de penalizar a los operadores de servicios portuarios, por beneficios pasados o logrados en la operación de los servicios, como tampoco no podrán ser usadas para compensar pérdidas incurridas derivados del riesgo empresarial, ni convalidar

ineficiencias.

REGISTRO Y PUBLICACION DE LAS TARIFAS

Artículo 197

Las tarifas portuarias de los servicios a las cargas y a los buques y sus modificaciones en su caso, aprobadas por la AMP, deberán ser registradas y publicadas en dos de los periódicos de circulación nacional, por lo menos diez días calendario, previos a su entrada en vigencia.

Capítulo V

REGIMEN DE RESPONSABILIDAD DE LOS OPERADORES PORTUARIOS

RESPONSABILIDAD CIVIL DEL OPERADOR PORTUARIO

Artículo 198

Los operadores portuarios serán responsables directos por todos los daños que causen tanto a las personas, los buques y las cargas por causa o debido a su accionar como responsables de la operación portuaria.

A tales efectos el operador portuario deberá poner la debida diligencia en realizar las tareas de carga y descarga de mercancías y tránsito de personas dentro del área de su responsabilidad, siendo responsable de los daños que pudieren causar.

PERIODO DE RESPONSABILIDAD

Artículo 199

El Operador Portuario será responsable por las mercancías que movilicen durante todo el período que las tenga bajo su custodia. Se entiende que las mercancías están bajo la custodia del Operador Portuario, desde el momento en que se hace cargo de ellas, recibéndolas del armador o transportador o del embarcador en su caso, hasta el momento en que las coloca en poder del consignatario o de la persona facultada para recibirlas. Cuando el embarcador o el transportista suministre las mercancías agrupadas en un contenedor, paleta u otro elemento de consolidación de la carga, o cuando estén embaladas, el término mercancía comprenderá ese elemento o ese embalaje.

La responsabilidad por daños a las personas se regirá por la legislación común.

OBLIGACION DE PROBAR

Artículo 200

El operador portuario será responsable de los perjuicios resultantes de la pérdida o daño de las mercancías, si el hecho que causa la pérdida o el daño, se produjo durante el período en que éstas permanecieron bajo su custodia, de conformidad con esta Ley, a menos que pruebe que él, sus empleados, mandatarios u otras personas a quien haya encomendado la prestación del servicio portuario, adoptaron las medidas que razonablemente podían exigirse para evitar el hecho y sus consecuencias.

LIMITE DE RESPONSABILIDAD.

Artículo 201

En aquellos casos en que el operador portuario, es designado por el armador o transportador, para la prestación de los servicios portuarios, aquel podrá invocar las exoneraciones y límites de responsabilidades que amparen a este último, de conformidad con la ley o a los convenios internacionales vigentes.

En los demás casos, el operador portuario podrá limitar su responsabilidad a una suma que no exceda de dos Derechos Especiales de Giro por kilogramo de peso bruto de las mercancías perdidas o dañadas y si se trata de mercancías no cargadas por bulto o pieza, por cada unidad de flete; excepto por aquellas mercancías en las cuales el cargador o el armador o transportador haya declarado el valor de ellas antes de su entrega.

Cuando el transporte se realice en contenedores o artefacto unitario de carga, todo bulto o unidad enumerado en el conocimiento de embarque como unidad o bulto, será considerado a los fines de la limitación.

En ningún caso el monto a indemnizar excederá el valor según factura, de la mercancía perdida o dañada.

PERDIDA DEL DERECHO DE LIMITAR LA RESPONSABILIDAD

Artículo 202

El operador portuario no podrá limitar su responsabilidad, si se prueba que la pérdida, el daño o el retraso provinieron de una acción u omisión del propio operador portuario o de sus empleados o mandatarios, realizada con intención de causar tal pérdida, daño o retraso, o intencionalmente y a sabiendas que sobrevendrían la pérdida o daño.

Esta disposición será igualmente aplicable al empleado o mandatario del operador portuario, u otra persona a quien éste haya encomendado la prestación de sus servicios, a quien se exija directamente su responsabilidad, si se prueba que la pérdida, el daño o el retraso provinieron de una acción u omisión de ese empleado, mandatario o persona, realizada con intención de causar tal pérdida o daño, o intencionalmente y a sabiendas que sobrevendrían dicha pérdida o daño.

CONCURRENCIA DE OTRAS CAUSAS

Artículo 203

Cuando el operador portuario, sus empleados, mandatarios u otras personas a cuyo trabajo haya encomendado la prestación del servicio, no hayan adoptado las medidas a que se refiere el artículo anterior, y ese incumplimiento concorra con otra causa para ocasionar la pérdida o el daño, el operador portuario será responsable sólo en la medida en que los perjuicios resultantes puedan atribuirse a tal incumplimiento y siempre que pueda probar el monto de los perjuicios que no le pueden ser atribuidos personalmente.

RECEPCION DE LAS MERCADERIAS

Artículo 204

Al momento de recibir las mercancías, el operador portuario deberá emitir por escrito los documentos necesarios o, al menos, una carta de recepción única o parcial firmada, en la que se identifiquen las mercancías y se acuse recibo de ellas, indicando las fechas en que fueron recibidas, y haciendo constar su estado y cantidad.

PRESUNCION LEGAL

Artículo 205

Si el operador portuario no emite los documentos a que se refiere el artículo anterior, se presumirá, salvo prueba en contrario, que ha recibido las mercancías en buen estado.

INTERCAMBIO ELECTRONICO DE DATOS

Artículo 206

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

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

PLAZO PARA DAR AVISO PRESUNCION

Artículo 207

El transportista, consignatario o cualquier otra persona facultada para recibir las mercancías de manos del operador portuario, dispondrá de un plazo de tres días hábiles contados desde la fecha en que haya recibido dichas mercancías, para dar a éste el aviso de pérdida o daño, especificando la naturaleza del perjuicio sufrido.

Se presume, salvo prueba en contrario, que el operador portuario ha entregado las mercancías en buen estado si no hubiere emitido ese documento.

INSPECCION

Artículo 208

Cuando se hubiere dado el aviso de pérdida o daño conforme al artículo anterior, el operador portuario, el transportista y la persona facultada para recibir las mercancías, darán todas las facilidades razonables para la inspección de las mercancías y la comprobación del número de bultos.

No obstante, si el operador portuario y la persona facultada para recibir las mercancías hubieren participado en un examen o en una inspección de las mismas, documentado mediante acta suscrita por ambas partes, en el momento que fueron puestas en poder de esta última, se omitirá el régimen de avisos y presunciones establecidas en el artículo precedente.

EXONERACIONES Y LIMITES DE RESPONSABILIDAD EN LOS RECINTOS EXTRAPORTUARIOS

Artículo 209

Las exoneraciones y límites de responsabilidad previstas en el presente Capítulo, serán aplicables en los recintos extra portuarios y similares que se encuentren bajo la administración y control del operador portuario.

RESPONSABILIDAD CONTRACTUAL Y EXTRA CONTRACTUAL

Artículo 210

Las exoneraciones y límites de responsabilidad establecidas en este Título, serán aplicables a toda acción contra el operador o administrador portuario respecto de la pérdida o el daño de la mercancía, o daños a los buques, independientemente que la acción se fundamente en la responsabilidad contractual, la responsabilidad extracontractual o en otra causa.

MERCANCIAS PELIGROSAS

Artículo 211

Cuando fueren puestas en poder del operador portuario mercancías peligrosas que no estén marcadas, etiquetadas, embaladas o documentadas como tales, o si, en el momento de hacerse cargo de ellas, no ha tenido conocimiento por otro medio de su carácter peligroso, aquel tendrá derecho a adoptar cualquiera de las medidas o conjunto de éstas, especificadas en el Artículo 94 de esta Ley.

Capítulo VI

NORMAS DE RESGUARDO DE LA LEAL COMPETENCIA

ACTOS PROHIBIDOS

Artículo 212

Se prohíbe expresamente realizar cualquier acto que tenga la intención o el resultado de restringir en forma indebida la competencia entre puertos y operadores de servicios portuarios.

Para estos efectos, se entenderán como restricciones a la leal competencia, las siguientes:

1. El cobro de precios inferiores a los costos de operación;
2. Servicios adicionales a los oficialmente publicados prestados en forma gratuita;
3. Los acuerdos de cualquier naturaleza para repartirse cuotas de servicios o suministros a naves o cargas para establecer niveles de precios interrelacionados;
4. Todas las transacciones, con sus precios, rebajas o descuentos, que no se contemplen en una factura oficial, detallada por cada clase, tipo o ítem de servicios o suministros prestados;
5. Todas aquellas que contemple sobre la materia la entidad nacional responsable de velar por las prácticas de libre competencia; y,
6. Las prácticas de abuso de posición dominante por alguno de los operadores de puertos.

PUBLICIDAD DE TARIFAS Y SERVICIOS

Artículo 213

Para salvaguardar el derecho de los usuarios a la mejor información, los operadores de los puertos deberán mantener a disposición de los usuarios, publicar y remitir a la AMP, en la forma en que ésta determine, el Pliego Tarifario de todos los servicios o suministros que presten en sus instalaciones.

DE LA EXONERACIÓN DE PAGO DE LAS NAVES DE GUERRA

Artículo 214

Las naves de la Fuerza Naval de El Salvador, así como las naves de guerra extranjeras que visiten El Salvador, tendrán libre acceso a las instalaciones portuarias, sean éstas públicas o privadas y se encuentren administradas por el Estado o por concesionarios privados y estarán exoneradas del pago de tarifas y precios por el uso de las mismas, en aplicación al principio de reciprocidad internacional.

DE LA EXONERACIÓN DE PAGO DE NAVES CON CARGA DE DONACION

Artículo 215

Las naves que utilicen los muelles para descargar objetos o productos donados por gobiernos extranjeros o instituciones multinacionales o privadas para programas de beneficio social, para centros de beneficencia, o para auxilio de damnificados en catástrofes nacionales o regionales, estarán exoneradas del pago de tarifas y precios portuarios, en los puertos estatales.

Capítulo VII DE LAS AUTORIZACIONES

SOLICITUD DE AUTORIZACIONES

Artículo 216

Las autorizaciones deberán ser solicitadas a la AMP, mediante la acreditación y presentación de toda la documentación que corresponda al proyecto portuario que se intente desarrollar.

DELEGACIÓN LOCAL

Artículo 217

La AMP deberá asignar en cada puerto una delegación local con facultades para resolver las situaciones siguientes:

1. Autorizar los arribos y despachos de los buques y artefactos navales;
2. Supervisar y controlar la navegación dentro de la zona portuaria y sus canales de acceso, estadía de embarcaciones, servicios de practica y remolque y ayudas a la navegación;
3. Controlar las condiciones de seguridad de los canales, vías de acceso y profundidades de los respectivos muelles; y
4. Registrar toda la información estadística referida al puerto o puertos incluidos en su delegación.

COLABORACIÓN DE OTRAS AUTORIDADES

Artículo 218

En todos los asuntos relativos a la soberanía nacional y de la seguridad pública, la Autoridad Marítima Portuaria deberá solicitar respectivamente la colaboración de la Fuerza Naval y de la Policía Nacional Civil, según la competencia de cada uno de éstos organismos del Estado.

TITULO V DE LAS INFRACCIONES Y SANCIONES EN EL AMBITO MARITIMO PORTUARIO

Capítulo I JURISDICCIÓN Y COMPETENCIAS DEL ENTE RESPONSABLE

COMPETENCIA PARA LA IMPOSICIÓN DE MULTAS

Artículo 219

Corresponde al Consejo Directivo de la AMP, con carácter indelegable, la competencia de imponer las

multas.

El importe de las multas y de las indemnizaciones por las infracciones establecidas en esta ley en el área marítima o en los puertos, las dársenas, las instalaciones marítimas o las marinas interiores adscritas a los puertos, se consideran ingreso propio de la AMP.

La persona a quien la AMP ha calificado con calidad de infractor, podrá presentar a ésta una solicitud de exoneración de la sanción, debidamente acompañada de los fundamentos en que basa su solicitud. Dicha persona tendrá que hacer uso de este recurso dentro de los primeros tres días hábiles y posteriores a la recepción formal del comunicado sancionatorio de la AMP, y ésta deberá resolver en el plazo máximo de quince días calendario contados a partir del registro de la solicitud. En caso que la AMP no resuelva en este plazo, la solicitud en referencia se tendrá como resuelta favorablemente.

Es requisito imprescindible que el infractor, con el requerimiento previo de la AMP y en el plazo reglamentario otorgado al efecto por ésta, haya corregido la situación alterada por la comisión de la infracción.

TIPIFICACIÓN DE INFRACCIONES ADMINISTRATIVAS

Artículo 220

Tienen la consideración de infracción administrativa en el ámbito marítimo portuario, las acciones y las omisiones tipificadas y sancionadas por la presente Ley. Estas infracciones se clasifican en leves, graves y muy graves.

INFRACCIONES LEVES

Artículo 221

Son infracciones leves las siguientes:

1. El incumplimiento de reglamentos sobre navegación, controles y regulaciones marítimas y las que se refieran a los puertos, en lo que respecta a la explotación de cada puerto, dársena, instalación marítima o marina interior;
2. No enarbolar la bandera en aguas salvadoreñas;
3. El incumplimiento de las instrucciones y órdenes reglamentarias de la AMP o de las autoridades portuarias locales dentro del ámbito de sus competencias;
4. La realización de operaciones marítimas que pongan en peligro las personas, las obras, las instalaciones, los equipos portuarios y los buques, en las cuales no se tomen las medidas de seguridad necesarias;
5. Cualquier acción u omisión que cause daños o perjuicios en los bienes de dominio público marítimo portuario o marítimo-terrestre adscrito, o en su uso o explotación, siempre que no impida su normal funcionamiento;
6. La ocupación del dominio público portuario o del dominio público marítimo-terrestre adscrito, con obras o instalaciones sin el título correspondiente, siempre que no se obstaculice la actividad normal del puerto, la dársena, la instalación marítima o la marina interior;
7. La realización de actividades portuarias en el recinto público portuario o adscrito, sin la autorización correspondiente;

8. La realización de obras, instalaciones o actividades portuarias en el dominio público del puerto o adscrito, con incumplimiento de las condiciones del título otorgado, sin perjuicio de su revocación, si procede;

9. La omisión o la aportación de forma defectuosa, voluntariamente o por negligencia inexcusable, de cualquier información que se tenga que suministrar a la Autoridad Portuaria Local o a la Autoridad Marítima Portuaria Nacional, ya sea por prescripción legal y a requerimiento suyo; y
10. El vertido de sustancias y de residuos no contaminantes en las aguas del puerto.

INFRACCIONES GRAVES

Artículo 222

Son infracciones graves:

1. Todas aquellas tipificadas como leves cuando provoquen lesiones a las personas o su baja laboral por un tiempo inferior a siete días, o bien causen daños y perjuicios que impidan parcialmente el funcionamiento de los bienes o de las instalaciones;
2. Cualquier acción u omisión que cause, por culpa o por negligencia, daño a los medios de transporte marítimos o terrestres, a las obras e instalaciones e inclusive equipos de buques y de infra y superestructura portuaria, así como a las mercancías, los contenedores o cualesquiera otros elementos, sea a bordo o situados en el espacio portuario, y también su utilización indebida o sin permiso cuando éste sea necesario;
3. La ocupación del dominio público portuario o adscrito sin el título administrativo otorgado para la ejecución de una o más actividades portuarias, cuando se perturbe la actividad normal del puerto, la dársena, la instalación marítima o la marina interior, o bien cuando se haya desatendido un requerimiento expreso de los órganos portuarios competentes para el cese de abuso de una posición dominante;
4. El falseamiento de cualquier información aportada a la Autoridad Portuaria Local o a la Autoridad Marítima Portuaria Nacional, en cumplimiento de una obligación legal o a requerimiento de ésta;
5. La obstrucción de las funciones de control y vigilancia de la Autoridad Portuaria Local o la negativa dolosa a colaborar en ellas; y
6. La reincidencia en cualquiera de las faltas leves, antes de que haya transcurrido el plazo de prescripción.

INFRACCIONES MUY GRAVES

Artículo 223

Son infracciones muy graves:

1. Las infracciones tipificadas como leves y como graves, cuando provoquen lesiones a las personas, determinantes de baja laboral por un tiempo superior a siete días, o bien cuando causen daños y perjuicios que impidan totalmente el funcionamiento o la utilización del bien o de la instalación;
2. La reincidencia en cualquiera de las faltas graves, antes de que haya transcurrido el plazo de prescripción.

INHABILITACIÓN

Artículo 224

Atendiendo a las circunstancias que concurran, la AMP para imponer la sanción correspondiente, podrá

acordar también la inhabilitación del infractor para ser titular de permisos, autorizaciones y contratos de servicios, de infraestructura, o de superestructura portuaria, por un plazo no superior a un año en caso de infracciones graves y hasta tres años en las muy graves.

PRESCRIPCIÓN DE LAS INFRACCIONES

Artículo 225

El plazo de prescripción de las infracciones es de tres años para las muy graves, dos años para las graves y un año para las leves. Este plazo se empieza a contar desde la fecha en que ha sido cometida la infracción. Si ésta es continuada, desde la fecha en que se ha realizado el último acto con que ha sido consumada. Si los hechos, los actos o las omisiones constitutivos de infracción son desconocidos por falta de signos externos, el plazo empieza a contar a partir de la fecha en que éstos se manifiesten.

PRESCRIPCIÓN DE LAS SANCIONES

Artículo 226

Las sanciones impuestas por infracciones muy graves prescriben a los tres años, las impuestas por infracciones graves a los dos años y las impuestas por infracciones leves al año. El plazo de prescripción de las sanciones se inicia el día siguiente a aquel en que ha adquirido firmeza la resolución que las impone.

CAPITULO II DE LAS RESPONSABILIDADES

RESPONSABILIDAD POR DAÑOS CAUSADOS AL DOMINIO PÚBLICO

Artículo 227

La imposición de sanciones es independiente de la obligación, exigible en cualquier momento, de restituir los bienes y de reponer la situación alterada al estado anterior a la comisión de la infracción, y de la obligación de indemnizar los daños y los perjuicios causados.

En el supuesto de que la reparación de un daño sea urgente para garantizar el buen funcionamiento del puerto, la dársena, la instalación marítima o la marina interior, el operador público o privado encargado de la explotación la llevará a cabo de forma inmediata. En este caso los gastos correspondientes van a cargo del causante.

Si la restitución y la reposición al estado anterior no es posible y se han producido daños y perjuicios, los responsables de la infracción abonarán las indemnizaciones que correspondan. La cuantía de la indemnización, que en ningún caso podrá ser inferior al valor del beneficio obtenido por el infractor, se fijará aplicando aquel que proporcione el valor mayor, de acuerdo a los siguientes criterios:

1. El valor de reposición.
2. El valor de los bienes maltrechos; y
3. El beneficio obtenido por el infractor con la actividad ilegal.

Corresponde a la AMP imponer la sanción y establecer la obligación de restituir y de reponer la situación alterada a su estado anterior, y también fijar el importe de la indemnización, con la instrucción previa del expediente administrativo correspondiente.

Las medidas previstas en este artículo no tienen carácter de sanción.

EJECUCIÓN FORZOSA

Artículo 228

El importe de las multas y de los gastos ocasionados por la ejecución de las actuaciones de restitución y de reposición de los bienes al estado anterior a la comisión de la infracción, y también el importe de las indemnizaciones por daños y perjuicios, pueden ser exigidos por vía ejecutiva.

La suspensión de las resoluciones dictadas requiere que el interesado garantice el importe mediante la constitución de una fianza o de un depósito suficiente.

RESPONSABILIDAD

Artículo 229

Son responsables de las infracciones administrativas las siguientes personas naturales o jurídicas:

1. Con carácter solidario; el autor o responsable de la acción o de la omisión con la empresa con la cual tiene relación de dependencia, si la infracción ha sido cometida en cumplimiento de sus funciones;
2. En caso de incumplimiento de las condiciones de un contrato o de un título administrativo, el titular de éste;
3. En caso de infracciones relacionadas con las embarcaciones, los armadores y los consignatarios respectivos con carácter solidario, y subsidiariamente, los capitanes o patrones; y
4. En caso de obras, instalaciones y actividades sin título suficiente, el promotor de la actividad, o el empresario que la ejecuta y el Director Técnico.

Si las infracciones son imputables a una persona jurídica, pueden ser consideradas como responsables subsidiarias las personas naturales que integren sus órganos rectores o de dirección, salvo las que hayan disentido de los acuerdos adoptados.

Las sanciones impuestas a los diferentes sujetos a consecuencia de una misma infracción tienen entre sí carácter independiente.

RESPONSABILIDAD PENAL

Artículo 230

Las sanciones que se señalan en este capítulo se aplicarán sin perjuicio de la responsabilidad penal que resulte, ni de la que proceda cuando la AMP revoque la concesión o permiso.

Para la aplicación de las sanciones a que se refiere esta ley, la AMP efectuará la correspondiente notificación oficial al presunto infractor de los hechos, y le otorgará un plazo de 15 días hábiles para que presente pruebas y manifieste por escrito lo que a su derecho convenga.

Transcurrido dicho plazo, la AMP dictará la resolución que corresponda, en un plazo no mayor de 30 días hábiles después de vencido el de recepción de pruebas.

PROCEDIMIENTO ADMINISTRATIVO PARA EL ESTABLECIMIENTO DE LAS SANCIONES

Artículo 231

El procedimiento administrativo sancionador se tramitará de acuerdo con lo que dispone la presente Ley y la normativa sobre procedimiento sancionador aplicable a los ámbitos de competencia establecidos en las leyes nacionales que rigen dicha materia.

Ante el conocimiento o las denuncias de posibles actuaciones infractoras en los puertos por sus operadores, presentadas por las instancias de fiscalización y control de la AMP, ésta tiene la obligación de formular y ejecutar los expedientes sancionadores correspondientes. En este sentido, una vez advertida la existencia de una posible infracción, la AMP después de hacer las diligencias previas oportunas, incoará al presunto infractor un expediente sancionador. En cualquier caso, es preceptiva la notificación del pliego de cargos al presunto infractor para que pueda formular las alegaciones que considere pertinentes antes de que se dicte la resolución.

En la tramitación de procedimientos sancionadores por hechos sucedidos en el ámbito de los puertos operados mediante contratos de servicios, es obligatoria la audiencia al concesionario por un término no mayor de cinco días hábiles, contados a partir de su notificación oficial.

En cualquier circunstancia, los afectados por medidas y sanciones de conformidad a esta ley, tendrán el derecho de audiencia en el que se les garantice el debido proceso.

MEDIDAS CAUTELARES

Artículo 232

Incoado el expediente sancionador, la AMP podrá adoptar mediante acuerdo motivado, las medidas cautelares de carácter provisional que sean necesarias para asegurar la eficacia de la resolución que pueda recaer, para preservar los intereses generales o para evitar el mantenimiento de los efectos de la infracción.

La AMP podrá ordenar la paralización inmediata de las obras o de las instalaciones y la suspensión de los usos y de las actividades que no disponen del título administrativo correspondiente o que no se ajustan a las condiciones del título otorgado.

La AMP puede cercar el recinto de las obras o de las instalaciones y ordenar la retirada de los materiales, de la maquinaria o de los equipos que se utilizan en las obras o actividades a cargo del interesado. A estos efectos, la AMP puede requerir, si lo considera conveniente, la colaboración de la fuerza pública.

En los casos de inexistencias de título correspondiente, la persona interesada solicitará a la AMP el título respectivo, o en su caso, ajustará las obras o la actividad a lo que tenga otorgado, en el plazo que fije la notificación de la orden de suspensión.

Transcurrido el plazo a que se refiere el inciso anterior sin que el interesado haya cumplido lo que se prescribe, la AMP podrá ordenar la demolición de las obras o el desmantelamiento de las instalaciones, a costa y cargo de la persona interesada, e impedirá definitivamente los usos o las actividades no autorizados. La AMP procederá de igual forma cuando el título sea denegado por no ajustarse a la normativa vigente.

Así mismo, la AMP puede ordenar la adopción inmediata de las medidas necesarias para evitar los daños que pueda provocar un buque u otra embarcación en peligro de hundimiento o en situación de causar daños a bienes o elementos portuarios o a otras embarcaciones. También podrá ordenar la inmediata retención, por causa justificada, de los buques y de las embarcaciones para garantizar las posibles responsabilidades administrativas o económicas de sus propietarios, representantes autorizados, capitanes o patrones, sin perjuicio de que esta medida cautelar pueda ser sustituida por la constitución de un aval suficiente.

CAPITULO III DE LAS MULTAS Y SU GRADUACIÓN

GRADUACIÓN DE LAS MULTAS

Artículo 233

Las infracciones, sean marítimas o portuarias, reguladas por la presente Ley, se sancionan con las multas siguientes:

1. Las infracciones leves, hasta 12,000.00 Derechos Especiales de Giro;
2. Las infracciones graves, de 12,001.00 hasta 48,000.00 Derechos Especiales de Giro; y
3. Las infracciones muy graves, de 48,001.00 hasta 96,000.00 Derechos Especiales de Giro.

La cuantía de las multas se graduará de acuerdo a la gravedad del hecho constitutivo de la infracción, considerando los daños y perjuicios producidos, el riesgo objetivo causado a los bienes o a las personas, la relevancia externa de la conducta infractora, la existencia de intencionalidad y la reincidencia.

A efectos de la graduación de sanciones, se considera reincidencia la comisión de una infracción de la misma naturaleza antes de que haya prescrito la infracción anterior.

Si un mismo hecho u omisión es constitutivo de dos infracciones o más, o si de la comisión de una infracción se deriva necesariamente otra, se impone únicamente la sanción correspondiente a la infracción más grave de las cometidas.

Capítulo IV DE LAS INFRACCIONES Y SANCIONES PORTUARIAS ESPECIALES

INFRACCIONES Y SANCIONES SOBRE CONSTRUCCIÓN Y OPERACIÓN DE PUERTOS

Artículo 234

Las autorizaciones para la construcción y la explotación de puertos, dársenas e instalaciones marítimas, en materia de infracciones y sanciones se regulan según los siguientes casos:

1. No cumplir con las condiciones de construcción, operación y explotación de los puertos, terminales marinas e instalaciones portuarias de acuerdo con lo establecido en los reglamentos, programa maestro de desarrollo portuario, contratos de gestión y normas oficiales salvadoreñas, de 6,000.00 a 120,000.00 Derechos Especiales de Giro;
2. Construir, operar y explotar terminales marinas e instalaciones portuarias sin la autorización respectiva de la AMP, de 60,000.00 a 120,000.00 Derechos Especiales de Giro;
3. Prestar servicios portuarios sin el permiso o contrato correspondiente, de 30,000.00 a 60,000.00 Derechos Especiales de Giro;
4. Construir embarcaderos, atracaderos, botaderos y demás similares sin el permiso o autorización de la AMP, de 12,000.00 a 30,000.00 Derechos Especiales de Giro;
5. Ceder totalmente los derechos y obligaciones derivados de la concesión sin la autorización de la AMP, de 180,000.00 a 240,000.00 Derechos Especiales de Giro;
6. Aplicar tarifas superiores a las autorizadas, con 60,000.00 a 90,000.00 Derechos Especiales de Giro;
7. Efectuar modificaciones substanciales al programa de inversiones del operador portuario sin autorización de la AMP, de 18,000.00 a 90,000.00 Derechos Especiales de Giro;

8. No presentar los informes solicitados por la AMPL o por la AMP, con 4,000.00 Derechos Especiales de Giro;
9. No registrar las modificaciones menores al programa de inversión de los operadores portuarios, de 18,000.00 a 30,000.00 Derechos Especiales de Giro; y
10. Las demás infracciones a esta ley o a sus reglamentos, de 4,000.00 a 60,000.00 Derechos Especiales de Giro.

En caso de reincidencia, se aplicará multa por el doble de las cantidades señaladas en este artículo.

Al imponer las sanciones a que se refiere el presente artículo, la AMP deberá considerar los criterios siguientes: La gravedad de la infracción, los daños causados y la reincidencia.

El que sin haber previamente obtenido una autorización o permiso de la AMP o sin el respectivo contrato de gestión, ocupe, construya o explote áreas, terminales marinas o instalaciones portuarias, o preste servicios portuarios, perderá en beneficio del Estado, las obras ejecutadas, las instalaciones establecidas y todos los bienes muebles e inmuebles, dedicados a la explotación, sin perjuicio de la aplicación de la multa que corresponda. En su caso, la AMP podrá ordenar que las obras e instalaciones sean demolidas y removidas por cuenta del infractor.

MANEJO DE COSTAS Y RESTRICCIONES SOBRE EL USO DE PLAYAS

Artículo 235

Se prohíbe a todas las embarcaciones la descarga de basura, petróleo y sus derivados, descargas de aguas residuales y otros elementos peligrosos o nocivos que pudieran contaminar o dañar las aguas bajo la jurisdicción de El Salvador.

En el Reglamento correspondiente, se deberán señalar las excepciones siguientes: cuando exista peligro inminente para la vida humana o para la seguridad de una nave; y cuando se efectúen dragados que tiendan a facilitar la navegación o a preservar el equilibrio ecológico marino.

La contaminación del mar que contravenga las disposiciones generales que se establezcan sobre la materia, estará sujeta a las multas y sanciones siguientes: multas de 36,000.00 a 120,000.00 Derechos Especiales de Giro; clausura temporal, definitiva, parcial o total de la instalación; arresto administrativo por hasta 36 horas; y suspensión o revocación de permisos, licencias o autorizaciones.

Además de las sanciones administrativas, se podrán imponer las sanciones establecidas en las demás leyes de la República.

FACULTAD DE LOS INSPECTORES NAVALES

Artículo 236

Los inspectores navales de la AMP podrán abordar a cualquier barco que se sospeche transporta una carga con intención de verterla ilegalmente al mar; examinar cualquier sustancia o carga; exigir la inspección de toda la documentación y permisos; acompañar a barcos a fin de asegurar que el vertimiento se realiza en los lugares adecuados; y detener a cualquier barco durante el tiempo que fuera necesario para realizar una debida inspección. Los propietarios y tripulación de una nave deben brindar plenas facilidades a la inspección.

Un inspector, de conformidad a la reglamentación respectiva, podrá requerir la detención de un buque en el puerto hasta que se haya subsanado una infracción a las normas nacionales que apliquen sobre la materia de vertimientos en el mar; además, los propietarios y la tripulación de un barco están sujetos a la serie ascendente de multas, de acuerdo con la gravedad de la infracción.

Estas sanciones incluyen:

1. Multas de 4,000.00 a 12,000.00 Derechos Especiales de Giro por vertimientos de sustancias no autorizadas y que poseen riesgos de contaminación;
2. Multas de 1,500.00 a 6,000.00 Derechos Especiales de Giro por vertimientos no autorizados de sustancias que no se incluyen en los anexos de vertimiento I o II, del Convenio Internacional Sobre la Prevención de la Contaminación del Mar por Vertidos de Desechos Sólidos y Otras Materias, del año 1972, pero que representan un riesgo de contaminación;
3. Multas de 3,000.00 a 6,000.00 Derechos Especiales de Giro por el abandono de barcos o plataformas; y
4. Multas de hasta 12,000.00 Derechos Especiales de Giro, además de las multas civiles correspondientes, cuando el propietario u operador de un barco efectúa un vertimiento por circunstancias contingentes y no informe a la Autoridad Portuaria Local de tal hecho.

La aplicación de las multas bajo el Reglamento de vertimientos en el mar es independiente de la aplicación de las sanciones o multas a que hubiera lugar de acuerdo con otras leyes y reglamentos, así como también de lo establecido en convenios y tratados internacionales suscritos y ratificados por el Gobierno de la República de El Salvador.

MULTAS FACULTADAS A LOS INSPECTORES NAVALES

Artículo 237

La AMP a través de sus inspectores navales, impondrá multas entre 200.00 a 1,500.00 Derechos Especiales de Giro, en los casos siguientes:

1. Cuando las empresas navieras incumplan los requisitos siguientes que se requieren para actuar como naviero o empresa naviera salvadoreña: Ser salvadoreño o sociedad constituida conforme a las leyes salvadoreñas; Tener domicilio social en territorio nacional y estar inscrito en el Registro Marítimo Portuario Nacional.
2. Cuando las empresas navieras y operadoras, carezcan de seguro de responsabilidad en caso de la muerte o lesiones de los viajeros por daños causados con motivo de la prestación del servicio, salvo que pruebe que el accidente no le es imputable; así como en los casos de equipajes registrados como si se tratara de transporte de mercancías, así como de los efectos personales y de los equipajes de cabina, si se prueba que la pérdida o avería se debe a falta suya o de sus empleados.

MULTAS A CAPITANES DE EMBARCACIONES

Artículo 238

La AMP impondrá multas de 12,000.00 a 25,000.00 Derechos Especiales de Giro a los capitanes de las embarcaciones, en los casos siguientes:

1. Cuando los capitanes de embarcaciones incurran en las infracciones siguientes:
 - a) Poseer embarcaciones abanderadas en más de un país y no tener marcado el nombre de las mismas y el puerto de matrícula;
 - b) Falta del despacho de salida del puerto de origen, de embarcaciones que arriben a puerto;
 - c) No utilizar el servicio de pilotaje o remolque, cuando éste sea obligatorio.
2. Hacerse a la mar, cuando por mal tiempo o previsión de él, la AMPL prohíba salir;
3. No justificar ante la AMPL las arribadas imprevistas o forzosas de las embarcaciones;

4. Atentar contra la seguridad de la embarcación, de los bienes y personas en ella transportadas, así como contra la infraestructura y superestructura de los puertos en donde recalá;
5. Cuando los capitanes o patrones de las embarcaciones incumplan con la asignación del número de tripulantes que corresponde a una embarcación, y que incumpla su respectiva capacitación;
6. Cuando los capitanes y patrones de embarcaciones, no posean a bordo de la embarcación el original del certificado de matrícula de la embarcación;
7. Cuando los capitanes de embarcaciones, incumplan los requerimientos sobre la seguridad común de la embarcación; y
8. Cuando los capitanes o patrones de las embarcaciones, incumplan con su responsabilidad de ejercer el mando, vigilando que se mantenga el orden y la disciplina a bordo, sin que tal ejercicio de competencia se interprete como una actuación en defecto de las autoridades salvadoreñas; asimismo, cuando tengan conocimiento de la comisión u omisión de actos que supongan el incumplimiento de los ordenamientos legales en vigor y no den aviso oportuno a las autoridades correspondientes.

MULTAS A PROPIETARIOS DE EMBARCACIONES

Artículo 239

La AMP impondrá multas de 12,000.00 a 30,000.00 Derechos Especiales de Giro, a los propietarios de embarcaciones o a las empresas navieras, en los casos siguientes:

1. Por proceder al desmantelamiento de una embarcación, sin la autorización de la AMP;
2. Por no efectuar en el plazo que fije la AMP, la señalización, remoción o extracción de embarcaciones, aeronaves o artefactos navales a la deriva, hundidos, varados o abandonados;
3. Cuando los navieros, para la explotación de embarcaciones en servicio de navegación interior y de cabotaje, no cuenten con el respectivo permiso de la AMP, en los casos de prestación de los siguientes servicios:
 - a) Transporte de pasajeros y cruceros turísticos;
 - b) Turismo náutico, con embarcaciones menores de recreo y deportivas salvadoreñas, o mediante las embarcaciones extranjeras depositadas en una marina turística autorizada;
 - c) Remolque maniobra y lanchaje en puerto, excepto cuando tengan celebrado contrato con el administrador portuario, conforme a lo que establece la presente Ley.
4. Por no cumplir con la prohibición relativa a que toda embarcación no deberá arrojar lastre, escombros, basura, derramar petróleo o sus derivados, aguas residuales de minerales u otros elementos nocivos o peligrosos, de cualquier especie que ocasionen daños o perjuicios en las aguas de jurisdicción salvadoreña;
5. Porque los buques que naveguen en las zonas marinas salvadoreñas no cuenten con seguro de protección e indemnización por responsabilidad civil;
6. Abanderar o matricular una embarcación o artefacto naval en otro Estado, sin haber obtenido previamente la dimisión de la bandera salvadoreña; y
7. Las personas naturales o jurídicas que actúen como agente naviero u operador, sin estar inscritos en el REMS.

DISPOSICIONES GENERALES EN MATERIA DE INFRACCIONES Y SANCIONES

INCUMPLIMIENTOS DE LAS PARTES

Artículo 240

El incumplimiento de cualquiera de los actos vinculados a la actividad marítima y portuaria, obligaciones contractuales o violaciones a las disposiciones y reglamentos de la AMP, constituyen infracciones sujetas de multas.

Las penalidades o multas que la AMP aplique ante infracciones de personas naturales o jurídicas vinculadas con la actividad marítima portuaria en El Salvador, serán sancionadas tanto por acción como por omisión de obligaciones legales, reglamentarias o contractuales. En los casos de operaciones portuarias privadas, el titular de éstas será responsable frente a la AMP por los hechos u omisiones que cometan personas naturales o jurídicas que desarrollen actividades en el área bajo su responsabilidad.

EJECUCIÓN DE GARANTIAS

Artículo 241

Toda penalidad o multa que establezca la AMP en el ejercicio de sus funciones jurisdiccionales, deberá ser cancelada por el responsable dentro de los diez días hábiles posteriores a ser declarada en firme. Vencido dicho plazo sin que la multa no haya sido cancelada, se faculta a la AMP a ejecutar las garantías contractuales que posea o a tomar otras medidas en el mismo sentido a fin de asegurar el cobro de su crédito.

INCUMPLIMIENTOS

Artículo 242

Todo incumplimiento a las disposiciones legales, reglamentarias o contractuales, cometido por personas naturales o jurídicas vinculadas con la actividad marítima y portuaria, será efectivo de multa a ser aplicada por la AMP. En especial, se aplicarán multas a las siguientes infracciones:

- a. Por atrasos no justificados en el pago de cánones y otras obligaciones a la AMP u otros organismos estatales; y
- b. Por falta de mantenimiento de garantías contractuales.

TITULO VI CAPITULO UNICO DISPOSICIONES TRANSITORIAS

ETAPA DE TRANSICIÓN

Artículo 243

En tanto no se encuentre en pleno funcionamiento la AMP, sus competencias y funciones serán ejercidas por el Ente Rector.

ASIGNACIÓN INICIAL

Artículo 244

Para iniciar el funcionamiento de la AMP, autorizase al Ministerio de Hacienda para transferir a la constitución de ésta, el efectivo necesario para el funcionamiento de sus tres primeros meses, en concepto de aporte inicial al patrimonio.

TRANSFERENCIA DE BIENES A LA AMP

Artículo 245

El Ministerio de Obras Públicas, Transporte y de Vivienda y Desarrollo Urbano deberá transferir a la AMP los bienes que estime necesarios para garantizar su adecuado funcionamiento.

CONSTITUCIÓN DE LA JUNTA DE DIRECTORES

Artículo 246

La Junta de Directores de la AMP deberá ser constituida dentro del plazo de treinta días posteriores a la fecha de entrada en vigencia de esta Ley.

NOMBRAMIENTO DEL DIRECTOR EJECUTIVO

Artículo 247

El primer Director Ejecutivo de la AMP será nombrado por el CDAMP.

LIBRE COMPETENCIA

Artículo 248

Mientras el país no cuente con una legislación específica que norme la libre competencia, en atención a las disposiciones de la presente Ley, será atribución de la Junta de Directores de la AMP velar porque se cumpla con los principios que rigen la materia dentro de las actividades marítimas y portuarias.

VIGENCIA DE REGLAMENTOS

Artículo 249

Los reglamentos de la presente Ley deberán ser decretados por el Presidente de la República, en el entendido que mientras no se emitan los nuevos reglamentos, continuará vigente la siguiente normativa: Las Regulaciones Portuarias para el Puerto de Acajutla contenidas en el Decreto Ejecutivo No. 43, de fecha 17 de junio de 1975, publicado en el Diario Oficial No. 278, Tomo No. 248, del 15 de agosto de ese mismo año.

Las tarifas del Puerto de Acajutla, permanecerán vigentes hasta en tanto la Comisión Ejecutiva Portuaria Autónoma, dentro del plazo de noventa días, someta a aprobación de la AMP el pliego de tarifas que serán aplicados para el referido puerto.

TITULO VII

CAPITULO UNICO
ESPECIALIDAD DE LA LEY Y PRESCRIPCIONES

CARÁCTER ESPECIAL DE LA LEY

Artículo 250

Las disposiciones de la presente Ley, por su especialidad, prevalecen sobre cualquier otra ley de carácter general o especial que regule la misma materia, exceptuándose aquéllas que de acuerdo al artículo 213 de la Constitución de la República disponga normativas legales para la Fuerza Armada en su rama permanente de la Fuerza Naval.

PRESCRIPCIONES

Artículo 251

Prescribirán en el plazo de cinco años todas las demás acciones que se contemplan en esta Ley, a las que no se les haya señalado un plazo especial.

AUTORIDAD PORTUARIA LOCAL DE LOS PUERTOS MERCANTES ESTATALES

Artículo 252

La CEPA será la autoridad marítima portuaria local de los puertos mercantes estatales bajo su jurisdicción y en éstos tendrá competencias en concepto de administración, operación, mantenimiento y conservación. En representación de CEPA, dicha autoridad será ejercida por el operador de esos puertos.

TITULO VIII
CAPITULO UNICO
DEROGATORIAS Y VIGENCIA

DEROGATORIAS

Artículo 253

Deróganse los siguientes cuerpos normativos:

- a. Decreto Legislativo de fecha 17 de marzo de 1904, publicado en el Diario Oficial No. 156, Tomo No. 57, del 4 de julio de ese mismo año, en la parte vigente del anterior Código de Comercio: Libro Tercero del Comercio Marítimo;
- b. Los Decretos Legislativos que reforman, adicionan o interpretan los Decretos derogados por las disposiciones contenidas en los literales anteriores.

Por lo demás, continuarán vigentes las leyes y reglamentos sobre legislación marítima portuaria, en lo referente a las materias sobre las que no se haya legislado en la presente Ley.

VIGENCIA

Artículo 254

El presente Decreto entrará en vigencia treinta días después de su publicación en el Diario Oficial.

DADO EN EL PALACIO LEGISLATIVO: San Salvador, a los diecinueve días del mes de septiembre del año dos mil dos.

Ciro Cruz Zepeda Peña,
Presidente.

Walter René Araujo Morales, Julio Antonio Gamero Quintanilla,
Primer Vicepresidente. Segundo Vicepresidente.

René Napoleón Aguiluz Carranza,
Tercer Vicepresidente.

Carmen Elena Calderón de Escalón, José Rafael Machuca Zelaya,
Primera Secretaria. Segundo Secretario.

Alfonso Arístides Alvarenga, William Rizziery Pichinte,
Tercer Secretario. Cuarto Secretario.

Rubén Orellana Mendoza,
Quinto Secretario.

A N E X O 1 2

**L e y d e M e d i a c i ó n ,
C o n c i l i a c i ó n y
A r b i t r a j e d e E l
S a l v a d o r**

ASAMBLEA LEGISLATIVA --- INDICE LEGISLATIVO

REPUBLICA DE EL SALVADOR --- AMERICA CENTRAL

DECRETO No. 914.-

LA ASAMBLEA LEGISLATIVA DE LA REPUBLICA DE EL SALVADOR,

CONSIDERANDO:

I.- Que nuestra Constitución establece en el Artículo 23 que ninguna persona que tenga la libre administración de sus bienes puede ser privada del derecho de terminar sus asuntos civiles o comerciales por transacción o arbitramento;

II.- Que es conveniente fomentar dentro de la cultura jurídica el acercamiento de los interesados en la solución de sus diferencias, por medio del diálogo y la utilización de medios alternativos, que a su vez permitan la búsqueda de soluciones creativas y ágiles a los asuntos tratados, con sencillez y mayor privacidad;

III.- Que si bien la legislación vigente reconoce algunos medios de solución alternativos de diferencias, éstos no han tenido el adecuado desarrollo, por lo que se vuelve necesario fortalecer tales figuras, especialmente la relativa a la mediación, conciliación y **arbitraje**;

POR TANTO,

en uso de sus facultades constitucionales y a iniciativa del Presidente de la República, por medio del Ministro de Gobernación y de los Diputados **Ciro Cruz Zepeda Peña, Julio Antonio Gamero Quintanilla, René Napoleón Aguiluz Carranza, Rubén Orellana Mendoza, Rosario del Carmen Acosta, Wilfredo Iraheta Sanabria, José Antonio Alamendaris Rivas, Rafael Edgardo Arévalo Pérez, José Orlando Arévalo Pineda, Nelson Edgardo Avalos, Rodrigo Avila Aviles, Juan Miguel Bolaños Torres, Carlos Antonio Borja Letona, Isidro Antonio Caballero Caballero, Mario Tenorio, Mauricio Membreño, Roberto d'Aubuisson Munguía, Jesús Guillermo Pérez Zarco, Juan Duch Martínez, Carmen Córdova, Rigoberto Trinidad, Nelson Funes, Guillermo Antonio Gallegos Navarrete, Elizardo González Lovo, Noe Orlando González, Elmer Roberto Charlaix, Manuel Durán, Gustavo Chiquillo, Mauricio Hernández Pérez, Vicente Menjivar, Francisco Alberto Jovel Urquilla, Carlos Mauricio Arias, Mauricio López Parker, Efigenio Marquez, Alejandro Dagoberto Marroquín, Juan Ramón Medrano Guzmán, William Eliú Martínez, José Francisco Merino López, José Luis Sánchez, Mariella Peña Pinto, Francisco Flores Zeledón, Ernesto Iraheta, José Mauricio Quinteros Cubias, Carlos Armando Reyes Ramos, Horacio Humberto Ríos Orellana, Héctor Nazario Salaverría Mathies, Gerardo Antonio Suvillaga García, David Humberto Trejo, Enrique Valdez Soto, Saúl Alfonso Monzón, Jorge Alberto Villacorta Muñoz, Fabio Balmore Villalobos Membreño, Roberto Villatoro, Martín Francisco Antonio Zaldivar Vides, Ernesto Angulo, Alba Teresa de Dueñas, Héctor Alfredo Guzmán, Emilio Guzmán y Alfredo Arbizu,**

DECRETA LA SIGUIENTE:

LEY DE MEDIACIÓN, CONCILIACIÓN Y ARBITRAJE

**TÍTULO PRIMERO
DISPOSICIONES GENERALES**

Objeto de la Ley

Art. 1.- Esta Ley establece el régimen jurídico aplicable al **arbitraje**, sin perjuicio de lo dispuesto en los tratados o convenios internacionales vigentes.

Asimismo, reconoce la eficacia de otros medios alternativos de solución de diferencias, que facultativamente pueden adoptar las personas naturales o jurídicas capaces, en asuntos civiles o comerciales, sobre los cuales tengan la libre disposición de sus bienes y que sean susceptibles de transacción o desistimiento.

Medios Alternativos de Solución de Diferencias

Art. 2.- Cuando en forma distinta de la prescrita en esta Ley dos o más personas, pacten la intervención dirimente de uno o más terceros y acepten expresa o tácitamente su decisión, después de emitida, el acuerdo será válido y obligatorio para las partes si en él concurren los requisitos necesarios para la validez de un contrato.

Definiciones

Art. 3.- Para los efectos de la presente Ley, se entenderá por:

- a) Mediación: un mecanismo de solución de controversias a través del cual, dos o más personas tratan de lograr por sí mismas la solución de sus diferencias con la ayuda de un tercero neutral y calificado que se denomina mediador;
- b) Conciliación: un mecanismo de solución de controversias a través del cual, dos o más personas tratan de lograr por sí mismas la solución de sus diferencias con la ayuda del Juez o árbitro, según el caso, quien actúa como tercero neutral, y procura avenir los intereses de las partes;
- c) **Arbitraje**: un mecanismo por medio del cual las partes involucradas en un conflicto de carácter transigible, difieren su solución a un tribunal arbitral, el cual estará investido de la facultad de pronunciar una decisión denominada laudo arbitral;
- d) Convenio Arbitral: es el acuerdo por el cual las partes deciden someter a **arbitraje** las controversias que hayan surgido o puedan llegar a surgir entre ellas, respecto de una determinada relación jurídica, de naturaleza contractual o extracontractual;
- e) Tribunal Arbitral: significa tanto un solo Árbitro como una pluralidad de árbitros;
- f) **Arbitraje** Ad-hoc: aquel en el cual las partes acuerdan autónomamente las reglas de procedimiento aplicables en la solución de su controversia;
- g) **Arbitraje** o Mediación Institucional: aquel en el que las partes se someten a un procedimiento establecido por el respectivo Centro de **Arbitraje** o de Mediación, autorizado de conformidad a esta ley;
- h) **Arbitraje** Internacional: el que se da en cualquiera de los siguientes casos:
 - 1.- Cuando las partes de un convenio arbitral tengan, al momento de celebración del mismo, sus domicilios en Estados diferentes.
 - 2.- Si uno de los lugares siguientes está situado fuera del Estado en el que las partes tienen sus domicilios:

a) El lugar del **arbitraje**, si éste se ha determinado en el Convenio Arbitral, o con arreglo al mismo sea distinto.

b) El lugar del cumplimiento de una parte sustancial de las obligaciones de la relación jurídica o el lugar con el cual el objeto del litigio tenga una relación más estrecha.

Para los efectos de este literal si alguna de las partes tiene más de un domicilio, éste será el que guarde una relación más estrecha con el Convenio Arbitral; si una parte no tiene ningún domicilio, se tomará en cuenta su residencia.

i) **Arbitraje** Extranjero: aquél cuyo laudo arbitral no ha sido pronunciado en El Salvador.

Principios

Art. 4.- El **arbitraje** se regirá por los siguientes principios:

1) Principio de libertad: es el reconocimiento de las facultades potestativas de las personas para adoptar medios alternativos al proceso judicial para la resolución de controversias;

2) Principio de flexibilidad: el cual se manifiesta mediante actuaciones informales, adaptables y simples;

3) Principio de privacidad: es el mantenimiento obligatorio de la necesaria reserva y confidencialidad;

4) Principio de idoneidad: consiste en la capacidad y requisitos que se deben cumplir para desempeñarse como árbitro o mediador;

5) Principio de celeridad: consiste en la continuidad de los procedimientos para la solución de las controversias;

6) Principio de igualdad: consiste en dar a cada parte las mismas oportunidades de hacer valer sus derechos;

7) Principio de audiencia: consiste en la oralidad de los procedimientos alternativos; y,

8) Principio de contradicción: consiste en la oportunidad de confrontación entre las partes.

Reglas de Interpretación

Art. 5.- Adóptase las siguientes reglas de interpretación comunes a la presente ley:

a) El **Arbitraje** puede ser en derecho, equidad o técnico.

El **Arbitraje** en derecho es aquel en el cual los árbitros fundamentan su decisión en el derecho positivo vigente.

El **Arbitraje** en equidad o de amigables componedores es aquel en que los árbitros proceden con entera libertad, deciden según sea más conveniente al interés de las partes, sin atender más que a su conciencia, la verdad y la buena fe.

En cambio, cuando los árbitros pronuncien su fallo en razón de sus específicos conocimientos en una determinada ciencia, arte u oficio, el **arbitraje** es técnico.

b) Cuando una disposición de la presente ley otorgue a las partes la facultad de decidir libremente sobre una cuestión determinada, dicha facultad implicará la de autorizar a una tercera persona,

natural o jurídica, a que adopte esa decisión.

c) Cuando una disposición de la presente ley, se refiera a un convenio arbitral celebrado o por celebrar, se entenderán comprendidas en ese convenio todas las disposiciones del Reglamento de **Arbitraje** que las partes hayan decidido adoptar.

d) Las normas referidas a la integración del Tribunal Arbitral y al procedimiento arbitral son de carácter supletorio con relación a la voluntad de las partes.

Cuantía

Art. 6.- Para los efectos de la presente ley, se considerarán asuntos de mayor cuantía aquellos en los cuales las pretensiones sean iguales o superiores a veinticinco mil colones y de menor cuantía los que tuvieren un monto inferior al indicado.

TÍTULO SEGUNDO DE LA MEDIACIÓN Y CONCILIACION CAPÍTULO ÚNICO

Solicitud de Mediación

Art. 7.- Presentada la solicitud de la Mediación al Centro, se designará por el Director del mismo, al mediador; éste procederá a citar a los interesados para llevar a cabo la primera audiencia común, señalándoles lugar, día y hora para ello, y les indicará los beneficios de resolver el asunto en forma amigable.

Primera Audiencia de Mediación

Art. 8.- En la primera audiencia común, el mediador deberá explicarles a los interesados, además del motivo de la reunión, el carácter confidencial del procedimiento, el trámite que habrá de dársele a la solicitud, la conducta que deben observar durante las audiencias o reuniones que al efecto se lleven a cabo y la conveniencia de lograr un arreglo.

En esta primera audiencia expondrá en primer lugar su punto de vista el solicitante, y luego expondrá el suyo el requerido.

Señalización de Más Audiencias

Art. 9.- Si fueren necesarias otras audiencias o reuniones comunes, el mediador lo hará saber a los interesados y señalará las fechas y horas para su celebración.

Audiencias por Separado

Art. 10.- Podrá el mediador celebrar audiencias separadas con cada uno de los interesados, comunicándoselos previamente.

Caso de Personas Jurídicas

Art. 11.- Las personas jurídicas comparecerán al procedimiento de la Mediación por medio de quien tenga la representación de las mismas.

Confidencialidad

Art. 12.- Todas las declaraciones y manifestaciones del requirente y requerido en las audiencias de Mediación son de carácter estrictamente confidencial y de ellas no se dejará constancia escrita. Los papeles de trabajo del mediador tendrán carácter personal, y de ellos no se dará traslado ni

copias, carecen de valor probatorio y no harán fe en juicio.

Fuerza Ejecutiva del Acuerdo

Art. 13.- La solución total o parcial de la disputa se consignará en acta y producirá los efectos de la transacción. La certificación que de ella extienda el Centro de Mediación tendrá fuerza ejecutiva en su caso.

Contenido del Acta

Art. 14.- El Acta que consigne el arreglo o solución de la disputa deberá contener:

- 1.- La identidad de los interesados, del mediador, de los abogados, de los peritos, en su caso; y de cualquier otra persona que haya intervenido en el procedimiento de Mediación;
- 2.- La identificación plena de la disputa;
- 3.- Las obligaciones, sometimientos, derechos y deberes que unilateral o recíprocamente acepten los interesados, incluyendo las formas, modalidades y términos de su cumplimiento o ejercicio, con la mayor claridad posible;
- 4.- La especificación de los puntos sobre los que no hubo acuerdo, en su caso;
- 5.- La firma de los interesados y del mediador. Si alguno de aquellos no pudiere firmar, lo hará otra persona a su ruego y dejará impresa cualquiera de sus huellas digitales;
- 6.- El lugar y fecha en que se levanta el acta.

Días y Horas Hábiles

Art. 15.- Todos los días y horas son hábiles para llevar a cabo los procedimientos de la Mediación.

Término de la Mediación

Art. 16.- El procedimiento de la Mediación termina cuando los interesados firman el acta de solución de la disputa, o de no haberse logrado la solución de la misma.

Prohibición

Art. 17.- Queda prohibido a los mediadores, peritos y a cualquier otra persona que haya intervenido en el procedimiento de la Mediación, excepto los abogados apoderados de las partes que hubieren podido intervenir; actuar en el procedimiento judicial que con posterioridad pudiera entablarse, bajo pena de nulidad de los actos en que intervenga.

Citaciones y Notificaciones

Art. 18.- Para las citaciones y notificaciones no habrá formalidades especiales, podrán hacerse vía telefónica y postal cuando el interesado así lo hubiere pedido y quede constancia para el mediador de haber efectuado la diligencia.

Recusación y Excusa

Art. 19.- Podrá recusarse al mediador ante el Director del Centro, sin necesidad de expresar causa; de igual forma podrán éstos excusarse. La manifestación respectiva deberá hacerse inmediatamente después de la primera audiencia común.

En ambas circunstancias, el Director del Centro designará un nuevo mediador para el caso.

Reglas de Conciliación

Art. 20.- La Conciliación se regirá principalmente por lo establecido en el Artículo 47, numeral 3 y Artículo 54 de esta Ley.

Las disposiciones de este Capítulo serán aplicables en lo pertinente a la Conciliación.

TÍTULO TERCERO
DEL **ARBITRAJE**
SECCIÓN PRIMERA
CAPÍTULO ÚNICO
DISPOSICIONES GENERALES

Ámbito de Aplicación

Art. 21.- La presente Ley se aplicará al **arbitraje** nacional. También se aplicará al **arbitraje** internacional, sin perjuicio de lo previsto en los tratados, pactos, convenciones o demás instrumentos de derecho internacional ratificados por El Salvador.

Materias Objeto de Arbitraje

Art. 22.- Podrán someterse a **arbitraje** las controversias que surjan o puedan surgir entre personas naturales o jurídicas capaces, sobre materias civiles o comerciales respecto de las cuales tengan libre disposición.

Materias Excluidas

Art. 23.- No podrán ser objeto de **arbitraje**:

- a) Los asuntos contrarios al orden público o directamente concernientes a las atribuciones o funciones de imperio del Estado o de personas de derecho público;
- b) Las causas penales, excepto en lo relativo a la responsabilidad civil proveniente del delito;
- c) Los alimentos futuros;
- d) Las controversias relativas a bienes o derechos de incapaces, sin previa autorización judicial;
- e) Aquellos conflictos relacionados con el estado familiar de las personas, excepto en lo relativo al régimen patrimonial atinente con éste; y,
- f) Las cuestiones sobre las cuales haya recaído sentencia judicial firme.

Expresa Exclusión de la Materia Laboral

Art. 24.- Las controversias de índole laboral no quedan sujetas a lo dispuesto por la presente ley.

Arbitraje en Controversias Estatales, Aplicación Preferente de Leyes Especiales y Tratados

Vigentes.

Art. 25.- Podrán someterse a **arbitraje** las controversias en las que el Estado y las personas jurídicas de derecho público son partes interesadas, siempre que versen sobre derechos disponibles y deriven de una relación jurídica patrimonial de derecho privado o de naturaleza contractual.

En las controversias derivadas de los contratos que el Estado salvadoreño o las personas de derecho público celebren con nacionales o con extranjeros domiciliados, se estará a lo dispuesto en leyes especiales o en tratados o convenios internacionales y, en su defecto, a lo establecido por esta Ley.

Podrán conocer del **arbitraje** para este tipo de controversias los Centros establecidos por la presente Ley.

Las empresas de derecho privado con capital estatal o las de economía mixta pueden acordar libremente y sin requisito de previa autorización que las controversias derivadas de los contratos que celebren con nacionales o extranjeros domiciliados o que se refieran a sus bienes propios, sean sometidas a **Arbitraje**.

Convenios Arbitrales Contenidos en Contratos de Adhesión

Art. 26.- Los convenios arbitrales referidos a relaciones jurídicas contenidas en cláusulas generales de contratación, contratos normalizados o contratos por adhesión, serán plenamente válidos entre las partes en tanto dichos convenios hayan sido conocidos o debían conocerse por la contraparte y su manifestación de voluntad de someterse al **arbitraje** se hiciera en forma expresa e independiente.

Se presume, sin admitir prueba en contrario, que el convenio arbitral debía conocerse, si se cumple con alguno de los siguientes supuestos:

- a) Si las condiciones generales que incluyen el convenio arbitral se hallan insertas en el cuerpo del contrato principal y éste último es por escrito y está firmado por ambas partes;
- b) Si las condiciones generales, a pesar de no estar reproducidas en el cuerpo del contrato principal, constan en el reverso del documento y se hace referencia al convenio arbitral en el cuerpo del contrato principal y éste es por escrito y firmado por la otra parte;
- c) Si el convenio arbitral se encuentra incluido en condiciones generales separadas del documento principal, pero se hace referencia en el cuerpo del contrato principal a la existencia del **arbitraje** y éste es por escrito y firmado por la otra parte; y,
- d) Fue puesto en conocimiento del público mediante adecuada publicidad.

La negativa del consumidor o usuario a someterse a un convenio arbitral no podrá impedir por sí misma la celebración del contrato principal.

Notificaciones y Comunicaciones Preliminares

Art. 27.- Las notificaciones y comunicaciones escritas previas a la iniciación del procedimiento arbitral se regirán por las siguientes reglas:

- a) Se considerará válida toda notificación y cualquier otra comunicación escrita que sea entregada personalmente al destinatario o a quien tenga su representación, en su domicilio especial, en el establecimiento donde ejerza su actividad principal o en su residencia;

b) Cuando no se logre determinar ninguno de los lugares señalados en el literal anterior, se considerará recibida toda notificación o comunicación escrita que haya sido remitida por carta certificada o cualquier otro medio que deje constancia del hecho, al último domicilio o residencia habitual conocidos;

c) En los dos casos anteriores, se considerará recibida la notificación o comunicación en la fecha en que se haya realizado la entrega; y,

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

Competencia y Auxilio Judicial

Art. 28.- En cuanto a la competencia y auxilio judicial, se estará a lo siguiente:

- a) En las controversias que se resuelvan con sujeción a la presente ley, solo tendrá competencia el tribunal arbitral correspondiente. Ningún otro tribunal o instancia podrá intervenir, salvo que esta Ley así lo autorizare expresamente; y,
- b) La autoridad judicial competente para prestar auxilio en los casos establecidos en la presente Ley, será la calificada para conocer de la controversia en ausencia de **arbitraje**. En defecto de ello, será la del lugar donde deba realizarse el **arbitraje**, si se hubiere previsto; a falta de ello y a elección del demandante, el del lugar de celebración del convenio arbitral o el del domicilio del de-mandado o el de cualquiera de ellos, si son varios.

SECCION SEGUNDA DEL **ARBITRAJE** NACIONAL CAPÍTULO I DEL CONVENIO ARBITRAL

Formalidades

Art. 29.- El convenio arbitral deberá constar por escrito.

Podrá adoptar la forma de una cláusula incluida en un contrato o la de un acuerdo independiente.

Se entenderá que el convenio se ha formalizado por escrito no solamente cuando esté contenido en documento único suscrito por las partes, sino también cuando resulte del intercambio de cartas o de cualquier otro medio de comunicación o correspondencia que inequívocamente deje constancia documental de la voluntad de las partes de someterse a **arbitraje**.

Asimismo, se presume que el convenio arbitral se ha formalizado por escrito cuando a pesar de no existir acuerdo previo, por iniciativa de una de las partes involucradas, se somete una controversia a la decisión de uno o más árbitros que aceptan resolver la controversia, mediando asentimiento posterior de la otra u otras partes a dicho sometimiento.

Se presumirá que hay asentimiento cuando, notificada la parte contraria de la iniciativa de quien promovió la intervención de él o los árbitros, se apersona al procedimiento arbitral sin objetar dicha intervención.

Autonomía

Art. 30.- Todo convenio arbitral que forme parte de un contrato principal se considera como un

acuerdo independiente de las demás estipulaciones del mismo.

En consecuencia, la nulidad total o parcial de un contrato u otro acto jurídico que contenga un convenio arbitral, no llevará consigo de modo necesario la del convenio arbitral accesorio.

Los árbitros podrán decidir libremente sobre la controversia sometida a su pronunciamiento, la que podrá versar, inclusive, sobre los vicios que afecten el contrato o acto jurídico que contenga el convenio arbitral.

Excepción de Arbitraje

Art. 31.- La excepción de **arbitraje** se regirá por los siguientes principios:

a) El convenio arbitral implica la renuncia de las partes a iniciar proceso judicial sobre las materias o controversias sometidas al **arbitraje**.

b) La autoridad judicial que tome conocimiento de una controversia sujeta a convenio arbitral debe declararse incompetente de conocer del caso cuando se lo solicite la parte judicialmente demandada. En este caso, dicha parte puede oponer la excepción de arbitraje que habrá de ser resuelta sin mayor trámite y sin lugar a recurso alguno contra la decisión.

Renuncia

Art. 32.- La renuncia al **arbitraje** se regirá por los siguientes principios:

a) La renuncia al **arbitraje** será válida únicamente cuando concurra la voluntad de las partes.

b) Las partes pueden renunciar expresamente al **arbitraje** mediante acuerdo de ellas al respecto que conste por escrito y sea firmado de manera conjunta, separada o sucesiva.

c) Se considera que existe renuncia tácita cuando una de las partes sea demandada judicialmente por la otra y no oponga una excepción de **arbitraje** en la oportunidad procesal correspondiente.

No se considera renuncia tácita al **arbitraje** el hecho de que cualquiera de las partes, antes o durante el procedimiento arbitral, solicite de una autoridad judicial competente la adopción de medidas precautorias o que dicha autoridad judicial conceda el cumplimiento de las mismas.

CAPITULO II DE LOS ÁRBITROS

Árbitros

Art. 33.- Los árbitros no representan los intereses de ninguna de las partes y ejercerán el cargo con estricta imparcialidad y absoluta discreción. En el desempeño de sus funciones tienen plena independencia y no están sometidos a orden, disposición o autoridad que menoscabe sus atribuciones, gozando además del secreto profesional.

Número de Árbitros

Art. 34.- Las partes determinarán el número de árbitros que, en todo caso, será impar. A falta de acuerdo de las partes los árbitros serán tres, si la controversia es de mayor cuantía, o uno, si ella es de menor cuantía.

Capacidad

Art. 35.- Sólo las personas naturales que se hallen en el pleno ejercicio de sus derechos ciudadanos podrán ser designadas como árbitros.

Cuando el **arbitraje** haya de decidirse con sujeción a derecho, los árbitros serán, además, abogados en el libre ejercicio de la profesión. Cuando el **arbitraje** se deba resolver conforme a normas o principios técnicos los árbitros deberán ser expertos en el arte, profesión u oficio respectivo.

Las partes podrán establecer requisitos o condiciones adicionales para los árbitros en el convenio arbitral.

Los árbitros tendrán los mismos poderes, deberes y responsabilidades de los Jueces comunes. En materia probatoria, los árbitros deberán analizar las pruebas y valorarlas conforme a las reglas de la sana crítica.

Inhabilitación

Art. 36.- No podrán actuar como árbitros quienes tengan con las partes o sus apoderados alguna de las causas de excusa y recusación que establecen las reglas procesales.

Tampoco podrán actuar como árbitros los Jueces, Magistrados, Fiscales, Diputados de la Asamblea Legislativa, funcionarios públicos y los empleados del Órgano Judicial.

Designación

Art. 37.- Las partes podrán designar los árbitros de manera directa y de común acuerdo o delegar en un tercero, persona natural o jurídica, la designación parcial o total de los árbitros.

Si no hubiere acuerdo entre las partes en la elección de los árbitros, cada parte elegirá uno y los dos árbitros designados elegirán un tercero, quien será el Presidente del Tribunal Arbitral.

En el **arbitraje** con árbitro único si alguna de las partes estuviere renuente a la designación, o no hubiere acuerdo entre las mismas o si los dos árbitros o el tercero o terceros delegados no pudieren acordar la designación del que faltare, éste o éstos serán designados por el Centro de **Arbitraje** que corresponda, cuando se trate de **arbitraje** institucional o, tratándose del **arbitraje** ad-hoc, por cualquiera de las instituciones arbitrales que estuvieren legalmente establecidas en el lugar del domicilio donde habrá de llevarse el **arbitraje**, a solicitud de cualquiera de las partes.

Nulidad

Art. 38.- Será nulo, en lo que se refiere a la forma de designación de los árbitros, el convenio arbitral que coloque a una de las partes en situación de privilegio en tal designación. En este caso, el resto del convenio conservará su validez y se aplicarán las reglas consagradas en la presente Ley para la designación de los árbitros.

Notificación y Aceptación del Nombramiento

Art. 39.- El nombramiento será comunicado a los árbitros designados de manera personal y tendrán cinco días hábiles para manifestar si lo aceptan o no. La falta de manifestación durante el término referido se tendrá como negativa y permitirá proceder al reemplazo respectivo.

Obligaciones

Art. 40.- La aceptación obliga a los árbitros y en el caso del **Arbitraje** Institucional a ellos y al Centro de **Arbitraje** respectivo, a cumplir su encargo con esmero y dedicación, incurriendo en la

obligación de reparar los daños y perjuicios que llegaren a causar a las partes o a terceros, en caso de no hacerlo así.

Honorarios y Gastos

Art. 41.- Los árbitros o el Centro de **Arbitraje**, en su caso, podrán exigir en cualquier momento a las partes la provisión de fondos que estime necesaria para atender a los honorarios de los árbitros y a los gastos que puedan producirse en la administración y tramitación del **arbitraje** o el ajuste de los mismos, si las condiciones del caso así lo ameritan. Los pagos habrán de producirse en la forma y momento en que los árbitros o la institución, así lo determinen. Los Centros, en sus reglamentos, deben establecer la cuantía y forma de pago de los honorarios de los árbitros, del Centro y los demás costos y gastos del trámite arbitral, siendo de obligatorio cumplimiento para las partes su observancia.

Impedimentos y Recusaciones

Art. 42.- Los árbitros podrán abstenerse de actuar como tales o ser recusados por las mismas causales establecidas por el Código de Procedimientos Civiles para los jueces. De igual manera podrán ser recusados por no reunir las condiciones que, conforme a la ley o a lo acordado por las partes, se hayan establecido para el caso.

La persona a quien se comunique su nombramiento como Árbitro deberá exponer ante quien lo nombró todas las circunstancias que puedan dar lugar a dudas justificadas respecto de su imparcialidad o independencia.

Los árbitros designados por las partes tan solo podrán ser recusados de manera inmediata y por causales que sobrevengan a su designación. También podrán serlo por causas anteriores cuando no hubieren sido nombrados directamente por las partes o cuando aquéllas fueren conocidas con posterioridad.

Procedimiento de Recusación y Sustitución

Art. 43.- Si el Árbitro no aceptare la recusación propuesta, la resolución de la misma se adoptará por el Centro de **Arbitraje**, en caso de tratarse de un **Arbitraje** Institucional o por los árbitros restantes, cuando fueren ad-hoc. En caso de Árbitro único, la decisión sobre la recusación se adoptará por el Juez que hubiere resultado competente para conocer el proceso objeto del **arbitraje**.

Contra la decisión de los árbitros, del Centro de **Arbitraje** o del Juez, en su caso, mediante la cual se resuelve la recusación, no cabrá recurso alguno.

Si el Árbitro se abstuviere de conocer del caso o aceptare la recusación o, conforme a las normas establecidas, resultare separado del conocimiento del caso o faltare al ejercicio de su cargo, se procederá a su reemplazo en la misma forma en que hubiere sido designado el Árbitro que deba sustituirse.

Organización del Tribunal Arbitral

Art. 44.- En el caso que el Tribunal estuviere conformado por más de un Árbitro, estos elegirán de su seno un Presidente del Tribunal Arbitral. A falta de acuerdo, ejercerá como Presidente el árbitro de mayor edad y si se tratare de **arbitraje** institucional, la designación del Presidente se hará de acuerdo con el reglamento respectivo.

En los casos en que existiere un solo Árbitro, éste ejercerá todas las funciones y atribuciones del Tribunal.

El Tribunal Arbitral, si lo considera pertinente, nombrará un Secretario o elegirá de entre ellos, si lo consideran conveniente, al que desempeñe las funciones de Secretario, quien en ningún caso podrá ser el Presidente del Tribunal Arbitral.

CAPÍTULO III DEL PROCEDIMIENTO ARBITRAL

Libertad de Procedimientos

Art. 45.- Las partes podrán sujetarse a las reglas de procedimiento del Centro de **Arbitraje** a que se someterá el Tribunal Arbitral.

Podrán asimismo determinar libremente las reglas de procedimiento o delegar en los árbitros el señalamiento de las mismas.

En caso que las partes no hayan resuelto sobre el particular, se seguirán las reglas del Centro de **Arbitraje** en el cual se haya de tramitar el **arbitraje**, cuando éste fuere institucional, o las que se establecen en esta ley, en caso de que se tratara de **arbitraje** ad-hoc.

En ningún caso cabrá dentro del trámite arbitral incidente alguno, excepto aquellos trámites contemplados en la presente Ley.

Actuaciones del Tribunal Arbitral

Art. 46.- En las actuaciones arbitrales en que hubiere más de un árbitro, toda decisión del Tribunal Arbitral se adoptará, salvo acuerdo en contrario de las partes, por mayoría de votos. Sin embargo, el árbitro presidente podrá decidir cuestiones de procedimiento, si así lo autorizan las partes o todos los Arbitros del Tribunal Arbitral.

La recepción de las pruebas sólo podrá realizarse con la presencia de la totalidad de los árbitros.

Reglas del **Arbitraje** Ad-hoc

Art. 47.- Salvo disposición en contrario adoptada por las partes o los árbitros, conforme a los términos del artículo precedente, el procedimiento arbitral, para el **arbitraje** ad-hoc, se sujetará a las siguientes reglas:

Demanda, Contestación, Plazos y Excepciones:

1.- La parte que promueva la iniciación del **arbitraje** deberá presentar ante los árbitros su demanda junto con sus anexos, dentro de los ocho días hábiles contados a partir de la aceptación del último Árbitro.

Recibida la demanda se correrá traslado de la misma de manera inmediata al demandado, quien tendrá ocho días hábiles para presentar su contestación, junto con los anexos respectivos. En este mismo plazo y oportunidad deberá presentar sus excepciones y demanda de reconvención si fuere el caso.

De las excepciones y la demanda de reconvención, en su caso, se correrá traslado al demandante para pronunciarse al respecto para cuyo efecto contara con diez días hábiles. En caso de proponer excepciones contra ella se dará el traslado en la forma y términos de la demanda principal.

Anexos a la demanda, su contestación o la demanda de reconvención, deberá agregarse toda la prueba documental que se pretenda hacer valer; en caso de no tenerla, se indicará su contenido, el lugar en que se encuentra y se pedirá su incorporación al proceso.

Caducidad y Rebeldía:

2.- En caso de que quien promueva la actuación arbitral no presentare su demanda dentro de la oportunidad prevista o no lo hiciere cumpliendo los requisitos legales, el Tribunal dará por terminadas sus funciones y devolverá las actuaciones a fin de que las partes promuevan su acción ante la justicia ordinaria.

No habrá acuse ni declaratoria de rebeldía, por lo que a falta de contestación de la demanda, el trámite continuará su curso.

Cita a Conciliación:

3.- Vencidos los plazos antes indicados, los árbitros citarán a las partes a una audiencia de conciliación en la forma que previene esta Ley. En caso de llegarse a un acuerdo los árbitros darán por terminado el trámite. Las partes podrán solicitar del Tribunal que el arreglo logrado sea elevado a la categoría de laudo arbitral definitivo.

Prueba:

4.- De no llegarse a un acuerdo total de las pretensiones, se continuará con el trámite en lo que hace relación a la evacuación de las pruebas las que, excepción hecha de las de carácter documental, serán practicadas en audiencia y deberán producirse dentro del plazo máximo de treinta días hábiles, contados desde la fecha de la contestación de la demanda o de la reconvención.

Alegatos:

5.- Evacuadas las pruebas los árbitros podrán solicitar a las partes la presentación de un resumen escrito de sus alegaciones.

Laudo:

6.- Verificado lo anterior, los árbitros procederán a emitir el laudo para lo cual deberán tener en cuenta el plazo máximo establecido para el trámite arbitral en la presente Ley.

Procedimiento de Mero Derecho:

7.- En aquellos eventos en que la materia disputada sea de mero derecho, una vez concluidas las diligencias a que se refiere el numeral 1 precedente, se dará curso a la audiencia de conciliación regulada en el numeral 3 anterior. De no haber acuerdo o siendo este parcial, el Tribunal procederá, de inmediato, a pronunciar su laudo, para lo cual contará con un plazo de quince días hábiles, si las partes no han fijado un plazo diferente. En el **Arbitraje** Institucional o en el evento de que el procedimiento sea establecido por las partes o los árbitros, conforme a lo establecido en esta Ley, se aplicará lo dispuesto en este numeral, salvo disposición de las partes en contrario.

Procedimiento de Menor Cuantía:

8.- En aquellos eventos en que se trate de **arbitraje** de menor cuantía, las partes podrán solicitar a los árbitros que, una vez concluidas las diligencias a que se refiere el numeral 1 precedente y fracasada la audiencia a que se refiere el numeral 3 anterior, se proceda en una sola audiencia a la práctica de pruebas y al dictado del laudo respectivo dentro de los cinco días hábiles siguientes a la práctica de las mismas. De no solicitarlo o en caso de no existir un procedimiento diferente,

se aplicará el procedimiento establecido en este artículo.

Procuración Obligatoria y Facultativa

Art. 48.- En los casos considerados de mayor cuantía las partes deberán actuar por conducto de un Abogado en el libre ejercicio de la profesión. En aquellos en que las pretensiones se tengan como de menor cuantía podrán actuar por si mismas o valerse de un profesional del derecho en ejercicio, a su elección.

Inicio y Duración del Procedimiento

Art. 49.- El procedimiento Arbitral se entiende iniciado cuando el último de los árbitros designados haya manifestado a las partes por escrito su aceptación del cargo. A partir de ese momento se contará el plazo de duración del Tribunal Arbitral que, salvo pacto en contrario de las partes, no podrá ser superior a tres meses, sin perjuicio de que las partes, de común acuerdo y en forma previa a su vencimiento, decidan prorrogarlo.

Transcurrido el plazo sin que se hubiere dictado el laudo, quedará sin efecto el convenio arbitral y expedita la vía judicial para plantear la controversia.

Suspensión Temporal y Desistimiento

Art. 50.- Las partes de común acuerdo, podrán en cualquier momento antes de dictarse el laudo, convenir el desistimiento del **arbitraje** o la suspensión del Trámite Arbitral; de igual manera se suspenderá en caso de muerte, renuncia, incapacidad definitiva, incapacidad temporal mayor de quince días o separación de un Árbitro, hasta tanto se haya reemplazado éste y el Árbitro designado haya aceptado el cargo.

En cualesquiera de los casos a que se ha hecho referencia, el término de suspensión del pro-ceso no se tendrá en cuenta para efectos del cómputo del plazo máximo de duración del trámite arbitral y, en consecuencia, deberá ser descontado en su totalidad.

Autonomía del Procedimiento

Art. 51.- Los árbitros están facultados para decidir acerca de su propia competencia, incluso sobre oposiciones relativas a la existencia, eficacia o a la validez del Convenio Arbitral.

La oposición total o parcial al **arbitraje** por ineficacia, invalidez o caducidad del Convenio Arbitral o por no estar pactado el **arbitraje** para resolver la materia controvertida, deberá formularse al presentar las partes sus pretensiones iniciales. Los árbitros, no obstante, podrán considerar estos temas de manera oficiosa.

Las partes no se verán impedidas de oponerse por el hecho de que hayan designado a un árbitro o participado en su designación.

Sin perjuicio de lo establecido en el Reglamento Arbitral de la Institución, en el caso del **Arbitraje** Institucional, o de lo acordado por los árbitros, o las partes, en el **arbitraje** ad-hoc, los árbitros resolverán estos temas como cuestión previa. Sin embargo, el Tribunal Arbitral podrá seguir adelante con las actuaciones y decidir acerca de tales objeciones en el laudo.

Lugar del **Arbitraje**

Art. 52.- Las partes podrán determinar libremente el lugar del **arbitraje**. Si no está previsto en el Convenio Arbitral, se estará a lo que dispongan al respecto las reglas del Centro de **Arbitraje**, cuando el **arbitraje** fuere institucional, o los árbitros, en los demás casos.

Idioma

Art. 53.- Las partes podrán acordar libremente el idioma que además del castellano haya de utilizarse en las actuaciones **arbitrajes**. A falta de tal acuerdo, el tribunal arbitral determinará el o los idiomas a emplearse en las actuaciones. Este acuerdo o esta determinación será aplicable, salvo pacto en contrario, a todos los escritos de las partes, a todas las audiencias y a cualquier laudo, decisión o comunicación de otra índole que emita el tribunal arbitral.

El tribunal arbitral podrá ordenar que cualquier prueba documental vaya acompañada de una traducción a uno de los idiomas convenidos por las partes o determinados por el tribunal arbitral.

Diligencias Previas y Conciliación

Art. 54.- El Director del Centro de **Arbitraje** deberá, antes que se dé inicio al trámite arbitral, citar a las partes para una audiencia de conciliación que habrá de llevarse a cabo bajo su dirección en el centro respectivo. Para tal efecto, la convocatoria se efectuará con anterioridad a la designación de los árbitros y, en caso de llegarse a un arreglo total de las pretensiones de las partes dará lugar a la conclusión del trámite arbitral. Si este fuere parcial, el Tribunal Arbitral se concretará a resolver tan solo las peticiones que quedaren pendientes del acuerdo.

En caso del **arbitraje** ad-hoc, se estará a lo previsto en el Artículo 47 número 3 precedente. Si hubiere acuerdo total entre las partes, éstas podrán solicitar que el mismo se registre en forma de laudo arbitral y se dará por terminado el trámite. Si no hubiere acuerdo o este fuere parcial, el trámite continuará para resolver las peticiones que quedaren pendientes.

En cualquier parte del trámite arbitral, sea ad-hoc o institucional, antes de pronunciar el laudo, las partes, de común acuerdo, podrán solicitar al tribunal sean convocadas a una nueva audiencia de conciliación que se sujetará a las mismas reglas establecidas en el presente Artículo o llegar a una transacción que se incorporará en un laudo arbitral si las partes así lo solicitan.

El tiempo que las partes tomen para la conciliación, desde la solicitud hasta el momento en que se produzca una definición entre ellas mediante un acuerdo o la negativa al mismo, no se tendrá en cuenta dentro del cómputo del plazo de duración máxima del trámite arbitral.

Reglas Probatorias

Art. 55.- Los árbitros tendrán la facultad exclusiva de determinar la admisibilidad, pertinencia y valor de las pruebas. De igual manera, estarán dotados con facultades suficientes para decretar oficiosamente, cuando lo consideren necesario, la práctica de pruebas de cualquier naturaleza.

En cualquier etapa del proceso, los árbitros podrán solicitar a las partes aclaraciones o informaciones.

Tratándose de prueba pericial, pueden ordenar que se explique o amplíe el dictamen.

Los árbitros pueden dar por vencidos los plazos de etapas ya cumplidas por las partes. La inactividad de las partes no impide la prosecución del proceso ni que se dicte el laudo basándose en lo ya actuado.

Los árbitros pueden prescindir motivadamente de las pruebas no evacuadas, si se consideran adecuadamente informados, mediante providencia que no tendrá recurso alguno.

La práctica de las pruebas, salvo en el caso de la prueba documental, se llevará a cabo en audiencia para cuyo efecto se citará a las partes con antelación suficiente de la fecha, hora y lugar en que la respectiva audiencia o diligencia se llevará a cabo.

Las pruebas serán practicadas por el Tribunal en pleno; para las pruebas que hayan de efectuarse fuera del lugar del domicilio, aquel podrá llevarlas a cabo directamente o comisionar a alguna autoridad judicial del lugar para que las practique. Para la práctica de pruebas en el extranjero, se estará a lo dispuesto en el Código de Procedimientos Civiles.

Las partes, de común acuerdo, podrán decidir que para la práctica de las pruebas fuera de la sede del Tribunal, se pueda acudir a la utilización de medios electrónicos o similares para la obtención de las mismas, no solo para la recepción de pruebas documentales sino para la de testimonios y demás pruebas, sin necesidad de comisionar en los términos antes indicados, en procura de mayor celeridad y abaratamiento de los costos del Trámite Arbitral.

Copias para las partes

Art. 56.- De todas las actuaciones, documentos y cualquier otra información que una de las partes suministre al Tribunal Arbitral se entregará copia a la otra sin necesidad de dictar providencia que así lo ordene. De igual manera, deberán ponerse a disposición de ambas partes los peritajes o los documentos probatorios en los que el Tribunal Arbitral pueda basarse para adoptar su decisión.

Auxilio Judicial

Art. 57.- El Tribunal Arbitral podrá solicitar el auxilio de cualquier autoridad judicial para la ejecución a práctica de pruebas que no pueda llevar a cabo por sí mismo.

Días y horas hábiles

Art. 58.- Para la práctica de las actuaciones arbitrales, todos los días y horas son hábiles.

CAPÍTULO IV DEL LAUDO ARBITRAL

Fundamento

Art. 59.- Los árbitros decidirán la cuestión sometida a su consideración con sujeción a derecho, equidad o conforme a normas y principios técnicos, de conformidad a lo estipulado en el Convenio Arbitral.

En caso de que las partes no hayan pactado al respecto, los árbitros deberán resolver con equidad.

Formalidades

Art. 60.- El laudo se pronunciará por escrito y deberá indicar:

- 1.- Lugar y fecha;
- 2.- Nombres, nacionalidad, domicilio y generales de las partes y de los árbitros;
- 3.- La cuestión sometida a **arbitraje** y una síntesis de las alegaciones y conclusiones de las partes;

4.- La valoración de las pruebas practicadas, si se tratare de **arbitraje** en derecho o su fundamentación, en caso de **arbitraje** en equidad;

5.- La resolución deberá ser clara, precisa y congruente con las demandas y demás pretensiones deducidas oportunamente en el pleito, haciendo las declaraciones que éstas exijan, condenando o absolviendo al demandado, y decidiendo todos los puntos litigiosos que hayan sido objeto del debate. Cuando éstos hubieren sido varios, se hará, con la debida separación, el pronunciamiento correspondiente a cada uno de ellos; guardando el orden lógico que corresponde;

6.- La determinación de las costas del proceso, si las hubiere; y,

7.- Las firmas de todos los miembros del Tribunal Arbitral o de la mayoría de ellos.

Votación

Art. 61.- El laudo podrá adoptarse por unanimidad o por simple mayoría de votos y estará firmado por los árbitros. El Árbitro disidente deberá manifestar por escrito las razones que motivan su separación del criterio de los árbitros mayoritarios. En caso de que no hubiese mayoría la decisión la tomará el Presidente del Tribunal.

Autenticidad

Art. 62.- El laudo arbitral en el caso de **arbitraje** institucional será tenido por auténtico con la firma del árbitro o árbitros que hubieren intervenido y el sello del Centro respectivo, sin necesidad de trámite judicial o notarial alguno.

En caso de **arbitraje** ad-hoc, el laudo se protocolizará notarialmente.

Cuando el laudo arbitral deba registrarse, bastará la presentación al registro de una copia del citado laudo, certificada por el Director del Centro de **Arbitraje**, en caso de **arbitraje** institucional, o por Notario, tratándose de **arbitraje** ad-hoc.

Efectos

Art. 63.- El laudo arbitral firme tiene la misma fuerza y validez de una sentencia judicial ejecutoriada y pasada en autoridad de cosa juzgada; se tendrá por notificado a las partes en la audiencia que los árbitros citarán para efectos de dictarlo, bien sea que ellas asistan o no a dicha audiencia. Del laudo se entregará copia auténtica a cada una de las partes.

Aclaración, Corrección o Adición

Art. 64.- El laudo estará sujeto a aclaración, corrección o adición y será firme una vez concluidas tales diligencias, cuando fuere el caso.

Dentro de los cinco días hábiles siguientes a la notificación del laudo a las partes, éstas podrán pedir aclaración de su parte resolutive; adición, para el evento de que algún extremo de la litis se hubiera quedado sin resolver o, corrección del mismo, por errores de cálculo, de copia o tipográfico, o los árbitros oficiosamente llevarla a cabo. El Tribunal deberá aclarar, complementar o corregir el laudo, si fuere del caso, dentro de un plazo no mayor de siete días hábiles contados a partir de la solicitud respectiva. Contra cualquiera de las decisiones a que se refiere este Artículo no cabe recurso alguno.

Laudo Ejecutorio

Art. 65.- El laudo arbitral firme causa ejecutoria en la misma forma y términos establecidos en el Código de Procedimientos Civiles para las sentencias judiciales.

CAPÍTULO V DE LOS RECURSOS

Regla General

Art. 66.- Contra las decisiones de los árbitros, diferentes del laudo, no procede recurso alguno.

Recurso de nulidad

Art. 67.- Contra el laudo arbitral únicamente podrá interponerse el recurso de nulidad dentro de los siete días hábiles siguientes a la notificación del mismo o de la providencia por medio de la cual se aclara, corrige o adiciona.

El recurso deberá interponerse por escrito y sólo procederá por las causales que de manera taxativa se establecen en la presente Ley. Su trámite corresponderá a la Cámara de Segunda Instancia de lo Civil de la jurisdicción del lugar donde se dictó el laudo. No obstante, las partes, a su costa, podrán estipular desde el Convenio Arbitral, que el recurso se tramitará y decidirá ante un nuevo Tribunal Arbitral, regulando en el mismo el trámite respectivo.

Causales

Art. 68.- Las únicas causales del recuso de nulidad del laudo son las siguientes:

- 1.- La nulidad absoluta del convenio arbitral proveniente de objeto o causa ilícitos. Los demás motivos de nulidad absoluta o relativa solo podrán invocarse cuando hayan sido alegados en el proceso arbitral y no se hayan saneado o convalidado en el transcurso del mismo.
- 2.- No haberse constituido el Tribunal Arbitral en forma legal, siempre que esta causal haya sido alegada de modo expreso desde la iniciación del Trámite Arbitral.
- 3.- No haberse hecho las notificaciones en la forma prevista en esta ley, salvo que de la actuación procesal se deduzca que el interesado conoció o debió conocer la providencia.
- 4.- Cuando sin fundamento legal se dejaren de decretar pruebas oportunamente solicitadas o se hayan dejado de practicar las diligencias necesarias para evacuarlas, siempre que tales omisiones tengan incidencia en la decisión y el interesado las hubiere reclamado en la forma y tiempo debidos, salvo el caso contemplado en el Artículo 55 inciso quinto de esta ley.
- 5.- Haberse pronunciado el laudo después del vencimiento del término fijado para el proceso arbitral o sus prórrogas.
- 6.- Haberse fallado en equidad debiendo ser en derecho, siempre que esta circunstancia aparezca manifiesta en el laudo.
- 7.- Contener la parte resolutive del laudo errores aritméticos o disposiciones contradictorias, siempre que se hayan alegado oportunamente ante el Tribunal Arbitral y no hubieren sido corregidas.
- 8.- Haberse recaído el laudo sobre puntos no sujetos a la decisión de los árbitros o haberse concedido más de lo pedido.
- 9.- No haberse decidido sobre cuestiones sujetas al arbitramento.

Admisibilidad y Rechazo

Art. 69.- La Cámara de Segunda Instancia rechazará el recurso de nulidad cuando aparezca manifiesto que su interposición es extemporánea o cuando las causales no corresponden a ninguna de las señaladas en el Artículo anterior.

En la providencia por medio de la cual la Cámara se avoque al conocimiento del recurso si éste resultare procedente, ordenará el traslado sucesivo por cinco días comunes al recurrente para que lo sustente y a la parte contraria para que presente su alegato. Los traslados se correrán en secretaría y sin necesidad de nueva providencia.

En caso de que el recurso no sea sustentado por el recurrente, la Cámara de Segunda Instancia lo declarará desierto con condena en costas a su cargo.

Procedimiento y Caducidad del Recurso

Art. 70.- Efectuado el traslado y practicadas las pruebas necesarias a juicio de la Cámara de Segunda Instancia, se decidirá el recurso para lo cual ésta contará con un plazo no superior a un mes.

Cuando prospere cualquiera de las causales señaladas en los numerales 1, 2, 3, 4, 5 y 6 del Artículo 68, la Cámara declarará la nulidad del laudo. En los demás se procederá a ordenar al Tribunal Arbitral que efectúe las correcciones o adiciones del caso.

Contra la providencia de la Cámara de Segunda Instancia no cabrá recurso alguno, incluido el de casación bien sea directo o "per saltum".

Medidas Precautorias

Art. 71.- Interpuesto el recurso de nulidad, la parte a quien interese podrá solicitar las providencias precautorias conducentes a asegurar la plena efectividad de aquel.

CAPÍTULO VI DE LA EJECUCION DEL LAUDO Y CESACION DE FUNCIONES DEL TRIBUNAL

Ejecución Judicial

Art. 72.- De la ejecución de los laudos arbitrales, conocerá el Juez competente calificado para conocer de la controversia en ausencia de **arbitraje**.

Cesación de Funciones

Art. 73.- El Tribunal Arbitral cesará en sus funciones:

- 1.- Cuando no se haga oportunamente la consignación de gastos y honorarios prevista en la presente ley.
- 2.- Por voluntad de las partes.
- 3.- Por encontrarse en firme el laudo con sus adiciones, correcciones o complementos.
- 4.- Por la interposición del recurso de nulidad, excepto cuando se trate de las causales 7, 8 ó 9

del Artículo 68 e esta Ley.

5.- Por la expiración del plazo fijado para el proceso o el de su prórroga, si la hubiere.

6.- Cuando hubiere acuerdo total en audiencia de conciliación.

Liquidación Final de Gastos

Art. 74.- Terminado el proceso, el Tribunal Arbitral deberá hacer la liquidación final de los gastos, entregará a los árbitros lo que les correspondiere, cubrirá los gastos pendientes y, previa cuenta razonada, devolverá el saldo a las partes, si lo hubiere.

SECCION TERCERA DEL **ARBITRAJE** INTERNACIONAL Y EXTRANJERO CAPÍTULO ÚNICO

Aplicación Supletoria

Art. 75.- Las disposiciones de este Capítulo se aplicarán al **Arbitraje** Internacional y extranjero, sin perjuicio de lo dispuesto en cualquier tratado, convención o pacto, multilateral o bilateral respecto de los cuales se haya cumplido la totalidad de los requisitos exigidos para su vigencia.

Primacía del Derecho Internacional Vigente

Art. 76.- En caso de conflicto entre Tratados, Pactos o Convenciones Internacionales y la presente Ley, prevalecerán los primeros.

Arbitraje Internacional del Estado

Art. 77.- Pueden ser sometidas a **Arbitraje** Internacional dentro o fuera del país, libremente y sin requisito de previa autorización, las controversias derivadas de los contratos que el Estado salvadoreño y las entidades de derecho público celebren con nacionales o extranjeros no domiciliados o deriven de una relación jurídica patrimonial de derecho privado, siempre que versen sobre derechos disponibles.

En todos estos supuestos, el **arbitraje** deberá realizarse ante un Centro de **Arbitraje** de reconocido prestigio y el Estado o sus entidades podrán someterse a los reglamentos y normas de las mismas.

Libertad de Elección

Art. 78.- Las partes en el **Arbitraje** Internacional, estarán habilitadas para escoger las normas sustanciales y de procedimiento aplicables conforme a las cuales los árbitros habrán de resolver el litigio, así como determinar el lugar del **arbitraje**.

Ejecución de Laudos Internacionales o Extranjeros

Art. 79.- Los laudos arbitrales pronunciados en el extranjero, así como aquellos considerados como Internacionales conforme a la presente ley, se ejecutarán en El Salvador de conformidad con los Tratados, Pactos o Convenciones que estén vigentes en la República o, en defecto de éstos, por las normas legales comunes.

Reconocimiento y Autorización

Art. 80.- El reconocimiento y la ejecución del laudo arbitral internacional o extranjero se pedirá ante la Corte Suprema de Justicia de acuerdo con las reglas establecidas en los tratados, pactos o convenciones vigentes en la República o, en su defecto, por el Código de Procedimientos Civiles.

No será necesaria conforme a lo previsto en la Ley Orgánica Judicial, la autorización para la ejecución de sentencias de Tribunales Arbitrales internacionales creados por convenios obligatorios para El Salvador.

Legalización o Traducción

Art. 81.- La parte que pida el reconocimiento y la ejecución, deberá presentar el laudo y el acuerdo de **arbitraje** debidamente legalizados, y traducidos en su caso.

Reglas de Reconocimiento y Ejecución

Art. 82.- El reconocimiento y ejecución de un laudo arbitral internacional o extranjero se llevará a cabo conforme a lo dispuesto en los Tratados, Pactos o Convenciones vigentes en la República; de no existir alguno vigente, se aplicarán las siguientes reglas:

1.- Se podrá denegar únicamente el reconocimiento y la ejecución de un laudo arbitral extranjero, a petición de parte interesada, en cualquiera de los siguientes casos:

- a) Que una de las partes en el convenio arbitral estaba afectada por alguna incapacidad;
- b) Que el convenio no es válido en virtud de la ley a que las partes lo sometieron o, si nada se hubiera indicado a este respecto, en virtud de la ley del país en que se haya dictado el laudo;
- c) Que la parte contra la cual se invoca el laudo no haya sido debidamente notificada de la designación de un Árbitro o de las actuaciones arbitrales o no ha podido, por cualquier otra razón, hacer valer sus derechos;
- d) Que el laudo se refiere a una controversia no prevista en el convenio arbitral o contenga decisiones que excedan los términos del convenio arbitral. No obstante, si las disposiciones del laudo que se refieren a las cuestiones sometidas al **arbitraje** pue-den separarse de la que no lo están, se podrá dar reconocimiento y ejecución a las primeras;
- e) Que la composición del Tribunal Arbitral o el procedimiento arbitral no se han ajustado al convenio celebrado entre las partes o, en defecto de tal convenio, que no se han ajustado a la ley del país donde se efectuó el **arbitraje**;
- f) Que el laudo aún no es obligatorio para las partes o haya sido anulado o suspendido por un tribunal cuya legislación fue aplicada para dictar el laudo; y,
- g) El objeto de la controversia no es susceptible de **arbitraje** de acuerdo a esta ley o que el reconocimiento o la ejecución del laudo son contrarios al orden público.

2.- La Corte Suprema de Justicia, de oficio, podrá denegar el reconocimiento o la ejecución cuando compruebe que según las leyes de la República el objeto de la controversia no es susceptible de **arbitraje**, o el laudo es contrario al orden público internacional.

Ejecución Judicial

Art 83.- La ejecución del laudo, una vez reconocido en la forma dispuesta por los Tratados, Pactos o Convenciones o, en su defecto en esta ley, se llevará a cabo ante el Juez que conforme a las disposiciones del Código de Procedimientos Civiles y Ley Orgánica Judicial, le correspondiere la ejecución de sentencias nacionales.

TÍTULO CUARTO DE LOS CENTROS DE **ARBITRAJE**

Centros de Arbitraje

Art. 84.- Las Cámaras de Comercio, las Asociaciones gremiales y las Universidades podrán fundar y organizar Centros de **Arbitraje** conforme a los términos establecidos en este capítulo. Dichos centros formarán parte integrante de la institución respectiva y podrán constituirse o no como personas jurídicas independientes de la entidad. Los Centros de **Arbitraje**, podrán brindar también el servicio de mediación.

Requisitos

Art. 85.- Los Centros **Arbitraje** deberán cumplir como mínimo con los siguientes requisitos para poder ejercer sus funciones:

1.- Establecer un reglamento que contendrá:

- a) La lista de árbitros, que no podrán ser menos de veinte; dicha lista indicará la forma como está estructurada, los requisitos para ingresar a ella, la vigencia de la lista, las causas de exclusión de la misma, así como la forma de hacer la designación de los árbitros que habrán de atender cada caso;
- b) Tarifas de honorarios para árbitros o mediadores, cuando proceda;
- c) Tarifas de gastos administrativos;
- d) Normas administrativas aplicables al centro;
- e) Organigrama del Centro, forma de designación de sus funcionarios y asignación de funciones;
- f) Normas de procedimiento **arbitraje**. Estas normas serán eficaces y eficientes con el fin de lograr de manera ágil y con respeto de los derechos de las partes la solución pronta de la controversia.

2.- Contar con un Código de Ética; y,

3.- Organizar un archivo de actas de mediación, cuando proceda, contratos de transacción y laudos arbitrales.

Los Centros tendrán las facilidades e instalaciones necesarias para poder atender debidamente sus funciones, así como con personal capacitado y calificado para el efecto.

Autorización

Art. 86.- El Ministerio de Gobernación será el encargado de autorizar el funcionamiento de los Centros de **Arbitraje**; previa verificación del cumplimiento de los requisitos señalados en esta Ley, llevando para tal efecto un registro público de los centros autorizados.

Para que dicha autorización sea otorgada se requiere:

- 1) La presentación de un estudio de factibilidad desarrollado con la metodología que para el efecto disponga el Reglamento de la ley; y,
- 2) La demostración de recursos logísticos, administrativos y financieros suficientes para que cumpla eficazmente con la función para la cual solicita ser autorizado.

Sanciones

Art. 87.- El Ministerio de Gobernación, una vez comprobada la infracción a la Ley o a sus reglamentos, podrá imponer a los Centros de **Arbitraje**, mediante resolución motivada cualquiera de las siguientes sanciones:

- a) Amonestación escrita;
- b) Multa hasta de doscientos salarios mínimos legales mensuales vigentes, teniendo en cuenta la gravedad de la falta y la capacidad económica del Centro de **Arbitraje**;
- c) Suspensión de la autorización de funcionamiento hasta por un término de seis meses;
- d) Revocatoria de la autorización de funcionamiento.

Cuando a un Centro de **Arbitraje** se le haya revocado la autorización de funcionamiento, sus representantes legales o administradores quedarán inhabilitados para solicitar nuevamente dicha autorización, por un término de cinco años.

Competencias de los Centros

Art. 88.- Los Centros de **Arbitraje** podrán dedicarse además a la mediación, previa aprobación por la autoridad competente de las reglas aplicables.

Imparcialidad

Art. 89.- Los Centros podrán intervenir en controversias que se susciten entre sus miembros o entre éstos y una persona que no sea miembro de la Institución de la cual forme parte el Centro, siempre que esta última exprese en el convenio arbitral que, a sabiendas de tal circunstancia, se somete a esa jurisdicción y acepta las reglas del procedimiento de **arbitraje** de ese centro.

TÍTULO QUINTO
DISPOSICIONES TRANSITORIAS, DEROGATORIA Y VIGENCIA
CAPÍTULO ÚNICO
Disposiciones Transitorias

Art. 90.- Los procedimientos arbitrales iniciados con anterioridad al entrar en vigencia esta ley, se regirán conforme a la legislación anterior.

Esta disposición comprende los recursos que se encuentren en trámite.

Las cláusulas compromisorias válidamente estipuladas antes de la vigencia de esta ley, se regirán

en cuanto a su eficacia por las disposiciones de la nueva Ley.

Reglamento

Art. 91.- El Reglamento General de la presente ley, deberá ser emitido por el Presidente de la República, en un plazo de 30 días, contados a partir de su vigencia.

Derogatorias

Art. 92.- Derógase:

- a) El Título II del Libro IV del Código de Comercio, que contiene los Artículos 1004 al 1012;
- b) El Capítulo III de la Ley de Procedimientos Mercantiles que contiene los Artículos 12 al 20;
- c) El ordinal 3º del artículo 1, el literal c) del artículo 2 y los artículos 21 y 22 de la Ley de Casación;
- d) La Sección Tercera, Capítulo II, Título I, Libro Primero, Parte Primera, del Código de Procedimientos Civiles, que contiene los Artículos 56 al 79; y,
- e) Cualquier otra disposición que se oponga a la presente ley.

Vigencia

Art. 93.- La presente Ley entrará en vigencia ocho días después de su publicación en el Diario Oficial.

DADO EN EL PALACIO LEGISLATIVO: San Salvador, a los once días del mes de julio del año dos mil dos.

Ciro Cruz Zepeda Peña,
Presidente.

Walter René Araujo Morales, Julio Antonio Gamero Quintanilla,
Primer Vicepresidente. Segundo Vicepresidente.

René Napoleón Aguiluz Carranza,
Tercer Vicepresidente.

Carmen Elena Calderón de Escalón, José Rafael Machuca Zelaya,
Primera Secretaria. Segundo Secretario.

Alfonso Arístides Alvarenga, William Rizziery Pichinte,
Tercer Secretario. Cuarto Secretario.

Rubén Orellana Mendoza,
Quinto Secretario.

CASA PRESIDENCIAL: San Salvador, a los veintitrés días del mes de julio del año dos mil dos.

PUBLIQUESE,

Francisco Guillermo Flores Pérez,
Presidente de la República.

Conrado López Andreu,
Ministro de Gobernación.

Tomo Nº 356
Fecha: 21 de agosto de 2002.

A N E X O 13

**L e y d e S i m p l i f i c a c i ó n
A d u a n e r a d e E l
S a l v a d o r**



ASAMBLEA LEGISLATIVA DE EL SALVADOR

Materia y Sub-Materia

Materia	Hacienda y Presupuesto
Siglas	HP
Sub-Materias	Aduanas

Decretos

Título:	Ley De Simplificacion Aduanera (Teledespacho)
Tipo de Decreto:	L
Número:	529
Fecha de Emisión:	13/01/1999
Diario Oficial #:	23
Tomo N :	342
Fecha de Publicación:	03/02/1999

Resumen

TEXTO ORIGINAL

Contenido

ASAMBLEA LEGISLATIVA --- INDICE LEGISLATIVO

REPUBLICA DE EL SALVADOR --- AMERICA CENTRAL

DECRETO N° 529.-

LA ASAMBLEA LEGISLATIVA DE LA REPUBLICA DE EL SALVADOR,

CONSIDERANDO:

I.- Que el crecimiento del tráfico internacional de mercancías y la profusión de negociaciones comerciales en que se encuentra inmerso el país imponen la necesidad de adecuar los servicios aduaneros a los estándares mundiales de calidad y eficiencia en términos de facilitación del comercio internacional, control de la recaudación fiscal y protección de la sociedad;

II.- Que en este mismo contexto, los países del área también han realizado esfuerzos para adecuar la legislación regional a las exigencias de simplificación y facilitación de los procedimientos aduaneros, habiéndose autorizado en tal sentido la modalidad de despacho conocida como autodeterminación o autoliquidación, regulada por el Art. 75 del Código Aduanero Uniforme Centroamericano, la cual debe ser desarrollada para su implementación en la legislación interna de cada país;

III.- Que la adecuación de los servicios aduaneros a las exigencias antes planteadas requiere de la implementación de un marco legal moderno y flexible que permita el desarrollo de nuevas modalidades de despacho que por su agilidad otorguen ventajas competitivas a los productores nacionales, en una relación de equilibrio con el control aduanero;

POR TANTO,

en uso de sus facultades constitucionales y a iniciativa del Presidente de la República, por medio del Ministro de Hacienda,

DECRETA, la siguiente:

LEY DE SIMPLIFICACION ADUANERA

Art. 1.- La presente Ley tiene por objeto establecer el marco jurídico básico para la adopción de mecanismos de simplificación, facilitación y control de las operaciones aduaneras, a través del uso de sistemas automáticos de intercambio de información.

Cuando en el texto de esta ley, se mencione Dirección General deberá entenderse que se refiere a la Dirección General de la Renta de Aduanas.

Art. 2.- Previo al arribo de las mercancías que habrán de declararse mediante el sistema de teledespacho, los transportistas están obligados a proporcionar mediante transmisión electrónica u otros medios autorizados, la información contenida en el manifiesto general de carga y en los demás documentos de viaje establecidos por la legislación aduanera.

Art. 3.- Corresponde al declarante o a su representante bajo el sistema de autoliquidación, realizar la determinación de las obligaciones tributarias aduaneras y cumplir con los demás requisitos y formalidades necesarios para la autorización del régimen que corresponda, previamente a la presentación de la declaración ante la autoridad aduanera.

Excepcionalmente, la autoridad aduanera efectuará la determinación de la obligación tributaria aduanera sobre la base de la información entregada por el declarante y el reconocimiento de las mercancías. Tales casos de excepción, serán determinados por la Dirección General a través de normas administrativas de aplicación general.

Art. 4.- Para efectos de la autodeterminación de las obligaciones aduaneras, el declarante o su representante tendrá derecho a efectuar, de acuerdo al procedimiento que establezca al efecto la Dirección General, el examen previo de las mercancías, que consiste en el reconocimiento físico de las mismas, previo a su despacho, para determinar sus características generales y los elementos determinantes de las obligaciones tributarias aduaneras y demás requisitos que se requieren para la autorización del régimen u operación aduanera a que serán destinadas.

Art. 5.- Dentro de los actos previos a la declaración, cualquier persona con un interés legítimo podrá efectuar consultas a la autoridad aduanera relacionadas con la aplicación de las disposiciones legales, reglamentarias o administrativas que regulan los

procedimientos aduaneros, la clasificación arancelaria, la valoración aduanera, los tributos que se causan con motivo de las operaciones aduaneras o sobre cualquier otro asunto que tenga relevancia tributaria aduanera. Dichas consultas podrán efectuarse por escrito y contener el criterio razonado que sobre el asunto consultado tenga el solicitante debiendo ser evacuadas por la autoridad aduanera dentro de los diez días hábiles siguientes a su recepción.

Si la evacuación de consultas requiere necesariamente de un análisis de laboratorio, el interesado podrá requerir los servicios del Departamento de Laboratorio de la Dirección General o presentar dictámenes emitidos por cualquier laboratorio particular que hubiera sido debidamente certificado por el Consejo Nacional de Ciencia y Tecnología.

Art. 6.- El despacho de las mercancías podrá ser solicitado por procedimientos informáticos, mediante el intercambio de información por vía electrónica, a través del sistema conocido como teledespacho.

Para efectos de esta Ley, teledespacho constituye el conjunto sistematizado de elementos tecnológicos de carácter informático y de comunicaciones que permiten dentro de un marco de mutuas responsabilidades, y mediante los procedimientos autorizados, el intercambio por vía electrónica de información de trascendencia tributaria entre la Dirección General, importadores, exportadores y los operadores e instituciones contraloras del comercio exterior en general.

Art. 7.- El uso de los medios informáticos para la formulación, presentación, registro y archivo de la declaración de mercancías y de la información relacionada con la misma gozará de plena validez.

En caso que se detectare una disconformidad de datos de un mismo documento, registrado en los archivos de los usuarios o auxiliares del sistema aduanero en relación con los de la Aduana, se presumirán correctos estos últimos, salvo prueba en contrario.

Art. 8.- Para la ejecución de las distintas actuaciones que conforman el sistema de teledespacho, la Dirección General asignará con carácter personal códigos y claves de acceso confidencial a los empleados, funcionarios y usuarios del servicio de aduanas que operarán dicho sistema.

La utilización de la clave de acceso electrónica asignada a los empleados, funcionarios y usuarios del sistema de aduanas equivale y sustituye, para todos los efectos legales, a su firma manuscrita o a la de su representante legal, según se trate de persona natural o jurídica.

Art. 9.- Los datos y registros recibidos y archivados en el sistema informático constituirán plena prueba de que el usuario del servicio aduanero realizó los actos que le corresponden y que el contenido de esos actos y registros fue suministrado por éste, haciendo uso de su clave de acceso confidencial.

Los empleados, funcionarios o autoridades que intervengan en la operación del sistema, serán responsables civil, administrativa y penalmente de sus actos y de los datos que suministren.

Cualquier información transmitida electrónicamente por medio de un sistema informático autorizado por la Dirección General será admisible en los procedimientos administrativos o judiciales como evidencia de la transmisión y del contenido de esa información.

Art. 10.- Las instituciones públicas y entidades privadas relacionadas con el servicio de aduanas, deberán transmitir electrónicamente a las autoridades aduaneras competentes los permisos, certificados, licencias, autorizaciones y demás información inherente al tráfico de mercancías o a la comprobación del pago de las obligaciones tributarias aduaneras, de conformidad a los procedimientos acordados entre tales entidades y la Dirección General.

Por su parte, la autoridad aduanera deberá proporcionar a estas instituciones o entidades la información atinente a su competencia sobre las operaciones aduaneras de acuerdo a los procedimientos que al efecto se hubieran convenido.

Art. 11.- La declaración de mercancías se considerará aceptada cuando se registre en el sistema informático autorizado por la Dirección General.

La realización de dicho acto no implica avalar el contenido de la declaración ni limita las facultades de comprobación o fiscalización a posteriori de la autoridad aduanera.

Art. 12.- La declaración de mercancías autoliquidada será sometida a un proceso selectivo y aleatorio que determine si corresponde efectuar la verificación inmediata de lo declarado. Dicha verificación no limita las facultades de fiscalización posterior de la autoridad aduanera.

Art. 13.- Cuando el sistema informático determine que debe efectuarse una verificación inmediata de lo declarado, la autoridad aduanera deberá disponer la práctica de dicha diligencia dentro del mismo día de tal determinación. En este caso, para efectos de la verificación, el declarante deberá presentar ante la autoridad aduanera competente la declaración de mercancías y los documentos que la sustentan, los cuales serán archivados por la autoridad aduanera.

Quando el sistema autorice el levante automático de la mercancía, la declaración y los documentos que la sustentan deberán ser archivados por el declarante o su agente de aduanas en su caso, quienes deberán conservarlos a disposición de la autoridad aduanera por un plazo de cinco años, contados a partir de la aceptación de la correspondiente declaración de mercancías. El incumplimiento del deber de custodia documental se sancionará con una multa equivalente al 1% del activo en giro de la empresa o negocio del supuesto infractor cuya aplicación se determinará después de conceder a éste una audiencia de tres días hábiles en la cual deberá manifestar su defensa y presentar las pruebas de descargo respectivas, dictándose la resolución que proceda dentro de los ochos días hábiles subsiguientes.

Art. 14.- La Dirección General tendrá amplias facultades de fiscalización, inspección, investigación y control con el fin de asegurar el exacto cumplimiento de las obligaciones tributarias aduaneras y de los demás requisitos no arancelarios que sean necesarios para la autorización del régimen solicitado, incluso respecto de los sujetos que gocen de exenciones, franquicias o incentivos tributarios, tanto en lo relativo a sus declaraciones como al cumplimiento de las condiciones que impone el régimen aduanero declarado o tratamiento tributario especial.

En su función fiscalizadora, la Dirección General podrá:

- a) Practicar inspecciones en locales ocupados a cualquier título por los sujetos pasivos de las obligaciones tributarias aduaneras;
- b) Exigir a los sujetos pasivos de los derechos e impuestos a la importación, en relación con las operaciones objeto de investigación, la exhibición de sus libros y balances; sistemas, programas, archivos y registros de contabilidad manual, mecánica o computarizada; documentos, correspondencia comercial, bienes y mercaderías; así como examinar y verificar los mismos y tomar medidas de seguridad para su conservación en el lugar en que se encuentren, aún cuando no correspondan al domicilio del contribuyente, quedando los mismos bajo la responsabilidad de éste;
- c) Requerir informaciones y declaraciones a los sujetos pasivos de la obligación tributaria aduanera y auxiliares de la función pública aduanera, relacionadas con hechos que en el ejercicio de sus actividades hayan contribuido a realizar o hayan debido conocer, así como la exhibición de documentación relativa a tales situaciones que se vincule con las obligaciones antes referidas;
- d) Exigir a los beneficiarios de franquicias e incentivos tributarios informes sobre el cumplimiento de los requisitos para gozar de tales beneficios;
- e) Requerir, cuando no exista prohibición legal, de las personas particulares, de los funcionarios, instituciones o empresas públicas y de las autoridades en general, todos los datos y antecedentes que se estimen necesarios para la fiscalización y control de las obligaciones aduaneras tributarias y no tributarias. Las personas naturales tendrán la obligación de rendir testimonio bajo juramento en calidad de terceros, pudiendo la Dirección General verificar estos testimonios, datos e informes. Se exceptúan de esta norma la Dirección General de Estadística y Censos y las entidades estatales en lo que concierne a informes confidenciales que su respectiva ley de creación o reglamento les prohíban divulgar;
- f) Fiscalizar el tránsito aduanero de mercancías por cualquier medio para verificar que se cumpla con los requisitos prescritos en la normativa aduanera;
- g) Citar a contribuyentes, responsables o a cualquier tercero para que conteste o informe, verbalmente, por escrito o por cualquier otro medio autorizado por la Dirección General, las preguntas o requerimientos que se estimen necesarios para la verificación del exacto cumplimiento de las obligaciones aduaneras. De esta diligencia deberá levantarse acta, firmada o no por el citado, que servirá de medio de prueba en los procedimientos respectivos;
- h) Examinar los hechos que puedan configurar infracciones y hacer del conocimiento de la Fiscalía General de la República sobre las infracciones penales, a efecto de asegurar los medios de prueba e individualizar a los infractores.

La Dirección General deberá potenciar además la fiscalización como un instrumento de orientación a los usuarios de los servicios aduaneros, de modo que se facilite a los mismos el cumplimiento voluntario de sus obligaciones aduaneras.

El plazo para la verificación posterior caducará en cinco años contados desde la fecha de aceptación de la declaración de mercancías correspondientes.

Art. 15.- Cuando con motivo de la verificación posterior la autoridad aduanera determine la existencia de derechos e impuestos a la importación o cualquier otro tributo que no hubiera sido cancelado total o parcialmente con la declaración de mercancías o establezca el incumplimiento de alguna de las regulaciones de comercio exterior, abrirá el proceso administrativo correspondiente.

Art. 16.- Los resultados de la fiscalización deberán ser notificados al declarante o a su agente de aduanas en su caso de acuerdo con las reglas siguientes:

Se notificará al supuesto infractor, a su representante legal, apoderado o mandatario aduanero, curador o heredero, en el lugar señalado para recibir notificaciones o en su domicilio. Tales notificaciones se harán por cualquier Delegado de la Dirección General, por la vía electrónica, telefax o telefacsimil, por correo certificado con constancia de recepción, o por los demás medios que autoricen las leyes.

Si no se encontrare al interesado o a cualquiera de sus representantes en el lugar señalado para recibir notificaciones o en su domicilio, se le notificará por medio de su cónyuge o compañera de vida, hijo mayor de edad, socio, dependiente o sirviente doméstico, o por medio de persona mayor de edad que esté al servicio del representante, apoderado, curador o heredero, o de la empresa, oficina o dependencia establecida en el lugar señalado.

Si no se encontrare ninguna de las personas señaladas en el inciso precedente, en la dirección indicada, o se negaren a recibirla, se fijará en la puerta de la casa u oficina, una esquila en la cual se notificará la resolución en extracto.

Si no se dieren las circunstancias para que la actuación quede legalmente notificada, ésta se hará por edicto, sujetándose a las formalidades siguientes: Se fijará en el tablero de la Dirección General o de la Aduana respectiva, un extracto breve y claro del auto o resolución correspondiente por un término de setenta y dos horas, pasadas las cuales se tendrá por hecha la notificación. Los interesados estarán obligados a concurrir a la Dirección General si desean conocer íntegramente la providencia que se ha hecho saber en extracto.

Debido a la solidaridad que se establece entre el declarante y su agente de aduanas en lo que respecta a sus obligaciones tributarias aduaneras y al mandato que de acuerdo con la legislación de la materia se establece entre los mismos, la notificación que se haga al agente de aduanas se entenderá extensiva para el declarante.

Art. 17.- El proceso administrativo a que alude el Art. 15 de esta Ley, se desarrollará de la siguiente manera:

- a) La apertura del proceso debe notificarse al declarante o a su agente de aduanas apoderado o representante, haciéndoles saber el contenido íntegro del informe de fiscalización correspondiente;
- b) El declarante contará con un plazo de quince días hábiles contados desde el siguiente día de la notificación para la presentación de sus alegatos y las pruebas de descargo que estime pertinentes;
- c) Vencido dicho plazo, la Dirección General dictará la resolución que proceda dentro de un plazo de diez días hábiles. La notificación de dicha resolución, deberá contener el texto íntegro de la misma.

Contra la resolución que se dicte, se admitirán los recursos administrativos establecidos por la legislación aduanera.

Art. 18.- Los empleados, funcionarios y usuarios del servicio de aduanas y demás personas autorizadas que utilicen los sistemas informáticos y medios de transmisión electrónica de datos de enlace con la autoridad aduanera, deberán acatar las medidas de seguridad que la Dirección General establezca, incluyendo las relativas al uso de códigos, claves de acceso confidenciales o de seguridad.

Art. 19.- Debido al carácter especial de la presente Ley, las normas de la misma prevalecerán sobre las contenidas en cualquier otra ley, decreto, reglamento o normativa que las contraríe.

Art. 20.- La Dirección General está facultada para emitir las normas administrativas que sean necesarias para el desarrollo de los principios contenidos en esta Ley, principalmente de aquellos que regulan la emisión, transferencia, uso y control de la información relacionada con las operaciones aduaneras.

Art. 21.- El Presidente de la República emitirá el reglamento de la presente ley dentro de los ciento ochenta días subsiguientes a la vigencia de la misma.

Art. 22.- El presente Decreto entrara en vigencia ocho días después de su publicación en el Diario Oficial.

DADO EN EL SALON AZUL DEL PALACIO LEGISLATIVO: San Salvador, a los trece días del mes de enero de mil novecientos noventa y nueve.

JUAN DUCH MARTINEZ
PRESIDENTE

GERSON MARTINEZ CIRO CRUZ ZEPEDA PEÑA
PRIMER VICEPRESIDENTE SEGUNDO VICEPRESIDENTE

RONAL UMAÑA NORMA FIDELIA GUEVARA DE RAMIRIOS
TERCER VICEPRESIDENTE CUARTA VICEPRESIDENTA

JULIO ANTONIO GAMERO QUINTANILLA JOSE RAFAEL MACHUCA ZELAYA
PRIMER SECRETARIO SEGUNDO SECRETARIO

ALFONSO ARISTIDES ALVARENGA GERARDO ANTONIO SUVILLAGA
TERCER SECRETARIO CUARTO SECRETARIO

ELVIA VIOLETA MENJIVAR JORGE ALBERTO VILLACORTA MUÑOZ
QUINTA SECRETARIA SEXTO SECRETARIO

CASA PRESIDENCIAL: San Salvador, a los veintiún días del mes de enero de mil novecientos noventa y nueve.

PUBLIQUESE,

ARMANDO CALDERON SOL
Presidente de la República

Manuel Enrique Hinds Cabrera,
Ministro de Hacienda.

D. O. N° 23
Tomo N° 342
Fecha: 3 de febrero de 1999.