C A P Í T U L O IV

LEYES Y REGLAMENTOS

4.1 Seguridad de la Información, Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas.

4.2 Régimen jurídico - Leyes en el Ecuador sobre las Firmas Digitales.

4.3 Reglamentos Nacionales que rigen las Técnicas de Certificación Digital.

4.4 Legislación Internacional – Normas de Seguridad

4.5 Autoridades Certificadoras

4.6 Anexos (Leyes y Reglamentos)

4.7 Conceptos y Definiciones

4.1 Seguridad de la Información, Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas.

Seguridad de la Información.- La seguridad en el comercio electrónico y el Internet debe proteger sobre todo los siguientes aspectos:

- ✓ Seguridad física de los equipos individuales, que pueden verse comprometidos por acciones de vandalismo o calamidad natural.
- ✓ Funcionalidad técnica de los sistemas informáticos, cuyo mayor riesgo es la perdida de información.
- ✓ Protección de los contenidos, que pueden ser alterados o mal utilizados ya sea por personas mal intencionadas desde cualquier punto de la red o por personal interno mal capacitado. [LIB 01].

Recursos Tecnológicos de Protección

- ✓ **La protección física de lo equipos.-** a todos los equipos informáticos, y los medios son los sistemas de vigilancia, control de acceso, prevención de accidentes, etc.
- ✓ **La protección de la funcionalidad (Virus y Caballos de Troya).-** la presencia de piratas informáticos [46] en la red y la deficiencia de programas usados para el comercio electrónico, dejan una puerta de entrada a elementos que pueden comprometer la seguridad de la información de los clientes.
- ✓ **Protección de los entornos.-** se basa en el principio de que es posible delimitar áreas de Internet dentro de las cuales el entorno es seguro, donde los accesos están controlados y las personas son fiables. Para ello se utilizan soluciones de ***Extranet e Intranet***, en las cuales se dispone de recursos como routers y firewall[47], que realizan tareas de vigilancia y control de acceso en bloque y cuyas

[46] Escuchas electrónicas, Hackers, crackers, etc.

tareas de protección se basan en los privilegios asignados a cada usuario. El objetivo de este tipo de solución es dar seguridad, facilitando la comunicación y el acceso a la información deseada de forma selectiva y controlada. Como se indica en la Tabla 4.1.

	Internet	**Intranet**	**Extranet**
Acceso	Público	Privado	Semi-privado
Usuario	Usuarios del Internet	Usuarios de Empresas	Usuarios Autorizados de empresas colaboradoras
Información	Fragmentada	Propiedad de la empresa	Compartida con empresas colaboradoras

Tabla 4.1 Internet, Intranet,

- ✓ **Protección de los mensajes y comunicaciones.-** se basa en diversas técnicas y soluciones desarrolladas para dar seguridad a la información.

Comercio Electrónico

"Es toda transacción comercial realizada en parte o en su totalidad, a través de redes electrónicas de". (Ley de Comercio Electrónico del Ecuador, disposición general Novena), que abarca todo tipo de acceso a información comercial, intercambio de medios digitales de bienes y servicios, suministro en línea de contenidos digitales, transferencias electrónicas de fondos, comercio electrónico de valores, contratación pública, mercadotecnia, servicios posventa directos al consumidor, certificación de identidades y transacciones, cibertribunales[48] y formas de resolución de conflictos y hoy en día pago de servicios públicos a través de los bancos por Internet. En general, todo lo relacionado a Internet, con implicaciones económicas y comerciales.

[47] Mecanismos de Seguridad para la información y los usuarios de las Intranets y Extranets.

El Comercio Electrónico tiene un amplio campo de acción y acogida con millones de consumidores que crece día a día, imparable en todo el mundo, es un fenómeno que ha ido globalizándose, uniendo ciudades, países y eliminando fronteras y seguirá haciéndolo sin límites. Según el ***Wall Street Journal,*** el total del comercio electrónico en Latinoamérica asciende a un 55% en Latinoamérica, y pese a que más de la mitad de los ínternautas[49] son brasileños, los más entusiastas frente al comercio electrónico parecen ser los panameños, ecuatorianos y venezolanos. Un 58%, 55% y 53%, respectivamente, considera a la red muy útil para las compras. [WWW 060].

Opciones de comercio electrónico

- ✓ Presencia y elección globalizada
- ✓ Aumento de competitividad y calidad de servicios
- ✓ Adecuación generalizada/productos y servicios personalizados
- ✓ Cadenas de entrega más cortas o inexistentes
- ✓ Respuesta inmediata a las necesidades
- ✓ Reducción de precios
- ✓ Nuevos negocios, productos o servicios

Estas alternativas deben estar respaldadas legalmente con un marco jurídico que respalde y garantice todo tipo de Transacciones Electrónicas.

Desde una perspectiva jurídica las ventajas del comercio electrónico son:

- ✓ Homologación con documentos de formato tradicional.
- ✓ Legalidad de mensajes de datos o documentos electrónicos (mensajes de correo electrónico, órdenes de compra, etc.)
- ✓ Los certificados digitales que garantizan tecnológicamente la identidad inequívoca de su propietario (receptor o emisor)

[48] Tribunales jurídicos en el Internet.
[49] Usuarios exploradores y navegadores del Internet

- ✓ Se evita la suplantación, vía infraestructura tecnológica o a través del registro público de claves.
- ✓ Imposibilidad de revocación: afirmar eventualmente que no se recibió o no se envió el mensaje de datos, hecho que es fácilmente comprobable a través de tecnología.

El problema de la inseguridad jurídica que rodea al comercio electrónico en la gran mayoría de los países de América Latina, dificulta su desarrollo e implementación. La acogida que tiene se ha visto truncada, limitando así las transacciones en la red, al acceso a portales con fines informativos y compra o utilización de productos y servicios con compañías que operan desde Estados Unidos y otros países y que por tanto pueden acceder a la denominada "*merchant account*" [50] que es la única vía posible para poder cobrar vía tarjeta de crédito las operaciones originadas en el Internet.

Los principales objetivos de la Ley de Comercio Electrónico en nuestro país son:

- ✓ Dotar de un marco jurídico a las transacciones y demás operaciones que tengan como escenario el Internet.
- ✓ Proteger al consumidor o usuario de este servicio, que asegure tecnológicamente la identidad del aceptante y ofertante y en general que avale los desarrollos tecnológicos sobre seguridad en materia de comercio electrónico.
- ✓ Homologar los documentos digitales, que en general son acuerdos de voluntades dentro de la red, con el mismo valor jurídico que los documentos o contratos tradicionales y por escrito.
- ✓ Introducir o modificar las infracciones, delitos y penas que pueden originarse de las operaciones virtuales dentro del comercio cibernético.

En Ecuador, Colombia, Panamá, Argentina, Chile y otros países con legislaciones sobre Comercio Electrónico como México, Italia, Alemania, España, se ha adoptado como esquema de seguridad la Infraestructura de Clave Pública (Public Key Infrastructure) de acuerdo a la Ley Modelo

UNCITRAL de las Naciones Unidas para el Comercio Electrónico, Esto significa que la ley establece la existencia de entidades certificadoras, legalmente facultadas para generar firmas digitales. [WWW 061]

4.2 Régimen jurídico - Leyes en el Ecuador sobre las Firmas Digitales.

Análisis de la Ley de Comercio Electrónico, Firmas Digitales y Mensajes de Datos del Ecuador

Con el apoyo de CORPECE[51], y con la participación activa de varios sectores interesados, se impulsó el Proyecto de Ley de Comercio Electrónico, Firmas Digitales y Mensajes de Datos. Para la elaboración y estructuración del Proyecto de Ley, se invitó a una amplia base de sectores involucrados y se contó con la participación de importantes empresas del medio. Se partió de la revisión de la legislación ecuatoriana y junto con el apoyo de distintos proyectos de ley, sobre todo de la Ley Modelo UNCITRAL, propuesta por las Naciones Unidas a través de la CNUDMI (Comisión de las Naciones Unidas para el Mercado Internacional); Directivas Europeas sobre comercio electrónico, firma digital, proyectos y anteproyectos de leyes de países europeos como Italia, España, Alemania, Luxemburgo, el Acta de Utah de los Estados Unidos de Norteamérica, estudios y proyectos latinoamericanos de Chile, Argentina, Uruguay, Colombia y Perú, investigaciones y publicaciones sobre el derecho de las nuevas tecnologías principalmente de universidades, así como doctrina especializada.

La ley de Comercio Electrónico del Ecuador recoge regulaciones sobre firmas digitales y mensajes de datos, entidades de certificación, de la contratación electrónica en el Ecuador y su regulación. El objetivo de la

[50] Cuenta Mercantil, que es usada y supervisada únicamente por los Estados Unidos.
[51] Corporación Ecuatoriana de Comercio Electrónico www.corpece.org.ec.

Ley es constituir un cuerpo legal de mayor alcance y aplicación práctica en el Ecuador, tiene su fundamentación en la ley modelo de CNUDMI y se aparta de las Directivas de la Comunidad Europea que legislan exclusivamente el tema del documento electrónico y la firma digital, regulaciones aplicables a toda clase de actos y entornos tecnológicos, aunque no tengan aplicación comercial o económica. Sin embargo en la Ley no se contemplan temas como: nombres de dominio (que a pesar que en el Ecuador la entidad que regula es NICECUADOR no se tiene ventajas sobre INTERNIC que regula internacionalmente aspectos de nombres de dominios), impuestos relacionados con el tema y publicidad virtual. Un aspecto importante que aún sigue en discusión es los cambios que impone el Internet en materia fiscal, en el Ecuador, se ha considerado como más conveniente delimitar los principios de política fiscal (Aduanas, Servicio de Rentas Internas, Comercio Exterior, Banca, etc.) en base a los cuales enfrentar los retos que supone el comercio electrónico, en tanto se instrumentan y perfeccionan soluciones prácticas. [WWW 062]

La Ley de Comercio Electrónico fue aprobada por el Congreso Nacional de la República, el **17 de Abril del 2002 como Ley No. 67. Publicada en el R.O.**[52] **Suplemento 557 de 17 de Abril del 2002.** lo que dio el inicio de regulación de las actividades Electrónicas en el Ecuador., luego de aprobada la Ley el Presidente de la República Dr. Gustavo Noboa Bejarano emitió el correspondiente **Reglamento a la Ley de Comercio Electrónico, Firmas y Mensajes de Datos,** para la correcta aplicación de la Ley, lo que se dio el 12 de diciembre del 2002. En dicho reglamento se delega a las diferentes instituciones encargadas por la ley para emitir

[52] Registro Oficial

reglamentos sobre ciertos aspectos como contratación electrónica, interconexión entre empresas, tales como Consejo Nacional de Telecomunicaciones (CONATEL), el Consejo de Comercio Exterior e Inversiones, (COMEXI), han demorado en expedir los correspondientes reglamentos de aplicación de ciertos aspectos que contempla la Ley.

Contenido básico de la Ley de Comercio Electrónico

TÍTULO I

Objeto de la ley:

De las Firmas Electrónicas.- se dan las definiciones de firma digital, sus efectos jurídicos, requisitos de validez, obligaciones del titular de la firma, duración y extinción de la Firma Electrónica. ***Artículos del 13 al 19.***

De los Certificados de Firma Electrónica.- trata aspectos sobre os certificados de firma electrónica, requisitos para obtenerlos, sus usos, su duración legal, su extinción, suspensión, revocación, así como su reconocimiento a nivel internacional. ***Artículos del 20 al 28.***

De las Entidades de Certificación de Información.- Se refiere a las entidades de certificación; su razón de ser, sus obligaciones, responsabilidades en cuanto a la protección de los datos de sus contratantes, así como aspectos que tiene que ver con la prestación de sus servicios, organismos de control, y funcionamiento. ***Artículos del 29 al 35***

De los organismos de promoción y difusión de los servicios Electrónicos, y de regulación y control de las entidades de certificación acreditadas.- Que trata temas sobre los diferentes organismos de promoción, difusión, regulación, registro y control de los servicios y comercio electrónicos, firmas digitales, inversiones y comercio

exterior. Así también de la autorización, registro, y regulación de las entidades de certificación acreditadas en el Ecuador. Se tratan temas sobre sus funciones, infracciones a reconocer y sancionar y tomar medidas cautelares, y los procedimientos a seguir en caso de sanciones administrativas, ***Artículos del 36 al 43.***

TITULO III

De los Servicios Electrónicos.- En donde se establece la obligatoriedad al cumplimiento de la Ley en cualquier tipo de actividad mercantil, financiera o transacciones que se realicen utilizando mensajes de datos a través de redes electrónicas y su sometimiento a los requisitos y solemnidades que la ley establece. ***Artículo 44.***

De la Contratación Electrónica y Telemática.- Se establece la validez de los contratos electrónicos, su aceptación con sus respectivas implicaciones como su recepción, apertura y su relación con el contrato electrónico. En caso de litigio se establece las normas para su proceso. ***Artículos del 45 al 47.***

De los derechos de los usuarios o Consumidores de servicios electrónicos.- Se establece todos los aspectos que tiene que ver con los derechos y obligaciones de los usuarios de servicios electrónicos así como las implicaciones que su consentimiento acarrea. Luego de que los oferentes de estos servicios tienen la obligación de informar adecuadamente sobre los riesgos y ventajas de estos servicios antes de su consentimiento y contratación. ***Artículos del 48 al 50.*** [WWW 062]

De los Instrumentos Públicos.- En donde se reconoce la validez jurídica de los mensajes de datos otorgados, conferidos, autorizados o expedidos por la autoridad competente y firmada electrónicamente. Los mismos que

deberán observar los requisitos, formalidades y solemnidades exigidos por la ley y demás normas aplicables. ***Artículo 51.***

TITULO IV

De la Prueba.- En este titulo se trata sobre los diferentes medios de prueba, sus prácticas, su presunción, en caso de que las partes contratantes tuvieran que llegar a este caso. Ya sea por impugnación de certificados, nulidad de firmas electrónicas, así como pertenencia de los mensajes de datos. Se establece también los procedimientos para que se pueda efectuar la prueba y su valoración con las autoridades correspondientes para llevar a cabo estas diligencias. ***Artículos del 52 al 56.***

TITULO V

De las Infracciones Informáticas.- Se consideran todas las infracciones informáticas y además se realizan las correspondientes modificaciones a los artículos correspondientes en el Código Penal y sus correspondientes sanciones en cuanto a los siguientes temas: penas por cualquier delito informático en el Ecuador en lo que tiene que ver con resguardo de datos, robo de información, mal uso y custodia de bases de datos, claves de accesos, usos fraudulentos o con beneficios a terceros, obtención no autorizada de información, falsificación electrónica en todas sus formas, alteración de mensajes de datos, y daños a la información infraestructura tecnológica, que puedan ser comprobados y especialmente "... Los que violaren el derecho a la intimidad, en los términos establecidos en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.". ***Artículos del 57 al 64.***

Efectos de la Ley: Así dispone la ley: "Art. 14.- Efectos de la Ley: Se reconoce la fuerza jurídica y la validez de los mensajes de datos, cualquiera sea su forma, así como la información que éstos contengan. Los mensajes de datos su información y contenido tendrán igual valor jurídico que los instrumentos públicos y privados, y su eficacia y valoración se someterán al cumplimiento de lo establecido en esta ley".

Firma Electrónica o digital.- El Art. 13 define a la firma electrónica como "Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos." La firma digital es indispensable dentro de las redes abiertas de información, como Internet y el comercio electrónico. Solamente a través de ella se genera un entorno seguro en relación con la autenticación digital vital para su desarrollo y expansión. El objetivo de la firma digital es el mismo de la firma escrita: dar asentimiento y compromiso con el documento firmado.

La ley establece que el mecanismo utilizado para la firma digital debe ser criptográfico, de modo que utiliza una Infraestructura de Clave Pública con dos claves diferentes: una para cifrar y otra para descifrar.

Requisitos

- ✓ Ser individual y estar vinculada exclusivamente a su titular;
- ✓ Que permita verificar la autoría e identidad del signatario, mediante dispositivos técnicos de comprobación establecidos por esta ley y sus reglamentos;
- ✓ Que su método de creación y verificación sea confiable, seguro e inalterable para el propósito para el cual el mensaje fue generado o comunicado;
- ✓ Que al momento de creación de la firma electrónica, los datos con los que se creare se hallen bajo control exclusivo del signatario, y,
- ✓ Que la firma sea controlada por la persona a quien pertenece.

Cualquier requisito adicional a los que la Ley señala, deberá constar expresamente en un acuerdo suscrito por las partes. La ley con el afán de permitir y fomentar el uso de firmas digitales o electrónicas en el Ecuador contempla aspectos como:

- ✓ Equiparación de la firma digital a la firma manuscrita (Art. 14)
- ✓ Obligaciones vinculadas con la firma electrónica (Art. 16)
- ✓ Obligaciones del titular de la firma electrónica (Art. 17)
- ✓ Revocación, cancelación y suspensión de la firma digital (Art. 18 y 19)

Entidades de Certificación.- La ley los define como: "Son las empresas unipersonales o personas jurídicas que emiten certificados de firma electrónica y pueden prestar otros servicios relacionados con la firma electrónica, autorizadas por el Consejo Nacional de Telecomunicaciones, según lo dispuesto en esta ley y el reglamento". Son aquellas entidades que dan fe de que una determinada clave pública corresponde a un sujeto específico mediante la expedición de un certificado. El certificado es muy importante ya que es el aval o respaldo de la firma digital: no existe legalmente el uno sin la otra.

La Ley ha otorgado a la Superintendencia de Telecomunicaciones las funciones de control de los proveedores, y para los proveedores de servicios de certificación relacionados con el sistema financiero nacional, será la Superintendencia de Bancos quien ejercerá estas funciones de control. De igual manera se establecen varios requisitos que deberán cumplir todos aquellos que quieran ser considerados proveedores de servicios de certificación, requisitos de carácter técnico, de probidad, económicos y de operabilidad en las funciones que han de prestar a la comunidad. (Art. 31) Así mismo se establece claramente una serie de obligaciones y responsabilidades que asumen los proveedores de los ya

mencionados servicios de certificación. (Art. 30), sin perjuicio de de las sanciones previstas en la Ley de Defensa del Consumidor (Art. 17 y 18).

Por la importancia de los servicios que prestan las entidades de certificación la Ley ha puesto especial énfasis en que dichas personas naturales o jurídicas: cumplan estrictamente los siguientes requisitos:

- ✓ Encontrarse legalmente constituidas, y estar registradas en CONATEL.
- ✓ Demostrar solvencia técnica, logística y financiera para prestar servicios a sus usuarios-
- ✓ Garantizar la prestación permanente, inmediata, confidencial, oportuna y segura del servicio de certificación de información.
- ✓ Mantener sistemas de respaldo de la información relativa a los certificados.
- ✓ Proceder de forma inmediata a la suspensión o revocatoria de certificados electrónicos previo mandato del Superintendente de Telecomunicaciones, en los casos que se especifiquen en esta ley.
- ✓ Mantener una publicación del estado de los certificados electrónicos emitidos.
- ✓ Proporcionar a los titulares de certificados de firmas electrónicas un medio efectivo y rápido para dar aviso que una firma electrónica tiene riesgo de uso indebido.
- ✓ Contar con una garantía de responsabilidad para cubrir daños y perjuicios que se ocasionaren por el incumplimiento de las obligaciones previstas en la presente ley, y hasta por culpa leve en el desempeño de sus obligaciones. Cuando certifiquen límites sobre responsabilidades o valores económicos, esta garantía será al menos del 5% del monto total de las operaciones que garanticen sus certificados. (Art. 30)

Contratos Electrónicos.- La Ley señala sobre la validez de los contratos electrónicos: "Los contratos podrán ser instrumentados mediante mensajes de datos. No se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación uno o más mensajes de datos". (Art. 28). El contrato electrónico puede realizarse mediante la utilización de algún elemento electrónico, Estos mensajes gozarán de completa validez y fuerza jurídica, sea que se trate de una

oferta, la aceptación de la misma o cualquier otra forma que genere obligaciones entre las partes.

Para el perfeccionamiento y funcionamiento de los contratos electrónicos y siempre que estas disposiciones no sean modificadas por las partes, la Ley señala: (Art. 46 y 47). [WWW 064]

Protección a los usuarios del Comercio Electrónico

Han existido gran cantidad de mecanismos para promover la protección del consumidor en el mercado tradicional fruto de ello se tiene la Ley Orgánica de Defensa del Consumidor[53], muchos de los cuales continuarán siendo útiles en el mercado electrónico. Sin embargo, en el ambiente digital existen nuevos retos para el consumidor y se requiere de nuevas estrategias que le den confianza en ese contexto. En este sentido la Organización de Cooperación Económica y Desarrollo (OCED) que ha colaborado en gran medida para la creación de la Ley modelo de la UNCITRAL, ha ayudado también a crear procedimientos y mecanismos para proteger los derechos de los consumidores y usuarios del comercio electrónico con su publicación de la "Guía de Protección al Consumidor en el Mercado Electrónico"[54]. Documento en el que se consideran como partes integrales de la protección al consumidor: la contratación electrónica, privacidad, seguridad y autenticación, fraude en línea, resarcimiento al consumidor, educación del consumidor y veracidad en publicidad.

La Ley de Comercio Electrónico garantiza los derechos de los usuarios de servicios de certificación y de quienes actúen intercambiando mensajes de datos, o transacciones de cualquier tipo relacionadas con el acceso a Internet, comercio electrónico, otros medios de comunicación y tecnologías de información. (Art. 39), así como la consagración del

[53] Registro Oficial 116, del 10 de Julio del 2000.

derecho a la intimidad y el derecho a no recibir información o mensajes de datos no solicitados, una vez rechazada una oferta electrónica por parte del destinatario, el oferente no podrá seguir enviando mensajes. Cualquier violación a estos principios faculta al usuario para hacer valer a su favor todas las acciones que le concede la ley.

Infracciones Informáticas.- Tanto en la ley modelo de la UNCITRAL, como la ley modelo de la cual nacen algunas de las leyes que existen actualmente en algunos de los países de América Latina, deja a criterio de cada país el tema de las sanciones o infracciones. Por ejemplo en la ley No. 527de 1999, de la República de Colombia no se establece infracciones ni sanciones, en el caso del Ecuador, la Ley de Comercio Electrónico ha hecho una reforma al Código Penal, que contempla la inclusión de 6 artículos y la reforma de otros 4 artículos que regulan el tema. Dentro de los cuales se encuentran como principales infracciones o delitos electrónicos o cibernéticos los siguientes:

- ✓ **Fraude informático.-** las personas que valiéndose de cualquier método o modo alteren, manipulen o modifiquen el funcionamiento de un programa, sistema informático, telemático o un sistema de datos para procurarse la transferencia no consentida de los bienes, valores, derechos o patrimonio de otra persona en perjuicio de esta o de un tercero.
- ✓ **Daño informático.-** las personas que de cualquier modo o utilizando cualquier método destruyan, alteren, utilicen, supriman o dañen los programas, datos, bases de datos, información, o cualquier mensaje de datos contenido en un soporte lógico, sistema de información o telemático.

[54] Publicada en 1999.

- ✓ **Falsificación electrónica**.- las personas que con ánimo de lucro, o bien para causar un perjuicio a un tercero, utilizando cualquier medio, alteren o modifiquen mensajes de datos, o la información incluida en éstos, que se encuentre contenida en cualquier soporte material, sistema de información o telemático, ya sea:
  a) Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial.
  b) Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad.
  c) Suponiendo en un acto la intervención de personas que no han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieren hecho.
  d) alterando o falsificando un instrumento electrónico público o Privado, de acuerdo a lo determinado por el Código Penal.
- ✓ **Intromisión indebida a los sistemas de información o telemáticos**.- las personas que por cualquier medio y con cualquier fin, con ánimo de conocer, apoderarse de la información contenida en dichos sistemas o descubrir los secretos comerciales o personales, o vulnerar la intimidad de otro sin su consentimiento interfieran, interrumpan, o se apoderen de cualquier mensaje de datos. [WWW 061]

4.3 Reglamentos Nacionales que rigen las Técnicas de Certificación Digital.

Para la correcta aplicación de a Ley cualquiera que sea ésta, es deber del Presidente de la República en el plazo que le da la ley expedir el correspondiente Reglamento de Aplicación para una correcta interpretación de la Ley, como es el Caso de la Ley de Comercio Electrónico, hecho que sucedió el 17 de Diciembre del 2002 cuando el Dr. Gustavo Noboa Bejarano expidió el Reglamento a la Ley de Comercio Electrónico del Ecuador y luego oficialmente fue publicado en el R.O. No. 735 del Martes 31 de Diciembre del 2002.

Aspecto importante es la oportunidad que tiene cualquier persona natural o jurídica que actúe como tercero de confianza, para prestar los servicios de conservación, almacenamiento y custodia de mensajes de datos siempre y cuando cumpla con los requisitos que la Ley y su reglamento lo establecen, prestación de servicios que incluye:

- ✓ Conservación, almacenamiento y custodia de la información en formato electrónico con las debidas seguridades.
- ✓ Preservación de la integridad de la información conservada.
- ✓ Administración del acceso a la información y la reproducción de la misma cuando se requiera.
- ✓ Respaldo y recuperación de información.
- ✓ Otros servicios relacionados con la conservación de los mensajes de datos.

La prestación de servicios de Registro de Datos se realizará bajo el régimen de libre competencia y contratación. Las partes que intervengan en la contratación de este tipo de servicios, podrán determinar las condiciones que regulan su relación. Por orden de autoridad competente, podrá ordenarse a los proveedores de servicios de Registro Electrónico de Datos mantener en sus sistemas respaldos de los mensajes de datos que tramite por el tiempo que se considere necesario. [WWW 061]

Una parte que comprende los Artículos del 10 al 16, en la que se reglamenta los aspectos de los certificados de firma electrónica como parte de la **Infraestructura de Llave Pública,** que es aceptada bajo el principio de neutralidad tecnológica, sin restringir la autonomía privada para el uso de otras firmas electrónicas generadas fuera de la infraestructura de llave pública, ni afecta los pactos que acuerden las partes sobre la validez y eficacia jurídica de la firma electrónica conforme a lo establecido en la ley y el reglamento. Los principios y elementos que respaldan a la firma electrónica son:

- ✓ No discriminación a cualquier tipo de firma electrónica, así como a sus medios de verificación o tecnología empleada.
- ✓ Practicas de certificación basadas en estándares internacionales o compatibles a los empleados internacionalmente.
- ✓ El soporte lógico o conjunto de instrucciones para los equipos de cómputo y comunicaciones, los elementos físicos y demás componentes adecuados al uso de las firmas electrónicas, a las prácticas de certificación y a las condiciones de seguridad adicionales.
- ✓ Sistema de gestión que permita el mantenimiento de las condiciones señaladas en los literales anteriores, así como la seguridad, confidencialidad, transparencia y no-discriminación en la prestación de sus servicios.
- ✓ Organismos de promoción y difusión de los servicios electrónicos, y de regulación y control de las entidades de certificación.

Las funciones que deben cumplir las entidades de certificación son: proporcionar las correspondientes Listas de Revocación de Certificados mediante mecanismos automáticos de acceso a listas de certificados revocados o suspendidos. Los periodos de actualización de las listas de certificados suspendidos, revocados o no vigentes por cualquier causa se establecerán contractualmente. También es obligación producir la revocación del certificado, que tendrá también como consecuencia la respectiva publicación y la desactivación del enlace que informa sobre el

certificado. Esta notificación y posterior publicación se lo hará por cualquiera de los siguientes medios:

- ✓ Siempre a la página electrónica determinada por el CONATEL en la que se reporta la situación y la validez de los certificados, así como en la página WEB de la entidad certificadora.
- ✓ Mediante un aviso al acceder al certificado de firma electrónica desde el hipervínculo de verificación, sea que éste forme parte de la firma electrónica, que conste en un Directorio electrónico o por cualquier procedimiento por el cual se consulta los datos del certificado de firma electrónica.

Se reconoce la validez que tienen internacionalmente los certificados de firma electrónica, los certificados emitidos en el extranjero tendrán validez legal en Ecuador, una vez obtenida la revalidación respectiva emitida por el CONATEL, quien deberá comprobar el grado de fiabilidad de los certificados y la solvencia técnica de quien los emite.

El reglamento además limita la acreditación, responsabilidades y funcionamiento de las entidades de certificación las cuales deberán estar registradas por el CONATEL, también se reconoce con el carácter de PROBATORIO a las empresas que operan directamente o a través de terceros relacionados en Ecuador. Las entidades que habiéndose registrado y obtenido autorización para operar, directamente o a través de terceros relacionados en Ecuador, no se acreditan en el CONATEL, tendrán la calidad de entidades de certificación de información no acreditadas y están obligados a informar de esta condición a quienes soliciten o hagan uso de sus servicios, debiendo también, a solicitud de autoridad competente, probar la suficiencia técnica y fiabilidad de los certificados que emiten. El reglamento faculta al CONATEL para verificar la autenticidad y exactitud de todos los datos de las entidades de certificación y en cualquier momento, podrá requerir los documentos de respaldo que confirmen la autenticidad y exactitud de los datos que contiene. [WWW 064]

4.4 Legislación Internacional – Normas de Seguridad

Para iniciar un análisis sobre la legislación internacional que sobre firmas digitales existe sobre todo en los países de América Latina y otros países que por su incidencia comercial sobre otros, se los considera dentro de este análisis, se puede mencionar a aquellos que actualmente cuentan con una legislación en materia de Firma electrónica:

- ✓ Argentina (Agosto 2001)
- ✓ Brasil (Septiembre 2000)
- ✓ Colombia (Agosto 1999)
- ✓ Chile **(** Marzo 2002)
- ✓ **Ecuador (Abril 2002)**
- ✓ México (Mayo 2000)
- ✓ Panamá ()
- ✓ Perú (Junio 2000)
- ✓ Puerto Rico (Agosto 1998)
- ✓ Venezuela (Marzo 2001)

Ley Modelo UNCITRAL de la ONU: La organización de las Naciones Unidas por conducto de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNDUMI, o UNCITRAL por sus siglas en inglés), con sedes en Nueva York y Viena, ha elaborando múltiples convenciones, además de reglas de arbitraje, modelos de contratos, de cláusulas contractuales y guías jurídicas, pero sobre todo Leyes Modelo como la de Ley de Arbitraje Internacional, Ley de Comercio Electrónico y Ley de Firma Electrónica. En la sesión del 12 de diciembre de 2001, fue aprobada por el pleno de la 85 Sesión Plenaria de la Asamblea General La Ley Modelo sobre las Firmas Electrónicas. Siendo ésta Ley Modelo la que ha sido más aceptada a nivel internacional para ser tomada como modelo para las legislaciones sobre el comercio electrónico en los diferentes países miembros de la ONU y sobre todo en América Latina y el Caribe. [WWW 065]

Argentina: El 17 de marzo de 1997, el Sub-Comité de Criptografía y Firma Digital, dependiente de la Secretaría de la Función Pública, emitió la Resolución 45/97 Firma Digital En La Administración Pública y el 14 de Diciembre del 2001 la Ley de Firma Digital para la República Argentina 25/506.

Brasil: DECRETO Nº 3.587, de 5 de septiembre del 2000 por el que se establece normas sobre infraestructura de claves públicas del Poder Ejecutivo Federal.

- ✓ **Ministerio de Ciencia y Tecnología**
- ✓ **Superintendencia de Industria y Comercio**

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

Colombia: Ley de Comercio Electrónico (Ley 527 de 1999) por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales.

Objetivo: la reglamentación y la definición del acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, además del establecimiento de las Entidades de Certificación. Su ámbito de aplicación es el uso de firmas digitales en mensajes de datos. La Ley colombiana reconoce a tres elementos principales como **Firma Digital, Mensaje de Datos, y Entidad de Certificación**. En cuanto a la **Supervisión y Control,** la ley les da la facultad a las Entidades de Certificación autorizadas por la Superintendencia de Industria y Comercio de Colombia.

La ley reconoce el **valor probatorio** de un mensaje de datos al igual que uno en papel siempre que cumpla con los siguientes requisitos:

- ✓ Es única a la persona que la usa.
- ✓ Es susceptible de ser verificada.
- ✓ Está bajo el control exclusivo de la persona que la usa.
- ✓ Está ligada a la información o mensaje, de tal manera que si éstos son cambiados, la firma digital es invalidada.
- ✓ Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional.

La ley Colombiana si da validez a Certificados Digitales Extranjeros. Las **sanciones** serán impuestas por la Superintendencia de Industria y Comercio de Colombia, de acuerdo con el debido proceso y el derecho de defensa, podrá imponer según la naturaleza y la gravedad de la falta, estas van de la Amonestación a la Revocación de la Autorización.

Perú: Ley No. 27269 Ley de Firmas y Certificados Digitales (2000). **Objetivo:** utilizar la firma electrónica otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad. Su **Ámbito de Aplicación** son aquellas Firmas electrónicas que, puestas sobre un mensaje de datos puedan vincular e identificar al firmante, y garantizar su integridad y autenticación.

Venezuela: Ley sobre Mensajes de Datos y Firmas Electrónicas (2001). **Objetivo:** otorgar y reconocer eficacia y valor jurídico al mensaje de datos, a la firma electrónica y a toda información inteligible en formato electrónico. Su **Ámbito de Aplicación** son los mensajes de datos y firmas electrónicas.

Reconoce a los **Proveedores de Servicios de Certificación**, y son los que emiten los certificados de firma electrónica de acuerdo a los

reglamentos establecidos para su funcionamiento. La firma tendrá **valor probatorio** cuando vincule al signatario con el mensaje de datos y se pueda atribuir su autoría. La ley reconoce **a los Certificados Extranjeros siempre y cuando estén garantizados por un proveedor de servicios de certificación acreditado, tendrán la misma validez y eficacia jurídica.** Las **Sanciones** para los proveedores de servicios de certificación van de entre 500 a 2,000 Unidades Tributarias.

Panamá: Ley 43 de Comercio Electrónico de Agosto del 2001.

Alemania: Ley sobre Firmas Digitales en Junio de 1997 y su reglamento publicado el 7 de junio del mismo año, Law Governing Framework Conditions for Electronic Signatures and Amending Other Regulations (Bundesgesetzblatt - BGBI. Teil 1 5. 876 vom 21. Mai 2001). Publicado el 16 de Mayo de 2001. Official Journal N° 22, 22 May 2001. In Force 22 May 2001).

España: Real Decreto Ley en Septiembre de 1999 sobre Firmas Electrónicas. Instrucción sobre el Uso de la Firma Electrónica de los Fedatarios Públicos Orden de 21 de febrero de 2000 por la que se aprueba el Reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de firma electrónica. -Ley de Servicios de la Sociedad de Información-) El Proyecto de Ley de firma electrónica, de 20 de junio de 2003, ha introducido diversas modificaciones respecto del vigente Real Decreto ley de 1999 de firma electrónica.

La ley otorga el **Reconocimiento de certificados extranjeros,** estos deben cumplir los siguientes requisitos:

- ✓ Que el prestador de servicios reúna los requisitos establecidos en la normativa comunitaria sobre firma electrónica y haya sido acreditado, conforme a un sistema voluntario establecido en un Estado miembro de la Unión Europea.
- ✓ Que el certificado esté garantizado por un prestador de servicios de la Unión Europea que cumpla los requisitos establecidos en la normativa comunitaria sobre firma electrónica.
- ✓ Que el certificado o el prestador de servicios estén reconocidos en virtud de un acuerdo bilateral o multilateral entre la Comunidad Europea y terceros países u organizaciones internacionales.

Francia: Décret n° 2001-272 du 30 mars 2001 pris pour 1 'application de 1 'article 1316-4 du code civil et relatif á la signature électronique. Loi 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de 1 'informtion et relative á la signature électronique.

Irlanda: Electronic Commerce Act, 2000 (Number 27 of 2000)

Italia: El 15 de marzo de 1997, fue publicado el "Reglamento sobre: Acto, Documento y Contrato en Forma Electrónica" aplicable a las diversas entidades de la Administración Pública, el 15 de abril de 1999 las reglas técnicas sobre firmas digitales y el 23 de enero del 2002 la ley sobre firma electrónica.

Japón: Ley sobre firma electrónica y Servicios de Certificación, Abril del 2001

Estados Unidos: La primera ley en materia de Firma Digital en el Mundo fue la denominada "Utah Digital Signature Act", publicada en mayo de 1995 en el Estado de UTAH, Su **objetivo** es facilitar mediante mensajes electrónicos y firmas digitales las transacciones. Procurar las transacciones seguras y la eliminación de fraudes. Establecer normas uniformes relativas a la autenticación y confiabilidad de los mensajes de

datos, en coordinación con otros Estados. Su **ámbito de aplicación** son las transacciones mediante mensajes electrónicos, su confiabilidad, así como las firmas digitales. Esta ley, reconoce a la **Firma Digital, al Criptosistema Asimétrico, al Certificado Electrónico.** En cuanto a la Supervisión y **al control,** estos recaen sobre la **División**, quien actúa como autoridad certificadora. También formula políticas para la adopción de las tecnologías de firma digital y realiza una labor de supervisión regulatoria. La **emisión de los certificados** corre a cargo de la autoridad certificadora que ha sido acreditada.

La ley no contempla el reconocimiento de **certificados extranjeros,** solo se menciona que la División puede reconocer la autorización emitida por Autoridades Certificadoras de otros Estados. No contempla sanciones. [WWW 063]

También se tiene algunas leyes y decretos en cuanto a la regulación de Firmas Electrónicas y seguridad de la Información.

- ✓ ABA.- El Comité de Seguridad de la Información, de la División de Comercio Electrónico, de la American Bar Association, emitió, en agosto de 1996, la "Guía de Firmas Digitales".
- ✓ NCCSL: El 15 de agosto de 1997, la Conferencia Nacional de Comisionados sobre Derecho Estatal Uniforme, elaboró la "Uniform Electronic Transactions Act" (UETA), y se aprobó el 30 de julio de 1999.
- ✓ El 4 de agosto del 2000 se aprobó la "Uniform Computer Information Transactions Act" (UCITA), la cual se encuentra en proceso de adopción por los diversos Estados de la Unión Americana.

- ✓ **Presidencia.-** El 30 de junio el 2000 se emite la "Electronic Signatures in Global and National Commerce Act" (E-Sign Act.) vigente a partir del 1 de octubre del 2000 (otorgando a la firma y documento electrónico un estatus legal equivalente a la firma autógrafa y al documento en papel).

Unión Europea: La Directiva del Parlamento Europeo y del Consejo estableció un marco común para la firma electrónica (1999). Su **Objetivo** es garantizar el buen funcionamiento del mercado interior en el área de la firma electrónica, instituyendo un marco jurídico homogéneo **y** adecuado para la Comunidad Europea, y definiendo criterios que fundamenten su reconocimiento legal. Su **Ámbito de aplicación** se limita al reconocimiento legal de la firma electrónica y establece un marco jurídico para determinados servicios de certificación accesibles al público. Define a la **Firma electrónica** a la realizada en forma digital integrada en unos datos, ajena a los mismos o asociada con ellos, que utiliza un signatario para expresar conformidad con su contenido y que cumple los siguientes requisitos:

- ✓ Estar vinculada al signatario de manera única
- ✓ Permitir la identificación del signatario
- ✓ Haber sido creada por medios que el signatario pueda mantener bajo su exclusivo control
- ✓ Estar vinculada a los datos relacionados de modo que se detecte cualquier modificación ulterior de los mismos.

Los Estados miembros velarán porque los certificados expedidos por un proveedor de servicios de certificación establecido en un tercer país tengan la misma validez que un local cuando cumplan con los siguientes requisitos:

- ✓ El proveedor de servicios de certificación cumple los requisitos establecidos en la presente Directiva y ha sido acreditado en el

marco de un sistema voluntario de acreditación establecido por un Estado miembro

- ✓ Un proveedor de servicios de certificación establecido en la Comunidad, que cumpla las prescripciones del Anexo II, avala el certificado en la misma medida que los suyos propios
- ✓ El certificado o el proveedor de servicios de certificación están reconocidos en virtud de un acuerdo bilateral o multilateral entre la Comunidad y terceros países u organizaciones internacionales.

4.5 Autoridades Certificadoras

Introducción

Las redes públicas como el Internet están compuestas por un sinnúmero de enlaces físicos que conectan los equipos, denominados routers[55] o "encaminadores" cuya función principal es redirigir los mensajes que les llegan de unas direcciones hacia las direcciones de destino, en donde la identidad de los nodos sólo consiste en las direcciones IP que se almacenan en éstos routers, pero no se tiene la seguridad de que esas IP son todas de buena procedencia o con fines lícitos. Dadas las múltiples ventajas al utilizar las redes públicas sea cual sea la actividad que se realice, se hace necesario la implantación de una **Identidad Digital** para todos los agentes de la red a fin de estar seguros. La Criptografía es una tecnología básica que permite conseguir dicho objetivo proporcionando servicios, mecanismos y algoritmos que permiten establecer esta **identidad**. La identidad es aquel reconocimiento que haríamos nosotros de las credenciales, físicas o informativas, que una persona nos muestra. Las credenciales físicas como: cédula de identidad, el Pasaporte, la licencia de conducir, etc., donde podemos probar que la persona es quien dice ser. El problema surge cuando no conocemos la procedencia de dichos datos para su verificación, sólo reconoceremos a aquellos que nos

[55] Dispositivos físicos de una red, enrutadores de datagramas IP a través de las redes de ordenadores.

presenten credenciales que ya habíamos visto antes y que, a nuestro entender, son auténticas. La autenticidad de las credenciales, a su vez, consiste en que encontremos en los documentos presentados, signos reconocibles cuyas características y dificultad de reproducción permitan confiar en que sólo una autoridad conocida ha podido expedirlos y que lo ha hecho en condiciones perfectamente definidas.

Al igual que en el mundo no digital, las transacciones de valor en redes públicas sólo podrán realizarse si dentro de ellas hay agentes especiales, entidades digitales que ofrezcan confianza a los demás agentes de la red. Estas entidades se denominan, **Terceras Partes Confiables** (TPC) **o Autoridades de Certificación** (AC), que pueden ser organizaciones o instituciones de carácter público o privado. La criptografía, por sí misma, no proporciona ese nivel de "tranquilidad" necesario, por lo que es necesario tener mecanismos de orden superior como lo es la firma digital realizada por **Terceras Partes Confiables**, para disponer del nivel de confianza digital que se requiere. Con la participación de éstas entidades como proveedores de la confianza digital, es posible transportar a las redes públicas del tipo Internet la emisión de certificados diversos como los de: identidad de los usuarios, de hechos que constan en los expedientes de las administraciones públicas o privadas, la documentación notarial, de la identificación de las partes en el comercio electrónico, etc.

La función principal que cumplen éstas organizaciones es emitir certificados y dar **Fe Pública** de que se ha realizado un contrato, se ha hecho una transacción y ser la que resguarde todos los documentos correspondientes a dicho acuerdo entre las partes como: términos y cláusulas del contrato, autenticidad de la documentación presentada,

identificación de las partes, fecha, lugar y hora en la que se firma el contrato, etc. En estos casos, tanto el notario público como los testigos particulares actúan como proveedores de confianza a las partes, ya que en el caso de que surjan conflictos o incumplimientos, aquellos serán requeridos por el demandante para que den fe de los términos y detalles que constituyeron el contrato o su firma.

Para que cualquier usuario pueda confiar en los demás usuarios o en los gestores que están en la red, se deben establecer ciertos protocolos de seguridad, mediante los cuales, si dos usuarios desconfían, pueden interaccionar con un tercero de tal modo que, al terminar con éxito el protocolo, puedan terminar confiando mutuamente para la realización de sus operaciones dentro de la red.

Existen diferentes tipos de protocolos en los que intervienen terceras partes confiables:

- ✓ Los **protocolos arbitrados.** En ellos una TPC o Autoridad de Certificación participa en la transacción para asegurar que ambos lados actúen según las reglas dadas por el protocolo.
- ✓ Los **protocolos notariados.** En este caso la tercera parte confiable, además de garantizar la correcta operación, también permite juzgar si ambas partes actuarán por derecho según la evidencia presentada a través de los documentos aportados por los participantes e incluidos dentro del protocolo notarial. En estos casos, se añade la firma digital del notario a la transacción, pudiendo éste testificar, posteriormente, en caso de disputa.
- ✓ Los **protocolos auto verificables.** En estos protocolos cada una de las partes puede darse cuenta si la otra parte actúa deshonestamente, durante el transcurso de la operación. La firma digital es un elemento básico de los protocolos auto verificable ya

que no precisa de la intervención de una Autoridad de Certificación para determinar la validez de una firma, pues tiene el mismo efecto que las firmas manuscritas, ya que es una "marca que sólo el emisor puede hacer y que todos los demás pueden reconocer y verificar en cualquier momento.

Una Autoridad de Certificación puede emitir diferentes tipos de certificados:

- ***Certificados de Identidad (personal o digital).-*** son los más utilizados actualmente dentro de los criptosistemas de clave pública y ligan una identidad personal (usuario) o digital (equipo, software, etc.) a una clave pública.
- ***Certificados de Autorización (potestad).-*** certifican otro tipo de atributos del usuario distintos a la identidad, como el pertenecer a una determinada asociación, disfrutar de una serie de privilegios, poseer un carnet de conducir, etc.
- ***Certificados Transaccionales (actas y resguardos).-*** son aquellos que atestiguan que algún hecho o formalidad acaeció o fue presenciada por un tercero; el agente de registro al servicio de la Autoridad de Certificación emisora.
- ***Certificados de Tiempo (estampillado o registro temporal). -*** Permiten dar fe de que un documento existía en un instante determinado de tiempo, por lo que constituyen un elemento fundamental de todos los servicios de registro documental y de protección de la propiedad intelectual o industrial que se están proponiendo.

Quién puede ser una autoridad de certificación

Cualquier institución que quiera ser Autoridad de Certificación debe regirse conforme a las leyes vigentes en cada país y siendo, a su vez, cada una de ellas suficientemente confiables como para ser aceptadas intemacionalmente. Desde el punto de vista técnico, para poder ser una Autoridad de Certificación las instalaciones y recursos humanos dedicados a tal propósito, deben cumplir con la normativa, en cada momento vigente, que afecte a su servicio y, además, demostrar incontestablemente cuales son los niveles de seguridad que realmente tienen.

La exigencia mínima que se le puede hacer a una Autoridad de Certificación es que cualquier ataque contra el secreto de su clave privada debe poder detectarse e impedirse. La Legislación Ecuatoriana permite a cualquier persona, organismo público o privado ser una entidad de certificación, una vez que haya cumplido con los requisitos establecidos por la Institución encargada en nuestro país que es el CONATEL, a través de sus reglamentos que para el efecto debe establecer.

4.6 Anexos (Leyes y Reglamentos)

En el apartado correspondiente a ANEXOS, se incluyen la Ley y Reglamento que sobre Comercio Electrónico, firmas y mensajes de Datos existen en el Ecuador. Entre éstas se tiene la Ley de Comercio Electrónico, Firmas y Mensajes de Datos, el Reglamento a la Ley de Comercio Electrónico, Firmas y Mensajes de Datos, los artículos de la Ley de Propiedad Intelectual que se refieren al tema en estudio, así como los artículos correspondientes al tema que en la Ley Orgánica de Defensa del Consumidor se tiene, también de la ley de Contratación Pública del

Ecuador, Ley de Conectividad, y sus correspondientes artículos de sus reglamentos.

4.7 Conceptos y Definiciones

Para efectos de aplicación de la Ley de Comercio Electrónico, dentro del Capítulo I, Principios Generales y el apartado de Disposiciones Generales se ha definido un Glosario de Términos Básicos que deberán ser utilizados.

Principios Generales

Reconocimiento jurídico de los mensajes de datos (Art. 2)

Incorporación por remisión (Art. 3

Propiedad intelectual (Art. 4)

Confidencialidad y reserva (Art. 5)

Información escrita (Art. 6)

Información original (Art. 7)

Conservación de los mensajes de datos (Art. 8)

Protección de datos (Art. 9)

Procedencia e identidad de un mensaje de datos (Art. 10)

a) Envío y recepción de los mensajes de datos (Art. 11)

b) Duplicación del mensaje de datos (Art. 12) [WWW 062]