UNION INTERNACIONAL
DE
TELECOMUNICACIONES

ASOCIACION DE EMPRESAS
DE TELECOMUNICACIONES
DE LA COMUNIDAD ANDINA

Legislación sobre Comercio Electrónico en los Países Miembros de la Comunidad Andina

Análisis comparativo

Recomendaciones para su armonización

ANEXO B:

Legislación vigente sobre Comercio Electrónico en los Países de la Comunidad Andina y anteproyectos Bolivianos.

ANEXO C:

Lista, no exhaustiva, de Entidades / Autoridades de Certificación.

Junio de 2002

Estudio realizado con el apoyo de la Unión Internacional de Telecomunicaciones -UIT-,
Oficina de Desarrollo de las Telecomunicaciones Unidad e-Strategy.

Especialista de la UIT
María Gabriela Sarmiento
Abogado
Administrador de proyectos
Unidad e-Strategy
Telf. +41 22 730 58 95
Fax +41 22 730 54 84
maria-gabriela.sarmiento@itu.int

« …Il faut que les États, à travers une volonté politique commune opèrent un rapprochement de leurs systèmes juridiques sur les questions relatives aux réseaux. Il faut qu'ils accordent sur un socle minimal de valeurs universelles dont il se chargent d'assurer l'application effective. »

« …La nécessité d'une harmonisation repose sur un constat d'inefficacité de carence ou de contradiction des règles existantes. »

« …Deux tentations extrêmes
menacent la qualité de l'harmonisation: celle de la réponse normative en temps réel au défi technologique et celle de l'abandon du droit à la technique. »

« …la régulation du commerce électronique, la mise en place des nouveaux modes d'adressage électronique ne nécessitent pas automatiquement une harmonisation « autoritaire » et « maximale » »

« …l'échelle d'intervention et la nécessaire prudence vis-à-vis des évolutions techniques conduisent naturellement à privilégier l'élaboration d'une norme générale, fixant davantage des standards que des règles précises. »

« …La complétude de l'harmonisation ne sera pas nécessairement recherchée au sein d'un texte unique mais dans l'application simultanée de plusieurs corps de règles d'importances et de sources différentes. »

Extractos del artículo: « *Faut-il une harmonisation minimale du droit ?*[1] » de Valérie Laure Benabou, Profesora de la Universidad de Lyon 2, Francia.

[1] Traducción no fidedigna del artículo: ¿Hace falta una armonización mínima del derecho?.
« … Por medio de una voluntad política común, los Estados deben realizar un acercamiento de sus sistemas jurídicos sobre las cuestiones relacionadas con las redes. Ello debe hacerse con fundamento en valores universales básicos. »
« …La necesidad de una armonización reposa en la constatación de ineficacia y carencia de normas existentes o de una contradicción entre las mismas. »
« …La calidad de la armonización de normas es amenazada por dos tentaciones extremas: la respuesta normativa en tiempo real en desafío a la tecnología y el abandono del derecho a la tecnología. »
« …la regulación del comercio electrónico y la puesta en práctica de nuevos usos electrónicos no necesitan de una armonización automática 'autoritaria' y 'extrema' »
« …la escala de intervención y la prudencia necesaria *vis à vis* de las evoluciones técnicas conducen, naturalmente, a privilegiar la elaboración de una norma general que establece estándares en lugar de crear reglas precisas. »
« …la armonización no será fruto de un texto único, sino de la aplicación simultánea de varios cuerpos legales de importancia y de diversas fuentes. » Traducción nuestra.

Indice de los Anexos

Página

Anexo A:

Cuadro comparativo de los textos legales sobre comercio electrónico en los países de la Comunidad Andina 6

Anexo B:

Legislación vigente sobre comercio electrónico en los Países Miembros de la Comunidad Andina y anteproyectos Bolivianos 194

A. BOLIVIA **195**

- Anteproyecto de Código de Comercio 195

- Proyecto de Código Civil 195

- Proyecto de Código del Proceso Civil 196

- Proyecto de Código Tributario 197

B. COLOMBIA **198**

- Ley 527 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, y se establecen las entidades de certificación y se dictan otras disposiciones 198

- Decreto Nº 1747 por el cual se reglamenta parcialmente la Ley 527, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales 209

- Resolución 26.930 de la Superintendencia de Industria y Comercio por la cual se fijan los estándares para la autorización y funcionamiento de las entidades de certificación y sus auditores 216

C. ECUADOR **224**

- Ley de comercio electrónico, firmas electrónicas y mensajes de datos 224

D. PERÚ **240**

- Ley Nº 27269 sobre Ley de firmas y certificados digitales 240

- Ley N° 27310 que modifica el artículo 11° de la Ley N° 27269 242

- Reglamento de la Ley N° 27269 de firmas y certificados digitales 243

- Ley 27291 que modifica el Código Civil permitiendo la utilización de los medios electrónicos para la comunicación de la manifestación de voluntad y la utilización de la firma electrónica 256

- Ley N° 27419 sobre notificación por correo electrónico 257

- Resolución 000103 de aduanas 258

E. VENEZUELA **260**

- Decreto 1024. Ley sobre mensajes de datos y firmas electrónicas 260

F. Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) ***272***

- Ley Modelo de la CNUDMI sobre comercio electrónico 272

- Guía para la incorporación al Derecho Interno de la Ley Modelo de la CNUDMI sobre comercio electrónico 279

- Ley Modelo de la CNUDMI sobre las firmas electrónicas 315

Anexo C:

Lista, no exhaustiva, de Entidades / Autoridades de Certificación 319

Anexo B :

Legislación vigente sobre comercio electrónico en los Países Miembros de la Comunidad Andina y anteproyectos Bolivianos

A. BOLIVIA

- Anteproyecto de Código de Comercio
- Proyecto de Código Civil
- Proyecto de Código del Proceso Civil
- Proyecto de Código Tributario

B. COLOMBIA

- Ley 527 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, y se establecen las entidades de certificación y se dictan otras disposiciones.

- Decreto Nº 1747 por el cual se reglamenta parcialmente la Ley 527, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales.

- Resolución 26.930 de la Superintendencia de Industria y Comercio por la cual se fijan los estándares para la autorización y funcionamiento de las entidades de certificación y sus auditores.

C. ECUADOR

- Ley de comercio electrónico, firmas electrónicas y mensajes de datos

D. PERU

- Ley N° 27269 sobre Ley de firmas y certificados digitale

- Ley N° 27310 que modifica el artículo 11° de la Ley N° 27269

- Reglamento de la Ley N° 27269 de firmas y certificados digitales

- Ley 27291 que modifica el Código Civil permitiendo la utilización de los medios electrónicos para la comunicación de la manifestación de voluntad y la utilización de la firma electrónica

- Ley N° 27419 sobre notificación por correo electrónico

- Resolución 000103 de aduanas

E. VENEZUELA

- Decreto 1024. Ley sobre mensajes de datos y firmas electrónicas

F. Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI)

- Ley Modelo de la CNUDMI sobre comercio electrónico
- Guía para la incorporación al Derecho Interno de la Ley Modelo de la CNUDMI sobre comercio electrónico
- Ley Modelo de la CNUDMI sobre las firmas electrónicas

Anexo B: Legislación vigente sobre comercio electrónico en los Países Miembros de la Comunidad Andina y ante-proyectos Bolivianos.

[2] A. BOLIVIA

ANTEPROYECTO DE CÓDIGO DE COMERCIO.

Se incorpora en el TITULO III del Libro Tercero Obligaciones y Contratos Comerciales con dos Capítulos: Disposiciones Generales y Validez y Comunicación de los Mensajes de Datos

CAPÍTULO I

- Ámbito de aplicación con alcances a todo tipo de información en forma de mensaje de datos generados en las relaciones jurídicas de carácter comercial.
- Orienta a los operadores en el uso de la terminología como mensaje de datos, emisor de un mensaje de datos, destinatario y sistema de información.
- Admite los contratos celebrado por mensaje de datos, desde el momento de la aceptación que surte efectos conforme las regulaciones previstas.
- Norma los actos y contratos escritos, establece los requisitos a ser cumplidos por las partes y determina cuando la información es accesible para ulterior consulta.
- No regula la firma electrónica, la admite por tener como base la firma autógrafa que no está legislada por ser distintivo de la personalidad.
- La elaboración de los libros contables, documentos y archivo de libros, será posible con el uso de medios electrónicos.

CAPÍTULO II

- Reconoce el valor probatorio de los mensajes de datos, concordante con las normas del Proceso Civil, para efectos de prueba plena. Le atribuye la presunción en cuanto al emisor, el destinatario le atribuye esa situación.
- El acuse de recibo surte efectos legales por disposición legal o por requerirlo el emisor. La recepción de un mensaje de datos que se determina en caso de que el destinatario haya designado un sistema de información o que de enviarse el mensaje de datos a un sistema de información del destinatario que no sea el sistema de información designado, se entiende como recibido en el momento de la recuperación del documento.
- Cuando no se ha designado el sistema, la recepción tiene lugar al ingresar el mensaje de datos en un sistema de información del destinatario, esta regla no se aplica cuando el sistema de información está en otro lugar.
- A falta de acuerdo, el mensaje de datos se tiene por expedido en el lugar donde el emisor tiene su establecimiento y recibido en el lugar donde el destinatario tenga el suyo. En caso de tener más de dos establecimientos, se considera el domicilio principal, de no tenerlo, se considera la residencia habitual.

PROYECTO DE CÓDIGO CIVIL

Artículo 453. Manifestación de la voluntad
Las partes pueden manifestar su voluntad en forma expresa o tácita.
Expresa si se la mantiene verbalmente o por escrito o bien por signos inequívocos y tácita si resulta presumible de ciertos hechos o actos.

[2] Flag courtesy of www.theodora.com/flags used with permission

Artículo 456. Modificaciones en la oferta y en la aceptación
III. Los contratos concluidos por teléfono, *Internet u otros medios tecnológicos* que pongan a las partes, sus mandatarios o representantes en comunicación directa, se consideran hechos entre presentes, salvo lo establecido en el parágrafo II del artículo 462.

Artículo 461. Lugar del contrato entre presentes
Entre presentes, el lugar del contrato es aquel donde los contratantes se encuentren

Artículo 462. Lugar del contrato entre no presentes
I. El lugar del contrato concluido entre no presentes es aquel donde ha sido propuesto, salvo pacto contrario u otra disposición de la ley.
II. Se estará a la regla del parágrafo anterior en el caso de, contrato celebrado por teléfono, telégrafo, télex, radio, fax, correo electrónico u otro medio similar, cuando corresponda.

PROYECTO DE CÓDIGO DEL PROCESO CIVIL

Artículo 170. Medios de Prueba
Son medios legales de prueba: los documentos, la confesión, el juramento, las declaraciones de testigos, el peritaje, las presunciones, la inspección judicial, *fotografías, facsímiles, cintas cinematográficas, de videos, de sonido, mensajes de datos, reconstrucciones de hecho y en general cualquier otra similar u objeto que sirva para averiguar la verdad.*

Artículo 182. Efectos jurídicos de los mensajes de datos
I. Se reconocen efectos jurídicos, validez y fuerza obligatoria a los mensajes de datos, entendidos como la información generada, enviada, recibida, archivada o comunicada por medios electrónicos, ópticos o a través de cualesquier otra tecnología.
II. Cuando la ley requiera que un documento sea presentado y conservado en su forma original, ese requisito quedará satisfecho si se acredita que el mensaje de datos al que se refiere el parágrafo anterior se ha conservado íntegro a partir del momento en que se generó por primera vez y en su forma definitiva y sea accesible para su ulterior consulta.
III. Para efectos de este artículo, se entenderá que la informará es íntegra cuando haya permanecido completa e inalterada, salvo algún cambio que sea inherente al proceso de su comunicación, archivo registro o presentación.

Artículo 183. Fuerza probatoria del Mensaje de Datos
I. Para valorar la fuerza probatoria de un mensaje de datos, se estimará primordialmente la fiabilidad del método por el que haya sido generado, archivado, comunicado o conservado.
II. Para considerar que el mensaje de datos ha sido adecuadamente conservado, será necesario que sea accesible para su ulterior consulta y haya sido preservado con el formato en que se haya generado, enviado o recibido o con alguno que acredite que la reproduce con exactitud y preserve todo dato que permita determinar su origen, destino, así como la fecha y hora de su envío y recepción.

Artículo 184. Valor probatorio de fotografías, mensaje de datos y otros
I. El valor de las pruebas fotográficas, taquigráficas y de otras emergentes de los descubrimientos científicos que aportaran las partes, quedarán al prudente arbitrio judicial. II. Las fotografías de personas, lugares, edificios, construcciones, papeles, documentos y objetos de cualquier especie deberán contener la certificación correspondiente que acredite el lugar, tiempo y circunstancia en que fueron tomadas, así como que corresponden a lo representado en ellas, para que constituyan prueba plena. Tratándose de mensaje de datos, se estará a lo dispuesto por los artículos 170, 181, 182 y 183.

PROYECTO DE CÓDIGO TRIBUTARIO

Artículo 89. Normas Reglamentarias Administrativas

II. En especial, podrá dictar normas obligatorias con relación a los siguientes puntos:
   4. Formas y plazos y medios de facturación, de presentación de declaraciones juradas y de toda otra información de importancia fiscal, de pago y de recepción de tributos, así como instrumentos o medios manuales, mecánicos o *informáticos* para el cumplimiento de sus obligaciones tributarias.
   6. Formas, plazos y medios de documentación de las obligaciones tributarias por parte del sujeto pasivo.

III. Las normas administrativas a dictarse, para su vigencia deberán observar lo dispuesto en este Código. Los órganos de difusión oficial a que se refiere el parágrafo II del artículo 6 del presente Código pueden publicarse conforme a las leyes aplicables a la materia, en cualquier medio tecnológicamente disponible, el medio a emplearse deberá ser comunicado al público por la Administración Tributaria dentro del primer mes de cada año calendario en medios de prensa de circulación nacional.

Artículo 109. Firma electrónica del sujeto pasivo, medios e instrumentos tecnológicos

En todo trámite, presentación de datos o información a la Administración Tributaria que se realice vía medios magnéticos o transferencia electrónica surtirá los mismos efectos legales que la firma manuscrita o autógrafa. A este efecto se entiende por firma electrónica el código numérico o alfa-numérico que con carácter único, individual y reservado asigne la Administración a cada obligado tributario, con arreglo a las normas que dicte la misma.

La facturación, la presentación de declaraciones juradas y de toda otra información de importancia fiscal, la retención, percepción y pago de tributos, el llevado de libros, registros y anotaciones contables y documentación de las obligaciones tributarias, siempre que sean autorizados por la Administración Tributaria a los sujetos pasivos y terceros responsables, así como las comunicaciones y notificaciones que aquella realice a estos últimos, podrán efectuarse por cualquier medio tecnológicamente disponible en el país, conforme a la legislación aplicable a la materia.

Estos medios incluidos los magnéticos, electrónicos, ópticos o de cualquier otra tecnología avanzada deberán permitir la identificación de quien los emite, garantizar la verificación de la integridad de la información y datos en ellos contenidos de forma tal que cualquier modificación de los mismos ponga en evidencia su alteración y cumpla los requisitos de pertenecer únicamente a su titular y encontrarse bajo su absoluto y exclusivo control.

Artículo 119. Notificación por correspondencia postal y otros sistemas de comunicación

Será válida la notificación practicada por correspondencia postal certificada, efectuada mediante correo público o privado. También será válida la notificación que se practique mediante o por sistemas de comunicación telegráficos, facsímiles, electrónicos o por cualquier otro medio tecnológicamente disponible y similares, siempre que los mismos permitan confirmar, verificar su recepción y se ajusten a las leyes aplicables a la materia.

En las notificaciones practicadas en esta forma, los plazos empezarán a correr desde el día de su recepción tratándose de día hábil; de lo contrario, se tendrá por practicada la notificación a efectos de cómputo, a primera hora del día hábil siguiente.

[3] B. COLOMBIA

LEY 527 18 DE AGOSTO 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, Y SE ESTABLECEN LAS ENTIDADES DE CERTIFICACIÓN Y SE DICTAN OTRAS DISPOSICIONES.

El Congreso de Colombia DECRETA:

PARTE I - PARTE 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, salvo en los siguientes casos:

a) En las obligaciones contraídas por el Estado colombiano en virtud de convenios o tratados internacionales.

b) En las 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.

Artículo 2. Definiciones

Para los efectos de la presente ley se entenderá por:

a) Mensaje de datos. La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax.

b) Comercio electrónico. Abarca las cuestiones suscitadas por toda relación de índole comercial, sea o no contractual, estructurada a partir de la utilización de uno o más mensajes de datos o de cualquier otro medio similar. Las relaciones de índole comercial comprenden, sin limitarse a ellas, las siguientes operaciones: toda operación comercial de suministro o intercambio de bienes o servicios; todo acuerdo de distribución; toda operación de representación o mandato comercial; todo tipo de operaciones financieras, bursátiles y de seguros; de construcción de obras; de consultoría; de ingeniería; de concesión de licencias; 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.

c) Firma digital. Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación.

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

e) Intercambio Electrónico de Datos (EDI). La transmisión electrónica de datos de una computadora a otra, que está estructurada bajo normas técnicas convenidas al efecto;

---

[3] Flag courtesy of www.theodora.com/flags used with permission

f) 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

En la interpretación de la presente ley habrán de tenerse en cuenta su origen internacional, la necesidad de promover la uniformidad de su aplicación y la observancia de la buena fe. 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

Salvo que se disponga otra cosa, en las relaciones entre partes que generan, envían, reciben, archivan o procesan de alguna otra forma mensajes de datos, las disposiciones del Capítulo III, Parte I, podrán ser modificadas mediante acuerdo.

Artículo 5. Reconocimiento jurídico de los mensajes de datos

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

CAPÍTULO II - Aplicación de los requisitos jurídicos de los mensajes de datos

Artículo 6. Escrito

Cuando cualquier norma 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 posterior consulta.

Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas prevén consecuencias en el caso de que la información no conste por escrito.

Artículo 7. Firma

Cuando cualquier norma exija la presencia de una firma o establezca ciertas consecuencias en ausencia de la misma, en relación con un mensaje de datos, se entenderá satisfecho dicho requerimiento si:

a) se ha utilizado un método que permita identificar al iniciador de un mensaje de datos y para indicar que el contenido cuenta con su aprobación;

b) que el método sea tanto confiable como apropiado para el propósito por el cual el mensaje fue generado o comunicado.

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.

Artículo 8. Original

Cuando cualquier norma requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos, si:

a) existe alguna garantía confiable 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 que se deba presentar.

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 la información no sea presentada o conservada en su forma original.

Artículo 9. Integridad de un mensaje de datos

Para efectos del artículo anterior, se considerará que la información consignada en un mensaje de datos es íntegra, si ésta ha permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación. 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 del caso.

Artículo 10. Admisibilidad y fuerza probatoria de los mensajes de datos

Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del Capítulo VIII del Título XIII, Sección Tercera, Libro Segundo del Código de Procedimiento Civil.

En toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el sólo hecho que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original.

Artículo 11. Criterio para valorar probatoriamente un mensaje 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 y demás criterios reconocidos legalmente para la apreciación de las pruebas.

Por consiguiente habrán de tenerse en cuenta: la confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje, la confiabilidad en la forma en que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente.

Artículo 12. Conservación de los mensajes de datos y documentos

Cuando la ley requiera que ciertos documentos, registros o informaciones sean conservados, ese requisito quedará satisfecho, siempre que se cumplan las siguientes condiciones:

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

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

3. Que se conserve, de haber alguna, toda 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, la información que tenga por única finalidad facilitar el envío o recepción de los mensajes de datos. Los libros y papeles del comerciante podrán ser conservados en cualquier medio técnico que garantice su reproducción exacta.

Artículo 13. Conservación de mensajes de datos y archivo de documentos a través de terceros

El cumplimiento de la obligación de conservar documentos, registros o informaciones en mensajes de datos, se podrá realizar directamente o a través de terceros, siempre y cuando se cumplan las condiciones enunciadas en el artículo anterior.

CAPÍTULO III - Comunicación de los mensajes de datos

Artículo 14. Formación y validez de los contratos

En la formación del contrato, salvo acuerdo expreso entre las partes, la oferta y su aceptación podrán ser expresadas por medio de un mensaje de da tos. 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.

Artículo 15. Reconocimiento de los mensajes de datos por las partes

En las relaciones entre el iniciador y el destinatario de un mensaje de datos, no se negarán efectos jurídicos, validez o fuerza obligatoria a una manifestación de voluntad u otra declaración por la sola razón de haberse hecho en forma de mensaje de datos.

Artículo 16. Atribución de un mensaje de datos

Se entenderá que un mensaje de datos proviene del iniciador, cuando éste ha sido enviado por:

1. El propio iniciador.

2. Por alguna persona facultada para actuar en nombre del iniciador respecto de ese mensaje, o

3. Por un sistema de información programado por el iniciador o en su nombre para que opere automáticamente.

Artículo 17. Presunción del origen de un mensaje de datos

Se presume que un mensaje de datos ha sido enviado por el iniciador, cuando:

1. haya aplicado en forma adecuada el procedimiento acordado previamente con el iniciador, para establecer que el mensaje de datos provenía efectivamente de éste, o

2. 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.

Artículo 18. Concordancia del mensaje de datos enviado con el mensaje de datos recibido

Siempre que un mensaje de datos provenga del iniciador o que se entienda que proviene de él, o siempre que el destinatario tenga derecho a actuar con arreglo a este supuesto, en las relaciones entre el iniciador y el destinatario, este último tendrá derecho a considerar que el mensaje de datos recibido corresponde al que quería enviar el iniciador, y podrá proceder en consecuencia.

El destinatario no gozará de este derecho si sabía o hubiera sabido, de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que la transmisión había dado lugar a un error en el mensaje de datos recibido.

Artículo 19. Mensajes de datos duplicados

Se presume que cada mensaje de datos recibido es un mensaje de datos diferente, 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.

Artículo 20. Acuse de recibo

Si al enviar o antes de enviar un mensaje de datos, el iniciador solicita o acuerda con el destinatario que se acuse recibo del mensaje de datos, pero no se ha acordado entre éstos una forma o método determinado para efectuarlo, se podrá acusar recibo mediante:

a) Toda comunicación del destinatario, automatizada o no, o

b) Todo acto del destinatario que baste para indicar al iniciador que se ha recibido el mensaje de datos.

Si el iniciador ha solicitado o acordado con el destinatario que se acuse recibo del mensaje de datos, y expresamente aquél ha 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 recepcionado el acuse de recibo.

Artículo 21. Presunción de recepción de un mensaje de datos

Cuando el iniciador recepcione acuse recibo del destinatario, se presumirá que éste ha recibido el mensaje de datos.

Esa presunción no implicará que el mensaje de datos corresponda al mensaje recibido. Cuando en el acuse de recibo se indique que el mensaje de datos recepcionado cumple con los requisitos técnicos convenidos o enunciados en alguna norma técnica aplicable, se presumirá que ello es así.

Artículo 22. Efectos jurídicos

Los artículos 20 y 21 únicamente rigen los efectos relacionados con el acuse de recibo. Las consecuencias jurídicas del mensaje de datos se regirán conforme a las normas aplicables al acto o negocio jurídico contenido en dicho mensaje de datos.

Artículo 23. Tiempo del envío de un mensaje de datos

De no convenir otra cosa el iniciador y el destinatario, el mensaje de datos se tendrá por expedido cuando ingrese en un sistema de información que no esté bajo control del iniciador o de la persona que envió el mensaje de datos en nombre de éste.

Artículo 24. Tiempo de la recepción de un mensaje de datos

De no convenir otra cosa el iniciador y el destinatario, el momento de la recepción de un mensaje de datos se determinará como sigue:

a) si el destinatario ha designado un sistema de información para la recepción de 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

2. 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 cuando el mensaje de datos ingrese a un sistema de información del destinatario.

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 al artículo siguiente.

Artículo 25. Lugar del envío y recepción del mensaje de datos

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 artículo:

a) 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;

b) si el iniciador o el destinatario no tienen establecimiento, se tendrá en cuenta su lugar de residencia habitual.

PARTE II - COMERCIO ELECTRÓNICO EN MATERIA DE TRANSPORTE DE MERCANCÍAS

Artículo 26. Actos relacionados con los contratos de transporte de mercancías

Sin perjuicio de lo dispuesto en la parte I de la presente ley, este 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 taxativa:

a)
I. Indicación de las marcas, el número, la cantidad o el peso de las mercancías.

II. Declaración de la naturaleza o valor de las mercancías.

III. Emisión de un recibo por las mercancías.

IV. Confirmación de haberse completado el embarque de las mercancías;

b)
I. Notificación a alguna persona de las cláusulas y condiciones del contrato.

II. Comunicación de instrucciones al transportador;

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 27. Documentos de transporte

Con sujeción a lo dispuesto en el inciso 3° del presente artículo, en los casos en que la ley requiera que alguno de los actos enunciados en el artículo 26 se lleve a cabo por escrito o mediante documento emitido en papel, ese requisito quedará satisfecho cuando el acto se lleve a cabo por medio de uno o más mensajes de datos.

El inciso anterior será aplicable, tanto si el requisito en él previsto está expresado en forma de obligación o si la ley simplemente prevé consecuencias en el caso de que no se lleve a cabo el acto por escrito o mediante un documento emitido en papel.

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 utilización de un documento emitido en papel, ese requisito quedará satisfecho si el derecho o la obligación se transfiere mediante la utilización de uno o más mensajes de datos, siempre que se emplee un método confiable para garantizar la singularidad de ese mensaje o esos mensajes de datos.

Para los fines del inciso tercero, el nivel de confiabilidad 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.

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 26, no será válido ningún documento emitido en papel 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 emitidos en papel. Todo documento con soporte en papel que se emita en esas circunstancias deberá contener una declaración en tal sentido. La sustitución de mensajes de datos por documentos emitidos en papel no afectará los derechos ni las obligaciones de las partes.

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 emitido en papel, esa norma no dejará de aplicarse, a dicho 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 documentos emitidos en papel.

PARTE III - FIRMAS DIGITALES, CERTIFICADOS Y ENTIDADES DE CERTIFICACIÓN

CAPÍTULO I - Firmas digitales

Artículo 28. Atributos jurídicos de una firma digital

Cuando una firma digital haya sido fijada en un mensaje de datos se presume que el suscriptor de aquella tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo.

Parágrafo. El uso de una firma digital tendrá la misma fuerza y efectos que el uso de una firma manuscrita, si aquélla incorpora los siguientes atributos:

1. Es única a la persona que la usa.

2. Es susceptible de ser verificada.

3. Está bajo el control exclusivo de la persona que la usa.

4. Está ligada a la información o mensaje, de tal manera que si éstos son cambiados, la firma digital es invalidada.

5. Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional.

CAPÍTULO II - Entidades de certificación

Artículo 29. Características y requerimientos de las entidades de certificación

Podrán ser entidad es de certificación, las personas jurídicas, tanto públicas como privadas, de origen nacional o extranjero y las cámaras de comercio, que previa solicitud sean autorizadas por la Superintendencia de Industria y Comercio y que cumplan con los requerimientos establecidos por el Gobierno Nacional, con base en las siguientes condiciones:

a) Contar con la capacidad económica y financiera suficiente para prestar los servicios autorizados como entidad de certificación.

b) Contar con la capacidad y elementos técnicos necesarios para la generación de firmas digitales, la emisión de certificados sobre la autenticidad de las mismas y la conservación de mensajes de datos en los términos establecidos en esta ley.

c) Los representantes legales y administradores no podrán ser personas que hayan sido condenadas a pena privativa de la libertad, excepto por delitos políticos o culposos; o que hayan sido suspendidas en el ejercicio de su profesión por falta grave contra la ética o hayan sido excluidas de aquélla. Esta inhabilidad estará vigente por el mismo período que la ley penal o administrativa señale para el efecto.

Artículo 30. Actividades de las entidades de certificación

Las entidades de certificación autorizadas por la Superintendencia de Industria y Comercio para prestar sus servicios en el país, podrán realizar, entre otras, las siguientes actividades:

1. Emitir certificados en relación con las firmas digitales de personas naturales o jurídicas.

2. Emitir certificados sobre la verificación respecto de la alteración entre el envío y recepción d el mensaje de datos.

3. Emitir certificados en relación con la persona que posea un derecho u obligación con respecto a los documentos enunciados en los literales f) y g) del artículo 26 de la presente ley.

4. Ofrecer o facilitar los servicios de creación de firmas digitales certificadas.

5. Ofrecer o facilitar los servicios de registro y estampado cronológico en la generación, transmisión y recepción de mensajes de datos.

6. Ofrecer los servicios de archivo y conservación de mensajes de datos.

Artículo 31. Remuneración por la prestación de servicios

La remuneración por los servicios de las entidades de certificación serán establecidos libremente por éstas.

Artículo 32. Deberes de las entidades de certificación.

Las entidades de certificación tendrán, entre otros, los siguientes deberes:

a) Emitir certificados conforme a lo solicitado o acordado con el suscriptor;

b) Implementar los sistemas de seguridad para garantizar la emisión y creación de firmas digitales, la conservación y archivo de certificados y documentos en soporte de mensaje de datos;

c) Garantizar la protección, confidencialidad y debido uso de la información suministrada por el suscriptor;

d) Garantizar la prestación permanente del servicio de entidad de certificación;

e) Atender oportunamente las solicitudes y reclamaciones hechas por los suscriptores;

f) Efectuar los avisos y publicaciones conforme a lo dispuesto en la ley;

g) Suministrar la información que le requieran las entidades administrativas competentes o judiciales en relación con las firmas digitales y certificados emitidos y en general sobre cualquier mensaje de datos que se encuentre bajo su custodia y administración;

h) Permitir y facilitar la realización de las auditorias por parte de la Superintendencia de Industria y Comercio;

i) Elaborar los reglamentos que definen las relaciones con el suscriptor y la forma de prestación d el servicio;

j) Llevar un registro de los certificados.

Artículo 33. Terminación unilateral

Salvo acuerdo entre las partes, la entidad de certificación podrá dar por terminado el acuerdo de vinculación con el suscriptor dando un preaviso no menor de noventa (90) días. Vencido este término, la entidad de certificación revocará los certificados que se encuentren pendientes de expiración.

Igualmente, el suscriptor podrá dar por terminado el acuerdo de vinculación con la entidad de certificación dando un preaviso no inferior a treinta (30) días.

Artículo 34. Cesación de actividades por parte de las entidades de certificación

Las entidades de certificación autorizadas pueden cesar en el ejercicio de actividades, siempre y cuando hayan recibido autorización por parte de la Superintendencia de Industria y Comercio.

CAPÍTULO III - Certificados

Artículo 35. Contenido de los certificados

Un certificado emitido por una entidad de certificación autorizada, además de estar firmado digitalmente por ésta, debe contener por lo menos lo siguiente:

1. Nombre, dirección y domicilio del suscriptor.

2. Identificación del suscriptor nombrado en el certificado.

3. El nombre, la dirección y el lugar donde realiza actividades la entidad de certificación.

4. La clave pública del usuario.

5. La metodología para verificar la firma digital del suscriptor impuesta en el mensaje de datos.

6. El número de serie del certificado.

7. Fecha de emisión y expiración del certificado.

Artículo 36. Aceptación de un certificado

Salvo acuerdo entre las partes, se entiende que un suscriptor ha aceptado un certificado cuando la entidad de certificación, a solicitud de éste o de una persona en nombre de éste, lo ha guardado en un repositorio.

Artículo 37. Revocación de certificados

El suscriptor de una firma digital certificada, podrá solicitar a la entidad de certificación que expidió un certificado, la revocación del mismo. En todo caso, estará obligado a solicitar la revocación en los siguientes eventos:

1. Por pérdida de la clave privada.

2. La clave privada ha sido expuesta o corre peligro de que se le dé un uso indebido.

Si el suscriptor no solicita la revocación del certificado en el evento de presentarse las anteriores situaciones, será responsable por las pérdidas o perjuicios en los cuales incurran terceros de buena fe exenta de culpa que confiaron en el contenido del certificado.

Una entidad de certificación revocará un certificado emitido por las siguientes razones:

1. A petición del suscriptor o un tercero en su nombre y representación.

2. Por muerte del suscriptor.

3. Por liquidación del suscriptor en el caso de las personas jurídicas.

4. Por la confirmación de que alguna información o hecho contenido en el certificado es falso.

5. La clave privada de la entidad de certificación o su sistema de seguridad ha sido comprometido de manera material que afecte la confiabilidad del certificado.

6. Por el cese de actividades de la entidad de certificación, y

7. Por orden judicial o de entidad administrativa competente.

Artículo 38. Término de conservación de los registros

Los registros de certificados expedidos por una entidad de certificación deben ser conservados por el término exigido en la ley que regule el acto o negocio jurídico en particular.

CAPÍTULO IV - Suscriptores de firmas digitales

Artículo 39. Deberes de los suscriptores

Son deberes de los suscriptores:

1. Recibir la firma digital por parte de la entidad de certificación o generarla, utilizando un método autorizado por ésta.

2. Suministrar la información que requiera la entidad de certificación.

3. Mantener el control de la firma digital.

4. Solicitar oportunamente la revocación de los certificados.

Artículo 40. Responsabilidad de los suscriptores

Los suscriptores serán responsables por la falsedad, error u omisión en la información suministrada a la entidad de certificación y por el incumplimiento de sus deberes como suscriptor.

CAPÍTULO V - Superintendencia de Industria y Comercio

Artículo 41. Funciones de la Superintendencia

La Superintendencia de Industria y Comercio ejercerá las facultades que legalmente le han sido asignadas respecto de las entidades de certificación, y adicionalmente tendrá las siguientes funciones:

1. Autorizar la actividad de las entidades de certificación en el territorio nacional.

2. Velar por el funcionamiento y la eficiente prestación del servicio por parte de las entidades de certificación.

3. Realizar visitas de auditoría a las entidades de certificación.

4. Revocar o suspender la autorización para operar como entidad de certificación.

5. Solicitar la información pertinente para el ejercicio de sus funciones.

6. Imponer sanciones a las entidades de certificación en caso de incumplimiento de las obligaciones derivadas de la prestación del servicio.

7. Ordenar la revocación de certificados cuando la entidad de certificación los emita sin el cumplimiento de las formalidades legales.

8. Designar los repositorios y entidades de certificación en los eventos previstos en la ley.

9. Emitir certificados en relación con las firmas digitales de las entidades de certificación.

10. Velar por la observancia de las disposiciones constitucionales y legales sobre la promoción de la competencia y prácticas comerciales restrictivas, competencia desleal y protección del consumidor, en los mercados atendidos por las entidades de certificación.

11. Impartir instrucciones sobre el adecuado cumplimiento de las normas a las cuales deben sujetarse las entidades de certificación.

Artículo 42. Sanciones

La Superintendencia de Industria y Comercio de acuerdo con el debido proceso y el derecho de defensa, podrá imponer según la naturaleza y la gravedad de la falta, las siguientes sanciones a las entidades de certificación:

1. Amonestación.

2. Multas institucionales hasta por el equivalente a dos mil (2.000) salarios mínimos legales mensuales vigentes, y personales a los administradores y representantes legales de las entidades de certificación, hasta por trescientos (300) salarios mínimos legales mensuales vigentes, cuando se les compruebe que han autorizado, ejecutado o tolerado conductas violatorias de la ley.

3. Suspender de inmediato todas o algunas de las actividades de la entidad infractora.

4. Prohibir a la entidad de certificación infractora prestar directa o indirectamente los servicios de entidad de certificación hasta por el término de cinco (5) años.

5. Revocar definitivamente la autorización para operar como entidad de certificación.

CAPÍTULO VI - Disposiciones varias

Artículo 43. Certificaciones recíprocas

Los certificados de firmas digitales emitidos por entidades de certificación extranjeras, podrán ser reconocidos en los mismos términos y condiciones exigidos en la ley para la emisión de certificados por parte de las entidades de certificación nacionales, siempre y cuando tales certificados sean reconocidos por una entidad de certificación autorizada que garantice en la misma forma que lo hace con sus propios certificados, la regularidad de los detalles del certificado, así como su validez y vigencia.

Artículo 44. 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 ese 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.

PARTE IV - REGLAMENTACIÓN Y VIGENCIA

Artículo 45

La Superintendencia de Industria y Comercio contará con un término adicional de doce (12) meses, contados a partir de la publicación de la presente ley, para organizar y asignar a una de sus dependencias la función de inspección, control y vigilancia de las actividades realizadas por las entidades de certificación, sin perjuicio de que el Gobierno Nacional cree una unidad especializada dentro de ella para tal efecto.

Artículo 46. Prevalencia de las leyes de protección al consumidor

La presente ley se aplicará sin perjuicio de las normas vigentes en materia de protección al consumidor.

Artículo 47. Vigencia y derogatoria

La presente ley rige desde la fecha de su publicación y deroga las disposiciones que le sean contrarias.

El Presidente del honorable Senado de la República, Fabio Valencia Cossio.

El Secretario General del honorable Senado de la República, Manuel Enríquez Rosero.

El Presidente de la honorable Cámara de Representantes, Emilio Martínez Rosales.

El Secretario General de la honorable Cámara de Representantes, Gustavo Bustamante Moratto.

REPUBLICA DE COLOMBIA GOBIERNO NACIONAL

Publíquese y ejecútese.

Dada en Santa Fe de Bogotá, D. C., a 18 de agosto de 1999.

ANDRÉS PASTRANA ARANGO

El Ministro de Desarrollo Económico, Fernando Araujo Perdomo.

La Ministra de Comercio Exterior, Martha Lucía Ramírez de Rincón.

La Ministra de Comunicaciones, Claudia De Francisco Zambrano.

El Ministro de Transporte, Mauricio Cárdenas Santamaría.

DECRETO NO. 1747 11 DE SEPTIEMBRE DE 2000 POR EL CUAL SE REGLAMENTA PARCIALMENTE LA LEY 527 DE 1999, EN LO RELACIONADO CON LAS ENTIDADES DE CERTIFICACIÓN, LOS CERTIFICADOS Y LAS FIRMAS DIGITALES.

El Presidente de la República de Colombia, en ejercicio de las facultades constitucionales y legales, en especial de las conferidas en el numeral 11 del artículo 189 de la Constitución Política y en desarrollo de lo previsto en la Ley 527 de 1999, DECRETA:

CAPÍTULO I - Aspectos generales

Artículo 1. Definiciones. Para efectos del presente decreto se entenderá por:

1. Iniciador: persona que actuando por su cuenta, o en cuyo nombre se haya actuado, envíe o genere un mensaje de datos.
2. Suscriptor: persona a cuyo nombre se expide un certificado.
3. Repositorio: sistema de información utilizado para almacenar y recuperar certificados y otra información relacionada con los mismos.
4. Clave privada: valor o valores numéricos que, utilizados conjuntamente con un procedimiento matemático conocido, sirven para generar la firma digital de un mensaje de datos.
5. Clave pública: valor o valores numéricos que son utilizados para verificar que una firma digital fue generada con la clave privada del iniciador.
6. Certificado en relación con las firmas digitales: mensaje de datos firmado por la entidad de certificación que identifica, tanto a la entidad de certificación que lo expide, como al suscriptor y contiene la clave pública de éste.
7. Estampado cronológico: mensaje de datos firmado por una entidad de certificación que sirve para verificar que otro mensaje de datos no ha cambiado en un período que comienza en la fecha y hora en que se presta el servicio y termina en la fecha en que la firma del mensaje de datos generado por el prestador del servicio de estampado, pierde validez.
8. Entidad de certificación cerrada: entidad que ofrece servicios propios de las entidades de certificación sólo para el intercambio de mensajes entre la entidad y el suscriptor, sin exigir remuneración por ello.
9. Entidad de certificación abierta: la que ofrece servicios propios de las entidades de certificación, tales que:
   a) Su uso no se limita al intercambio de mensajes entre la entidad y el suscriptor, o
   b) Recibe remuneración por éstos.
10. Declaración de Prácticas de Certificación (DPC): manifestación de la entidad de certificación sobre las políticas y procedimientos que aplica para la prestación de sus servicios.

Artículo 2. Sistema confiable. Los sistemas utilizados para el ejercicio de las actividades de certificación se considerarán confiables si satisfacen los estándares establecidos por la Superintendencia de Industria y Comercio.

CAPÍTULO II- De las entidades de certificación y certificados digitales

Sección I - De las entidades de certificación cerradas

Artículo 3. Acreditación de requisitos de las entidades de certificación cerradas. Quienes pretendan realizar las actividades propias de las entidades de certificación cerradas deberán acreditar ante la Superintendencia de Industria y Comercio que:

1. los administradores y representantes legales no están incursos en las causales de inhabilidad previstas en el literal c) del artículo 29 de la Ley 527 de 1999, y

2. están en capacidad de cumplir los estándares mínimos que fije la Superintendencia de Industria y Comercio de acuerdo a los servicios ofrecidos.

Artículo 4. Información en certificados. Los certificados emitidos por las entidades de certificación cerradas deberán indicar expresamente que sólo podrán ser usados entre la entidad emisora y el suscriptor. Las entidades deberán informar al suscriptor de manera clara y expresa, previa expedición de los certificados, que éstos no cumplen los requisitos del artículo 15 del presente decreto.

Sección II - De las entidades de certificación abiertas

Artículo 5. Acreditación de requisitos de las entidades de certificación abiertas. Quienes pretendan realizar las actividades propias de las entidades de certificación abiertas deberán particularizarlas y acreditar ante la Superintendencia de Industria y Comercio:

1. Personería jurídica o condición de notario o cónsul. Cuando se trate de una entidad extranjera, se deberá acreditar el cumplimiento de los requisitos contemplados en el libro segundo, título VIII del Código de Comercio para las sociedades extranjeras que pretendan ejecutar negocios permanentes en territorio colombiano. Igualmente deberá observarse lo establecido en el artículo 48 del Código de Procedimiento Civil.

2. Que los administradores y representantes legales no están incursos en las causales de inhabilidad previstas en el literal c) del artículo 29 de la Ley 527 de 1999.

3. Declaración de Prácticas de Certificación (DPC) satisfactoria, de acuerdo con los requisitos establecidos por la Superintendencia de Industria y Comercio.

4. Patrimonio mínimo de 400 salarios mínimos mensuales legales vigentes al momento de la autorización.

5. Constitución de las garantías previstas en este decreto.

6. Infraestructura y recursos por lo menos en la forma exigida en el artículo 9° de este decreto.

7. Informe inicial de auditoría satisfactorio a juicio de la misma Superintendencia.

8. Un mecanismo de ejecución inmediata para revocar los certificados digitales expedidos a los suscriptores, a petición de estos o cuando se tenga indicios de que ha ocurrido alguno de los eventos previstos en el artículo 37 de la Ley 527 de 1999.

Parágrafo 1°. La Superintendencia de Industria y Comercio tendrá la facultad de solicitar ampliación o aclaración sobre los puntos que estime conveniente.

Parágrafo 2°. Si se solicita autorización para certificaciones recíprocas, se deberán acreditar adicionalmente la entidad reconocida, los certificados reconocidos y el tipo de certificados al cual se remite, la vigencia y los términos del reconocimiento.

Artículo 6. Declaración de Prácticas de Certificación (DPC). La Superintendencia de Industria y Comercio definirá el contenido de la Declaración de Prácticas de Certificación, DPC, la cual deberá incluir, al menos lo siguiente:

1. Identificación de la entidad de certificación.
2. Política de manejo de los certificados.
3. Obligaciones de la entidad y de los suscriptores del certificado y precauciones que deben observar los terceros.
4. Manejo de la información suministrada por los suscriptores.
5. Garantías que ofrece para el cumplimiento de las obligaciones que se deriven de sus actividades.
6. Límites de responsabilidad por el ejercicio de su actividad.
7. Tarifas de expedición y revocación de certificados.

8. Procedimientos de seguridad para el manejo de los siguientes eventos:
   a) Cuando la seguridad de la clave privada de la entidad de certificación se ha visto comprometida;
   b) Cuando el sistema de seguridad de la entidad de certificación ha sido vulnerado;
   c) Cuando se presenten fallas en el sistema de la entidad de certificación que comprometan la prestación del servicio;
   d) Cuando los sistemas de cifrado pierdan vigencia por no ofrecer el nivel de seguridad contratados por el suscriptor.
9. El plan de contingencia encaminado a garantizar la continuidad del servicio de certificación.
10. Modelos y minutas de los contratos que utilizarán con los usuarios.
11. Política de manejo de otros servicios que fuere a prestar, detallando sus condiciones.

Artículo 7. Patrimonio mínimo. Para determinar el patrimonio mínimo, sólo se tomarán en cuenta las cuentas patrimoniales de capital suscrito y pagado, reserva legal, superávit por prima en colocación de acciones y se deducirán las pérdidas acumuladas y las del ejercicio en curso.
El patrimonio mínimo deberá acreditarse:

1. En el caso de personas jurídicas, por medio de estados financieros, con una antigüedad no superior a 6 meses, certificados por el representante legal y el revisor fiscal si lo hubiere.
2. Tratándose de entidades públicas, por medio del proyecto de gastos y de inversión que generará la actividad de certificación, conjuntamente con los certificados de disponibilidad presupuestal que acrediten la apropiación de recursos para dicho fin.
3. Para las sucursales de entidades extranjeras, por medio del capital asignado.
4. En el caso de los notarios y cónsules, por medio de los recursos dedicados exclusivamente a la actividad de entidad de certificación.

Artículo 8. Garantías. La entidad debe contar con al menos una de las siguientes garantías:

1. Seguros vigentes que cumplan con los siguientes requisitos:

a) Ser expedidos por una entidad aseguradora autorizada para operar en Colombia. En caso de no ser posible lo anterior, por una entidad aseguradora del exterior que cuente con la autorización previa de la Superintendencia Bancaria.
b) Cubrir todos los perjuicios contractuales y extra-contractuales de los suscriptores y terceros de buena fe exenta de culpa derivados de errores y omisiones, o de actos de mala fe de los administradores, representantes legales o empleados de la certificadora en el desarrollo de las actividades para las cuales solicita autorización o cuenta con autorización.
c) Cubrir los anteriores riesgos por una cuantía asegurada por evento igual o superior al mayor entre:
   i. 7.500 salarios mínimos mensuales legales por evento; o
   ii. el límite de responsabilidad definido en las prácticas de certificación;
d) Incluir cláusula de restitución automática del valor asegurado.
e) Incluir una cláusula que obligue a la entidad aseguradora a informar previamente a la Superintendencia de Industria y Comercio la terminación del contrato o las modificaciones que reduzcan el alcance o monto de la cobertura.

2. Contrato de fiducia con patrimonio autónomo que cumpla con las siguientes características:

a) Tener como objeto exclusivo el cubrimiento de las pérdidas sufridas por los suscriptores y terceros de buena fe exentos de culpa, que se deriven de los errores y omisiones o de actos de mala fe de los administradores, representantes legales o empleados de la certificadora en el desarrollo de las actividades para las cuales solicita o cuenta con autorización.
b) Contar con recursos suficientes para cubrir pérdidas por una cuantía por evento igual o superior al mayor entre:
   i. 7.500 salarios mínimos mensuales legales por evento; o
   ii. el límite de responsabilidad definido en las prácticas de certificación.
c) Que los fideicomitentes se obliguen a restituir los recursos de la fiducia en caso de una reclamación, por lo menos hasta el monto mínimo exigido en el punto anterior.

d) Que la fiduciaria se obligue a obtener permiso de la Superintendencia de Industria y Comercio, previamente a cualquier cambio en los reglamentos, disminución en el monto o alcance de la cobertura, así como para el retiro de fideicomitentes y para la terminación del contrato.
e) Que las inversiones estén representadas en títulos de renta fija, alta seguridad y liquidez emitidos o garantizados por la Nación, el Banco de la República o calificados como de mínimo riesgo por las sociedades calificadoras de riesgo.

La entidad que pretenda otorgar el reconocimiento recíproco, deberá acreditar la cobertura de las garantías requeridas en este decreto para los perjuicios que puedan causar los certificados reconocidos.

Artículo 9. Infraestructura y recursos. En desarrollo de lo previsto en el literal b) del artículo 29 de la Ley 527 de 1999, la entidad deberá contar con un equipo de personas, una infraestructura física y tecnológica y unos procedimientos y sistemas de seguridad, tales que:

1. Puedan generar las firmas digitales propias y todos los servicios para los que soliciten autorización.
2. Se garantice el cumplimiento de lo previsto en la Declaración de Prácticas de Certificación (DPC).
3. Se pueda calificar el sistema como confiable de acuerdo con lo señalado en el artículo 2° del presente decreto.
4. Los certificados expedidos por las entidades de certificación cumplan con:
   a) Lo previsto en el artículo 35 de la ley 527 de 1999; y
   b) Alguno de los estándares de certificados que admita de manera general la Superintendencia de Industria y Comercio.
5. Se garantice la existencia de sistemas de seguridad física en sus instalaciones, un monitoreo permanente de toda su planta física, y acceso restringido a los equipos que manejan los sistemas de operación de la entidad.
6. El manejo de la clave privada de la entidad esté sometido a un procedimiento propio de seguridad que evite el acceso físico o de otra índole a la misma, a personal no autorizado.
7. Cuente con un registro de todas las transacciones realizadas, que permita identificar el autor de cada una de las operaciones.
8. Los sistemas que cumplan las funciones de certificación sólo sean utilizados con ese propósito y por lo tanto no puedan realizar ninguna otra función.
9. Todos los sistemas que participen directa o indirectamente en la función de certificación estén protegidos por sistemas y procedimientos de autenticación y seguridad de alto nivel de protección, que deben ser actualizados de acuerdo a los avances tecnológicos para garantizar la correcta prestación del servicio.

Artículo 10. Infraestructura prestada por un tercero. Cuando quiera que la entidad de certificación requiera o utilice infraestructura o servicios tecnológicos prestados por un tercero, los contratos deberán prever que la terminación de los mismos está condicionada a que la entidad haya implementado o contratado una infraestructura o servicio tecnológico que le permita continuar prestando sus servicios sin ningún perjuicio para los suscriptores. Si la terminación de dichos contratos supone el cese de operaciones, el prestador de infraestructura o servicios no podrá interrumpir sus servicios antes de vencerse el plazo para concluir el proceso previsto en el procedimiento autorizado por la Superintendencia de Industria y Comercio. Éstos deben ser enviados con los demás documentos de la solicitud de autorización y remitidos cada vez que sean modificados.

La contratación de esta infraestructura o servicios no exime a la entidad certificadora de la presentación de los informes de auditoría previstos en este decreto, los cuales deben incluir los sistemas y seguridades de dicho prestador.

Artículo 11. Informe de Auditoría. El informe de Auditoría dictaminará que la entidad de certificación actúa o está en capacidad de actuar, de acuerdo con los requerimientos de la Ley 527 de 1999, lo previsto en este decreto y en las normas que los sustituyan, complementen o reglamenten. Asimismo, evaluará todos los servicios a que hace referencia el literal d) del artículo 2° de la Ley 527 de 1999 y que sean prestados o pretenda prestar la entidad de certificación.

Artículo 12. Requisitos de las firmas auditoras. La auditoría deberá ser realizada por una entidad del sistema nacional de normalización, certificación y metrología acreditada para el efecto por la Superintendencia de Industria y Comercio.

En caso de tratarse de entidades de certificación que requieran o utilicen infraestructura o servicios tecnológicos prestados desde el extranjero, la auditoría podrá ser realizada por una persona o entidad facultada para realizar este tipo de auditorías en el lugar donde se encuentra la infraestructura, siempre y cuando permita constatar el cumplimiento de lo señalado en el artículo anterior.

En caso de que no existan en el país al menos dos entidades acreditadas para llevar a cabo estas auditorías, las entidades de certificación nacionales podrán hacer uso de firmas de auditorías extranjeras, siempre y cuando el informe cumpla con las instrucciones impartidas por la Superintendencia de Industria y Comercio y la firma auditora se encuentre facultada para realizar este tipo de auditorías en su país de origen.

Artículo 13. Deberes. Además de lo previsto en el artículo 32 de la Ley 527 de 1999, las entidades de certificación deberán:

1. Comprobar por sí o por medio de una persona diferente que actúe en nombre y por cuenta suya, la identidad y cualesquiera otras circunstancias de los solicitantes o de datos de los certificados, relevantes para los fines propios de su procedimiento de verificación previo a su expedición.
2. Mantener a disposición permanente del público la declaración de prácticas de certificación.
3. Cumplir cabalmente con las políticas de certificación acordadas con el suscriptor y con su Declaración de Prácticas de Certificación (DPC).
4. Informar al suscriptor de los certificados que expide, su nivel de confiabilidad, los límites de responsabilidad, y las obligaciones que el suscriptor asume como usuario del servicio de certificación.
5. Garantizar la prestación permanente e ininterrumpida de los servicios autorizados, salvo las interrupciones que autorice la Superintendencia de Industria y Comercio.
6. Informar a la superintendencia de manera inmediata la ocurrencia de cualquier evento establecido en la Declaración de Prácticas de Certificación, que comprometa la prestación del servicio.
7. Abstenerse de acceder o almacenar la clave privada del suscriptor.
8. Mantener actualizado el registro de los certificados revocados. Las entidades de certificación serán responsables de los perjuicios que se causen a terceros por incumplimiento de esta obligación.
9. Garantizar el acceso permanente y eficiente de los suscriptores y de terceros al repositorio de la entidad.
10. Disponer de una línea telefónica de atención permanente a suscriptores y terceros, que permita las consultas y la pronta solicitud de revocación de certificados por los suscriptores.
11. Garantizar la confidencialidad de la información que no figure en el certificado.
12. Conservar la documentación que respalda los certificados emitidos, por el término previsto en la ley para los papeles de los comerciantes y tomar las medidas necesarias para garantizar la integridad y la confidencialidad que le sean propias.
13. Informar al suscriptor dentro de las 24 horas siguientes, la suspensión del servicio o revocación de sus certificados.
14. Capacitar y advertir a los suscriptores de firmas y certificados digitales, sobre las medidas de seguridad que deben observar para la utilización de estos mecanismos.
15. Mantener el control exclusivo de su clave privada y establecer las seguridades necesarias para que no se divulgue o comprometa.
16. Remitir oportunamente a la Superintendencia de Industria y Comercio, la información prevista en este decreto.
17. Remover en el menor término que el procedimiento legal permita, a los administradores o representantes que resulten incursos en las causales establecidas en el literal c) del artículo 29 de la Ley 527 de 1999.
18. Informar a los suscriptores o terceros que lo soliciten, sobre el tiempo y recursos computacionales requeridos para derivar la clave privada a partir de la clave pública contenida en los certificados en relación con las firmas digitales que expide la entidad.
19. Mantener actualizada la información registrada en la solicitud de autorización y enviar la información que la Superintendencia de Industria y Comercio establezca.
20. Cumplir con las demás instrucciones que establezca la Superintendencia de Industria y Comercio.

Artículo 14. Certificaciones recíprocas. El reconocimiento de los certificados de firmas digitales emitidos por entidades de certificación extranjeras, realizado por entidades de certificación autorizadas para tal efecto en Colombia, se hará constar en un certificado expedido por estas últimas.

El efecto del reconocimiento de cada certificado, se limitará a las características propias del tipo de certificado reconocido y por el período de validez del mismo.

Los suscriptores de los certificados reconocidos y los terceros tendrán idénticos derechos que los suscriptores y terceros respecto de los certificados propios de la entidad que hace el reconocimiento.
Parágrafo. La Superintendencia de Industria y Comercio determinará el contenido mínimo de los certificados recíprocos.

Artículo 15. Uso del certificado digital. Cuando quiera que un suscriptor firme digitalmente un mensaje de datos con su clave privada, y la respalde mediante un certificado digital, se darán por satisfechos los atributos exigidos para una firma digital en el parágrafo del artículo 28 de la Ley 527 de 1999, si:

1. El certificado fue emitido por una entidad de certificación abierta autorizada para ello por la Superintendencia de Industria y Comercio.
2. Dicha firma se puede verificar con la clave pública que se encuentra en el certificado con relación a firmas digitales, emitido por la entidad de certificación.
3. La firma fue emitida dentro del tiempo de validez del certificado, sin que éste haya sido revocado.
4. El mensaje de datos firmado se encuentra dentro de los usos aceptados en la DPC, de acuerdo al tipo de certificado.

Artículo 16. Unicidad de la firma digital. No obstante lo previsto en el artículo anterior, una firma digital en un mensaje de datos deja de ser única a la persona que la usa si, estando bajo su control exclusivo, dada la condición del numeral 3 del parágrafo del artículo 28 de la Ley 527 de 1999, la probabilidad de derivar la clave privada, a partir de la clave pública, no es o deja de ser remota.

Para establecer si la probabilidad es remota se tendrán en cuenta la utilización del máximo recurso computacional disponible al momento de calcular la probabilidad, durante un período igual al que transcurre entre el momento en que se crean el par de claves y aquel en que el documento firmado deja de ser idóneo para generar obligaciones.

Sección III - De la decisión y las responsabilidades

Artículo 17. Decisión. En la resolución de autorización expedida por la Superintendencia de Industria y Comercio, se precisarán las actividades y servicios que puede prestar la entidad de certificación. En todo caso, la entidad de certificación podrá solicitar autorización para prestar actividades y servicios adicionales.

Artículo 18. Responsabilidad. Las entidades de certificación responderán por todos los perjuicios que causen en el ejercicio de sus actividades.
La entidad certificadora será responsable por los perjuicios que puedan causar los prestadores de servicios a que hace referencia del artículo 10 del presente decreto, a los suscriptores o a las personas que confíen en los certificados.

Artículo 19. Cesación de actividades. La cesación de actividades de una entidad de certificación sin la autorización de la Superintendencia de Industria y Comercio o la continuación de actividades después de producida ésta, la hará responsable de todos los perjuicios que cause a sus suscriptores y a terceros y la hará acreedora a las sanciones que imponga la Superintendencia.

Artículo 20. Responsabilidad derivada de la administración de los repositorios. Cuando las entidades de certificación contraten los servicios de repositorios, continuarán siendo responsables frente a sus suscriptores y terceros por el mismo.

Artículo 21. Información periódica y esporádica. La información prevista en los artículos 3°, 5°, 6°, 7°, 8°, 9°, 10 y 11 del presente decreto, deberá actualizarse ante la Superintendencia de Industria y Comercio cada vez que haya cambio o modificación de algunos de los datos suministrados. La Superintendencia señalará, además, la forma y periodicidad en que se debe demostrar el continuo cumplimiento de las condiciones de que se ocupan los artículos señalados.

Artículo 22. Responsabilidad derivada de la no-revocación. Una vez cumplidas las formalidades previstas para la revocación, la entidad será responsable por los perjuicios que cause la no-revocación.

Sección IV - De los certificados digitales

Artículo 23. Información relativa a la revocación. Cada certificado revocado debe indicar si el motivo de revocación incluye la pérdida de control de la clave privada, evento en el cual, las firmas generadas con dicha clave privada carecerán del atributo de unicidad previsto en el numeral 1 del parágrafo del artículo 28 de la Ley 527 de 1999, salvo que se demuestre lo contrario, mediante un mecanismo adicional que pruebe inequívocamente que el documento fue firmado digitalmente en una fecha previa a la revocación del certificado.

Las revocaciones deberán ser publicadas de manera inmediata en los repositorios correspondientes y notificadas al suscriptor dentro de las 24 horas siguientes. Si dichos repositorios no existen al momento de la publicación del aviso, ésta se efectuará en un repositorio que designe la Superintendencia de Industria y Comercio.

Artículo 24. Registro de certificados. Toda entidad de certificación autorizada deberá llevar un registro de público acceso que contenga todos los certificados emitidos y sus fechas de emisión, expiración o revocación.

Artículo 25. Información. Las entidades de certificación estarán obligadas a respetar las condiciones de confidencialidad y seguridad, de acuerdo con las normas vigentes respectivas.

Salvo la información contenida en el certificado, la suministrada por los suscriptores a las entidades de certificación se considerará privada y confidencial.

CAPÍTULO III - Facultades de la Superintendencia de Industria y Comercio

Artículo 26. Suspensión y revocación de autorización. Cuando quiera que la Superintendencia de Industria y Comercio ejerza la facultad contenida en el numeral 4 del artículo 41 de la Ley 527 de 1999, ordenará a la entidad de certificación la ejecución de medidas tendientes a garantizar la integridad, seguridad y conservación de los certificados expedidos, así como la compensación económica que pudiera generar la cesación de actividades.

Artículo 27. Estándares. La Superintendencia de Industria y Comercio determinará los estándares admisibles con respecto a los cuales las entidades - de certificación deberán acreditar el cumplimiento de los requisitos relativos a:

1. La generación de pares de claves.
2. La generación de firmas.
3. Los certificados.
4. Los sistemas de cifrado.
5. Las comunicaciones.
6. La seguridad de los sistemas de información y de las instalaciones, o
7. Cualquier otro aspecto que redunde en la confiabilidad y seguridad de los certificados, o de la información que repose en la entidad de certificación.

Para la determinación de los estándares admisibles, la superintendencia deberá adoptar aquellos que tengan carácter internacional y que estén vigentes tecnológicamente o los desarrollados por el organismo nacional de normalización o los que sean ampliamente reconocidos para los propósitos perseguidos. En todo caso, deberá tener en cuenta su aplicabilidad a la luz de la legislación vigente.
La Superintendencia podrá eliminar la admisibilidad de un estándar cuando haya dejado de cumplir alguno de los requisitos precisados en este artículo.

Artículo 28. Facultades. Las atribuciones otorgadas a la Superintendencia de Industria y Comercio en el presente decreto, se ejercerán conforme a las facultades establecidas en los artículos 41 de la Ley 527 de 1999 y en los Decretos 2269 de 1993 y 2153 de 1992.

Artículo 29. Vigencia. El presente decreto rige a partir de la fecha de su publicación y deroga las disposiciones que le sean contrarias.

Publíquese y cúmplase.

Dado en Bogotá, D. C., a 11 de septiembre de 2000.
ANDRES PASTRANA ARANGO

El Ministro de Desarrollo Económico,
Augusto Ramírez Ocampo.

La Ministra de Comercio Exterior,
Marta Lucía Ramírez de Rincón.

La Ministra de Comunicaciones,
María del Rosario Sintes Ulloa.

RESOLUCIÓN 26.930 DEL 26 DE OCTUBRE DE 2000 DE LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO DEL MINISTERIO DE DESARROLLO ECONÓMICO DE LA REPÚBLICA DE COLOMBIA "POR LA CUAL SE FIJAN LOS ESTÁNDARES PARA LA AUTORIZACIÓN Y FUNCIONAMIENTO DE LAS ENTIDADES DE CERTIFICACIÓN Y SUS AUDITORES"

El Superintendente de Industria y Comercio, en uso de las facultades legales, en especial las conferidas en los artículos 29, 34, 41 y 42 de la ley 527 de 1999 y los decretos 2153 de 1992, 2269 de 1993 y 1747 de 2000, y

CONSIDERANDO:
En los términos del artículo 41 de la ley 527 de 1999, se faculta a la Superintendencia de Industria y Comercio para autorizar la actividad de las entidades de certificación en el territorio nacional, así como velar por su funcionamiento y la prestación eficiente del servicio.

En el numeral 11 del artículo 41 de la ley 527 de 1999 y en el 21 del artículo 2 del decreto 2153 de 1992, se faculta a la Superintendencia de Industria y Comercio para impartir instrucciones sobre el adecuado cumplimiento de las normas a las cuales deben sujetarse las entidades de certificación.

En el artículo 34 de la ley 527 de 1999 se determina que la Superintendencia de Industria y Comercio autorizará la cesación de actividades de las entidades de certificación.

En el numeral 10 del artículo 2 del decreto 2153 de 1992 y en el numeral 5 del artículo 41 de la ley 527 de 1999, se determina que la Superintendencia de Industria y Comercio podrá solicitar a las personas naturales o jurídicas el suministro de información, datos, informes, libros y papeles de comercio que se requieran para el correcto ejercicio de sus funciones.
RESUELVE:

CAPÍTULO I - Entidades de certificación cerradas

Artículo 1 Autorización de entidad de certificación cerrada. La persona que solicite autorización como entidad de certificación cerrada, según lo dispuesto en numeral 8 del artículo 1 del decreto 1747 de 2000, deberá demostrar el cumplimiento de las condiciones establecidas en el artículo 29 de la ley 527 de 1999 y

en los artículos 3 y 4 del decreto 1747 de 2000, para lo cual deberá diligenciar el anexo 1 de esta resolución y adjuntando la siguiente información:
Certificado de existencia y representación legal, o copia de las normas que le otorgan la calidad de representante legal de una entidad pública o de notario o cónsul.
Un formato diligenciado del anexo 2 por cada uno de los administradores o representantes legales.

Artículo 2. Cambio de servicios ofrecidos en entidad de certificación cerrada. Cuando la entidad de certificación cerrada pretenda ofrecer nuevos servicios como entidad de certificación dentro del entorno cerrado, según lo dispuesto en el numeral 8 del artículo 1 del decreto 1747 de 2000, deberá solicitar autorización previa ante esta Superintendencia, mediante el diligenciamiento del anexo 4.

Artículo 3. Remisión de información por cambio o actualización de datos en entidad de certificación cerrada. De conformidad con el artículo 21 del decreto 1747 de 2000, cuando alguno de los datos de la entidad de certificación cerrada que reposan en esta Superintendencia cambie, la entidad de certificación deberá remitir la información correspondiente al cambio, dentro de los 10 días posteriores a la modificación.
En caso de modificación de la información o inclusión de un representante legal o administrador, el nuevo represente legal o administrador deberá diligenciar el anexo 2 y remitirlo a esta Superintendencia.

Artículo 4. Información periódica de entidad de certificación cerrada. La entidad de certificación cerrada deberá almacenar la información de toda su actividad y enviar a esta Superintendencia dentro de los 10 primeros días del inicio de cada trimestre (enero-marzo, abril-junio, julio-septiembre, octubre-diciembre), un archivo de texto según el anexo 5, con la siguiente información sobre la actividad del trimestre inmediatamente anterior, discriminada mes a mes:
Número de certificados emitidos, de acuerdo con el tipo de certificados.
Número de certificados vigentes, de acuerdo con el tipo de certificados.
Número de certificados revocados.

Artículo 5. Cesación de actividades en la entidad de certificación cerrada. Conforme lo dispuesto en el artículo 34 de la ley 527 de 1999 y el artículo 19 del decreto 1747 de 2000, las entidades de certificación cerradas deberán solicitar la autorización de cesación de una o más actividades ante esta superintendencia diligenciando el anexo 3.
Una vez autorizada la cesación, la entidad de certificación deberá concluir el ejercicio de las actividades autorizadas para cesar, en la forma y siguiendo el cronograma que para el efecto se señale.

Artículo 6. Publicidad de la entidad de certificación cerrada. En cualquier publicidad o en cualquier medio en el cual la entidad de certificación ofrezca los servicios deberá indicar que cuenta con autorización de la Superintendencia de Industria y Comercio para operar, según el siguiente texto : "Entidad de certificación cerrada autorizada por la Superintendencia de Industria y Comercio".

CAPÍTULO II - Entidades de certificación abiertas

SECCIÓN I - Autorización

Artículo 7. Autorización de entidad de certificación abierta. La persona que solicite autorización como entidad de certificación abierta según lo dispuesto en numeral 9 del artículo 1 del decreto 1747 de 2000, deberá demostrar que la actividad está prevista en el objeto social principal, el cumplimiento de las condiciones establecidas en los artículos 29 de la ley 527 de 1999 y 5, 6, 7, 8, 9, 10, 11 del decreto 1747 de 2000 y los estándares, planes y procedimientos de seguridad establecidos en la sección V de esta resolución, diligenciando el anexo 1 y adjuntando la siguiente información:

1. Anexo 2 debidamente diligenciado por cada uno de los administradores o representantes legales adjuntando:
   Certificado judicial vigente o documento equivalente proveniente del país o países donde haya residido.
   Copia del certificado de existencia y representación legal, o copia de las normas que le otorgan la calidad de representante legal de una entidad pública o de notario o cónsul.
2. Copia del acto que le otorga la personería jurídica, y copia de las normas que le otorgan la calidad de representante legal de una entidad pública o de notario o cónsul, o certificado de existencia y representación legal. Cuando se trate de persona extranjera se deberá acreditar el cumplimiento de lo señalado en el libro II titulo XIII del código de comercio y el artículo 48 del código de procedimiento civil, según lo dispuesto en el numeral 1 artículo 5 del decreto 1747 de 2000.
3. Informe de auditoría en los términos del artículo 15 de esta resolución.
4. Estados financieros certificados con forme a la ley y con una antigüedad no superior a seis meses, según lo dispuesto en el numeral 1 del artículo 7 del decreto 1747 de 2000.
5. Copia del documento que acredite que se han constituido las garantías de acuerdo a lo dispuesto en el artículo 8 del decreto 1747 de 2000.
6. Documento con descripción detallada de la infraestructura, procedimientos, recursos según lo previsto en el artículo 9 del decreto 1747 de 2000. El cumplimiento de los requisitos deberá acreditarse según lo previsto en la sección V del capítulo II de esta resolución.
   En caso de que la infraestructura sea prestada por un tercero, copia de los contratos o convenios con estos, en idioma español.
7. Declaración de prácticas de certificación, en adelante DPC.

SECCIÓN II - Cumplimiento requisitos permanentes

Artículo 8. Cambio de servicios ofrecidos en entidad de certificación abierta. Cuando la entidad de certificación abierta pretenda ofrecer nuevos servicios, deberá solicitar autorización previa ante esta Superintendencia, mediante el diligenciamiento del anexo 4, adjuntando el informe de auditoría correspondiente al nuevo servicio.

Artículo 9. Remisión de información por cambio o actualización de datos en entidad de certificación abierta. De conformidad con el artículo 21 del decreto 1747 de 2000, cuando alguno de los datos de la entidad de certificación abierta que reposan en esta Superintendencia cambie, la entidad de certificación deberá remitir la información correspondiente al cambio, dentro de los 10 días posteriores a la modificación.
En caso de modificación de la información o inclusión de un representante legal o administrador, el nuevo represente legal o administrador deberá diligenciar el anexo 2 y remitirlo a esta Superintendencia adjuntando:
Certificado de Judicial vigente o documento equivalente provenientes del país o países donde haya residido.
Certificado del órgano competente de los países en que haya residido que certifique que no ha sido excluido o suspendido por actos graves contra la ética de la profesión.

Artículo 10. Información periódica de entidad de certificación abierta. La entidad de certificación abierta deberá almacenar la información de toda su actividad y enviar a esta Superintendencia dentro de los 10 primeros días del inicio de cada trimestre (enero-marzo, abril-junio, julio-septiembre, octubre-diciembre), un archivo de texto según el anexo 5, con la siguiente información sobre la actividad del trimestre inmediatamente anterior, discriminada mes a mes:
Número de certificados emitidos, de acuerdo con el tipo de certificados.
Número de certificados vigentes, de acuerdo con el tipo de certificados.
Número de certificados revocados
Compromisos adquiridos por cada tipo de certificado.

Artículo 11. Actualización anual de información de estados financieros, garantías y e informe de auditoría. La entidad de certificación abierta deberá remitir a esta Superintendencia los estados financieros de fin ejercicio, el informe de auditoría contemplado en el numeral 3 del artículo 7 de esta resolución, dentro de los primeros 15 días corrientes de febrero de cada año calendario.

Artículo 12. Suspensión programada del servicio. Durante cada año calendario, las entidades de certificación podrán cesar temporalmente sus actividades por un lapso máximo de 3 días continuos o discontinuos, para mantenimiento del sistema. Cualquier otra suspensión deberá ser solicitada y aprobada por la Superintendencia de Industria y Comercio, previa justificación.
La suspensión permitida deberá informarse a los usuarios con por lo menos con 15 días de antelación y constancia del aviso remitirse a esta Entidad, a más tardar el primer día de la suspensión.

Artículo 13. Publicidad de la entidad de certificación abierta. En cualquier publicidad o en cualquier medio en el cual la entidad de certificación ofrezca los servicios deberá indicar que cuenta con autorización de la Superintendencia de Industria y Comercio para operar, según el siguiente texto : "Entidad de certificación abierta autorizada por la Superintendencia de Industria y Comercio".

SECCIÓN III - Firmas auditoras de entidades de certificación

Artículo 14. Firmas auditoras. La firma auditora nacional que realice el informe de auditoría referido en el artículo 12 del decreto 1747 de 2000, deberá ser un organismo de inspección del sistema nacional de normalización, certificación y metrología acreditada para realizar inspecciones en sistemas informáticos de seguridad y contabilidad, de conformidad con lo señalado en el decreto 2269 de 1993, la resolución 140 de 1994 de la Superintendencia de Industria y Comercio y las disposiciones que los sustituyan o complementen.
Estas firmas deberán cumplir, además de lo requerido en el decreto 2269 de 1993, lo siguiente:
Estar compuesta por un grupo interdisciplinario de profesionales que incluirá por lo menos 1 ingeniero de sistemas especializado en sistemas de seguridad, 1 contador y 1 abogado con amplios conocimientos en el tema, quienes deberán cumplir con las normas vigentes relacionadas con cada una de las profesiones.
Acreditar experiencia de la firma o de uno de sus socios o funcionarios, en auditorías en sistemas informáticos de seguridad y contabilidad por lo menos de 3 años.
Acreditar capacidad para certificar el cumplimiento de los requisitos técnicos y estándares exigidos en la ley 527 de 1999, el decreto 1747 de 2000 y esta resolución.

Artículo 15. Contenido obligatorio del informe de auditoría. Tratándose de entidades extranjeras que obren en las condiciones previstas en el artículo 12 del decreto 1747 de 2000, los informes de auditoría deberán anexar certificación que demuestre que está facultada para realizar este tipo de auditorías en su país de origen.

El informe de auditoria deberá indicar por lo menos:
Nombre e identificación de la firma auditora.
Fecha de inicio y terminación de la auditoría.
Declaración de conformidad de cada una de las condiciones previstas en el artículo 29 de la ley 527 de 1999, el decreto 1747 de 2000, a la presente resolución y las normas que los modifiquen y adicionen.
Manifestación de conformidad de la declaración de prácticas de certificación y evaluación de la efectividad de los planes, políticas y procedimientos de seguridad contenidos tanto en la declaración como los exigidos en la sección V de esta resolución.
Manifestación del cumplimiento de los estándares indicados en el artículo 23 de esta resolución, teniendo en cuenta criterios reconocidos para el efecto, que cumplan por los menos con los objetivos del nivel de protección 2 (*Evaluation Assurance Level 2*) definido por *Common Criteria for Information Technology Security Evaluation* (CC 2.1) CCIMB-99-031 desarrollado por el *Common Criteria Project Sponsoring*

Organization en su parte 3 o su equivalente en la norma ISO/IEC 15408. En el informe deberá precisar para cada uno de estos objetivos del artículo 23 de esta resolución el criterio que observó, la fuente de ese criterio y el reconocimiento que tiene.
Firma del representante legal de la firma auditora.

SECCIÓN IV - Cesación de actividades

Artículo 16. Autorización de cesación de entidades de certificación abiertas Conforme lo dispuesto en el artículo 34 de la ley 527 de 1999 y el artículo 19 del decreto 1747 de 2000, las entidades de certificación abiertas deberán solicitar autorización de cesación de una o más actividades ante esta Superintendencia, diligenciando el anexo 3 y adjuntando la siguiente información:
Plan que garantice la protección de la información confidencial de los suscriptores.
Plan de conservación de los archivos necesarios para futuras verificaciones de los certificados que emitió, hasta el otorgamiento de la autorización de cesación del servicio. Dicho plan debe permitir el acceso y posterior consulta de los documentos y extenderse hasta una fecha posterior a la fecha en que se extingan las responsabilidades que se puedan derivar de los certificados expedidos y el plazo que prevean las normas de conservación documental para cada uno de los documentos.
Plan que garantice la publicación en los repositorios propios si no cesa todas las actividades o en los de otra entidad de certificación abierta que la Superintendencia de Industria y Comercio determine, si cesará todas las actividades.
En caso de cesar todas las actividades de entidad de certificación, un plan de seguridad que garantice la adecuada destrucción de la clave privada de la entidad

Artículo 17. Procedimiento para la cesación de actividades. Una vez la Superintendencia autorice la cesación de actividades, la entidad de certificación deberá informar a todos los suscriptores, mediante dos avisos publicados en diarios de amplia circulación nacional, con un intervalo de 15 días, sobre:
La terminación de su actividad o actividades y la fecha precisa de cesación.
Las consecuencias jurídicas de la cesación respecto de los certificados expedidos.
En todo caso los suscriptores podrán solicitar la revocación y el reembolso equivalente al valor del tiempo de vigencia restante del certificado, si lo solicitan dentro de los dos (2) meses siguientes a la segunda publicación.
La terminación de la actividad o actividades se hará en la forma y siguiendo el cronograma que para el efecto señale la Superintendencia.

SECCIÓN V - Estándares, planes y procedimientos de seguridad

Artículo 18. Estándares. Para los efectos previstos en el artículo 27 del decreto 1747 de 2000, admitirán siguientes estándares:
Para algoritmos de firma.

a) Algoritmos definidos en el "*draft Representation of Public Keys and Digital Signatures in Internet X.509 Public Key Infrastructure Certificates*" desarrollado por el *PKIX Working group del Internet Engineering Task Force (IETF)*, excluyendo el MD2.
b) El algoritmo y la longitud de la clave seleccionados deben garantizar la unicidad de la firma digital de los documentos que se firmen de acuerdo con los usos permitidos del certificado. Esta longitud debe ser superior o igual a 1024 bits en el algoritmo de RSA o su equivalente. Longitudes inferiores serán admitidas, pero no menores de 512 bits o su equivalente, previa justificación de garantía de la unicidad.

Para generación de par de claves: Un método de generación de claves privada y pública que garantice la unicidad y la imposibilidad de estar incurso en situaciones contempladas en el artículo 16 del decreto 1747 de 2000.

Para generación de firma digital. Un sistema de generación de firma digital que utilice un algoritmo de firma digital admitido.
Para certificados en relación con firma digital. Los certificados compatibles con el estándar de la *International Telecommunication Union (ITU - T)* X – 509 versión 3.
Para listas de certificados revocados. El estándar de CRL de la ITU X-509 Versión 2.

Artículo 19. Declaración de Prácticas de Certificación. La declaración de prácticas de certificación a que se hace referencia en el artículo 6 del decreto 1747 de 2000, deberá estar asequible desde el "*homepage*" de la entidad de certificación, disponible al público en todo momento y tendrá que incluir:

La identificación de la entidad que presta los servicios de certificación. Esta información incluirá el nombre, razón o denominación social de la entidad, el domicilio social, teléfono, fax, dirección de correo electrónico y la oficina responsable de las peticiones, consultas y reclamos de los suscriptores y usuarios. Si la entidad de certificación tiene entidades subordinadas o subcontratadas, deberá incluir esta misma información respecto de cada una de ellas.
La política de manejo de los certificados, que debe incluir:

Los requisitos y el procedimiento de expedición de certificados, incluyendo los procedimientos de identificación del suscriptor y de las entidades reconocidas, de acuerdo con lo previsto en el artículo 43 de la Ley 527 de 1999.

Los tipos de certificados que ofrece, sus diferencias, el grado de confiabilidad y los posibles usos de cada uno de ellos, límites de responsabilidad y el tiempo durante el cual se garantiza la condición de unicidad de la firma digital.

El contenido de cada uno de los distintos tipos de certificados.

El procedimiento para la actualización de la información contenida en los certificados.

El procedimiento, las verificaciones, la oportunidad y las personas que podrán invocar las causales de suspensión o revocación de los certificados.

La vigencia de cada uno de los tipos de certificados.

La Información sobre el sistema de seguridad para proteger la información que se recoge con el fin de expedir los certificados.

Las obligaciones de la entidad de certificación y de los suscriptores del certificado y las precauciones que deben observar los terceros que confían en el certificado.

La información que se le va a solicitar a los suscriptores.

El manejo de la información que se obtiene de los suscriptores de acuerdo a las normas aplicables en la materia, detallando:

El manejo de la información de naturaleza confidencial.

Los eventos en que se revelará la información confidencial dada por el suscriptor, de acuerdo con las normas vigentes.

Las garantías que ofrece la entidad para el cumplimiento de las obligaciones que se deriven de sus actividades y los clausulados de los seguros que protegen a los terceros por los perjuicios que pueda causar la entidad y/o los reglamentos de los contratos de fiducia constituidos para el efecto.

Los límites de responsabilidad de la entidad de certificación en cada uno de los tipos de certificados y por cada documento firmado.

Las tarifas de expedición y revocación de certificados y los servicios que incluyen.
Los procedimientos de seguridad para el manejo de los siguientes eventos:

Cuando la seguridad de la clave privada de la entidad de certificación se ha visto comprometida.

Cuando el sistema de seguridad de la entidad de certificación ha sido vulnerado.

Cuando se presenten fallas en el sistema de la entidad de certificación que comprometan la prestación del servicio.

Cuando los sistemas de cifrado pierdan vigencia por no ofrecer el nivel de seguridad contratado por el suscriptor.

El plan de contingencia encaminado a garantizar la continuidad del servicio de certificación, en caso de que ocurra algún evento que comprometa la prestación del servicio.

Modelos y minutas de los contratos que utilizará. En caso de prever su existencia, texto de las cláusulas compromisorias que establezcan el procedimiento jurídico para la resolución de conflictos, especificando al menos la jurisdicción y ley aplicable en el caso en que alguna de las partes no tenga domicilio en el territorio colombiano.

La política de manejo de otros servicios que fuere a prestar, detallando sus condiciones.

Artículo 20. Sistema confiable. Para los efectos del artículo 2 del decreto 1747 de 2000 un sistema será confiable cuando cumpla con lo señalado en los artículos 21, 22 y 23 de la presente resolución.

Artículo 21. Políticas, planes y procedimientos de seguridad. La entidad debe definir y poner en práctica después de autorizada las políticas, planes y procedimientos de seguridad tendientes a garantizar la prestación continua de los servicios de certificación, que deben ser revisados y actualizados periódicamente. Estos deben incluir al menos:

Políticas y procedimientos de seguridad de las instalaciones físicas y los equipos.

Políticas de acceso a los sistemas e instalaciones de la entidad, monitoreo constante.

Procedimientos de actualización de hardware y software, utilizados para la operación de entidades de certificación.

Procedimientos de contingencia en cada uno de los riesgos potenciales que atenten en contra del funcionamiento de la entidad, según estudio que se actualizará periódicamente.

Plan de manejo, control y prevención de virus informático.
Procedimiento de generación de claves de la entidad de certificación que garantice que:

Sólo se hace ante la presencia de los administradores de la entidad.

Los algoritmos utilizados y la longitud de las claves utilizadas son tales que garanticen la unicidad de las firmas generadas en los certificados, por el tiempo de vigencia máximo que duren los mensajes de datos firmados por sus suscriptores.

Artículo 22. Corta fuegos (*Firewall*). La entidad de certificación debe aislar los servidores de la red interna y externa mediante la instalación de un corta fuegos o *firewall*, en el cual deben ser configuradas las políticas de acceso y alertas pertinentes.
La red del centro de cómputo debe estar ubicada en segmentos de red físicos independientes de la red interna del sistema, garantizando que el corta fuegos sea el único elemento que permita el acceso lógico a los sistemas de certificación.

Artículo 23. Sistemas de emisión y administración de certificados. Los sistemas de emisión y administración de certificados deben prestar en forma segura y continua el servicio. En todo caso las entidades deberán cumplir al menos con una de las siguientes condiciones:
cumplir el *Certificate Issuing and Management Components Protection Profile* nivel 2 desarrollado por el *National Institute of Standards and Technologies*; o
cumplir con requerimientos técnicos que correspondan por lo menos con los objetivos del nivel de protección 2 (*Evaluation Assurance Level 2*) definido por *Common Criteria for Information Technology Security*

Evaluation (CC 2.1) CCIMB-99-031 desarrollado por el *Common Criteria Project Sponsoring Organization* en su parte 3 o su equivalente en la norma ISO/IEC 15408, de:

sistema de registro de auditoría de todas las operaciones relativas al funcionamiento y administración de los elementos de emisión y administración de certificados, que permita reconstruir en todo momento cualquier actividad de la entidad;

sistema de almacenamiento secundario de toda la información de la entidad, en un segundo dispositivo que cuente por lo menos con la misma seguridad que el dispositivo original, para poder reconstruir la información de forma segura en caso necesario;

dispositivo de generación y almacenamiento de la clave privada, tal que se garantice su privacidad y destrucción en caso de cualquier intento de violación. El dispositivo y los procedimientos deben garantizar que la generación de la clave privada de la entidad solo puede ser generada en presencia de los representantes legales de la misma; y

sistema de chequeo de integridad de la información del sistema, los datos y en particular de sus claves.

CAPÍTULO III - Certificados

Artículo 24. Contenido de los certificados. Los certificados deberán cumplir con lo señalado en el numeral 4 del artículo 18 y con los requisitos exigidos en artículo 35 de la ley 527 de 1999.

Artículo 25. Contenido de los certificados recíprocos. Los certificados recíprocos señalados en el parágrafo del artículo 14 del decreto 1747 de 2000 deben contener al menos la siguiente información:

Identificador único del certificado.

Clave pública de la entidad que se está reconociendo.

Tipos de certificados a los que se remite el reconocimiento.

Duración del reconocimiento.

Referencia de los límites de responsabilidad del tipo de certificado al cual se remite el reconocimiento.

Artículo 26. Vigencia. La presente resolución rige a partir de la fecha de su publicación en diario oficial.

PUBLÍQUESE Y CÚMPLASE

Dada en Bogotá, D.C. a los ....

El Superintendente de Industria y Comercio,

EMILIO JOSÉ ARCHILA PEÑALOSA

[4] C. ECUADOR

LEY DE COMERCIO ELECTRONICO, FIRMAS ELECTRONICAS Y MENSAJES DE DATOS

EL H. CONGRESO NACIONAL

Considerando:

Que, el uso de sistemas de información y de redes electrónicas, incluida la Internet ha adquirido importancia para el desarrollo del comercio y la producción, permitiendo la realización y concreción de múltiples negocios de trascendental importancia, tanto para el sector público como para el sector privado.

Que, es necesario impulsar el acceso de la población a los servicios electrónicos que se generan por y a través de diferentes medios electrónicos.

Que, se debe generalizar la utilización de servicios de redes de información e Internet, de modo que éstos se conviertan en un medio para el desarrollo del comercio, la educación y la cultura.

Que, a través del servicio de redes electrónicas, incluida la Internet se establecen relaciones económicas y de comercio, y se realizan actos y contratos de carácter civil y mercantil que es necesario normarlos, regularlos y controlarlos, mediante la expedición de una Ley especializada sobre la materia.

Que, es indispensable que el Estado Ecuatoriano cuente con herramientas jurídicas que le permitan el uso de los servicios electrónicos, incluido el comercio electrónico y acceder con mayor facilidad a la cada vez más compleja red de los negocios internacionales.

En uso de sus atribuciones, expide la siguiente:

"LEY DE COMERCIO ELECTRONICO, FIRMAS ELECTRONICAS Y MENSAJES DE DATOS"

TÍTULO PRELIMINAR

Artículo 1.- Objeto de la Ley .- Esta Ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas.

TÍTULO I DE LOS MENSAJES DE DATOS

CAPÍTULO I - PRINCIPIOS GENERALES

Artículo 2.- Reconocimiento jurídico de los mensajes de datos.- Los mensajes de datos tendrán igual valor jurídico que los documentos escritos. Su eficacia, valoración y efectos se someterá al cumplimiento de lo establecido en esta Ley y su reglamento.

Artículo 3.- Incorporación por remisión.- Se reconoce validez jurídica a la información no contenida directamente en un mensaje de datos, siempre que figure en el mismo, en forma de remisión o de anexo accesible mediante un enlace electrónico directo y su contenido sea conocido y aceptado expresamente por las partes.

Artículo 4.- Propiedad Intelectual.- Los mensajes de datos estarán sometidos a las leyes, reglamentos y acuerdos internacionales relativos a la propiedad intelectual.

[4] Flag courtesy of www.theodora.com/flags used with permission

Artículo 5.- Confidencialidad y reserva.- Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta Ley y demás normas que rigen la materia.

Artículo 6.- Información escrita.- Cuando la Ley requiera u obligue que la información conste por escrito, este requisito quedará cumplido con un mensaje de datos, siempre que la información que éste contenga sea accesible para su posterior consulta.

Artículo 7.- Información original.- Cuando la Ley requiera u obligue que la información sea presentada o conservada en su forma original, este requisito quedará cumplido con un mensaje de datos, si siendo requerido conforme a la Ley, puede comprobarse que 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.

Se considera que un mensaje de datos permanece íntegro, si se mantiene completo e inalterable su contenido, salvo algún cambio de forma, propio del proceso de comunicación, archivo o presentación.

Por acuerdo de las partes y cumpliendo con todas las obligaciones previstas en esta Ley, se podrán desmaterializar los documentos que por ley deban ser instrumentados físicamente.
Los documentos desmaterializados deberán contener las firmas electrónicas correspondientes debidamente certificadas ante una de las entidades autorizadas, según lo dispuesto en el artículo 30 de la presente Ley y deberán ser conservados conforme a lo establecido en el artículo siguiente.

Artículo 8.- Conservación de los mensajes de datos.- Toda información sometida a esta Ley, podrá ser conservada; este requisito quedará cumplido mediante el archivo del mensaje de datos, siempre que se reúnan las siguientes condiciones:

a. que la información que contenga sea accesible para su posterior consulta;
b. que sea conservado con el formato en el que se haya generado, enviado o recibido, o con algún formato que sea demostrable que reproduce con exactitud la información generada, enviada o recibida;
c. que se conserve todo dato que permita determinar el origen, el destino del mensaje, la fecha y hora en que fue creado, generado, procesado, enviado, recibido y archivado; y,
d. Que se garantice su integridad por el tiempo que se establezca en el Reglamento a esta Ley.

Toda persona podrá cumplir con la conservación de mensajes de datos, usando los servicios de terceros, siempre que se cumplan las condiciones mencionadas en este artículo.

Para la información que tenga por única finalidad facilitar el envío o recepción del mensaje de datos, no será obligatorio el cumplimiento de lo establecido en los literales anteriores.

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

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

No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato.
El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo.

Artículo 10.- Procedencia e identidad de un mensaje de datos.- Salvo prueba en contrario se entenderá que un mensaje de datos proviene de quien lo envía y, autoriza a quien lo recibe, para actuar conforme al contenido del mismo, cuando de su verificación exista concordancia entre la identificación del emisor y su firma electrónica, excepto en los siguientes casos:

a) Si se hubiere dado aviso que el mensaje de datos no proviene de quien consta como emisor; en este caso, el aviso se lo hará antes de que la persona que lo recibe actúe conforme a dicho mensaje. En caso contrario, quien conste como emisor deberá justificar plenamente que el mensaje de datos no se inició por orden suya o que el mismo fue alterado; y,

b) Si el destinatario no hubiere efectuado diligentemente las verificaciones correspondientes o hizo caso omiso de su resultado.

Artículo 11.- Envío y recepción de los mensajes de datos.- Salvo pacto en contrario, se presumirá que el tiempo y lugar de emisión y recepción del mensaje de datos, son los siguientes:

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

b) **Momento de recepción del mensaje de datos.-** Cuando el mensaje de datos ingrese al sistema de información o red electrónica señalado por el destinatario. Si el destinatario designa otro sistema de información o red electrónica, el momento de recepción se presumirá aquel en que se produzca la recuperación del mensaje de datos. De no haberse señalado un lugar preciso de recepción, se entenderá que ésta ocurre cuando el mensaje de datos ingresa a un sistema de información o red electrónica del destinatario, independientemente de haberse recuperado o no el mensaje de datos; y,

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

Artículo 12.- Duplicación del mensaje de datos.- Cada mensaje de datos será considerado diferente. En caso de duda, las partes pedirán la confirmación del nuevo mensaje y tendrán la obligación de verificar técnicamente la autenticidad del mismo.

TITULO II DE LAS FIRMAS ELECTRÓNICAS, CERTIFICADOS DE FIRMA ELECTRONICA, ENTIDADES DE CERTIFICACION DE INFORMACIÓN, ORGANISMOS DE PROMOCIÓN DE LOS SERVICIOS ELECTRÓNICOS, Y DE REGULACIÓN Y CONTROL DE LAS ENTIDADES DE CERTIFICACIÓN ACREDITADAS.

CAPÍTULO I - DE LAS FIRMAS ELECTRÓNICAS

Artículo 13.- Firma electrónica.- 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.

Artículo 14.- Efectos de la firma electrónica.- La firma electrónica tendrá igual validez y se le reconocerán los mismos efectos jurídicos que a una firma manuscrita en relación con los datos consignados en documentos escritos, y será admitida como prueba en juicio.

Artículo 15.- Requisitos de la firma electrónica.- Para su validez, la firma electrónica reunirá los siguientes requisitos, sin perjuicio de los que puedan establecerse por acuerdo entre las partes:

a) ser individual y estar vinculada exclusivamente a su titular**;**

b) que permita verificar inequívocamente la autoría e identidad del signatario, mediante dispositivos técnicos de comprobación establecidos por esta Ley y sus reglamentos;

c) que su método de creación y verificación sea confiable, seguro e inalterable para el propósito para el cual el mensaje fue generado o comunicado.

d) que al momento de creación de la firma electrónica, los datos con los que se creare se hallen bajo control exclusivo del signatario; y,

e) que la firma sea controlada por la persona a quien pertenece.

Artículo 16.- La firma electrónica en un mensaje de datos.- Cuando se fijare la firma electrónica en un mensaje de datos, aquélla deberá enviarse en un mismo acto como parte integrante del mensaje de datos o lógicamente asociada a éste. Se presumirá legalmente que el mensaje de datos firmado electrónicamente conlleva la voluntad del emisor, quien se someterá al cumplimiento de las obligaciones contenidas en dicho mensaje de datos, de acuerdo a lo determinado en la Ley.

Artículo 17.- Obligaciones del titular de la firma electrónica.- El titular de la firma electrónica deberá:

a) cumplir con las obligaciones derivadas del uso de la firma electrónica;

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;

c) notificar por cualquier medio a las personas vinculadas, cuando exista el riesgo de que su firma sea controlada por terceros no autorizados y utilizada indebidamente;

d) verificar la exactitud de sus declaraciones;

e) responder por las obligaciones derivadas del uso no autorizado de su firma, cuando no hubiere obrado con la debida diligencia para impedir su utilización, salvo que el destinatario conociere de la inseguridad de la firma electrónica o no hubiere actuado con la debida diligencia;

f) notificar a la entidad de certificación de información los riesgos sobre su firma y solicitar oportunamente la cancelación de los certificados, y

g) las demás señaladas en la Ley y sus reglamentos.

Artículo 18.- Duración de la firma electrónica.- Las firmas electrónicas tendrán duración indefinida, podrán ser revocadas, anuladas o suspendidas de conformidad con lo que el Reglamento a esta Ley señale.

Artículo 19.- Extinción de la firma electrónica.- La firma electrónica se extinguirá por:

a) voluntad de su titular;

b) fallecimiento o incapacidad de su titular**;**

c) disolución o liquidación de la persona jurídica, titular de la firma;

d) por causa judicialmente declarada.

La extinción de la firma electrónica no exime a su titular de las obligaciones previamente contraídas derivadas de su uso.

CAPÍTULO II - DE LOS CERTIFICADOS DE FIRMA ELECTRÓNICA

Artículo 20.- Certificado de firma electrónica.- Es el mensaje de datos que certifica la vinculación de una firma electrónica con una persona determinada, a través de un proceso de comprobación que confirma su identidad.

Artículo 21.- Uso del certificado de firma electrónica.- El certificado de firma electrónica se empleará para certificar la identidad del titular de una firma electrónica y para otros usos, de acuerdo a esta Ley y su reglamento.

Artículo 22.- Requisitos del certificado de firma electrónica.- El certificado de firma electrónica para ser considerado válido contendrá los siguientes requisitos:

a) Identificación de la entidad de certificación de información.

b) Domicilio legal de la entidad de certificación de información.

c) Los datos del titular del certificado que permitan su ubicación e identificación.

d) El método de verificación de la firma del titular del certificado.

e) Las fechas de emisión y expiración del certificado.

f) El número único de serie que identifica el certificado.

g) La firma electrónica de la entidad de certificación de información.

h) Las limitaciones o restricciones para los usos del certificado, y

i) Los demás señalados en esta Ley y los reglamentos.

Artículo 23.- Duración del certificado de firma electrónica.- Salvo acuerdo contractual**,** el plazo de validez de los certificados de firma electrónica será el establecido en el reglamento a esta Ley.

Artículo 24.- Extinción del certificado de firma electrónica.- Los certificados de firma electrónica**,** se extinguen, por las siguientes causas:

a) Solicitud de su titular;

b) Extinción de la firma electrónica, de conformidad con lo establecido en el Art. 19 de esta Ley; y,

c) Expiración del plazo de validez del certificado de firma electrónica.

La extinción del certificado de firma electrónica se producirá desde el momento de su comunicación a la entidad de certificación de información, excepto en el caso de fallecimiento del titular de la firma electrónica, en cuyo caso se extingue a partir de que acaece el fallecimiento. Tratándose de personas secuestradas o desaparecidas, se extingue a partir de que se denuncie ante las autoridades competentes tal secuestro o desaparición. La extinción del certificado de firma electrónica no exime a su titular de las obligaciones previamente contraídas derivadas de su uso.

Artículo 25.- Suspensión del certificado de firma electrónica.- La entidad de certificación de información podrá suspender temporalmente el certificado de firma electrónica cuando:

a) sea dispuesto por el Consejo Nacional de Telecomunicaciones, de conformidad con lo previsto en esta Ley;

b) se compruebe por parte de la entidad de certificación de información, falsedad en los datos consignados por el titular del certificado; y,

c) se produzca el incumplimiento del contrato celebrado entre la entidad de certificación de información y el titular de la firma electrónica.

La suspensión temporal dispuesta por la entidad de certificación de información deberá ser inmediatamente notificada al titular del certificado y al organismo de control, dicha notificación deberá señalar las causas de la suspensión.

La entidad de certificación de información deberá levantar la suspensión temporal una vez desvanecidas las causas que la originaron, o cuando mediare resolución del Consejo Nacional de Telecomunicaciones, en cuyo caso, la entidad de certificación de información está en la obligación de habilitar de inmediato el certificado de firma electrónica.

Artículo 26.- Revocatoria del certificado de firma electrónica.- El certificado de firma electrónica podrá ser revocado por el Consejo Nacional de Telecomunicaciones, de conformidad con lo previsto en esta Ley, cuando:

a) La entidad de certificación de información cese en sus actividades y los certificados vigentes no sean asumidos por otra entidad de certificación; y,

b) Se produzca la quiebra técnica de la entidad de certificación judicialmente declarada.

La revocatoria y sus causas deberán ser inmediatamente notificadas al titular del certificado.

Artículo 27.- Tanto la suspensión temporal, como la revocatoria, surtirán efectos desde el momento de su comunicación con relación a su titular; y, respecto de terceros, desde el momento de su publicación que deberá efectuarse en la forma que se establezca en el respectivo reglamento, y no eximen al titular del certificado de firma electrónica, de las obligaciones previamente contraídas derivadas de su uso.

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

Artículo 28.- Reconocimiento internacional de certificados de firma electrónica.- Los certificados electrónicos emitidos por entidades de certificación extranjeras, que cumplieren con los requisitos señalados en esta Ley y presenten un grado de fiabilidad equivalente, tendrán el mismo valor legal que los certificados acreditados, expedidos en el Ecuador**.** El Consejo Nacional de Telecomunicaciones dictará el reglamento correspondiente para la aplicación de este artículo.

Las firmas electrónicas creadas en el extranjero, para el reconocimiento de su validez en el Ecuador se someterán a lo previsto en esta Ley y su reglamento.

Cuando las partes acuerden entre sí la utilización de determinados tipos de firmas electrónicas y certificados, se reconocerá que ese acuerdo es suficiente en derecho.

Salvo aquellos casos en los que el Estado, en virtud de convenios o tratados internacionales haya pactado la utilización de medios convencionales, los tratados o convenios que sobre esta materia se suscriban, buscarán la armonización de normas respecto de la regulación de mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico, la protección a los usuarios de estos sistemas, y el reconocimiento de los certificados de firma electrónica entre los países suscriptores.

CAPÍTULO III - DE LAS ENTIDADES DE CERTIFICACIÓN DE INFORMACIÓN

Artículo 29.- Entidades de Certificación de Información.- 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 ésta Ley y el Reglamento que deberá expedir el Presidente de la República.

Artículo 31.- Obligaciones de las entidades de certificación de información acreditadas.- Son obligaciones de las entidades de certificación de información acreditadas:

a) encontrarse legalmente constituidas, y estar registradas en el Consejo Nacional de Telecomunicaciones;

b) demostrar solvencia técnica, logística y financiera para prestar servicios a sus usuarios según parámetros que determinará el Presidente de la República;

c) garantizar la prestación permanente, inmediata, confidencial, oportuna y segura del servicio de certificación de información;

c) mantener sistemas de respaldo de la información relativa a los certificados;

d) proceder de forma inmediata a la suspensión o revocatoria de certificados electrónicos previo mandato del Superintendente de Telecomunicaciones, en los casos que especifique en ésta Ley;

e) mantener una publicación del estado de los certificados electrónicos emitidos;

f) 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;

g) 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, y

h) las demás establecidas en esta Ley y los Reglamentos.

Artículo 32.- Responsabilidades de las entidades de certificación de información acreditadas.- Las entidades de certificación de información serán responsables hasta de culpa leve y responderán por los daños y perjuicios que causen a cualquier persona natural o jurídica, en el ejercicio de su actividad, cuando incumplan las obligaciones que les impone esta Ley o actúen con negligencia, sin perjuicio de las sanciones previstas en la Ley Orgánica de Defensa del Consumidor. Serán también responsables por el uso indebido del certificado de firma electrónica acreditado, cuando éstas no hayan consignado en dichos certificados, de forma clara, el límite de su uso y del importe de las transacciones válidas que pueda realizar. Para la aplicación de este artículo, la carga de la prueba le corresponderá a la entidad de certificación de información.

Los contratos con los usuarios deberán incluir una cláusula de responsabilidad que reproduzca lo que señala el primer inciso.

Cuando la garantía constituida por las entidades de certificación de información acreditadas no cubra las indemnizaciones por daños y perjuicios, aquellas responderán con su patrimonio.

Artículo 33.- Protección de datos por parte de las entidades de certificación de información acreditadas.- Las entidades de certificación de información garantizarán la protección de los datos personales obtenidos en función de sus actividades, de conformidad con lo establecido en el artículo 9 de esta Ley.

Artículo 34.- Prestación de servicios de certificación por parte de terceros.- Los servicios de certificación de información podrán ser proporcionados y administrados en todo o en parte por terceros. Para efectuar la prestación, éstos deberán demostrar su vinculación con la Entidad de Certificación de Información.

El Consejo Nacional de Telecomunicaciones, establecerá los términos bajo los cuales las Entidades de Certificación de Información podrán prestar sus servicios por medio de terceros.

Artículo 35.- Terminación contractual.- La terminación del contrato entre las entidades de certificación acreditadas y el suscriptor se sujetará a las normas previstas en la Ley Orgánica de Defensa del Consumidor.
Artículo 36.- Notificación de cesación de actividades.- Las entidades de certificación de información acreditadas, deberán notificar al Organismo de Control, por lo menos con noventa días de anticipación, la cesación de sus actividades y se sujetarán a las normas y procedimientos establecidos en los reglamentos que se dicten para el efecto.

CAPÍTULO IV - DE LOS ORGANISMOS DE PROMOCIÓN Y DIFUSIÓN DE LOS SERVICIOS ELECTRÓNICOS, Y DE REGULACIÓN Y CONTROL DE LAS ENTIDADES DE CERTIFICACIÓN ACREDITADAS.

Artículo 37.- Organismo de Promoción y Difusión.- Para efectos de esta Ley, el Consejo de Comercio Exterior e Inversiones, "COMEXI", será el organismo de promoción y difusión de los servicios electrónicos, incluido el comercio electrónico, y el uso de las firmas electrónicas en la promoción de inversiones y comercio exterior.

Artículo 38.- Organismo de Regulación, Autorización y Registro de las entidades de certificación acreditadas.- El Consejo Nacional de Telecomunicaciones "CONATEL", o la entidad que haga sus veces, será el organismo de autorización, registro y regulación de las entidades de certificación de información acreditadas.

En su calidad de organismo de autorización podrá además:

a) Cancelar o suspender la autorización a las entidades de certificación acreditadas, previo informe motivado de la Superintendencia de Telecomunicaciones.
b) Revocar o suspender los certificados de firma electrónica, cuando la entidad de certificación acreditada los emita con inobservancia de las formalidades legales, previo informe motivado de la Superintendencia de Telecomunicaciones; y
c) Las demás atribuidas en la Ley y en los reglamentos.

Artículo 39.- Organismo de Control de las entidades de certificación de información acreditadas.- Para efectos de esta Ley, la Superintendencia de Telecomunicaciones, será el organismo encargado del control de las entidades de certificación de información acreditadas.

Artículo 40.- Funciones del Organismo de Control.- Para el ejercicio de las atribuciones establecidas en esta Ley, la Superintendencia de Telecomunicaciones tendrá las siguientes funciones:

a) Velar por la observancia de las disposiciones constitucionales y legales sobre la promoción de la competencia y las prácticas comerciales restrictivas, competencia desleal y protección al consumidor, en los mercados atendidos por las entidades de certificación de información acreditadas.
b) Ejercer el control de las entidades de certificación de información acreditadas en el territorio nacional y velar por su eficiente funcionamiento.

c) Realizar auditorías técnicas a las entidades de certificación de información acreditadas.

d) Requerir de las entidades de certificación de información acreditadas, la información pertinente para el ejercicio de sus funciones.

e) Imponer de conformidad con la Ley sanciones administrativas a las entidades de certificación de información acreditadas, en caso de incumplimiento de las obligaciones derivadas de la prestación del servicio.

f) Emitir los informes motivados previstos en esta Ley.

g) Disponer la suspensión de la prestación de servicios de certificación para impedir el cometimiento de una infracción; y

h) Las demás atribuidas en la Ley y en los reglamentos.

Artículo 41.- Infracciones administrativas.- Para los efectos previstos en la presente Ley, las infracciones administrativas se clasifican en leves y graves.

Infracciones leves:

1. La demora en el cumplimiento de una instrucción o en la entrega de información requerida por el organismo de control, y
2. cualquier otro incumplimiento de las obligaciones impuestas por esta Ley y sus reglamentos a las entidades de certificación acreditadas.

Estas infracciones serán sancionadas, de acuerdo a los literales a) y b) del artículo siguiente.

Infracciones graves:

1. Uso indebido del certificado de firma electrónica por omisiones imputables a la entidad de certificación de información acreditada.
2. Omitir comunicar al organismo de control, de la existencia de actividades presuntamente ilícitas realizada por el destinatario del servicio.
3. Desacatar la petición del organismo de control de suspender la prestación de servicios de certificación para impedir el cometimiento de una infracción.
4. El incumplimiento de las resoluciones dictadas por los Organismos de Autorización Registro y Regulación, y de Control, y
5. No permitir u obstruir la realización de auditorías técnicas por parte del organismo de control.

Estas infracciones se sancionarán de acuerdo a lo previsto en los literales c) y d) del artículo siguiente.

Las sanciones impuestas al infractor, por las infracciones graves y leves, no le eximen del cumplimiento de sus obligaciones.

Si los infractores fueren empleados de instituciones del sector público, las sanciones podrán extenderse a la suspensión, remoción o cancelación del cargo del infractor, en cuyo caso deberán observarse las normas previstas en la Ley.

Para la cuantía de las multas, así como para la gradación de las demás sanciones, se tomará en cuenta:

a) La gravedad de las infracciones cometidas y su reincidencia;

b) El daño causado o el beneficio reportado al infractor; y,

c) La repercusión social de las infracciones.

Artículo 42.- Sanciones.- La Superintendencia de Telecomunicaciones, impondrá de oficio o a petición de parte, según la naturaleza y gravedad de la infracción, a las entidades de certificación de información acreditadas, a sus administradores y representantes legales, o a terceros que presten sus servicios, las siguientes sanciones:

a) Amonestación escrita;

b) Multa de quinientos a tres mil dólares de los Estados Unidos de Norteamérica;

c) Suspensión temporal de hasta dos años de la autorización de funcionamiento de la entidad infractora, y multa de mil a tres mil dólares de los Estados Unidos de Norteamérica;

d) Revocatoria definitiva de la autorización para operar como entidad de certificación acreditada y multa de dos mil a seis mil dólares de los Estados Unidos de Norteamérica;

Artículo 43.- **Medidas cautelares**.- En los procedimientos instaurados por infracciones graves, se podrá solicitar a los órganos judiciales competentes, la adopción de las medidas cautelares previstas en la Ley que se estimen necesarias, para asegurar la eficacia de la resolución que definitivamente se dicte.

Artículo 44.- Procedimiento.- El procedimiento para sustanciar los procesos y establecer sanciones administrativas, será el determinado en la Ley Especial de Telecomunicaciones.

TÍTULO III DE LOS SERVICIOS ELECTRÓNICOS, LA CONTRATACIÓN ELECTRÓNICA Y TELEMÁTICA, LOS DERECHOS DE LOS USUARIOS, E INSTRUMENTOS PÚBLICOS.

CAPÍTULO I - DE LOS SERVICIOS ELECTRÓNICOS

Artículo 45.- **Cumplimiento de formalidades.-** Cualquier actividad, transacción mercantil, financiera o de servicios, que se realice con mensajes de datos, a través de redes electrónicas, se someterá a los requisitos y solemnidades establecidos en la Ley que las rija, en todo lo que fuere aplicable, y tendrá el mismo valor y los mismos efectos jurídicos que los señalados en dicha Ley.

CAPÍTULO II DE LA CONTRATACIÓN ELECTRÓNICA Y TELEMÁTICA.

Artículo 46.- 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.

Artículo 47.- Perfeccionamiento y Aceptación de los contratos electrónicos.- El perfeccionamiento de los contratos electrónicos se someterá a los requisitos y solemnidades previstos en las Leyes y se tendrá como lugar de perfeccionamiento el que acordaren las partes.

La recepción, confirmación de recepción, o apertura del mensaje de datos, no implica aceptación del contrato electrónico, salvo acuerdo de las partes.

Artículo 48.- Jurisdicción.- En caso de controversias las partes se someterán a la jurisdicción estipulada en el contrato; a falta de ésta, se sujetarán a las normas previstas por el Código de Procedimiento Civil Ecuatoriano y esta Ley, siempre que no se trate de un contrato sometido a la Ley Orgánica de Defensa del Consumidor, en cuyo caso se determinará como domicilio el del consumidor o usuario.

Para la identificación de la procedencia de un mensaje de datos, se utilizarán los medios tecnológicos disponibles, y se aplicarán las disposiciones señaladas en esta Ley y demás normas legales aplicables.

Cuando las partes pacten someter las controversias a un procedimiento arbitral, en la formalización del convenio de arbitraje como en su aplicación, podrán emplearse medios telemáticos y electrónicos, siempre que ello no sea incompatible con las normas reguladoras del arbitraje.

CAPÍTULO III - DE LOS DERECHOS DE LOS USUARIOS O CONSUMIDORES DE SERVICIOS ELECTRÓNICOS

Artículo 49.- Consentimiento para aceptar mensajes de datos.- Previamente a que el consumidor o usuario exprese su consentimiento para aceptar registros electrónicos o mensajes de datos, debe ser informado clara, precisa y satisfactoriamente, sobre los equipos y programas que requiere para acceder a dichos registros o mensajes.

El usuario o consumidor, al otorgar o confirmar electrónicamente su consentimiento, debe demostrar razonablemente que puede acceder a la información objeto de su consentimiento.

Si con posterioridad al consentimiento del consumidor o usuario existen cambios de cualquier tipo, incluidos cambios en equipos, programas o procedimientos, necesarios para mantener o acceder a registros o mensajes electrónicos, de forma que exista el riesgo de que el consumidor o usuario no sea capaz de acceder o retener un registro electrónico o mensaje de datos sobre los que hubiera otorgado su consentimiento, se le deberá proporcionar de forma clara, precisa y satisfactoria la información necesaria para realizar estos cambios, y se le informará sobre su derecho a retirar el consentimiento previamente otorgado sin la imposición de ninguna condición, costo alguno o consecuencias. En el caso de que estas modificaciones afecten los derechos del consumidor o usuario, se le deberán proporcionar los medios necesarios para evitarle perjuicios, hasta la terminación del contrato o acuerdo que motivó su consentimiento previo.

Artículo 50.- Consentimiento para el uso de medios electrónicos.- De requerirse que la información relativa a un servicio electrónico, incluido el comercio electrónico, deba constar por escrito, el uso de medios electrónicos para proporcionar o permitir el acceso a esa información, será válido si:

a) El consumidor ha consentido expresamente en tal uso y no ha objetado tal consentimiento; y,

b) El consumidor en forma previa a su consentimiento ha sido informado, a satisfacción, de forma clara y precisa, sobre:
   1) Su derecho u opción de recibir la información en papel o por medios no electrónicos;
   2) Su derecho a objetar su consentimiento en lo posterior y las consecuencias de cualquier tipo al hacerlo, incluidas la terminación contractual o el pago de cualquier tarifa por dicha acción;
   3) Los procedimientos a seguir por parte del consumidor para retirar su consentimiento y para actualizar la información proporcionada; y,
   4) Los procedimientos para que, posteriormente al consentimiento, el consumidor pueda obtener una copia impresa en papel de los registros electrónicos y el costo de esta copia, en caso de existir.

Artículo 51.- Información al consumidor.- En la prestación de servicios electrónicos en el Ecuador, el consumidor deberá estar suficientemente informado de sus derechos y obligaciones, de conformidad con lo previsto en la Ley Orgánica de Defensa del Consumidor y su Reglamento.

Cuando se tratare de bienes o servicios a ser adquiridos, usados o empleados por medios electrónicos, el oferente deberá informar sobre todos los requisitos, condiciones y restricciones para que el consumidor pueda adquirir y hacer uso de los bienes o servicios promocionados.

La publicidad, promoción e información de servicios electrónicos, por redes electrónicas de información, incluida la Internet, se realizará de conformidad con la Ley, y su incumplimiento será sancionado de acuerdo al ordenamiento jurídico vigente en el Ecuador.

En la publicidad y promoción por redes electrónicas de información, incluida la Internet, se asegurará que el consumidor pueda acceder a toda la información disponible sobre un bien o servicio sin restricciones, en las mismas condiciones y con las facilidades disponibles para la promoción del bien o servicio de que se trate.

En el envío periódico de mensajes de datos con información de cualquier tipo, en forma individual o a través de listas de correo, directamente o mediante cadenas de mensajes, el emisor de los mismos deberá proporcionar medios expeditos para que el destinatario, en cualquier tiempo, pueda confirmar su suscripción o solicitar su exclusión de las listas, cadenas de mensajes o bases de datos, en las cuales se halle inscrito y que ocasionen el envío de los mensajes de datos referidos.

La solicitud de exclusión es vinculante para el emisor desde el momento de la recepción de la misma. La persistencia en el envío de mensajes periódicos no deseados de cualquier tipo, se sancionará de acuerdo a lo dispuesto en la presente Ley.

El usuario de redes electrónicas, podrá optar o no por la recepción de mensajes de datos que, en forma periódica, sean enviados con la finalidad de informar sobre productos o servicios de cualquier tipo.

CAPÍTULO IV - DE LOS INSTRUMENTOS PÚBLICOS

Artículo 52.- Instrumentos Públicos Electrónicos.- Se reconoce la validez jurídica de los mensajes de datos otorgados, conferidos, autorizados o expedidos por y ante autoridad competente y firmados electrónicamente.

Dichos instrumentos públicos electrónicos deberán observar los requisitos, formalidades y solemnidades exigidos por la Ley y demás normas aplicables.

TÍTULO IV - DE LA PRUEBA Y NOTIFICACIONES ELECTRÓNICAS

CAPÍTULO I - DE LA PRUEBA

Artículo 53.- Medios de prueba.- Los mensajes de datos, firmas electrónicas, documentos electrónicos y los certificados electrónicos nacionales o extranjeros, emitidos de conformidad con esta Ley, cualquiera sea su procedencia o generación, serán considerados medios de prueba. Para su valoración y efectos legales se observará lo dispuesto en el Código de Procedimiento Civil.

Artículo 54.- Presunción.- Cuando se presentare como prueba una firma electrónica certificada por una entidad de certificación de información acreditada, se presumirá que ésta reúne los requisitos determinados en la Ley, y que por consiguiente, los datos de la firma electrónica no han sido alterados desde su emisión y que la firma electrónica pertenece al signatario.

Artículo 55.- Práctica de la prueba.- La prueba se practicará de conformidad con lo previsto en el Código de Procedimiento Civil y observando las normas siguientes:

a) Al presentar un mensaje de datos dentro de un proceso judicial en los juzgados o tribunales del país, se deberá adjuntar el soporte informático y la transcripción en papel del documento electrónico, así como los elementos necesarios para su lectura y verificación, cuando sean requeridos.

b) En el caso de impugnación del certificado o de la firma electrónica por cualesquiera de las partes, el juez o tribunal, a petición de parte, ordenará a la entidad de certificación de información correspondiente, remitir a ese despacho los certificados de firma electrónica y documentos en los que se basó la solicitud del firmante, debidamente certificados.

c) El facsímil, será admitido como medio de prueba, siempre y cuando haya sido enviado y recibido como mensaje de datos, mantenga su integridad, se conserve y cumpla con las exigencias contempladas en esta Ley.

En caso de que alguna de las partes niegue la validez de un mensaje de datos, deberá probar, conforme a la Ley, que éste adolece de uno o varios vicios que lo invalidan, o que el procedimiento de seguridad, incluyendo los datos de creación y los medios utilizados para verificar la firma, no puedan ser reconocidos técnicamente como seguros.

Cualquier duda sobre la validez podrá ser objeto de comprobación técnica.

Artículo 56.- Valoración de la prueba.- La prueba será valorada bajo los principios determinados en la Ley y tomando en cuenta la seguridad y fiabilidad de los medios con los cuales se la envió, recibió, verificó, almacenó o comprobó si fuese el caso, sin perjuicio de que dicha valoración se efectúe con el empleo de otros métodos que aconsejen la técnica y la tecnología. En todo caso la valoración de la prueba se someterá al libre criterio judicial, según las circunstancias en que hayan sido producidos.

Para la valoración de las pruebas, el juez o árbitro competente que conozca el caso deberá designar los peritos que considere necesarios para el análisis y estudio técnico y tecnológico de las pruebas presentadas.

Artículo 57.- Notificaciones Electrónicas.- Todo el que fuere parte de un procedimiento judicial, designará el lugar en que ha de ser notificado, que no puede ser otro que el casillero judicial y/o el domicilio judicial electrónico en un correo electrónico, de un Abogado legalmente inscrito, en cualquiera de los Colegios de Abogados del Ecuador.

Las notificaciones a los representantes de las personas jurídicas del sector público y a los funcionarios del Ministerio Público que deben intervenir en los juicios, se harán en las oficinas que estos tuvieren o en el domicilio judicial electrónico en un correo electrónico que señalaren para el efecto.

TITULO V DE LAS INFRACCIONES INFORMÁTICAS

CAPÍTULO I - DE LAS INFRACCIONES INFORMATICAS

Artículo 58.- Infracciones Informáticas.- Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente Ley.

Reformas al Código Penal

Artículo 59.- **A continuación del Art. 202, inclúyanse los siguientes artículos innumerados:**

Artículo ....- El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica.

La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, será sancionada con pena de reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Si la divulgación o la utilización fraudulenta se realiza por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Artículo ...- Obtención y utilización no autorizada de Información.- La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica.

Artículo 60.- Sustitúyase el Art. 262 por el siguiente:

"Serán reprimidos con 3 a seis años de reclusión menor, todo empleado público y toda persona encargada de un servicio público, que hubiere maliciosa y fraudulentamente, destruido o suprimido documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, de que fueren depositarios, en su calidad de tales, o que les hubieren sido encomendados en razón de su cargo.

Artículo 61.- A continuación del Art. 353, agréguese el siguiente artículo innumerado:

Falsificación electrónica.- Son reos de falsificación electrónica la persona o 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:

1.- Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial;

2.- Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad;

3.- Suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieren hecho.

El delito de falsificación electrónica será sancionado de acuerdo a lo dispuesto en este capítulo.

Artículo 62.- A continuación del Art. 415 del Código Penal, inclúyanse los siguientes artículos innumerados:

Art.....- Daños informáticos.- El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica.

La pena de prisión será de tres a cinco años y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica, cuando se trate de programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, destinada a prestar un servicio público o vinculada con la defensa nacional.

Artículo Inmunerado.....- Si no se tratare de un delito mayor, la destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos, será reprimida con prisión de ocho meses a cuatro años y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica.

Artículo 63.- A continuación del artículo 553 del Código Penal, añádanse los siguientes artículos innumerados:

Art. Inn.- Apropiación Ilícita.- Serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos.

Art. Inn.- La pena será de prisión de uno a cinco años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica, si el delito se hubiere cometido empleando los siguientes medios:

1.- Inutilización de sistemas de alarma o guarda.

2.- Descubrimiento o descifrado de claves secretas o encriptadas.

3.- Utilización de tarjetas magnéticas o perforadas.

4.- Utilización de controles o instrumentos de apertura a distancia.

5.- Violación de seguridades electrónicas, informáticas u otras semejantes.

Artículo 64.- Añádase como segundo inciso del artículo 563 del Código Penal el siguiente:

Será sancionado con el máximo de la pena prevista en el inciso anterior y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, el que cometiere el delito utilizando medios electrónicos o telemáticos.

Artículo 65.- A continuación del numeral 19 del Art. 606 añádase el siguiente:
...Los que violaren el derecho a la intimidad, en los términos establecidos en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

DISPOSICIONES GENERALES

Primera.- Los certificados de firmas electrónicas, emitidos por entidades de certificación extranjeras y acreditados en el exterior, podrán ser revalidados en el Ecuador siempre que cumplan con los términos y condiciones exigidos por la Ley. La revalidación se realizará a través de una entidad de certificación de información acreditada que garantice en la misma forma que lo hace con sus propios certificados, dicho cumplimiento.

Segunda.- Las entidades de certificación de información acreditadas podrán prestar servicios de sellado de tiempo. Este servicio deberá ser acreditado técnicamente por el Consejo Nacional de Telecomunicaciones. El Reglamento de aplicación de la Ley recogerá los requisitos para este servicio.

Tercera.- Adhesión.- Ninguna persona está obligada a usar o aceptar mensajes de datos o firmas electrónicas, salvo que se adhiera voluntariamente en la forma prevista en esta Ley.

Cuarta.- No se admitirá ninguna exclusión restricción o limitación al uso de cualquier método para crear o tratar un mensaje de datos o firma electrónica, siempre que se cumplan los requisitos señalados en la presente Ley y su reglamento.

Quinta.- Se reconoce el derecho de las partes para optar libremente por el uso de tecnología y por el sometimiento a la jurisdicción que acuerden mediante convenio, acuerdo o contrato privado, salvo que la prestación de los servicios electrónicos o uso de estos servicios se realice de forma directa al consumidor.

Sexta.- El Consejo Nacional de Telecomunicaciones tomará las medidas necesarias, para que no se afecten los derechos del titular del certificado o de terceros, cuando se produzca la revocatoria del certificado, por causa no atribuible al titular del mismo.

Séptima.- La prestación de servicios de certificación de información por parte de entidades de certificación de información acreditadas, requerirá de autorización previa y registro.

Octava.- El ejercicio de actividades establecidas en esta ley, por parte de instituciones públicas o privadas, no requerirá de nuevos requisitos o requisitos adicionales a los ya establecidos, para garantizar la eficiencia técnica y seguridad jurídica de los procedimientos e instrumentos empleados.

Novena.- Glosario de Términos.- Para efectos de esta Ley, los siguientes términos serán entendidos conforme se definen en este artículo**:**

Mensaje de datos: Es toda información creada, generada, procesada, enviada, recibida, comunicada o archivada por medios electrónicos, que puede ser intercambiada por cualquier medio. Serán considerados como mensajes de datos, sin que esta enumeración limite su definición, los siguientes: documentos electrónicos, registros electrónicos, correo electrónico, servicios web, telegrama, télex, fax e intercambio electrónico de datos.

Red Electrónica de Información: Es un conjunto de equipos y sistemas de información interconectados electrónicamente.

Sistema de información: Es todo dispositivo físico o lógico utilizado para crear, generar, enviar, recibir, procesar, comunicar o almacenar, de cualquier forma, mensajes de datos.

Servicio Electrónico: Es toda actividad realizada a través de redes electrónicas de información.

Comercio Electrónico: Es toda transacción comercial realizada en parte o en su totalidad, a través de redes electrónicas de información.

Intimidad.- El derecho a la intimidad previsto en la Constitución Política de la República, para efectos de esta Ley, comprende también el derecho a la privacidad, a la confidencialidad, a la reserva, al secreto sobre los datos proporcionados en cualquier relación con terceros, a la no-divulgación de los datos personales y a no recibir información o mensajes no solicitados.

Datos personales: Son aquellos datos o información de carácter personal o íntimo, que son materia de protección en virtud de esta Ley.

Datos Personales Autorizados: Son aquellos datos personales que el titular ha accedido a entregar o proporcionar de forma voluntaria, para ser usados por la persona, organismo o entidad de registro que los solicita, solamente para el fin para el cual fueron recolectados, el mismo que debe constar expresamente señalado y ser aceptado por dicho titular.

Datos de creación.- Son los elementos confidenciales básicos y necesarios para la creación de una firma electrónica.

Certificado electrónico de información.- Es el mensaje de datos que contiene información de cualquier tipo.

Dispositivo electrónico: Instrumento físico o lógico utilizado independientemente para iniciar o responder mensajes de datos, sin intervención de una persona al momento de dicho inicio o respuesta.

Dispositivo de emisión.- Instrumento físico o lógico utilizado por el emisor de un documento para crear mensajes de datos o una firma electrónica.

Dispositivo de comprobación: Instrumento físico o lógico utilizado para la validación y autenticación de mensajes de datos o firma electrónica.

Emisor: Persona que origina un mensaje de datos.

Destinatario: Persona a quien va dirigido el mensaje de datos.

Signatario: Es la persona que posee los datos de creación de la firma electrónica, quién, o en cuyo nombre, y con la debida autorización se consigna una firma electrónica.

Desmaterialización electrónica de documentos: Es la transformación de la información contenida en documentos físicos a mensajes de datos.

Quiebra técnica: Es la imposibilidad temporal o permanente de la entidad de certificación de información, que impide garantizar el cumplimiento de las obligaciones establecidas en esta Ley y su reglamento.

Factura electrónica.- Conjunto de registros lógicos archivados en soportes susceptibles de ser leídos por equipos electrónicos de procesamiento de datos que documentan la transferencia de bienes y servicios, cumpliendo los requisitos exigidos por las Leyes Tributarias, Mercantiles y más normas y reglamentos vigentes.

Sellado de tiempo: Anotación electrónica firmada electrónicamente y agregada a un mensaje de datos en la que conste como mínimo la fecha, la hora y la identidad de la persona que efectúa la anotación.

DISPOSICIONES TRANSITORIAS

Primera.- Hasta que se dicte el reglamento y más instrumentos de aplicación de esta Ley, la prestación del servicio de sellado de tiempo, deberá cumplir con los requisitos de seguridad e inalterabilidad exigidos para la firma electrónica y los certificados electrónicos.

Segunda.- El cumplimiento del artículo 57 sobre las notificaciones al correo electrónico se hará cuando la infraestructura de la Función Judicial lo permita, correspondiendo al organismo competente de dicha función organizar y reglamentar los cambios que sean necesarios para la aplicación de esta Ley y sus normas conexas.

Para los casos sometidos a Mediación o Arbitraje por medios electrónicos, las notificaciones se efectuarán obligatoriamente en el domicilio judicial electrónico en un correo electrónico señalado por las partes.

DISPOSICIÓN FINAL

El Presidente de la República, en el plazo previsto en la Constitución Política de la República del Ecuador dictará el reglamento a la presente Ley.

La presente Ley entrará en vigencia a partir de su publicación en el Registro Oficial.

Dada en la cuidad de San francisco de Quito, Distrito Metropolitano, en la Sala de Sesiones del Pleno del Congreso Nacional del Ecuador a los veintisiete días del mes de febrero del año dos mil dos.

H. José Cordero Acosta
Presidente

Andrés Aguilar Moscoso
Secretario General

[5] D. PERÚ

LEY NO. 27269 SOBRE LEY DE FIRMAS Y CERTIFICADOS DIGITALES.

Promulgada el 26 de mayo de 2000. Publicada el 28 de mayo de 2000.

EL PRESIDENTE DE LA REPÚBLICA; 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 una firma manuscrita.

Artículo 2 - Ámbito 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 digital es 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 digital es 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 y a 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 un par de 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.

[5] Flag courtesy of www.theodora.com/flags used with permission

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.
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 es inexacta o ha 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 de 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. Las Entidades de Certificación podrán igualmente asumir las funciones de Entidades de Registro o Verificación.

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. El Poder Ejecutivo reglamentará la presente ley en un plazo de 60 (sesenta) días calendario, contados a partir de la vigencia de la presente ley.

DISPOSICIONES COMPLEMENTARIAS, TRANSITORIAS Y FINALES

PRIMERA.- Mientras se cree el Registro señalado en el artículo 15o, 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 TREVIÑO
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

LEY N° 27310 QUE MODIFICA EL ARTÍCULO 11° DE LA LEY N° 27269

EL PRESIDENTE DE LA REPÚBLICA

POR CUANTO:

EL CONGRESO DE LA REPÚBLICA
ha dado la Ley siguiente:

LEY QUE MODIFICA EL ARTÍCULO 11° DE LA LEY N° 27269

Artículo Único.- Objeto de la ley. Modifíquese el Artículo 11° de la Ley N° 27269, el mismo que quedará redactado de la siguiente manera:

"**Artículo 11.-** Los Certificados de Firmas Digitales emitidos por Entidades Extranjeras tendrán la misma validez y eficacia jurídica reconocidas en el presente Ley, siempre y cuando tales certificados sean reconocidos por la autoridad administrativa competente."

Comuníquese al señor Presidente de la República para su promulgación.

En Lima, a los veintiséis días del mes de junio del dos mil.

MARTHA HILDEBRANDT PÉREZ TREVIÑO
Presidenta del Congreso de la República

LUIS DELGADO APARICIO
Segundo 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 quince días del mes de julio del año dos mil.

ALBERTO FUJIMORI FUJIMORI
Presidente Constitucional de la República

ALBERTO BUSTAMANTE BELAUNDE
Presidente del Consejo de Ministros y Ministro de Justicia

REGLAMENTO DE LA LEY N° 27269 DE FIRMAS Y CERTIFICADOS DIGITALES. DECRETO SUPREMO No. 019-2002-JUS

TÍTULO I Normas Generales

CAPÍTULO I

Artículo 1 - Objeto. El presente Reglamento regula, para el sector público y privado, la utilización de firmas electrónicas en mensaje de datos y documentos electrónicos, generadas bajo la Infraestructura Oficial de Firma Electrónica comprendiendo el régimen de acreditación y supervisión de las entidades de certificación, así como de las entidades de registro o verificación, establecidas en la Ley N° 27269 -Ley de Firmas y Certificados Digitales-, modificada en su artículo 11° por la Ley 27310, en adelante se denominará "la Ley".

Cuando en el Reglamento se haga referencia a la Ley, debe entenderse referida a la Ley No. 27.269, Ley de Firmas y Certificados Digitales. Cuando se mencione el Reglamento debe entenderse referido al presente Reglamento, de la Ley No. 27.269.

Las firmas electrónicas aprobadas por la autoridad administrativa competente, tienen, desde su aprobación los mismos efectos que las firmas generadas bajo la Infraestructura Oficial de Firma Electrónica conforme a lo establecido en el Reglamento.

Artículo 2 - Principio de la autonomía de la voluntad. Las disposiciones contenidas en el presente Reglamento no restringen la autonomía privada para el uso de otras firmas electrónicas generadas fuera de la Infraestructura Oficial de Firmas Electrónicas.

Artículo 3 - Régimen de servicios de certificación. La prestación de servicios de certificación así como los de registro o verificación se realiza en el régimen de libre competencia.

Artículo 4 - Definiciones. Para efectos del presente Reglamento, entiéndase por:

*Acreditación***.-** Proceso a través del cual la autoridad administrativa competente, previo cumplimiento de las exigencias establecidas en la Ley, faculta a las entidades solicitantes reguladas en el Reglamento a prestar los servicios solicitados en el marco de la Infraestructura Oficial de Firma Electrónica.

Agente automatizado.- Procesos y equipos programados para atender requerimientos predefinidos y dar una respuesta automática sin intervención humana.

Algoritmo.- Conjunto ordenado y finito de operaciones matemáticas que permiten hallar la solución a un problema.

Autenticación.- Proceso técnico que permite determinar la identidad de la persona que emite un mensaje de datos firmado electrónicamente, vinculándolo con dicho mensaje; este proceso no otorga certificación notarial ni fe pública.

Autoridad Administrativa Competente.- Organismo público responsable de acreditar a las entidades de certificación y a las entidades de registro o verificación, de reconocer los estándares tecnológicos aplicables en la Infraestructura Oficial de Firma Electrónica, de supervisar dicha Infraestructura, así como la reglamentación y prestación de servicios de valor añadido relacionados con la misma y las otras funciones señaladas en el Reglamento o aquellas que requiera en el transcurso de sus operaciones.

Certificado digital.- Documento electrónico generado y firmado digitalmente por una entidad de certificación el cual vincula un par de claves con una persona natural o jurídica confirmando su identidad.

Certificación cruzada.- Acto por el cual una entidad de certificación acreditada reconoce la corrección y validez de un certificado digital emitido por otra entidad de certificación, sea nacional, extranjera o internacional, previa autorización de la autoridad administrativa competente; y asume tal certificado como si fuera de propia emisión, bajo su responsabilidad.

Clave privada.- En un sistema de criptografía asimétrica, es aquella que se emplea para generar una firma digital sobre un mensaje de datos y es mantenida en reserva por el titular de la firma digital.

Clave pública.- En un sistema de criptografía asimétrica, es aquella usada por el receptor de un mensaje de datos para verificar la firma digital puesta en dicho mensaje y que puede ser conocida por cualquier persona.

Código de verificación.- Secuencia de "bits" de longitud fija obtenida como resultado de procesar un mensaje de datos con un algoritmo, de tal manera que: (1) El mensaje de datos produzca siempre el mismo código de verificación cada vez que se le aplique dicho algoritmo. (2) Sea improbable, a través de medios técnicos, que el mensaje de datos pueda ser derivado o reconstruido a partir del código de verificación producido por el algoritmo. (3) Sea improbable que, por medios técnicos, se pueda encontrar dos mensajes de datos que produzcan el mismo código de verificación al usar el mismo algoritmo.

Criptografía asimétrica.- Es una técnica basada en el uso de un par de claves únicas; una clave privada y una clave pública relacionadas matemáticamente entre sí de tal manera que una no pueda operar sin la otra y de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave privada.

Declaración de Prácticas de Certificación.- Conjunto de políticas y procedimientos que sigue una entidad de certificación para la prestación de sus servicios.

Declaración de Prácticas de registro y verificación.- Documento oficialmente presentado por una Entidad de Registro o Verificación a la Autoridad Administrativa Competente, mediante la cual define sus Prácticas de Registro y Verificación.

Depósito de certificados digitales.- Sistema de almacenamiento y recuperación de certificados digitales, así como de la información relativa a éstos, disponible por medios telemáticos.

Destinatario.- Persona designada por el emisor para recibir un mensaje de datos o un documento electrónico, siempre y cuando no actúe a título de intermediario.

Documento Electrónico.- Conjunto de datos basados en bits o impulsos electromagnéticos, elaborados, generados, transmitidos, comunicados y archivados a través de medios electrónicos, ópticos o cualquier otro análogo.

Entidad de Certificación.- Persona jurídica que presta servicios de emisión, gestión, cancelación u otros servicios inherentes a la certificación digital. Asimismo, puede asumir las funciones de registro o verificación.

Entidad de Registro o Verificación.- Persona jurídica encargada del levantamiento de datos, la comprobación de éstos respecto a un solicitante de certificado digital, la identificación y autenticación del suscriptor de una firma digital, la aceptación y autorización de las solicitudes para la emisión de certificados digitales, así como de la aceptación y autorización de las solicitudes de cancelación de certificados digitales.

Estándares Técnicos Internacionales.- Requisitos de orden técnico y de uso internacional que deben observarse en las Prácticas de Certificación para garantizar el intercambio de claves públicas, y la emisión de firmas y certificados digitales, mediante criptografía asimétrica.

Estándares Técnicos Nacionales.- Estándares técnicos aprobados mediante Normas Técnicas Peruanas por la Comisión de Reglamentos Técnicos y Comerciales – CRT del INDECOPI, en su calidad de Organismo Nacional de Normalización.

Firma digital.- Aquella firma electrónica que utiliza una técnica de criptografía asimétrica y que tiene la finalidad de asegurar la integridad del mensaje de datos a través de un código de verificación, así como la vinculación entre el titular de la firma digital y el mensaje de datos remitido.

Firma electrónica.- Cualquier símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención precisa de vincularse, autenticar y garantizar la integridad de un documento electrónico o un mensaje de datos cumpliendo todas o algunas de las funciones características de una firma manuscrita. Se incluye dentro de esta definición a la firma o signatura informática.

Reconocimiento.- Proceso a través del cual la autoridad administrativa competente, equipara y reconoce oficialmente a las entidades de certificación extrajeras.

Infraestructura Oficial de Firma Digital.- Sistema confiable, acreditado, regulado, y supervisado por la autoridad administrativa competente en el marco de la Infraestructura Oficial de Firma Electrónica mediante el uso de tecnología de firma digital, en la que participan entidades de certificación y entidades de registro o verificación acreditadas ante la autoridad administrativa competente.

Infraestructura Oficial de Firma Electrónica.- Sistema confiable, acreditado, regulado, y supervisado por la autoridad administrativa competente constituido por programas, equipos, estándares, políticas, procesos, procedimientos u otros recursos que permiten la generación de firmas electrónicas y que garantizan la autenticación e integridad de los documentos electrónicos.

Iniciador.- Persona que haya actuado por su cuenta o a cuyo nombre se haya actuado para enviar o generar un mensaje de datos antes de ser archivado, pero que no haya actuado a título de intermediario.

Integridad.- Característica que indica que un mensaje de datos o un documento electrónico no han sido alterados desde la transmisión por el emisor hasta su recepción por el destinatario.

Medios Telemáticos.- Conjunto de bienes y elementos técnicos informáticos que en unión con las telecomunicaciones permiten la generación, procesamiento, transmisión, comunicación y archivo de datos e información.

Mensaje de datos.- Es la información generada, transmitida, recibida, archivada, comunicada por medios electrónicos, ópticos o cualquier otro análogo; tales como, el Intercambio Electrónico de Datos (EDI, por sus siglas en inglés), el correo electrónico, el telegrama, el télex, el telefax, entre otros.

Neutralidad Tecnológica.- Principio que fomenta la creación y uso de diversas tecnologías, sin preferir, restringir, ni discriminar a ninguna de ellas.

Par de claves.- En un sistema de criptografía asimétrica, comprende una clave privada y su correspondiente clave pública, ambas asociadas matemáticamente.

Servicio de Valor Añadido.- Servicio complementario a las funciones de certificación, verificación o registro al interior de la Infraestructura Oficial de Firma Electrónica.

Tiempo Universal Coordinado (UTC).- Hora relacionada con el Meridiano de *Greenwich*.

Titular de certificado digital.- Persona natural o jurídica a quien se le atribuye de manera exclusiva un certificado digital.

Titular de firma digital.- Persona natural a quien se le vincula de manera exclusiva con un mensaje de datos firmado digitalmente utilizando su clave privada.

Por excepción, en el caso de firmas digitales generadas a través de agentes automatizados, se considera titular de la firma digital a la persona natural o jurídica titular del certificado digital a partir del cual se generan dichas firmas digitales.

CAPÍTULO II VALIDEZ Y EFECTOS JURÍDICOS DE LAS FIRMAS Y DOCUMENTOS ELECTRÓNICOS

Artículo 5 - Firmas en la Infraestructura Oficial de Firma Electrónica. Toda firma electrónica añadida o asociada lógicamente a un mensaje de datos y generada bajo la Infraestructura Oficial de Firma Electrónica, cumple con lo dispuesto en la Ley y el Reglamento.

Artículo 6 - Validez de las firmas electrónicas. Para efectos de la manifestación de voluntad, las firmas electrónicas añadidas o asociadas lógicamente a un mensaje de datos o a un documento electrónico y generadas fuera de la Infraestructura Oficial de Firma Electrónica tendrán la misma validez y eficacia jurídica que las firmas manuscritas, siempre que sean acreditadas o reconocidas por la autoridad administrativa competente.

Artículo 7 - Documentos Firmados Electrónicamente como medio de prueba. Las firmas electrónicas así como los mensajes de datos y documentos firmados electrónicamente podrán ser admitidos como prueba en toda clase de procesos o procedimientos. El juez podrá solicitar a la autoridad administrativa competente el nombramiento de un perito especializado en firmas electrónicas.

Artículo 8 - Presunciones acerca de las firmas electrónicas bajo la Infraestructura Oficial de Firma Electrónica. Tratándose de mensajes de datos o documentos firmados electrónicamente con firmas generadas bajo la Infraestructura Oficial de Firma Electrónica, se presume que el documento o mensaje de datos fue firmado por su titular de manera tal que identifica y vincula al firmante, y garantiza la autenticidad e integridad del mismo.

Las disposiciones y presunciones del Reglamento no excluyen el cumplimiento de las formalidades específicas requeridas para los actos jurídicos y el otorgamiento de fe pública.

Artículo 9 – Tecnología de firmas electrónicas al interior de la Infraestructura Oficial de Firma Electrónica La Infraestructura Oficial de Firma Electrónica se puede basar en la siguiente tecnología de firmas electrónicas:

a) Tecnología de firmas digitales, sobre la cual se basa la Infraestructura Oficial de Firma Digital.

b) Otras tecnologías de firmas electrónicas que sean aprobadas por la autoridad administrativa competente de acuerdo con el principio de neutralidad tecnológica.

Artículo 10 - Conservación de documentos electrónicos. Cuando el usuario lo solicite o la legislación exija que los documentos, registros o informaciones requieran de una formalidad adicional para la conservación de mensajes de datos o documentos electrónicos firmados electrónicamente, deberá cumplirse con lo siguiente:

a) Que sean accesibles para su posterior consulta.

b) Que sean conservados con su formato original de generación, envío, recepción u otro formato que reproduzca en forma demostrable la exactitud e integridad del contenido digital o electrónico.

c) Que sea conservado todo dato que permita determinar el origen, destino, fecha y hora del envío y recepción, en concordancia con lo establecido en el Decreto Legislativo No. 681 y sus normas complementarias.

Cuando los documentos y mensajes de datos firmados electrónicamente sean conservados mediante microformatos y almacenados en microarchivos, se sujetarán a lo dispuesto por el Decreto Legislativo N. 681 y sus normas modificatorias y reglamentarias. El notario o federatario responsable, que cuente con certificado o diploma de idoneidad técnica, certifica el cumplimiento de los requisitos establecidos en el presente artículo.

TÍTULO II - DE LA INFRAESTRUCTURA OFICIAL DE FIRMA DIGITAL

CAPÍTULO I - ASPECTOS GENERALES

Artículo 11 - Elementos de la Infraestructura Oficial de Firma Digital. La Infraestructura Oficial de Firma Digital está constituida por:

a) Prácticas de certificación basadas en estándares internacionales o compatibles a los empleados internacionalmente, de acuerdo con lo establecido por la autoridad administrativa competente.

b) El soporte lógico o conjunto de instrucciones para los equipos de cómputo y comunicaciones, los elementos físicos y demás componentes adecuados a los procedimientos de certificación y a las condiciones de seguridad adicionales, comprendidas en los estándares señalados en el literal a).

c) Personal competente para la conducción de los procedimientos de certificación y el mantenimiento de la Infraestructura Oficial de Firma Digital.

d) 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.

e) autoridad administrativa competente, así como entidades de certificación y entidades de registro o verificación debidamente acreditadas o reconocidas.

Artículo 12 - Estándares aplicables bajo la Infraestructura Oficial de Firma Digital. Las prácticas de certificación comprendidas en la Infraestructura Oficial de Firma Digital deben estar basados sobre los estándares técnicos internacionales vigentes que aseguren la interoperabilidad y las funciones exigidas en la Ley como en el Reglamento.

La autoridad administrativa competente determinará los estándares compatibles aplicando el principio de neutralidad tecnológica con la necesidad de cumplir los requisitos mencionados en el párrafo anterior.

CAPÍTULO II - DE LA FIRMA DIGITAL

Artículo 13 - Firmas digitales generadas bajo la Infraestructura Oficial. Las Firmas digitales que gozan de las presunciones establecidas en los artículos 6° y 8° del Reglamento son las generadas a partir de certificados digitales:

a) Emitidos conforme a lo dispuesto en el Reglamento por entidades de certificación acreditadas ante la autoridad administrativa competente.

b) Incorporados a la Infraestructura Oficial de Firma Digital bajo acuerdos de certificación cruzada, conforme al artículo 49° del Reglamento.

c) Reconocidos al amparo de acuerdos de reconocimiento mutuo suscritos por la autoridad administrativa competente conforme al artículo 47º del Reglamento.

d) Emitidos por entidades de certificación extranjeras que hayan sido incorporados a la Infraestructura Oficial de Firma Digital conforme al artículo 48° del Reglamento.

Artículo 14 - Características de la firma digital. Las características mínimas de la firma digital generadas bajo la Infraestructura Oficial de Firma Digital son:

a) Se genera al cifrar el código de verificación de un mensaje de datos usando la clave privada del titular del certificado digital.

b) Es única al titular de la firma digital y a cada mensaje de datos firmado por éste.

c) Es susceptible de ser verificada usando la clave pública del titular de la firma digital.

d) Su generación está bajo el control exclusivo del titular de la firma digital.

e) Está añadida o asociada lógicamente al mensaje de datos de tal manera que es posible detectar si la firma digital o el mensaje de datos ha sido alterado.

Artículo 15 - Funciones de la firma digital. Dadas las características señaladas en el artículo anterior, técnicamente la firma digital debe garantizar:

a) Que el mensaje de datos fuera firmado con la clave privada del titular de la firma digital.

b) La integridad del mensaje de datos firmado digitalmente, dado que cualquier alteración en el mensaje de datos o en la firma digital puede ser detectada.

c) Que el titular de la firma digital no pueda repudiar o desconocer un mensaje de datos que ha sido firmado digitalmente usando su clave privada, dado que ésta se mantiene bajo su control exclusivo.

Artículo 16 - Del titular de la firma digital. Dentro de la Infraestructura Oficial de Firma Digital, la responsabilidad sobre los efectos jurídicos generados por la utilización de una firma digital corresponde al titular del certificado digital.

Tratándose de personas naturales, éstas son titulares del certificado y de las firmas digitales que se generen a partir de aquél, incluyendo las firmas digitales que genere a través de agentes automatizados.

En el caso de personas jurídicas, son éstas las titulares del certificado digital, y sus representantes los titulares de la firma digital, con excepción de las **f**rmas digitales que se generen a través de agentes automatizados, situación en la cual las personas jurídicas son titulares del certificado y las firmas digitales generadas a partir de éstos.

Artículo 17 - Obligaciones del titular de la firma digital. Las obligaciones del titular de la firma digital son:

a) Entregar información veraz bajo su responsabilidad.

b) Generar la clave privada y firmar digitalmente mediante los procedimientos señalados por la entidad de certificación;

c) Mantener el control y la reserva de la clave privada bajo su responsabilidad.

d) Observar las condiciones establecidas por la entidad de certificación para la utilización del certificado digital y la generación de firmas digitales.

Artículo 18 - Invalidez de la firma digital. Una firma digital generada bajo la Infraestructura Oficial de Firma Digital pierde validez si es utilizada:

a) En fines distintos para el que fue extendido el certificado digital.

b) Cuando el certificado haya sido cancelado conforme a lo establecido en el Capítulo IV del Título.

CAPÍTULO III - DEL CERTIFICADO DIGITAL

Artículo 19 - Requisitos para obtener un certificado digital. Para la obtención de un certificado digital el solicitante deberá acreditar lo siguiente:

a) Tratándose de personas naturales, tener plena capacidad de ejercicio de sus derechos civiles.

b) Tratándose de personas jurídicas, acreditar la existencia de la misma y su vigencia mediante instrumentos públicos o norma legal respectivos.

Artículo 20 - Especificaciones adicionales para ser titular de un certificado digital. Para ser titular de un certificado digital adicionalmente se deberá cumplir con:

Entregar la información solicitada por la entidad de certificación o la entidad de registro o verificación, asumiendo responsabilidad por la veracidad y exactitud de la información proporcionada, sin perjuicio de la respectiva comprobación.

En el caso de personas naturales, la solicitud del certificado digital y el registro o verificación de su identidad son estrictamente personales. La persona natural solicitante se constituirá en titular del certificado digital y de las firmas digitales que se generen.

Para el caso de personas jurídicas, la solicitud del certificado digital del cual ésta será titular y el registro o verificación de su identidad deben ser realizados a través de un representante debidamente acreditado. Conjuntamente con la solicitud debe indicarse el representante, persona natural, al cual se le asignará la facultad de generar y usar la clave privada, señalando para tal efecto las atribuciones y los poderes de representación correspondientes. Dicha persona natural será el titular de las firmas digitales. Tratándose de certificados digitales solicitados por personas jurídicas para su utilización a través de agentes automatizados, la titularidad del certificado digital y de las firmas digitales generadas a partir de dicho certificado digital corresponderá a la persona jurídica. La atribución de responsabilidad, para tales efectos, corresponde al representante legal, que en nombre de la persona jurídica solicita el certificado digital.

Artículo 21 - Procedimiento para ser titular de un certificado digital. Para el caso de personas naturales, éstas deberán presentar una solicitud a la entidad de registro o verificación, según sea el caso; dicha solicitud deberá estar acompañada de toda la información requerida por la declaración de prácticas de certificación o en los procedimientos declarados. La entidad de registro o verificación deberá comprobar la identidad del solicitante a través de su documento oficial de identidad. La entidad de certificación cumplirá con lo dispuesto en el presente artículo, en el supuesto previsto en el segundo párrafo del Artículo 12 de la Ley.

En el caso de una persona jurídica, la solicitud deberá ser presentada por la persona facultada para tal fin, debiendo acreditar la existencia y vigencia de la persona jurídica mediante los instrumentos públicos o norma legal respectiva, así como las facultades del representante. Asimismo, deberá presentar toda la información requerida por la declaración de prácticas de la entidad correspondiente.

Artículo 22 - Obligaciones del titular de certificado digital.

a) Actualizar permanentemente la información proveída tanto a la entidad de certificación como a la entidad de registro o verificación, asumiendo responsabilidad por la veracidad y exactitud de ésta.

b) Solicitar de inmediato la cancelación de su certificado digital en caso de que la reserva sobre la clave privada se haya visto comprometida, bajo responsabilidad.

c) Observar permanentemente las condiciones establecidas por la entidad de certificación para la utilización del certificado digital.

Artículo 23 - Contenido del certificado digital. Los certificados digitales emitidos dentro de la Infraestructura Oficial de Firma Digital deberán contener como mínimo lo establecido en el artículo 7° de la Ley.

La entidad de certificación podrá incluir, a pedido del solicitante del certificado digital, información adicional siempre y cuando la entidad de registro o verificación compruebe fehacientemente la veracidad de ésta.

Artículo 24 - Periodo de vigencia. El periodo de vigencia de los certificados digitales comienza y finaliza en las fechas indicadas en él, salvo en los supuestos de cancelación conforme al artículo 9º de la Ley.

CAPÍTULO IV - DE LA CANCELACIÓN DE CERTIFICADOS DIGITALES

Artículo 25 - Causales de cancelación del certificado digital.

a) Por solicitud del titular sin previa justificación, siendo necesaria para tal efecto la aceptación y autorización de la entidad de certificación o la entidad de registro o verificación, según sea el caso. La misma que deberá ser aceptada y autorizada como máximo dentro del plazo establecido por la autoridad administrativa competente, si en el plazo indicado la entidad no se pronuncia, se entenderá la cancelación del certificado; la misma que no podrá ser opuesta al tercero de buena fé.

b) Por revocatoria de la entidad de certificación que lo emitió.

c) Por expiración del plazo de vigencia.

d) Por el cese de operaciones de la entidad de certificación que lo emitió.

e) Por resolución administrativa o judicial que lo ordene.

f) Por interdicción civil judicialmente declarada, declaración de ausencia o de muerte presunta, del titular del certificado digital.

g) Por extinción de la personería jurídica o declaración judicial de quiebra.

h) Otras causales que establezca la autoridad administrativa competente.

Artículo 26 - Cancelación del certificado digital a solicitud de su titular. La solicitud de cancelación de un certificado digital puede ser realizada por su titular o a través de un representante debidamente acreditado; pudiendo realizarse mediante documento electrónico firmado digitalmente, de acuerdo con los procedimientos definidos en cada caso por las entidades de certificación.

El titular del certificado digital está obligado, bajo responsabilidad, a solicitar la cancelación al tomar conocimiento de la ocurrencia de alguna de las siguientes circunstancias:

a) Por exposición, puesta en peligro o uso indebido de la clave privada.

b) Por deterioro, alteración o cualquier otro hecho u acto que afecte la clave privada.

Artículo 27 - Cancelación por revocación. Para efectos de la cancelación de oficio o revocación de certificados digitales, la entidad de certificación debe contar con procedimientos detallados en su declaración de prácticas de certificación.

La revocación también puede ser solicitada por un tercero que informe fehacientemente de alguno de los supuestos de revocación contenidos en los numerales 1) y 2) del artículo 10° de la Ley.

La revocación debe indicar el momento desde el cual se aplica, precisando como mínimo la fecha y el tiempo del mismo, que deberá estar expresado en minutos y segundos. La revocación no puede ser aplicada retroactivamente y debe ser notificada al titular del certificado digital. La entidad de certificación debe inmediatamente incluir la revocación del certificado en la relación que corresponda.

CAPÍTULO V - DE LA ENTIDAD DE CERTIFICACIÓN

Artículo 28 - De las funciones de la Entidad de Certificación. Las entidades de certificación tienen las siguientes funciones:

a) Emitir certificados digitales manteniendo su numeración correlativa.

b) Cancelar certificados digitales.

c) Gestionar certificados digitales emitidos en el extranjero.

d) Adicionalmente a las anteriores, las señaladas en el artículo 32° del Reglamento, en caso opten por asumir las funciones de entidad de registro o verificación.

Las entidades de certificación podrán brindar otros servicios inherentes a los de certificación, cuyas características y procedimientos estarán contenidos en su declaración de prácticas de certificación.

Artículo 29 - De las obligaciones de la Entidad de Certificación. Las entidades de certificación tienen las siguientes obligaciones:

a) Cumplir con su declaración de prácticas de certificación.

b) Informar a los usuarios todas las condiciones de emisión y de uso de sus certificados digitales, incluyendo las referidas a la cancelación de éstos.

c) Mantener el control y la reserva de la clave privada que emplea para firmar los certificados digitales que emite, bajo responsabilidad.

d) Mantener depósito de los certificados digitales emitidos y cancelados, consignando su fecha de emisión y vigencia.

e) Publicar permanente e ininterrumpidamente por medios telemáticos la relación de los certificados digitales emitidos y cancelados.

f) Cancelar el certificado digital a solicitud de su titular o, de ser el caso, a solicitud del titular de la firma digital; o cuando advierta que la información contenida en el certificado digital fuera inexacta o hubiera sido modificada, o que el titular incurriera en alguna de las causales previstas en el artículo 25° del Reglamento.

g) Mantener la confidencialidad de la información relativa a los solicitantes y titulares de certificados digitales, limitando su empleo a las necesidades propias del servicio de certificación, salvo orden judicial o pedido expreso del titular del certificado digital.

h) Brindar todas las facilidades al personal autorizado por la autoridad administrativa competente para efectos de supervisión y auditoría.

i) Mantener la información relativa a los certificados digitales que hubieren sido cancelados, por un período mínimo de diez (10) años a partir de su cancelación.

j) Cumplir los términos bajo los cuales obtuvo la acreditación, así como los requerimientos adicionales que establezca la autoridad administrativa competente conforme a lo establecido en el Reglamento.

k) Informar y solicitar autorización a la autoridad administrativa competente para realizara acuerdos de certificación cruzada que proyecte celebrar, así como los términos bajo los cuales dichos acuerdos se suscribirían.

l) Informar y solicitar autorización a la autoridad administrativa competente para efectos del reconocimiento de certificados emitidos por entidades extranjeras.

m) Cumplir sus funciones dentro de los plazos señalados en su declaración de prácticas de certificación.

n) Contratar los seguros o garantías bancarias necesarias que permitan indemnizar al titular por los daños que pueda ocasionar como resultado de las actividades de certificación.

Artículo 30 - Respaldo financiero. Las entidades de certificación acreditadas deberán contar con el respaldo económico suficiente para operar bajo la Infraestructura Oficial de Firma Digital, así como para afrontar el riesgo de responsabilidad por daños, de conformidad con lo dispuesto en la Ley y el Reglamento. La autoridad administrativa competente definirá los criterios para evaluar el cumplimiento de este requisito.

Artículo 31 - Del cese de operaciones de la Entidad de Certificación. La entidad de certificación cesa sus operaciones en el marco de la Infraestructura Oficial de Firma Digital, en los siguientes casos:

a) Por decisión unilateral comunicada ante la autoridad administrativa competente, asumiendo la responsabilidad del caso por dicha decisión.
b) Por extinción de su personería jurídica.
c) Por revocación de su registro.
d) Por disposición de la autoridad administrativa competente.
e) Por resolución judicial.
f) Por liquidación, decidida por la junta de acreedores en el marco de la legislación concursal, o resolución judicial de quiebra.

Para los supuestos contemplados en los incisos a) y b) la autoridad administrativa competente establecerá el plazo en el cual las entidades de certificación notificarán tanto a aquélla como a los titulares de certificados digitales el cese de sus actividades. La autoridad administrativa competente deberá adoptar las medidas necesarias para preservar las obligaciones contenidas en los incisos d), g) e i) del artículo 29° del Reglamento.

La autoridad administrativa competente reglamentará los procedimientos para hacer público el cese de operaciones de las entidades de certificación.

Los certificados digitales emitidos por una entidad de certificación cuyas operaciones han cesado deben ser cancelados a partir del día, hora, minuto y segundo en que se aplica el cese. El uso de certificados digitales con posterioridad a su cancelación implica la pérdida de las presunciones descritas en los artículos 6° y 8° del Reglamento.

CAPÍTULO VI - DE LA ENTIDAD DE REGISTRO O VERIFICACIÓN

Artículo 32- De las funciones de la Entidad de Registro o Verificación. Las entidades de registro o verificación tienen las siguientes funciones:

a) Identificar al solicitante del certificado digital mediante el levantamiento de datos y la comprobación de la información brindada por aquél.

b) Aceptar, autorizar según sea el caso, la conformidad de las solicitudes de emisión, modificación o cancelación de certificados digitales, comunicándolo a la entidad de certificación bajo responsabilidad.

Artículo 33 - De las obligaciones de la Entidad de Registro o Verificación. Las entidades de registro o verificación acreditadas tienen las siguientes obligaciones:

a) Cumplir los procedimientos declarados para la prestación del servicio.

b) Determinar objetivamente y en forma directa la veracidad de la información proporcionada por el solicitante de certificado digital bajo responsabilidad.

c) Mantener la confidencialidad de la información relativa a los solicitantes y titulares de certificados digitales limitando su empleo a las necesidades propias del servicio de registro o verificación, salvo orden judicial o pedido expreso del titular del certificado digital.

d) Recoger únicamente información o datos personales de relevancia para la emisión de los certificados.

e) Informar y solicitar autorización a la autoridad administrativa, especialmente en el supuesto previsto en el artículo 48º del Reglamento.

f) Acreditar domicilio en el Perú.

g) Contratar los seguros necesarios que le permitan indemnizar por los daños que puedan ocasionar como resultado de las actividades de registro o verificación.

Artículo 34 - Respaldo financiero. Las entidades de registro o verificación acreditada deberán contar con el respaldo económico suficiente para operar bajo la Infraestructura Oficial de Firma Digital; así como para afrontar el riesgo de responsabilidad por daños, de conformidad con lo dispuesto en la Ley y por el Reglamento. La autoridad administrativa competente definirá los criterios para evaluar el cumplimiento de este requisito.

Artículo 35 - Del cese de operaciones de la entidad de registro o verificación. La entidad de registro o verificación cesa de operar en el marco de la Infraestructura Oficial de Firma Digital:

a) Por decisión unilateral comunicada ante la autoridad administrativa competente, asumiendo la responsabilidad del caso por dicha decisión.

b) Por extinción de su personería jurídica.

c) Por revocación de su registro.

d) Por sanción dispuesta por la autoridad administrativa competente.

e) Por orden judicial.

f) Por liquidación, decidida por la junta de acreedores en el marco de la legislación concursal, o resolución judicial de quiebra.

Para los supuestos contenidos en los incisos a) y b), la entidad de registro o verificación debe notificar el cese de sus actividades a la autoridad administrativa competente con una anticipación mínima que será

establecida por ésta, debiendo dejar constancia ante aquélla de los mecanismos utilizados para preservar el cumplimiento de lo dispuesto en el inciso c) del artículo 33º del Reglamento.

TÍTULO III - DE LA AUTORIDAD ADMINISTRATIVA COMPETENTE

CAPÍTULO I - FUNCIONES DE LA AUTORIDAD ADMINISTRATIVA COMPETENTE

Artículo 36 – Designación y funciones. Conforme a lo establecido en el Artículo 15 de la Ley, se designa al Instituto Nacional de Defensa de la Competencia y la Protección de la Propiedad Intelectual (INDECOPI) como la autoridad administrativa competente. La autoridad administrativa competente tiene las siguientes funciones:

a) Aprobar la política de certificación y las declaraciones de prácticas de certificación.

b) Acreditar entidades de certificación nacionales y reconocer a las entidades de certificación extranjeras.

c) Acreditar entidades de registro o verificación.

d) Supervisar a las entidades de certificación y a las entidades de registro o verificación, estableciendo de ser el caso las sanciones correspondientes.

e) Cancelar las acreditaciones otorgados a las entidades de certificación y a las entidades de registro o verificación conforme a lo dispuesto en el Reglamento.

f) Publicar ininterrumpidamente la relación de entidades acreditadas.

g) Aprobar el empleo de estándares técnicos internacionales dentro de la Infraestructura Oficial de Firma Electrónica y determinar la compatibilidad de otros estándares técnicos con los estándares internacionales.

h) Formular los criterios para el establecimiento de la idoneidad técnica que deberán cumplir quienes presten servicios en las materias reguladas por la Ley y el Reglamento, así como aquellas relacionadas con la prevención y solución de conflictos.

i) Establecer los requisitos mínimos para la prestación de los servicios de certificación y los servicios de registro o verificación.

j) Impulsar la solución de conflictos por medio de la conciliación y el arbitraje.

k) Definir los criterios para evaluar la suficiencia del respaldo financiero con el que deben contar las entidades de certificación y las entidades de registro o verificación.

l) Aprobar la utilización de otras tecnologías de firmas electrónicas distintas a las firmas digitales, previa verificación del cumplimiento de los requisitos establecidos en el artículo 2º de la Ley y regular su utilización al interior de la Infraestructura Oficial de Firma Electrónica.

m) Suscribir acuerdos de reconocimiento mutuo con autoridades administrativas extranjeras que cumplan funciones similares a las de la autoridad administrativa competente.

n) Autorizar la realización de certificaciones cruzadas con entidades de certificación extranjeras.

o) Delegar a terceros bajo sus órdenes y responsabilidad las funciones que determine.

p) Fomentar y coordinar el uso y desarrollo de la Infraestructura oficial de firma electrónica al interior de las entidades del sector público nacional.

q) Aprobar y regular los servicios de valor añadido al interior de la Infraestructura Oficial de Firma Electrónica.

r) Las demás que sean necesarias para el buen funcionamiento de la Infraestructura Oficial de Firma Electrónica.

CAPÍTULO II - RÉGIMEN DE ACREDITACIÓN DE ENTIDADES DE CERTIFICACIÓN Y DE LAS ENTIDADES DE REGISTRO O VERIFICACIÓN

Artículo 37 - Acreditación de Entidades de Certificación. Las entidades que soliciten su acreditación como entidades de certificación ante la autoridad administrativa competente deben contar con los elementos de la Infraestructura Oficial de Firma Digital señalados en los incisos a), b), c) y d) del artículo 11°, y someterse al procedimiento de evaluación comprendido en el artículo 41° del Reglamento.

Cuando alguno de los elementos señalados en el párrafo precedente sea administrado por un tercero, la entidad solicitante deberá demostrar su vinculación con aquél, asegurando la viabilidad de sus servicios bajo

dichas condiciones, y la disponibilidad de estos elementos para la evaluación y supervisión que la autoridad administrativa competente considere necesarias. La autoridad administrativa competente, de ser el caso, precisará los términos bajo los cuales se rigen estos supuestos del servicio de certificación.

Artículo 38 - Presentación de la solicitud de acreditación de Entidad de Certificación. La solicitud de acreditación de entidades de certificación debe presentarse a la autoridad administrativa competente, observando lo dispuesto en el artículo anterior y adjuntando lo siguiente:

a) Acreditación de la existencia y vigencia de la persona jurídica mediante los instrumentos públicos o norma legal respectivos, así como las facultades del representante.

b) Acreditar domicilio en el país.

c) Declaración jurada de contar con la infraestructura e instalaciones necesarias para la prestación del servicio, así como la declaración jurada de aceptación de la visita comprobatoria de la autoridad administrativa competente.

d) Declaración de prácticas de certificación y documentación que comprenda el sistema de gestión implementado conforme a los incisos a) y d) del artículo 11° del Reglamento.

e) Declaración jurada del cumplimiento de los requisitos señalados en los incisos b) y c) del artículo 11° del Reglamento; información que será comprobada por la autoridad administrativa competente.

f) Documentación que acredite el cumplimiento de lo dispuesto en el artículo 29° y 30° del Reglamento y demás que la autoridad administrativa competente señale.

g) Informe favorable de la entidad sectorial correspondiente, cuando lo solicite la autoridad administrativa competente, para el caso de las personas jurídicas supervisadas, respecto de la legalidad y seguridad para el desempeño de actividades de certificación.

Artículo 39 - Acreditación de Entidades de Registro o Verificación. Las entidades que soliciten su acreditación como entidades de registro o verificación ante la autoridad administrativa competente deben contar con procedimientos para la prestación de sus servicios, los mismos que tendrán que asegurar la verificación directa de la identidad del solicitante.

Artículo 40 - Presentación de la solicitud de acreditación de Entidades de Registro o Verificación. La solicitud para la acreditación de entidades de registro o verificación debe presentarse a la autoridad administrativa competente, observando lo dispuesto en el artículo anterior y adjuntando la información y documentos siguientes:

a) Acreditación de la existencia y vigencia de la persona jurídica mediante los instrumentos públicos o norma legal respectivos, así como las facultades del representante.

b) Acreditar domicilio en el país.

c) Declaración jurada de contar con la infraestructura e instalaciones necesarias para la prestación del servicio, así como la declaración jurada de aceptación de la visita comprobatoria de la autoridad administrativa competente.

d) Procedimientos detallados que garanticen el cumplimiento de las funciones establecidas en el Reglamento.

e) Declaración de prácticas de verificación o registro.

Declaración jurada del cumplimiento de los requisitos señalados en los artículos 33° y 34° del Reglamento.

Artículo 41 - Procedimiento Administrativo de la Acreditación. Admitida la solicitud, la autoridad administrativa competente procederá a la evaluación del cumplimiento de los requisitos establecidos en la Ley como en el Reglamento.

La evaluación de los requisitos de competencia técnica de la entidad de certificación solicitante podrá ser realizada directamente por la autoridad administrativa competente, o a través de terceros, o reconociendo aquéllas realizadas en el extranjero por otras autoridades extranjeras que cumplan funciones equivalentes a

las de la autoridad administrativa competente, y siempre que los requisitos evaluados por ellas sean equivalentes a los requisitos comprendidos en el Reglamento.

Artículo 42 - Reconocimiento de evaluaciones en el extranjero. La autoridad administrativa competente reconocerá las evaluaciones sobre los requisitos de competencia técnica de la entidad de certificación solicitante realizadas en el extranjero siempre y cuando se cumplan con las normas establecidas por la autoridad administrativa competente en el marco del Reglamento.

Artículo 43 - Subsanación de observaciones. Dentro del procedimiento podrán subsanarse las deficiencias técnicas observadas durante la evaluación. Las entidades podrán solicitar la suspensión del procedimiento a fin de implementar las medidas necesarias para superar estas dificultades.

Si culminada la etapa de evaluación, se mantienen observaciones, se denegará el Registro y se archivará el procedimiento.

Artículo 44 - Costos del Registro. Las entidades solicitantes asumirán los costos por la tramitación del procedimiento, y aquellos por evaluación, auditoría y demás previstos por la autoridad administrativa competente.

Artículo 45 - Cancelación de la Acreditación. La acreditación se otorga por un período de 10 años, renovables por períodos similares. Durante dicho período la Entidad beneficiaria estará sujeta a evaluaciones anuales para mantener la vigencia de la referida acreditación.

Artículo 46 - Cancelación de la Acreditación. La cancelación de la acreditación procede por:

a) Solicitud de la entidad de certificación o de la entidad de verificación o registro.

b) Extinción de su personería jurídica.

c) Sanción impuesta por la autoridad administrativa competente o por decisión judicial.

d) Por liquidación, decidida por la junta de acreedores en el marco de la legislación concursal o resolución judicial de quiebra.

CAPÍTULO III - DE LOS CERTIFICADOS EMITIDOS POR ENTIDADES EXTRANJERAS

Artículo 47 - Acuerdos de reconocimiento mutuo. La autoridad administrativa competente podrá suscribir acuerdos de reconocimiento mutuo con entidades similares, a fin de reconocer la validez de certificados digitales otorgados en el extranjero y extender la validez de la Infraestructura Oficial de Firma Digital. Los acuerdos de reconocimiento mutuo deben garantizar en forma equivalente las funciones exigidas por la Ley como en el Reglamento.

Artículo 48 - Reconocimiento de certificados emitidos por entidades extranjeras. La autoridad administrativa competente podrá reconocer certificados digitales emitidos por entidades extranjeras, de acuerdo con las prácticas y políticas que para tal efecto apruebe, las mismas que deben velar por el cumplimiento de las obligaciones y responsabilidades establecidas en el Reglamento u otra norma posterior. Asimismo, podrá autorizar la operación de aquellas entidades de certificación nacionales que utilicen servicios de entidades de certificación extranjeras, de verificarse tal supuesto, las entidades nacionales asumirán las responsabilidades del caso.

Para los efectos de lo dispuesto en el párrafo precedente, la entidad extranjera deberá comunicar a la autoridad administrativa competente el nombre de aquellas entidades que autorizarán las solicitudes de emisión de certificados digitales así como la gestión de los mismos.

La autoridad administrativa competente emitirá las normas que aseguren el cumplimiento de lo establecido en el presente artículo; así como los mecanismos adecuados de información a los agentes del mercado.

Artículo 49 - Certificación cruzada. Las entidades de certificación acreditadas pueden realizar certificaciones cruzadas con entidades de certificación extranjeras a fin de reconocer los certificados digitales que éstas emitan en el extranjero incorporándolos como suyos dentro de la Infraestructura Oficial de Firma Digital de conformidad con el artículo 11º de la Ley, siempre y cuando obtengan autorización previa de la autoridad administrativa competente.

Las entidades que presten servicios de acuerdo a lo establecido en el párrafo precedente, asumirán responsabilidad de daños y perjuicios por la gestión de tales certificados.

Las entidades de certificación acreditadas que realicen certificaciones cruzadas conforme al primer párrafo del presente artículo, garantizarán ante la autoridad administrativa competente que los certificados digitales reconocidos han sido emitidos bajo requisitos equivalentes a los exigidos en la Infraestructura Oficial de Firma Digital, y que cumplen las funciones señaladas en el artículo 2º de la Ley.

CAPÍTULO IV - SUPERVISIÓN DE ENTIDADES ACREDITADAS

Artículo 50 - Facultades de supervisión. La autoridad administrativa competente tiene la facultad de verificar la correcta prestación de los servicios de certificación así como de los servicios de registro o verificación y el cumplimiento de las obligaciones legales y técnicas por parte de las entidades acreditadas que operen bajo la Infraestructura Oficial de Firma Electrónica, así como la facultad de verificar el cumplimiento de las disposiciones establecidas en la Ley, en el Reglamento, y en sus Resoluciones.

Disposiciones Finales

Artículo Primero.- Las entidades del Sector Público Nacional pueden suscribir acuerdos de cooperación con sus similares a nivel mundial o con instituciones de cooperación, para recibir apoyo, asesoría y financiamiento para el desarrollo del comercio electrónico en general, las firmas electrónicas, las firmas y certificados digitales en particular.

Artículo Segundo.- Las entidades de certificación deben establecer procedimientos ágiles y sencillos para que sus usuarios puedan presentar directamente reclamaciones por la prestación de sus servicios, las mismas que deberán ser atendidas en el más breve plazo. La autoridad administrativa competente aprueba o reforma estos procedimientos y regula todo lo relativo a las reclamaciones. Agotada la vía previa de la reclamación ante la entidad de certificación, procede recurrir en vía administrativa ante la autoridad administrativa competente, con sujeción a la Ley N° 27444 - Ley del Procedimiento Administrativo General.

La autoridad administrativa competente determinará todos aquellos procedimientos necesarios para la aplicación del Reglamento. En los casos que proceda la reclamación, adoptará las medidas correctivas pertinentes.

 *LEY 27.291 - MODIFICA EL CODIGO CIVIL PERMITIENDO LA UTILIZACION DE LOS MEDIOS ELECTRONICOS PARA LA COMUNICACION DE LA MANIFESTACION DE VOLUNTAD Y LA UTILIZACION DE LA FIRMA ELECTRÓNICA.*

Promulgada el 23.6.2000 y publicada el 24.6.2000

Artículo 1 - Modificación del Código Civil. Modifíquense los artículos 141o y 1374o del Código Civil, con los siguientes textos:

Artículo 141 - Manifestación de voluntad. La manifestación de voluntad puede ser expresa o tácita. Es expresa cuando se realiza en forma oral o escrita, a través de cualquier medio directo, manual, mecánico, electrónico u otro análogo. Es tácita cuando la voluntad se infiere indubitablemente de una actitud o de circunstancias de comportamiento que revelan su existencia.

No puede considerarse que existe manifestación tácita cuando la ley exige declaración expresa o cuando el agente formula reserva o declaración en contrario.

Artículo 1374 - Conocimiento y contratación entre ausentes. La oferta, su revocación, la aceptación y cualquier otra declaración contractual dirigida a determinada persona se consideran conocidas en el momento en que llegan a la dirección del destinatario, a no ser que este pruebe haberse encontrado, sin su culpa, en la imposibilidad de conocerla.

Si se realiza a través de medios electrónicos, ópticos u otro análogo, se presumirá la recepción de la declaración contractual, cuando el remitente reciba el acuse de recibo.

Artículo 2 - Adición de artículo al Código Civil. Adiciónese el artículo 141-A al Código Civil, con el siguiente texto:

Artículo 141-A- Formalidad. En los casos en que la ley establezca que la manifestación de voluntad deba hacerse a través de alguna formalidad expresa o requiera de firma, ésta podrá ser generada o comunicada a través de medios electrónicos, ópticos o cualquier otro análogo.

Tratándose de instrumentos públicos, la autoridad competente deberá dejar constancia del medio empleado y conservar una versión íntegra para su ulterior consulta.

Artículo 3 - Reglamentación para relaciones con el Estado. El Poder Ejecutivo, por decreto supremo refrendado por el Ministro de Justicia y dentro del plazo de 90 (noventa) días, reglamentará la aplicación de la presente Ley en las relaciones entre el Estado y los particulares.

LEY N° 27419 SOBRE NOTIFICACIÓN POR CORREO ELECTRONICO.

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 SOBRE NOTIFICACIÓN POR CORREO ELECTRONICO

Artículo único.- Objeto de la ley. Modifíquense los Artículos163° y 164° del Código Procesal Civil, con el siguiente texto:

"**Artículo 163** - **Notificación por telegrama o facsímil, correo electrónico u otro medio**. En los casos del Artículo 157°, salvo el traslado de la demanda o de la reconvención, citación para absolver posiciones y la sentencia, las otras resoluciones pueden, a pedido de parte, ser notificadas, además, por telegrama, facsímil, correo electrónico u otro medio idóneo, siempre que los mismos permitan confirmar su recepción.

La notificación por correo electrónico sólo se realizará para la parte que lo haya solicitado.

Los gastos para la realización de esta notificación quedan incluidos en la condena de costas.

"**Artículo 164** - **Diligenciamiento de la notificación por facsímil, correo electrónico u otro medio**. El documento para la notificación por facsímil, correo electrónico u otro medio, contendrá los datos de la cédula.

El facsímil u otro medio se emitirá en doble ejemplar, uno de los cuales será entregado para su envío y bajo constancia al interesado por el secretario respectivo, y el otro con su firma se agregará al expediente. La fecha de la notificación será la de la constancia de la entrega del facsímil al destinatario. En el caso del correo Electrónico, será, en lo posible, de la forma descrita anteriormente, dejándose constancia en el expediente del ejemplar entregado para su envío, anexándose además el correspondiente reporte técnico que acredite su envío.

El Consejo Ejecutivo del Poder judicial podrá disponer la adopción de un texto uniforme para la redacción de estos documentos."

Comuníquese al señor Presidente de la República para su promulgación.

En Lima, a los veinticinco días del mes de enero de dos mil uno.

CARLOS FERRERO
Presidente a.i. del Congreso de la República

HENRY PEASE GARCÍA
Segundo Vicepresidente del Congreso de la República

AL SEÑOR PRESIDENTE CONSTITUCIONAL DE LA REPUBLICA, POR TANTO:

Mando se publique y cumpla.

Dado en la Casa de Gobierno, en Lima, a los seis días del mes de febrero del año dos mil uno.
VALENTIN PANIAGUA CORAZAO
Presidente Constitucional de la República

DIEGO GARCIA SAYAN LARRABURE
Ministro de Justicia

RESOLUCIÓN 000103 DE ADUANAS

SE RESUELVE

Artículo 1 - Establecer a nivel nacional el uso obligatorio por parte del personal de ADUANAS del "Formato electrónico de documentos internos" (FEDI) en la tramitación interna de documentos que no estén relacionados con el Despacho de Mercancías.

Artículo 2 - Precisar que es obligación de los trabajadores de ADUANAS abrir y consultar permanentemente su correo electrónico, así como responder los mensajes a la brevedad posible.

Artículo 3 - Salvo disposición expresa en contrario, los plazos se computan a partir del día siguiente de la recepción de los documentos, siendo el acuse de recibo y lectura el que indique la fecha y hora en que el destinatario recibió la comunicación.

Artículo 4 - El personal de ADUANAS, bajo responsabilidad, debe mantener el carácter de secretas e intransferibles las claves de acceso a la red, correo electrónico y aplicaciones del sistema de información aduanera, así como hacer un correcto uso de los equipos de computación asignados y aplicaciones autorizadas.

Artículo 5 - Adicionar como inciso r) del articulo 34 del Reglamento interno de Trabajo aprobado por Resolución de Superintendencia de Aduanas Nro. 001607 del 2.JUL.97, el siguiente texto:

"r) guardar la confidencialidad en el manejo de los códigos y claves de acceso a la red, correo electrónico y aplicaciones del sistema de información aduanera, así como la conservación de los equipos de computación y el mantenimiento de la reserva y seguridad de la información."

Artículo 6 - Autorizar el uso obligatorio de firmas y certificados digitales en las Resoluciones que se expidan.

Artículo 7 - Establecer como medio de comunicación entre ADUANAS y los operadores de comercio exterior, proveedores y entidades, el Portal de ADUANAS y los sistemas inter-organizacionales basados en el intercambio electrónico de datos, con el efecto que la Ley les concede.

Artículo 8 - La validez, seguridad, integridad, confidencialidad y archivo de los formatos documentales y electrónicos a que se contrae la presente resolución, estarán resguardadas conforme a las disposiciones legales de la materia.

Artículo 9 - Las copias autenticadas de los documentos electrónicos serán expedidas por los fedatarios públicos juramentados autorizados, autenticándolas con su signo y firma, mediante sello *Ad hoc*, conforme a lo establecido.

Artículo 10 - Aprobar la versión 3 del instructivo de trabajo SG-IT.02-Formulario y Tramitación de documentos institucionales.

Artículo 11 - La presente Resolución entrará en vigencia a partir del día siguiente de su publicación.

Regístrese, comuníquese y publíquese

ARTURO RAMIREZ SALOMON
Superintendente Nacional de Aduanas.

[6] *E. VENEZUELA*

DECRETO 1.024. LEY SOBRE MENSAJES DE DATOS Y FIRMAS ELECTRÓNICAS

10 de febrero de 2001

HUGO CHÁVEZ FRIAS. PRESIDENTE DE LA REPÚBLICA BOLIVARIANA DE VENEZUELA

En ejercicio de la atribución que le confiere el numeral 8 del artículo 236 de la Constitución de la República Bolivariana de Venezuela, en concordancia con el artículo 1, numeral 5, literal b de la Ley que Autoriza al Presidente de la República para dictar Decretos con Fuerza de Ley en las Materias que se delegan, en Consejo de Ministros,

LEY SOBRE MENSAJES DE DATOS Y FIRMAS ELECTRÓNICAS

CAPÍTULO I - ÁMBITO DE APLICACIÓN Y DEFINICIONES

Objeto y aplicabilidad del Decreto-Ley

Artículo 1 - El presente Decreto-Ley tiene por objeto otorgar y reconocer eficacia y valor jurídico a la Firma Electrónica, al Mensaje de Datos y a toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, así como regular todo lo relativo a los Proveedores de Servicios de Certificación y los Certificados Electrónicos.

El presente Decreto-Ley será aplicable a los Mensajes de Datos y Firmas Electrónicas independientemente de sus características tecnológicas o de los desarrollos tecnológicos que se produzcan en un futuro. A tal efecto, sus normas serán desarrolladas e interpretadas progresivamente, orientadas a reconocer la validez y eficacia probatoria de los Mensajes de datos y Firmas Electrónicas.

La certificación a que se refiere el presente Decreto-Ley no excluye el cumplimiento de las formalidades de registro público o autenticación que, de conformidad con la ley, requieran determinados actos o negocios jurídicos.

Definiciones

Artículo 2 - A los efectos del presente Decreto-Ley, se entenderá por:

Persona: Todo sujeto jurídicamente hábil, bien sea natural, jurídica, pública, privada, nacional o extranjera, susceptible de adquirir derechos y contraer obligaciones.

Mensajes de datos: Toda información inteligible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio.

Emisor: Persona que origina un Mensaje de Datos por sí mismo, o a través de terceros autorizados.

Firma Electrónica: Información creada o utilizada por el Signatario, asociada al Mensaje de Datos, que permite atribuirle su autoría bajo el contexto en el cual ha sido empleado.

Signatario: Es la persona titular de una Firma Electrónica o Certificado Electrónico.

Destinatario: Persona a quien va dirigido el Mensaje de Datos.

Proveedor de Servicios de Certificación: Persona dedicada a proporcionar Certificados Electrónicos y demás actividades previstas en este Decreto-Ley.

---

[6] Flag courtesy of www.theodora.com/flags used with permission

Acreditación: es el título que otorga la Superintendencia de servicios de Certificación Electrónica a los Proveedores de Servicios de Certificación para proporcionar certificados electrónicos, una vez cumplidos los requisitos y condiciones establecidos en este Decreto-Ley.

Certificado Electrónico: Mensaje de Datos proporcionado por un Proveedor de Servicios de Certificación que le atribuye certeza y validez a la Firma Electrónica.
Sistema de Información: Aquel utilizado para generar, procesar o archivar de cualquier forma Mensajes de Datos.

Usuario: Toda persona que utilice un sistema de información.

Inhabilitación técnica: Es la incapacidad temporal o permanente del Proveedor de Servicios de Certificación que impida garantizar el cumplimiento de sus servicios, así como, cumplir con los requisitos y condiciones establecidos en este Decreto-Ley para el ejercicio de sus actividades.

El reglamento del presente Decreto-Ley podrá adaptar las definiciones antes señaladas a los desarrollos tecnológicos que se produzcan en el futuro. Así mismo, podrá establecer otras definiciones que fueren necesarias para la eficaz aplicación de este Decreto-Ley.

Adaptabilidad del Decreto-Ley

Artículo 3 - El Estado adoptará las medidas que fueren necesarias para que los organismos públicos puedan desarrollar sus funciones, utilizando los mecanismos descritos en este Decreto-Ley.

CAPÍTULO II - DE LOS MENSAJES DE DATOS

Eficacia Probatoria

Artículo 4 - Los Mensajes de Datos tendrán la misma eficacia probatoria que la ley otorga a los documentos escritos, sin perjuicio de lo establecido en la primera parte del artículo 6 de este Decreto-Ley. Su promoción, control, contradicción y evacuación como medio de prueba, se realizará conforme a lo previsto para las pruebas libres en el Código de Procedimiento Civil.

La información contenida en un Mensaje de Datos, reproducida en formato impreso, tendrá la misma eficacia probatoria atribuida en la ley a las copias o reproducciones fotostáticas.

Sometimiento a la Constitución y a la ley.

Artículo 5 - Los Mensajes de Datos estarán sometidos a las disposiciones constitucionales y legales que garantizan los derechos a la privacidad de las comunicaciones y de acceso a la información personal.

Cumplimiento de solemnidades y formalidades.
Artículo 6 - Cuando para determinados actos o negocios jurídicos la ley exija el cumplimiento de solemnidades o formalidades, éstas podrán realizarse utilizando para ello los mecanismos descritos en este Decreto-Ley.

Cuando para determinados actos o negocios jurídicos la ley exija la firma autógrafa, ese requisito quedará satisfecho en relación con un Mensaje de Datos al tener asociado una Firma Electrónica.

Integridad del Mensaje de Datos.

Artículo 7 - Cuando la ley requiera que la información sea presentada o conservada en su forma original, ese requisito quedará satisfecho con relación a un Mensaje de Datos si se ha conservado su integridad y cuando la información contenida en dicho Mensaje de Datos esté disponible. A tales efectos, se considerará que un Mensaje de Datos permanece íntegro, si se mantiene inalterable desde que se generó, salvo algún cambio de forma propio del proceso de comunicación, archivo o presentación.

Constancia por escrito del Mensaje de Datos

Artículo 8 - Cuando la ley requiera que la información conste por escrito, ese requisito quedará satisfecho con relación a un Mensaje de Datos, si la información que éste contiene es accesible para su ulterior consulta.

Cuando la ley requiera que ciertos actos o negocios jurídicos consten por escrito y su soporte deba permanecer accesible, conservado o archivado por un período determinado o en forma permanente, estos requisitos quedarán satisfechos mediante la conservación de los Mensajes de Datos, siempre que se cumplan las siguientes condiciones:

Que la información que contengan pueda ser consultada posteriormente.

Que conserven el formato en que se generó, archivó o recibió o en algún formato que sea demostrable que reproduce con exactitud la información generada o recibida.

Que se conserve todo dato que permita determinar el origen y el destino del Mensaje de Datos, la fecha y la hora en que fue enviado o recibido.

Toda persona podrá recurrir a los servicios de un tercero para dar cumplimiento a los requisitos señalados en este artículo.

CAPÍTULO III - DE LA EMISIÓN Y RECEPCIÓN DE LOS MENSAJES DE DATOS

Verificación de la emisión del Mensaje de Datos

Artículo 9 - Las partes podrán acordar un procedimiento para establecer cuándo el Mensaje de Datos proviene efectivamente del Emisor. A falta de acuerdo entre las partes, se entenderá que un Mensajes de Datos proviene del Emisor, cuando éste ha sido enviado por:

El propio Emisor.

Persona autorizada para actuar en nombre del Emisor respecto de ese mensaje.

Por un Sistema de Información programado por el Emisor, o bajo su autorización, para que opere automáticamente.

Oportunidad de la emisión

Artículo 10 - Salvo acuerdo en contrario entre las partes, el Mensaje de Datos se tendrá por emitido cuando el sistema de información del Emisor lo remita al Destinatario.

Reglas para la determinación de la recepción

Artículo 11 - Salvo acuerdo en contrario entre el Emisor y el Destinatario, el momento de recepción de un Mensaje de Datos se determinará conforme a las siguientes reglas:

Si el Destinatario ha designado un sistema de información para la recepción de Mensajes de Datos, la recepción tendrá lugar cuando el Mensaje de Datos ingrese al sistema de información designado.

Si el Destinatario no ha designado un sistema de información, la recepción tendrá lugar, salvo prueba en contrario, al ingresar el Mensaje de Datos en un sistema de información utilizado regularmente por el Destinatario.

Lugar de emisión y recepción

Artículo 12 - Salvo prueba en contrario, el Mensaje de Datos se tendrá por emitido en el lugar donde el Emisor tenga su domicilio y por recibido en el lugar donde el Destinatario tenga el suyo.

Del acuse de recibo

Artículo 13 - El Emisor de un Mensaje de Datos podrá condicionar los efectos de dicho mensaje a la recepción de un acuse de recibo emitido por el Destinatario.

Las partes podrán determinar un plazo para la recepción del acuse de recibo. La no-recepción de dicho acuse de recibo dentro del plazo convenido, dará lugar a que se tenga el Mensaje de Datos como no emitido.

Cuando las partes no establezcan un plazo para la recepción del acuse de recibo, el Mensaje de Datos se tendrá por no emitido si el Destinatario no envía su acuse de recibo en un plazo de veinticuatro (24) horas a partir de su emisión.

Cuando el Emisor reciba el acuse de recibo del Destinatario conforme a lo establecido en el presente artículo, el Mensaje de Datos surtirá todos sus efectos.

Mecanismos y métodos para el acuse de recibo

Artículo 14 - Las partes podrán acordar los mecanismos y métodos para el acuse de recibo de un Mensaje de Datos. Cuando las partes no hayan acordado que para el acuse de recibo se utilice un método determinado, se considerará que dicho requisito se ha cumplido cabalmente mediante:

Toda comunicación del Destinatario, automatizada o no, que señale la recepción del Mensaje de Datos.

Todo acto del Destinatario que resulte suficiente a los efectos de evidenciar al Emisor que ha recibido su Mensaje de Datos.

Oferta y aceptación en los contratos

Artículo 15 - En la formación de los contratos, las partes podrán acordar que la oferta y aceptación se realicen por medio de Mensajes de Datos.

CAPÍTULO IV - DE LAS FIRMAS ELECTRONICAS

Validez y eficacia de la Firma Electrónica. Requisitos

Artículo 16 - La Firma Electrónica que permita vincular al Signatario con el Mensaje de Datos y atribuir la autoría de éste, tendrá la misma validez y eficacia probatoria que la ley otorga a la firma autógrafa. A tal efecto, salvo que las partes dispongan otra cosa, la Firma Electrónica deberá llenar los siguientes aspectos:
Garantizar que los datos utilizados para su generación puedan producirse sólo una vez, y asegurar, razonablemente, su confidencialidad.
Ofrecer seguridad suficiente de que no pueda ser falsificada con la tecnología existente en cada momento.
No alterar la integridad del Mensaje de Datos.

A los efectos de este artículo, la Firma Electrónica podrá formar parte integrante del Mensaje de Datos, o estar inequívocamente asociada a éste; enviarse o no en un mismo acto.

Efectos jurídicos. Sana critica

Artículo 17 - La Firma Electrónica que no cumpla con los requisitos señalados en el artículo anterior no tendrá los efectos jurídicos que se le atribuyen en el presente Capítulo, sin embargo, podrá constituir un elemento de convicción valorable conforme a las reglas de la sana crítica.

La certificación

Artículo 18 - La Firma Electrónica, debidamente certificada por un Proveedor de Servicios de Certificación conforme a lo establecido en este Decreto-Ley, se considerará que cumple con los requisitos señalados en el artículo 16.

Obligaciones del signatario

Artículo 19 - El Signatario de la Firma Electrónica tendrá las siguientes obligaciones:

Actuar con diligencia para evitar el uso no autorizado de su Firma Electrónica.

Notificar a su Proveedor de Servicios de Certificación que su Firma Electrónica ha sido controlada por terceros no autorizados o indebidamente utilizada, cuando tenga conocimiento de ello.

El Signatario que no cumpla con las obligaciones antes señaladas será responsable de las consecuencias del uso no autorizado de su Firma Electrónica.

CAPÍTULO V - DE LA SUPERINTENDENCIA DE SERVICIOS DE CERTIFICACIÓN ELECTRÓNICA

Creación de la Superintendencia

Artículo 20 - Se crea la Superintendencia de Servicios de Certificación Electrónica, como un servicio autónomo con autonomía presupuestaria, administrativa, financiera y de gestión, en las materias de su competencia, dependiente del Ministerio de Ciencia y Tecnología.

Objeto de la Superintendencia

Artículo 21 - La Superintendencia de Servicios de Certificación Electrónica tiene por objeto acreditar, supervisar y controlar, en los términos previstos en este Decreto-Ley y sus reglamentos, a los Proveedores de Servicios de Certificación públicos o privados.

Competencias de la Superintendencia

Artículo 22 - La Superintendencia de Servicios de Certificación Electrónica tendrá las siguientes competencias:

Otorgar la acreditación y la correspondiente renovación a los Proveedores de Servicios de Certificación una vez cumplidas las formalidades y requisitos de este Decreto-Ley, sus reglamentos y demás normas aplicables.

Revocar o suspender la acreditación otorgada cuando se incumplan las condiciones, requisitos y obligaciones que se establecen en el presente Decreto-Ley.

Mantener, procesar, clasificar, resguardar y custodiar el Registro de los Proveedores de Servicios de Certificación públicos o privados.

Verificar que los Proveedores de Servicios de Certificación cumplan con los requisitos contenidos en el presente Decreto-Ley y sus reglamentos.

Supervisar las actividades de los Proveedores de Servicios de Certificación conforme a este Decreto-Ley, sus reglamentos y las normas y procedimientos que establezca la Superintendencia en el cumplimiento de sus funciones.

Liquidar, recaudar y administrar las tasas establecidas en el artículo 24 de este Decreto-Ley.

Liquidar y recaudar las multas establecidas en el presente Decreto-Ley.

Administrar los recursos que se le asignen y los que obtenga en el desempeño de sus funciones.

Coordinar con los organismos nacionales o internacionales cualquier aspecto relacionado con el objeto de este Decreto-Ley.

Inspeccionar y fiscalizar la instalación, operación y prestación de servicios realizados por los Proveedores de Servicios de Certificación.

Abrir, de oficio o a instancia de parte, sustanciar y decidir los procedimientos administrativos relativos a presuntas infracciones a este Decreto-Ley.

Requerir de los Proveedores de Servicios de Certificación o sus usuarios, cualquier información que considere necesaria y que esté relacionada con materias relativas al ámbito de sus funciones.

Actuar como mediador en la solución de conflictos que se susciten entre los Proveedores de Servicios de Certificados y sus usuarios, cuando ello sea solicitado por las partes involucradas, sin perjuicio de las atribuciones que tenga el organismo encargado de la protección, educación y defensa del consumidor y el usuario, conforme a la ley que rige esta materia.

Seleccionar los expertos técnicos o legales que considere necesarios para facilitar el ejercicio de sus funciones.

Presentar un informe anual sobre su gestión al Ministerio de adscripción.

Tomar las medidas preventivas o correctivas que considere necesarias conforme a lo previsto en este Decreto-Ley.

Imponer las sanciones establecidas en este Decreto-Ley.

Determinar la forma y alcance de los requisitos establecidos en los artículos 31 y 32 del presente Decreto-Ley.

Las demás que establezcan la ley y los reglamentos.

Ingresos de la Superintendencia

Artículo 23 - Son ingresos de la Superintendencia de Servicios de Certificación Electrónica:

Los recursos que le sean asignados en la Ley de Presupuesto a través del Ministerio de Ciencia y Tecnología.

Los provenientes de su gestión conforme a lo establecido en esta Ley.

Cualquier otro ingreso permitido por ley.

De las tasas

Articulo 24 - La Superintendencia de Servicios de Certificación Electrónica cobrará las siguientes tasas:

Por la acreditación de los Proveedores de Servicios de Certificación se cobrará una tasa de un mil unidades tributarias (1.000 U.T.).

Por la renovación de la acreditación de los Proveedores de Servicios de Certificación se cobrará una tasa de quinientas unidades tributarias (500 U.T.).

Por la cancelación de la acreditación de los Proveedores de Servicios de Certificación se cobrará una tasa de quinientas unidades tributarias (500 U.T.).

Por la autorización que se otorgue a los Proveedores de Servicios de Certificación debidamente acreditados en relación a la garantía de los Certificados Electrónicos proporcionados por Proveedores de Servicios de Certificación extranjeros, conforme a lo establecido en el artículo 44 del presente Decreto-Ley, se cobrará una tasa de quinientas unidades tributarias (500 U.T.).

Los Proveedores de Servicios de Certificación constituidos por entes públicos estarán exentos del pago de las tasas previstas en este artículo.

Mecanismos de control

Artículo 25 - La Contraloría Interna del Ministerio de Ciencia y Tecnología, ejercerá las funciones de control, vigilancia y fiscalización de los ingresos, gastos y bienes públicos sobre este servicio autónomo, de conformidad con la ley que regula la materia.

De la supervisión

Artículo 26 - La Superintendencia de Servicios de Certificación Electrónica supervisará a los Proveedores de Servicios de Certificación con el objeto de verificar que cumplan con los requerimientos necesarios para ofrecer un servicio eficaz a sus usuarios. A tal efecto, podrá directamente o a través de expertos, realizar las inspecciones y auditorias que fueren necesarias para comprobar que los Proveedores de Servicios de Certificación cumplen con tales requerimientos.

Medidas para garantizar la confiabilidad

Artículo 27 - La Superintendencia de Servicios de Certificación Electrónica podrá adoptar las medidas preventivas o correctivas necesarias para garantizar la confiabilidad de los servicios prestados por los Proveedores de Servicios de Certificación. A tal efecto, podrá ordenar, entre otras medidas, el uso de estándares o prácticas internacionalmente aceptadas para la prestación de los servicios de certificación electrónica, o que el Proveedor se abstenga de realizar cualquier actividad que ponga en peligro la integridad o el buen uso del servicio.

Designación del Superintendente

Artículo 28 - La Superintendencia de Servicios de Certificación Electrónica estará a cargo de un Superintendente, será de libre designación y remoción del Ministro de Ciencia y Tecnología.

Requisito para ser Superintendente

Artículo 29 - El Superintendente de Servicios de Certificación Electrónica, debe reunir los siguientes requisitos:

Ser venezolano.

De reconocida competencia técnica y profesional para el ejercicio de sus funciones.

No podrán ser Superintendente, los miembros directivos, agentes, comisarios, administradores o accionistas de empresas o instituciones sometidas al control de la Superintendencia. Tampoco podrá ejercer tal cargo el que tenga parentesco hasta el cuarto grado de consanguinidad o segundo de afinidad con personas naturales también sometidas al control de la Superintendencia.

Atribuciones del Superintendente

Artículo 30 - Son atribuciones del Superintendente:

Dirigir el Servicio Autónomo Superintendencia de Servicios de Certificación Electrónica.

Suscribir los actos y documentos relacionados con las materias especificadas en el artículo 22 de este Decreto-Ley.

Administrar los recursos e ingresos del Servicio Autónomo Superintendencia de Servicios de Certificación Electrónica.

Celebrar previa delegación del Ministro de Ciencia y Tecnología, convenios con organismos públicos o privados, nacionales e internacionales, derivados del cumplimiento de las atribuciones que corresponden a la Superintendencia de Servicios de Certificación Electrónica.

Elaborar el proyecto de presupuesto anual, de conformidad con las previsiones legales correspondientes.

Proponer escalas especiales de remuneración para el personal de la Superintendencia, de conformidad con las disposiciones legales aplicables.

Presentar al Ministro de Ciencia y Tecnología el Proyecto de Reglamento Interno.

Celebrar previa delegación del Ministro de Ciencia y Tecnología, los contratos de trabajo y de servicios de personal, que requiera la Superintendencia de Servicios de Certificación Electrónica para su funcionamiento.

Elaborar anualmente la memoria y cuenta de la Superintendencia de Servicios de Certificación Electrónica.

Las demás que le sean asignadas por el Ministro de Ciencia y Tecnología.

CAPÍTULO VI - DE LOS PROVEEDORES DE SERVICIOS DE CERTIFICACIÓN

Requisito para ser Proveedor

Artículo 31 - Podrán ser Proveedores de Servicios de Certificación, las personas, que cumplan y mantengan los siguientes requisitos:

La capacidad económica y financiera suficiente para prestar los servicios autorizados como Proveedor de Servicios de Certificación. En el caso de organismos públicos, éstos deberán contar con un presupuesto de gastos y de ingresos que permitan el desarrollo de esta actividad.

La capacidad y elementos técnicos necesarios para proveer Certificados Electrónicos.

Garantizar un servicio de suspensión, cancelación y revocación, rápido y seguro, de los Certificados Electrónicos que proporcione.

Un sistema de información de acceso libre, permanente, actualizado y eficiente en el cual se publiquen las políticas y procedimientos aplicados para la prestación de sus servicios, así como los Certificados Electrónicos que hubiere proporcionado, revocado, suspendido o cancelado y las restricciones o limitaciones aplicables a éstos.

Garantizar que en la emisión de los Certificados Electrónicos que provea se utilicen herramientas y estándares adecuados a los usos internacionales, que estén protegidos contra su alteración o modificación, de tal forma que garanticen la seguridad técnica de los procesos de certificación.

En caso de personas jurídicas, éstas deberán estar legalmente constituidas de conformidad con las leyes del país de origen.

Personal técnico adecuado con conocimiento especializado en la materia y experiencia en el servicio a prestar.

Las demás que señale el reglamento de este Decreto-Ley.

El incumplimiento de cualesquiera de los requisitos anteriores dará lugar a la revocatoria de la acreditación otorgada por la Superintendencia de Servicios de Certificación Electrónica, sin perjuicio de las sanciones previstas en este Decreto-Ley.

De la acreditación

Artículo 32 - Los Proveedores de Servicios de Certificación presentarán ante la Superintendencia de Servicios de Certificación Electrónica, junto con la correspondiente solicitud, los documentos que acrediten el cumplimiento de los requisitos señalados en el artículo 31. La Superintendencia de Servicios de Certificación Electrónica, previa verificación de tales documentos, procederá a recibir y procesar dicha solicitud y deberá pronunciarse sobre la acreditación del Proveedor de Servicios de Certificación, dentro de los veinte (20) días hábiles siguientes a la fecha de presentación de la solicitud.

Una vez aprobada la solicitud del Proveedor de Servicios de Certificación, éste presentará, a los fines de su acreditación, garantías que cumplan con los siguientes requisitos:

Ser expedidas por una entidad aseguradora o bancaria autorizada para operar en el país, conforme a las disposiciones que rigen la materia.

Cubrir todos los perjuicios contractuales y extra-contractuales de los signatarios y terceros de buena fe derivados de actuaciones dolosas, culposas u omisiones atribuibles a los administradores, representantes legales o empleados del Proveedor de Servicios de Certificación.

El Proveedor de Servicios de Certificación deberá mantener vigente la garantía aquí solicitada por el tiempo de vigencia de su acreditación. El incumplimiento de este requisito dará lugar a la revocatoria de la acreditación otorgada por la Superintendencia de Servicios de Certificación Electrónica.

Negativa de la acreditación

Artículo 33 - La Superintendencia de Servicios de Certificación Electrónica podrá negar la solicitud a que se refiere el artículo anterior, en caso de que el solicitante no reúna los requisitos señalados en este Decreto-Ley y sus reglamentos.

Actividades de los Proveedores de Servicios de Certificación

Artículo 34 - Los Proveedores de Servicios de Certificación realizarán entre otras, las siguientes actividades:

Proporcionar, revocar o suspender los distintos tipos o clases de Certificados Electrónicos.

Ofrecer o facilitar los servicios de creación de Firmas Electrónicas.

Ofrecer servicios de archivo cronológicos de las Firmas Electrónicas certificadas por el Proveedor de Servicios de Certificación.

Ofrecer los servicios de archivo y conservación de mensajes de datos.

Garantizar Certificados Electrónicos proporcionados por Proveedores de Servicios de Certificación extranjeros.

Las demás que se establezcan en el presente Decreto-Ley o en sus reglamentos.
Los Certificados Electrónicos proporcionados por los Proveedores de Servicios de Certificación garantizarán la validez de las Firmas Electrónicas que certifiquen, y la titularidad que sobre ellas tengan sus Signatarios.

Obligaciones de los Proveedores

Artículo 35 - Los Proveedores de Servicios de Certificación tendrán las siguientes obligaciones:

Adoptar las medidas necesarias para determinar la exactitud de los Certificados Electrónicos que proporcionen y la identidad del Signatario.

Garantizar la validez, vigencia y legalidad del Certificado Electrónico que proporcione.

Verificar la información suministrada por el Signatario para la emisión del Certificado Electrónico.

Mantener en medios electrónicos o magnéticos, para su consulta, por diez (10) años siguientes al vencimiento de los Certificados Electrónicos que proporcionen, un archivo cronológico con la información relacionada con los referidos Certificados Electrónicos.

Garantizar a los Signatarios un medio para notificar el uso indebido de sus Firmas Electrónicas.

Informar a los interesados en sus servicios de certificación, utilizando un lenguaje comprensible en su pagina en la Internet o en cualquier otra red mundial de acceso público, los términos precisos y condiciones para el uso del Certificado Electrónico y, en particular, de cualquier limitación sobre su responsabilidad, así como de los procedimientos especiales existentes para resolver cualquier controversia.

Garantizar la integridad, disponibilidad y accesibilidad de la información y documentos relacionados con los servicios que proporcione. A tales efectos, deberán mantener un respaldo confiable y seguro de dicha información.

Garantizar la adopción de las medidas necesarias para evitar la falsificación de Certificados Electrónicos y de las Firmas Electrónicas que proporcionen.

Efectuar las notificaciones y publicaciones necesarias para informar a los signatarios y personas interesadas acerca del vencimiento, revocación, suspensión o cancelación de los Certificados Electrónicos que proporcione, así como de cualquier otro aspecto de relevancia para el público en general, en relación con dichos Certificados Electrónicos.

Notificar a la Superintendencia de Servicios de Certificación Electrónica cuando tenga conocimiento de cualquier hecho que pueda conllevar a su Inhabilitación Técnica.

El incumplimiento de cualesquiera de los requisitos anteriores dará lugar a la suspensión de la acreditación otorgada por la Superintendencia de Servicios de Certificación Electrónica, sin perjuicio de las sanciones establecidas en el presente Decreto-Ley.

La contraprestación del servicio

Artículo 36 - La contraprestación por los servicios que los Proveedores de Servicios de Certificación presten, estará sujeta a las reglas de la oferta y la demanda.

Notificación del cese de actividades

Artículo 37 - Cuando los Proveedores de Servicios de Certificación decidan cesar en sus actividades, lo notificarán a la Superintendencia de Servicios de Certificación Electrónica, al menos con treinta (30) días de anticipación a la fecha de cesación.

En el caso de Inhabilitación Técnica, el Proveedor de Servicios de Certificación notificará inmediatamente a la Superintendencia de Servicios de Certificación Electrónica.

Recibida cualesquiera de las notificaciones señaladas en este artículo, la Superintendencia de Servicios de Certificación Electrónica emitirá un acto por el cual se declare públicamente la cesación de actividades del Proveedor de Servicios de Certificación como prestador de ese servicio, sin perjuicio de las investigaciones que pueda realizar a fin de determinar las causas que originaron el cese de las actividades del Proveedor, y las medidas que fueren necesarias adoptar con el objeto de salvaguardar los derechos de los usuarios. En ese acto la Superintendencia podrá ordenar al Proveedor que realice los trámites que considere necesarios para hacer del conocimiento público la cesación de esas actividades, y para garantizar la conservación de la información que fuere de interés para sus usuarios y el público en general.

En todo caso, el cese de las actividades de un Proveedor de Servicios de Certificación conllevará su retiro del registro llevado por la Superintendencia de Servicios de Certificación Electrónica.

CAPÍTULO VII - CERTIFICADOS ELECTRONICOS

Garantía de la autoría de la Firma Electrónica

Artículo 38 - El Certificado Electrónico garantiza la autoría de la Firma Electrónica que certifica así como la integridad del Mensaje de Datos. El Certificado Electrónico no confiere la autenticidad o fe pública que conforme a la ley otorguen los funcionarios públicos a los actos, documentos y certificaciones que con tal carácter suscriban.

Vigencia del Certificado Electrónico

Artículo 39 - El Proveedor de Servicios de Certificación y el Signatario, de mutuo acuerdo, determinarán la vigencia del Certificado Electrónico.

Cancelación

Artículo 40 - La cancelación de un Certificado Electrónico procederá cuando el Signatario así lo solicite a su Proveedor de Servicios de Certificación. Dicha cancelación no exime al Signatario de las obligaciones contraídas durante la vigencia del Certificado, conforme a lo previsto en este Decreto-Ley.

El Signatario estará obligado a solicitar la cancelación del Certificado Electrónico cuando tenga conocimiento del uso indebido de su Firma Electrónica. Si el Signatario en conocimiento de tal situación no solicita dicha cancelación, será responsable por los daños y perjuicios sufridos por terceros de buena fe como consecuencia del uso indebido de la Firma Electrónica certificada mediante el correspondiente Certificado Electrónico.

Suspensión temporal voluntaria

Artículo 41 - El Signatario podrá solicitar la suspensión temporal del Certificado Electrónico, en cuyo caso su Proveedor deberá proceder a suspender el mismo durante el tiempo solicitado por el Signatario.

Suspensión o revocatoria forzosa

Artículo 42 - En los contratos que celebren los Proveedores de Servicios de Certificación con sus usuarios, se deberán establecer como causales de suspensión o revocatoria del Certificado Electrónico de la Firma Electrónica, las siguientes:

Sea solicitado por una autoridad competente de conformidad con la ley.

Se compruebe que alguno de los datos del Certificado Electrónico proporcionado por el Proveedor de Servicios de Certificación es falso.

Se compruebe el incumplimiento de una obligación principal derivada del contrato celebrado entre el Proveedor de Servicios de Certificación y el Signatario.

Se produzca una Quiebra Técnica del sistema de seguridad del Proveedor de Servicios de Certificación que afecte la integridad y confiabilidad del certificado contentivo de la Firma Electrónica.

Asimismo, se preverá en los referidos contratos que los Proveedores de Servicios de Certificación podrán dejar sin efecto la suspensión temporal del Certificado Electrónico de una Firma Electrónica al verificar que han cesado las causas que originaron dicha suspensión, en cuyo caso el Proveedor de Servicios de Certificación correspondiente estará en la obligación de habilitar de inmediato el Certificado Electrónico de que se trate.

La vigencia del Certificado Electrónico cesará cuando se produzca la extinción o incapacidad absoluta del Signatario

Contenido de los Certificados Electrónicos

Artículo 43 - Los Certificados Electrónicos deberán contener la siguiente información:

Identificación del Proveedor de Servicios de Certificación que proporciona el Certificado Electrónico, indicando su domicilio y dirección electrónica.

El código de identificación asignado al Proveedor de Servicios de Certificación por la Superintendencia de Servicios de Certificación Electrónica.

Identificación del titular del Certificado Electrónico, indicando su domicilio y dirección electrónica.

Las fechas de inicio y vencimiento del periodo de vigencia del Certificado Electrónico.

La Firma Electrónica del Signatario.

Un serial único de identificación del Certificado Electrónico.

Cualquier información relativa a las limitaciones de uso, vigencia y responsabilidad a las que esté sometido el Certificado Electrónico.

Certificados electrónicos extranjeros

Artículo 44 - Los Certificados Electrónicos emitidos por proveedores de servicios de certificación extranjeros tendrán la misma validez y eficacia jurídica reconocida en el presente Decreto-Ley, siempre que tales certificados sean garantizados por un Proveedor de Servicios de Certificación, debidamente acreditado conforme a lo previsto en el presente Decreto-Ley, que garantice, en la misma forma que lo hace con sus propios certificados, el cumplimiento de los requisitos, seguridad, validez y vigencia del certificado. Los certificados electrónicos extranjeros, no garantizados por un Proveedor de Servicios de Certificación debidamente acreditado conforme a lo previsto en el presente Decreto-Ley, carecerán de los efectos jurídicos que se atribuyen en el presente Capítulo, sin embargo, podrán constituir un elemento de convicción valorable conforme a las reglas de la sana crítica.

CAPÍTULO VIII - DE LAS SANCIONES

A los Proveedores de Servicios de Certificación

Artículo 45 - Los Proveedores de Servicios de Certificación serán sancionados con multa de Quinientas Unidades Tributarias (500 U.T.) a Dos Mil Unidades Tributarias (2.000 U.T.), cuando incumplan las obligaciones que les impone el artículo 35 del presente Decreto-Ley.

Los Proveedores de Servicios de Certificación serán sancionados con multa de Quinientas Unidades Tributarias (500 U.T.) a Dos Mil Unidades Tributarias (2.000 U.T.), cuando dejen de cumplir con alguno de los requisitos establecidos en el artículo 31 del presente Decreto-Ley.

Las sanciones serán impuestas en su término medio, pero podrán ser aumentadas o disminuidas en atención a las circunstancias agravantes o atenuantes existentes.

Circunstancias agravantes y atenuantes:

Artículo 46 - Son circunstancias agravantes:

La reincidencia y la reiteración.

La gravedad del perjuicio causado al Usuario.

La gravedad de la infracción.

La resistencia o reticencia del infractor para esclarecer los hechos.

Son circunstancias atenuantes:

No haber tenido la intención de causar el hecho imputado de tanta gravedad.

Las que se evidencien de las pruebas aportadas por el infractor en su descargo.

En el proceso se apreciará el grado de la culpa para agravar o atenuar la pena.

Prescripción de las sanciones

Artículo 47 - Las sanciones aplicadas prescriben por el transcurso de tres (3) años, contados a partir de la fecha de notificación al infractor.

Falta de acreditación

Artículo 48 - Serán sancionadas con multa de dos mil (2000) a cinco mil (5000) Unidades Tributarias (U.T.), las personas que presten los servicios de Proveedores de Servicios de Certificación previstos en este Decreto-Ley, sin la acreditación de la Superintendencia de Servicios de Certificación Electrónica, alegando tenerla.

Procedimiento ordinario

Artículo 49 - Para la imposición de las multas previstas en los artículos anteriores, la Superintendencia de Servicios de Certificación Electrónica aplicará el procedimiento administrativo ordinario previsto en la Ley Orgánica de Procedimientos Administrativos.

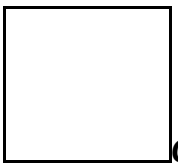
CAPÍTULO X - DISPOSICIONES FINALES

Primera - El presente Decreto-Ley entrará en vigencia a partir de su publicación en la Gaceta Oficial de la República Bolivariana de Venezuela.

Segunda - Los procedimientos, trámites y recursos contra los actos emanados de la Superintendencia de Servicios de Certificación Electrónica, se regirán por lo previsto en la Ley Orgánica de Procedimientos Administrativos.

Tercera - Sin limitación de otros que se constituyan, el Estado creará un Proveedor de Servicios de Certificación de carácter público, conforme a las normas del presente Decreto-Ley. El Presidente de la República determinará la forma y adscripción de este Proveedor de Servicios de Certificación.

Cuarta - La Administración Tributaria y Aduanera adoptará las medidas necesarias para ejercer sus funciones utilizando los mecanismos descritos en este Decreto-Ley, así como para que los contribuyentes puedan dar cumplimiento a sus obligaciones tributarias mediante dichos mecanismos.



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

Resolución aprobada por la Asamblea General sobre la base del informe de la Sexta Comisión (A/51/628) 1/162. 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 Comisión[1] a fin de garantizar la seguridad jurídica en el contexto de la utilización más amplia posible del procesamiento automático de datos en el comercio internacional,

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.

85a. sesión plenaria. 6 de diciembre de 1996

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;
   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) al 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 transfiere 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 dimanan 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 atendría 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 cual 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 (por ejemplo, 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 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 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 añada 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 archivarse, 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. Ésta 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 irrebatible 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 artículos 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) dimanan 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 sirviesen 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 recalcarse 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 Comisión[19] 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]

Notas (referencias generales):

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 28º y 29º, 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 No. 17 (A/50/17), párr. 306.
15 Ibid., párr. 307.
16 Ibid., Cuadragésimo noveno período de sesiones, Suplemento No. 17 (A/49/17), párr. 201.
17 Ibid., Quincuagésimo período de sesiones, Suplemento No. 17 (A/50/17), párr. 309.
18 Ibid., párr. 306.
19 Ibid., cuadragésimo período de sesiones, Suplemento No. 17 (A/40/17), párrs. 354 a 360.
20 Ibid., quincuagésimo primer período de sesiones, Suplemento No. 17 (A/51/17), párr. 209.

LEY MODELO DE LA CNUDMI SOBRE LAS FIRMAS ELECTRÓNICAS

Año 2001. (Extracto del informe de la Comisión de las Naciones Unidas sobre el Derecho Mercantil Internacional sobre la labor de su trigésimo cuarto período de sesiones, celebrado en Viena, desde el 25 de junio al 13 de julio de 2001. El texto de la Ley Modelo de la CNUDMI sobre Firmas Electrónicas fue adoptado el 5 de julio de 2001 [Nota: la versión final de la Guía para la incorporación al derecho interno de la Ley Modelo será publicada durante el segundo semestre del año 2001])

Anexo II - Ley Modelo de la CNUDMI sobre las Firmas Electrónicas (2001)

Artículo 1
Ámbito de aplicación
La presente Ley será aplicable en todos los casos en que se utilicen firmas electrónicas en el contexto* de actividades comerciales**. No derogará 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, aunque no exclusivamente, las operaciones siguientes: toda operación comercial de suministro o intercambio de bienes o servicios; acuerdos de distribución; representación o mandato comercial; facturaje (*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 recogida en el mensaje de datos.
b) Por "certificado" se entenderá todo mensaje de datos u otro registro que confirme el vínculo entre un firmante y los datos de creación de la firma.
c) Por "mensaje de datos" se entenderá la información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax.
d) Por "firmante" se entenderá la persona que posee los datos de creación de la firma y que actúa por cuenta propia o por cuenta de la persona a la que representa.
e) Por "prestador de servicios de certificación" se entenderá la persona que expide certificados y puede prestar otros servicios relacionados con las firmas electrónicas.
f) Por "parte que confía" se entenderá la persona que pueda actuar sobre la base de un certificado o de una firma electrónica.

Artículo 3
Igualdad de tratamiento de las tecnologías para la firma
Ninguna de las disposiciones de la presente Ley, con la excepción del artículo 5, será aplicada de modo que excluya, restrinja o prive de efecto jurídico cualquier método para crear una firma electrónica que cumpla los requisitos enunciados en el párrafo 1) del artículo 6 o que cumpla de otro modo los requisitos del derecho aplicable.

Artículo 4
Interpretación

1. En la interpretación de la presente Ley se tendrán en cuenta su origen internacional y la necesidad de promover la uniformidad en su aplicación y de asegurar la observancia de la buena fe.
2. Las cuestiones relativas a las materias que se rigen por la presente Ley que no estén expresamente resueltas en ella se dirimirán de conformidad con los principios generales en los que se basa esta Ley.

Artículo 5
Modificación mediante acuerdo

Las partes podrán establecer excepciones a la presente Ley o modificar sus efectos mediante acuerdo, salvo que ese acuerdo no sea válido o eficaz conforme al derecho aplicable.

Artículo 6
Cumplimiento del requisito de firma

1. Cuando la ley exija la firma de una persona, ese requisito quedará cumplido en relación con un mensaje de datos si se utiliza una firma electrónica que, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo aplicable, sea fiable y resulte igualmente apropiada para los fines con los cuales se generó o comunicó ese mensaje.
2. El párrafo 1) será aplicable tanto si el requisito a que se refiere está expresado en forma de una obligación como si la ley simplemente prevé consecuencias para el caso de que no haya firma.
3. La firma electrónica se considerará fiable a los efectos del cumplimiento del requisito a que se refiere el párrafo 1) si:
   a) los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante;
   b) los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante;
   c) es posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma; y
   d) cuando uno de los objetivos del requisito legal de firma consista en dar seguridades en cuanto a la integridad de la información a que corresponde, es posible detectar cualquier alteración de esa información hecha después del momento de la firma.
4. Lo dispuesto en el párrafo 3) se entenderá sin perjuicio de la posibilidad de que cualquier persona:
   a) demuestre de cualquier otra manera, a los efectos de cumplir el requisito a que se refiere el párrafo 1), la fiabilidad de una firma electrónica; o
   b) aduzca pruebas de que una firma electrónica no es fiable.
5. Lo dispuesto en el presente artículo no será aplicable a: [Y].

Artículo 7
Cumplimiento de lo dispuesto en el artículo 6

1. [*La persona, el órgano o la entidad, del sector público o privado, a que el Estado promulgante haya expresamente atribuido competencia*] podrá determinar qué firmas electrónicas cumplen lo dispuesto en el artículo 6 de la presente Ley.
2. La determinación que se haga con arreglo al párrafo 1) deberá ser compatible con las normas o criterios internacionales reconocidos.
3. Lo dispuesto en el presente artículo se entenderá sin perjuicio de la aplicación de las normas del derecho internacional privado.

Artículo 8
Proceder del firmante

1. Cuando puedan utilizarse datos de creación de firmas para crear una firma con efectos jurídicos, cada firmante deberá:
   a) actuar con diligencia razonable para evitar la utilización no autorizada de sus datos de creación de la firma;
   b) sin dilación indebida, utilizar los medios que le proporcione el prestador de servicios de certificación conforme al artículo 9 de la presente Ley, o en cualquier caso esforzarse razonablemente, para dar aviso a cualquier persona que, según pueda razonablemente prever el firmante, pueda considerar fiable la firma electrónica o prestar servicios que la apoyen si:
      i) el firmante sabe que los datos de creación de la firma han quedado en entredicho; o
      ii) las circunstancias de que tiene conocimiento el firmante dan lugar a un riesgo considerable de que los datos de creación de la firma hayan quedado en entredicho;

c) cuando se emplee un certificado para refrendar la firma electrónica, actuar con diligencia razonable para cerciorarse de que todas las declaraciones que haya hecho en relación con el ciclo vital del certificado o que hayan de consignarse en él son exactas y cabales.

2. Serán de cargo del firmante las consecuencias jurídicas que entrañe el hecho de no haber cumplido los requisitos enunciados en el párrafo 1).

Artículo 9
Proceder del prestador de servicios de certificación

1. Cuando un prestador de servicios de certificación preste servicios para apoyar una firma electrónica que pueda utilizarse como firma con efectos jurídicos, ese prestador de servicios de certificación deberá:
   a) actuar de conformidad con las declaraciones que haga respecto de sus normas y prácticas;
   b) actuar con diligencia razonable para cerciorarse de que todas las declaraciones importantes que haya hecho en relación con el ciclo vital del certificado o que estén consignadas en él son exactas y cabales;
   c) proporcionar a la parte que confía en el certificado medios razonablemente accesibles que permitan a ésta determinar mediante el certificado:
      i) la identidad del prestador de servicios de certificación;
      ii) que el firmante nombrado en el certificado tenía bajo su control los datos de creación de la firma en el momento en que se expidió el certificado;
      iii) que los datos de creación de la firma eran válidos en la fecha en que se expidió el certificado o antes de ella;
   d) proporcionar a la parte que confía en el certificado medios razonablemente accesibles que, cuando proceda, permitan a ésta determinar mediante el certificado o de otra manera:
      i) el método utilizado para comprobar la identidad del firmante;
      ii) cualquier limitación de los fines o del valor respecto de los cuales puedan utilizarse los datos de creación de la firma o el certificado;
      iii) si los datos de creación de la firma son válidos y no están en entredicho;
      iv) cualquier limitación del alcance o del grado de responsabilidad que haya establecido el prestador de servicios de certificación;
      v) si existe un medio para que el firmante dé aviso de que los datos de creación de la firma están en entredicho, conforme a lo dispuesto en el apartado b) del párrafo 1) del artículo 8 de la presente Ley;
      vi) si se ofrece un servicio para revocar oportunamente el certificado;
   e) cuando se ofrezcan servicios conforme al inciso v) del apartado d), proporcionar un medio para que el firmante dé aviso conforme al apartado b) del párrafo 1) del artículo 8 de la presente Ley y, cuando se ofrezcan servicios en virtud del inciso vi) del apartado d), cerciorarse de que existe un servicio para revocar oportunamente el certificado;
   f) utilizar, al prestar sus servicios, sistemas, procedimientos y recursos humanos fiables.
2. Serán de cargo del prestador de servicios de certificación las consecuencias jurídicas que entrañe el hecho de no haber cumplido los requisitos enunciados en el párrafo 1).

Artículo 10
Fiabilidad

A los efectos del apartado f) del párrafo 1) del artículo 9, para determinar si los sistemas, procedimientos o recursos humanos utilizados por un prestador de servicios de certificación son fiables, y en qué medida lo son, podrán tenerse en cuenta los factores siguientes:

a) los recursos humanos y financieros, incluida la existencia de activos;
b) la calidad de los sistemas de equipo y programas informáticos;
c) los procedimientos para la tramitación del certificado y las solicitudes de certificados, y la conservación de registros;
d) la disponibilidad de información para los firmantes nombrados en el certificado y para las partes que confíen en éste;
e) la periodicidad y el alcance de la auditoría realizada por un órgano independiente;
f) la existencia de una declaración del Estado, de un órgano de acreditación o del prestador de servicios de certificación respecto del cumplimiento o la existencia de los factores que anteceden; o
g) cualesquiera otros factores pertinentes.

Artículo 11
Proceder de la parte que confía en el certificado

Serán de cargo de la parte que confía en el certificado las consecuencias jurídicas que entrañe el hecho de que no haya tomado medidas razonables para:

a) verificar la fiabilidad de la firma electrónica; o
b) cuando la firma electrónica esté refrendada por un certificado:
   i) verificar la validez, suspensión o revocación del certificado; y
   ii) tener en cuenta cualquier limitación en relación con el certificado.

Artículo 12
Reconocimiento de certificados extranjeros y de firmas electrónicas extranjeras

1. Al determinar si un certificado o una firma electrónica producen efectos jurídicos, o en qué medida los producen, no se tomará en consideración:
   a) el lugar en que se haya expedido el certificado o en que se haya creado o utilizado la firma electrónica; ni
   b) el lugar en que se encuentre el establecimiento del expedidor o del firmante.
2. Todo certificado expedido fuera [*del Estado promulgante*] producirá los mismos efectos jurídicos en [*el Estado promulgante*] que todo certificado expedido en [*el Estado promulgante*] si presenta un grado de fiabilidad sustancialmente equivalente.
3. Toda firma electrónica creada o utilizada fuera [*del Estado promulgante*] producirá los mismos efectos jurídicos en [*el Estado promulgante*] que toda firma electrónica creada o utilizada en [*el Estado promulgante*] si presenta un grado de fiabilidad sustancialmente equivalente.
4. A efectos de determinar si un certificado o una firma electrónica presentan un grado de fiabilidad sustancialmente equivalente para los fines de párrafo 2), o del párrafo 3), se tomarán en consideración las normas internacionales reconocidas y cualquier otro factor pertinente.
5. Cuando, sin perjuicio de lo dispuesto en los párrafos 2), 3) y 4), las partes acuerden entre sí la utilización de determinados tipos de firmas electrónicas o certificados, se reconocerá que ese acuerdo es suficiente a efectos del reconocimiento transfronterizo, salvo que el acuerdo no sea válido o eficaz conforme al derecho aplicable.

Anexo C :

Lista, no exhaustiva, de Entidades / Autoridades de Certificación

Anexo C: Lista, no exhaustiva, de Entidades / Autoridades de Certificación (cuya información se encuentra en castellano)[7].

COLOMBIA

- **LATIN TRUST ANDINA S.A**. antes CERTYNET S.A.
  Entidad de certificación cerrada.
  Carrera 7 No. 71-52 torre B oficina 509, Bogotá D.C.
  www.certynet.com

- **CERTICAMARAS**.
  Entidad de certificación abierta.
  Carrera 9 No. 16-21 Bogotá D.C.
  Apartado aéreo 29824
  www.certicamara.com

ESPAÑA

- **Servicio de Certificación de la Cámara de Comercio de Madrid**
- **Fundación Calitax**

Principales prestadores de servicios de certificación españoles:

- **Agencia de Certificación Electrónica** (ACE)
  C/ Rosario Pino, 14-16, 3º dcha.
  28020 Madrid
  Tel: 91 571 65 77
  Fax: 91 571 05 35
  E-mail: info@ace.es
  www.ace.es

- **Cámaras de Comercio** (Camerfirma)
  http://www.camerfirma.com/

- **Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda** (FNMT-RCM),
  http://www.cert.fnmt.es/

- **Fundación para el Estudio de la Seguridad en las Telecomunicaciones** (FESTE)
  C/ Tuset, 20-24, 6º, 6ª
  08006 Barcelona
  Tel: 93 416 1540
  Fax: 93 416 0353
  E-mail: info@feste.org
  http://www.feste.com

- **Internet Publishing Services, s.l** (IPS Seguridad)
  CIF B60929452
  Edificio ECU
  Ctra. de La Coruña, Km. 23,200
  28290 - Parque Rozas
  (Madrid)
  Tel. 91 640 20 52
  Fax 91 640 20 41
  E-mail: ips@mail.ips.es
  http://www.ips.es/

[7] La información sobre las entidades de certificación mencionadas en este documento fue sustraída del Internet.

- **Banco Español de Crédito S.A**. (BANESTO)

Entidades de certificación en España Acreditadas por la Entidad Nacional de Acreditación (ENAC) [8]

- **AENOR** (Asociación Española de Normalización y Certificación)
  C/ Génova, 6 / 28004 Madrid
  Tel: +34 91 432 60 08
  Fax: +34 91 310 40 32
  E-mail: aenor@aenor.es
  Internet: http://www.aenor.es
- **BVQI** (Bureau Veritas Quality International)
  C/ Dr. Fleming 31, 1º. 28036 Madrid
  Tel: +34 91 350 39 59
  Fax: +34 91 350 34 81
- **DNV** (Det Norske Veritas)
  C/ Garrotxa, 10-12. Edf. Océano Parque de Negocios Mas Blau
  08820 El Prat de Llobregat, Barcelona
  Tel: +34 93 902 10 90 00
  Fax: +34 93 478 75 78
- **LGAI** (Laboratori General d'Assaigs i Investigacions)
  Ctra. Acceso Facultad de Medicina de la U.A.B.
  08290 Cerdanyola de Vallès, Barcelona
  Tel: +34 93 691 92 11
  Fax: +34 93 691 59 11
- **ECA, S.A.** (Entidad de Certificación y Aseguramiento, S.A.)
  C/ Raimundo Fernández Villaverde, 57 / 28003 Madrid
  Tel: +34 91 554 13 90
  Fax: +34 91 554 65 58
  E-mail: certificacion@ecaglobal.com
  http://www.ecacertificacion.com/
- **SGS** (TECNOS Garantía de Calidad, S.A.)
  SGS-ICS IBÉRICA AEIE
  C/ Trespaderne, 29. Edf. Barajas,1 / 28042 Madrid
  Tel: +34 91 313 81 16
  Fax: +34 91 313 80 80
- **LRQA** (Lloyd's Register Quality Assurance)
  C/ Las Mercedes, 31-2º / 48930 Getxo, Vizcaya
  Tel: +34 91 806 17 50
  Fax: +34 94 806 01 57

Entidades de certificación en España No Acreditadas por ENAC

- **EQA** (European Quality Assurance Spain)
  C/ Sagasta 12, 2ºA. 28004 Madrid
  Tel: +34 91 448 08 30
  Fax: +34 91 448 87 59
- **Germanischer Lloyd**
  C/ Villanueva, 2 / 28001 Madrid
  Tel: +34 91 431 89 54
  Fax: +34 91 578 12 83

[8] Para mayor información, visite: http://www.cigal.igatel.net/html/cert.htm

- **ICICT**
  C/Garrotxa, 10-12, Edf. Océano. Parque de Negocio Mas Blau
  08820 El Prat Llobregat, Barcelona
  Tel: +34 93 478 11 31
  Fax: +34 93 478 07 68

- **IVAC** (Instituto Valenciano de Certificación)
  C/ Finlandia 21, 2º - Puerta 4. 46010 Valencia
  Tel: +34 93 361 34 08
  Fax: +34 93 361 17 39

- **TÜV Management Service**
  (Grupo Tüv Suddeutchland)
  Avda. de la Industria, 51bis / 28760 Tres Cantos, Madrid
  Tel: +34 91 806 17 50
  Fax: +34 91 804 01 57

- **TÜV Product Service**
  C/ Gascó Oliag 8, 2º- 3ª. 46010 Valencia
  Tel: +34 96 360 11 55
  Fax: +34 91 360 22 40

- **TÜV Rheinland Ibérica, S.A.**
  C/ José Silva, 17. 28043 Madrid
  Tel: +34 91 413 85 55
  Fax: +34 91 413 55 90

- **Quality Management System**
  C/ Machado Palmanova, Edf. Olivia - Local 18 B
  07181Calviá, Palma de Mallorca
  Tel: +34 968 10 04
  Fax: +34 968 19 36

REINO UNIDO

- **European Quality Assurance (EQA).** UK Limited
  Navigation House
  48 Millgate
  NEWARK
  Nottinghamshire NG24 4TY
  Telephone: 01636 611226
  Fax: 01636 611704
  E-mail: Eqaltd@aol.com
  URL: http://www.eqa.es/sistemas_calidad.htm

Lista de Entidades de Certificación Acreditadas por el Forest Stewardship Council (fSC):[9]

AFRICA DEL SUR

- **South African Bureau for Standards (SABS),**
  Louw Bekker; Private Bag X191, Pretoria 0001 África del Sur.
  Tel: + 27 12 428 7911
  Fax: + 27 12 344 1568
  E-mail: debruic@sabs.co.za
  Alcances de la acreditación: Evaluación para la Cadena de Custodia
  en África del Sur y en la Asociación para el Desarrollo de África del Sur.

[9] Para mayor información, visite: http://www.fscoax.org/html/5-3-1_esp.html

ALEMANIA

- **GFA Terra Systems**, Hans-Joachim Droste;
  Eulenkrugstrasse 82, Hamburg 22359 Alemania
  Tel: + 49 40 6030 6140
  Fax:+ 49 40 6030 6189
  E-mail: info@gfa-terra.de
  Website: www.gfa-certification.de
  Alcances de la acreditación: En todo el mundo para
  Manejo de Bosque y Cadena de Custodia

CANADA

- **Silva Forest Foundation,** Susan Hammond;
  P.O. Box 9, Slocan Park BC V0G 2EO Canadá
  Tel: + 1 250 226 7222 Fax: + 1 250 226 7446
  E-mail: silvafor@netidea.com
  Website: www.silvafor.org
  Alcances de la acreditación: Dentro de Canadá
  para Manejo de Bosque y Cadena de Custodia

ESTADOS UNIDOS

- **Rainforest Alliance Smart Wood Program**, Richard Donovan;
  #61 Millet Street, Goodwin Baker Building, Richmond
  Vermont 05477 Estados Unidos
  Tel: + 1 802 434 5491
  Fax: + 1 802 434 3116
  E-mail: info@smartwood.org
  Website: www.smartwood.org
  Alcances de la acreditación: En todo el mundo para
  Manejo de Bosque y Cadena de Custodia

- **Scientific Certification Systems,** Dr. Robert Hrubes;
  Park Plaza Building, 1939 Harrison Street, Suite 400,
  Oakland California 94612-3532 Estados Unidos
  Tel: + 1 510 832 1415
  Fax: + 1 510 832 0359
  E-mail: rhrubes@igc.org
  Website: www.scs1.com
  Alcances de la acreditación: En todo el mundo para
  Manejo de Bosque y Cadena de Custodia

ITALIA

- **ICILA** (Istituto per la Certificazione ed I Servizi per Imprese
  dell'arrendemento e del legno), Ricardo Giordanno;
  Via Braille 5, Lissone (Milano) I-20035 Italia
  Tel: + 39 039 465239
  Fax: + 39 039 465168
  E-mail: envcert@icila.org
  Website: www.icila.org
  Alcances de la acreditación:
  En todo el mundo para Cadena de Custodia

PAÍSES BAJOS

- **SKAL,** Arjan van der Weijden; P.O. Box 161, Zwolle AD 8000 Países Bajos
  Tel: + 31 38 426 01 00
  Fax: + 31 38 423 70 40
  E-mail: avdweijden@skalint.com
  Website: www.skalint.com
  Alcances de la acreditación: En todo el mundo
  para Manejo de Bosque y Cadena de Custodia

REINO UNIDO

- **BM TRADA Certification**, Alasdair McGregor;
  Stirling Business Centre, Wellgreen Place, Stirling
  FK8 2DZ Reino Unido
  Tel:+ 44 1259 272142
  Fax:+ 44 1259 272144
  E-mail: amcgregor@bmtrada.com
  Website: www.bmtrada.com
  Alcances de la acreditación: En todo el mundo
  para Cadena de Custodia

- **SGS Forestry QUALIFOR Programme,** Neil Judd;
  58 St. Aldates, Oxford OX1 1ST Reino Unido
  Tel:+ 44 1865 202 345
  Fax:+ 44 1865 790 441
  E-mail: neil_judd@sgsgroup.ocm
  Website: www.qualifor.com
  Alcances de la acreditación: En todo el mundo para
  Manejo de Bosque y Cadena de Custodia

- **Soil Association, Kevin Jones /** Meriel Robson; Bristol House,
  40-56 Victoria Street, Bristol BSI 6BY Reino Unido
  Tel: + 44 117 914 2435
  Fax: + 44 117 925 2504
  E-mail: kjones@soilassociation.org / mrobson@soilassociation.org
  Website: www.soilassociation.org
  Alcances de la acreditación: En todo el mundo para Manejo
  de Bosque y Cadena de Custodia

SUIZA

- **Institut für Marktökologie IMO,** Thomas Papp-Vary;
  Poststrasse 8, Sulgen CH-8583 Suiza
  Tel: + 41 71 644 9880
  Fax: + 41 71 644 9883
  E-mail: forest@imo.ch
  Website: www.imo.ch
  Alcances de la acreditación: En todo el mundo para
  Manejo de Bosque y Cadena de Custodia

Lista de Entidades de Certificación Solicitantes de acreditación por parte del FSC[10]. las siguientes entidades de certificación han solicitado formalmente la acreditación del FSC. La inclusión en esta lista NO implica reconocimiento de estas organizaciones ni de ninguno de los bosques certificados por ellos. Los bosques certificados por estas organizaciones pueden no traer la marca registrada del FSC hasta y a menos que hayan obtenido la acreditación del FSC.

CANADÁ

- **KPMG FCSI (Forest Certification Services Inc),** Mr. Chris Ridley- Thomas;
  Box 10426 777 Dunsmuir Street, Vancouver BC V7Y 1K3 Canadá
  Tel: + 1 604 691 3000/3376
  Fax: + 1 604 691 3031
  Email: cridley-thomas@kpmg.ca
  Website: www.kpmg.ca

[10] Para mayor información visite: http://www.fscoax.org/html/5-3-2_esp.html

FRANCIA

- **Eurocertifor S.A.,** Mr. Richard Garrigue; 10, mail Raymond Menand,
  Issy les Moulineaux 92130 Francia
  Tel: + 33 1 41 90 67 90
  Fax:+ 33 1 41 90 67 95
  Email: info@eurocertifor.com

ITALIA

- **Certiquality,** Prof. Pietro de Pietri-Tonelli; Certiagro División,
  Via G. Giardino, 4, Milano 20123 Italia
  Tel: + 39 02 8069 1742
  Fax: + 39 02 864 65295
  Email: p.depietri@certiquality.it

MÉXICO

- **Fundación vida para el bosque A.C.,** Mr. Walter Bishop Velarde;
  Apdo. Postal 670, Durango Durango 34000 México
  Tel: + 52 1 812 0262
  Fax: + 52 1 825 0682
  Email: vibo@bosquevibo.org.mx

SUIZA

- **Swiss Association for Quality and Management Systems**,
  Mr. Alfred Urfer; Bernstrasse 103. P.O Box 686, Zollikofen CH-3052 Suiza
  Tel:+31 910 35 35
  Fax:+31 910 35 45
  Email:alfred.urfer@sqs.ch