**LEY MODELO DE LA COMISIÓN DE LAS NACIONES UNIDAS PARA EL DERECHO MERCANTIL INTERNACIONAL (CNUDMI) SOBRE FIRMAS ELECTRÓNICAS**

Proyecto de Ley Modelo y proyecto de guía para la incorporación al derecho interno aprobado por el Grupo de Trabajo en su 38º periodo de Sesiones (Nueva York 12 al 23 de Marzo de 2001) que se presentará a la Comisión para su examen y aprobación en el 34º período de sesiones de ésta, que se celebraría del 25 de junio al 13 de julio de 2001 en Viena.

**Ley Modelo de la CNUDMI para las firmas electrónicas (2001)**

**(aprobada por el Grupo de Trabajo de la CNUDMI sobre Comercio Electrónico en su 37º período de sesiones, celebrado del 18 al 29 de septiembre de 2000 en Viena)**

**Artículo 1. Ámbito de aplicación**

La presente Ley será aplicable en todos los casos en que se utilicen firmas electrónicas en el contexto\* de actividades comerciales\*\*. No 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, sin que esta lista sea taxativa, las operaciones siguientes: toda operación comercial de suministro o intercambio de bienes o servicios; acuerdos de distribución;

representación o mandato comercial; facturaje (Afactoring@); arrendamiento con opción de compra (Aleasing@); construcción de obras; consultoría; ingeniería; concesión de licencias; inversiones; financiación; banca; seguros; acuerdos o concesiones de explotación; empresas conjuntas y otras formas de cooperación industrial o comercial; transporte de mercancías o de pasajeros por vía aérea, marítima y férrea o por carretera.

**Artículo 2. Definiciones**

Para los fines de la presente Ley:

a) Por “firma electrónica” se entenderán los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información contenida en el mensaje de datos;

b) Por “certificado” se entenderá todo mensaje de datos u otro registro que confirme el vínculo entre un firmante y los datos de creación de la firma;

c) Por “mensaje de datos” se entenderá la información generada, enviada, recibida o archivada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax;

d) Por “firmante” se entenderá la persona que posee los datos de creación de la firma y que actúa en nombre propio o de la persona a la que representa;

e) Por “prestador de servicios de certificación” se entenderá la persona que expide certificados y puede prestar otros servicios relacionados con las firmas electrónicas;

f) Por “parte que confía” se entenderá la persona que pueda actuar sobre la base de un certificado o de una firma electrónica.

**Artículo 3. Igualdad de tratamiento de las tecnologías para la firma**

Ninguna de las disposiciones de la presente Ley, con la excepción del artículo 5, será aplicada de modo que excluya, restrinja o prive de efecto jurídico cualquier método para crear una firma electrónica que cumpla los requisitos enunciados en el párrafo 1) del artículo 6 o que cumpla de otro modo los requisitos del derecho aplicable.

**Artículo 4. Interpretación**

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

2) Las cuestiones relativas a materias que se rijan por la presente Ley y que no estén expresamente resueltas en ella serán dirimidas de conformidad con los principios generales en que se inspira.

**Artículo 5. Modificación mediante acuerdo**

Las partes podrán hacer excepciones a la presente Ley o modificar sus efectos mediante acuerdo, salvo que ese acuerdo no sea válido o eficaz conforme al derecho aplicable.

**Artículo 6. Cumplimiento del requisito de firma**

1) Cuando la ley exija la firma de una persona, ese requisito quedará cumplido en relación con un mensaje de datos si se utiliza una firma electrónica que, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo aplicable, sea tan fiable como resulte apropiado a los fines para los cuales se generó o comunicó ese mensaje.

2) El párrafo 1) será aplicable tanto si el requisito a que se refiere está expresado en la forma de una obligación como si la ley simplemente prevé consecuencias para el caso de que no haya firma.

3) La firma electrónica se considerará fiable a los efectos del cumplimiento del requisito a que se refiere el párrafo 1) si:

a) los datos de creación de la firma, en el contexto en que son utilizados,corresponden exclusivamente al firmante;

b) los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivodel firmante;

c) es posible detectar cualquier alteración de la firma electrónica hecha después del momento de lafirma; y

d) cuando uno de los objetivos del requisito legal de firma consista en dar seguridades en cuanto a la integridad de la información a que corresponde, es posible detectar cualquier alteración de esa información hecha después del momento de la firma.

4) Lo dispuesto en el párrafo 3) se entenderá sin perjuicio de la posibilidad de que cualquier persona:

a) demuestre de cualquier otra manera, a los efectos de cumplir el requisito a que se refiere el párrafo 1), la fiabilidad de una firma electrónica; o

b) aduzca pruebas de que una firma electrónica no es fiable.

5) Lo dispuesto en el presente artículo no será aplicable a: [Y].

**Artículo 7. Cumplimiento de lo dispuesto en el artículo 6**

1) [La persona, el órgano o la entidad, del sector público o privado, a que el Estado promulgante haya expresamente atribuido competencia] podrá determinar qué firmas electrónicas cumplen lo dispuesto en el artículo 6.

2) La determinación que se haga con arreglo al párrafo 1) deberá ser compatible con las normas o criterios internacionales reconocidos.

3) Lo dispuesto en el presente artículo se entenderá sin perjuicio de la aplicación de las normas del derecho internacional privado.

**Artículo 8. Proceder del firmante**

1) Cuando puedan utilizarse datos de creación de firmas para crear una firma con efectos jurídicos, cada firmante deberá:

a) actuar con diligencia razonable para evitar la utilización no autorizada de sus datos de creación de la firma;

b) dar aviso sin dilación indebida a cualquier persona que, según pueda razonablemente prever, pueda considerar fiable la firma electrónica o prestar servicios que la apoyen si:

i) sabe que los datos de creación de la firma han quedado en entredicho; o

ii) las circunstancias de que tiene conocimiento dan lugar a un riesgo considerable de que los datos de creación de la firma hayan quedado en entredicho;

c) cuando se emplee un certificado para refrendar la firma electrónica, actuar con diligencia razonable para cerciorarse de que todas las declaraciones que haya hecho en relación con su ciclo vital o que hayan de consignarse en él sean exactas y cabales.

2) El firmante incurrirá en responsabilidad por el incumplimiento de los requisitos enunciados en el párrafo 1).

**Artículo 9. Proceder del prestador de servicios de certificación**

1) Cuando un prestador de servicios de certificación preste servicios para apoyar una firma electrónica que pueda utilizarse como firma con efectos jurídicos, ese prestador de servicios de certificación deberá:

a) actuar de conformidad con las declaraciones que haga respecto de sus normas y prácticas;

b) actuar con diligencia razonable para cerciorarse de que todas las declaraciones importantes que haya hecho en relación con el ciclo vital del certificado o que estén consignadas en él sean exactas y cabales;

c) proporcionar medios de acceso razonablemente fácil que permitan a la parte que confía en el certificado determinar mediante éste:

i) la identidad del prestador de servicios de certificación;

ii) que el firmante nombrado en el certificado tenía bajo su control los datos de creación de la firma en el momento en que se expidió el certificado;

iii) que los datos de creación de la firma eran válidos en la fecha en que se expidió el certificado o antes de ella;

d) proporcionar medios de acceso razonablemente fácil que, según proceda, permitan a la parte que confía en el certificado determinar mediante éste o de otra manera:

i) el método utilizado para identificar al firmante;

ii) cualquier limitación en los fines o el valor respecto de los cuales puedan utilizarse los datos de creación de la firma o el certificado;

iii) si los datos de creación de la firma son válidos y no están en entredicho;

iv) cualquier limitación en cuanto al ámbito o el alcance de la responsabilidad indicada por el prestador de servicios de certificación;

v) si existe un medio para que el firmante dé aviso de que los datos de creación de la firma están en entredicho, conforme a lo dispuesto en el apartado b) del párrafo 1) del artículo 8;

vi) si se ofrece un servicio de revocación oportuna del certificado;

e) cuando se ofrezcan servicios conforme al inciso v) del apartado d), proporcionar un medio para que el firmante dé aviso conforme al apartado b) del párrafo 1) del artículo 8 y, cuando se ofrezcan servicios en virtud del inciso vi) del apartado d), cerciorarse de que exista un servicio de revocación oportuna del certificado;

f) utilizar, al prestar sus servicios, sistemas, procedimientos y recursos humanos fiables.

2) El prestador de servicios de certificación incurrirá en responsabilidad por el incumplimiento de los requisitos enunciados en el párrafo 1).

**Artículo 10. Fiabilidad**

A los efectos del apartado f) del párrafo 1) del artículo 9, para determinar si los sistemas, procedimientos o recursos humanos utilizados por un prestador de servicios de certificación son fiables, y en qué medida lo son, podrán tenerse en cuenta los factores siguientes:

a) los recursos humanos y financieros, incluida la existencia de un activo;

b) la calidad de los sistemas de equipo y programas informáticos;

c) los procedimientos para la tramitación del certificado y las solicitudes de certificados, y la conservación de registros;

d) la disponibilidad de información para los firmantes nombrados en el certificado y para las partes que confíen en éste;

e) la periodicidad y el alcance de la auditoría por un órgano independiente;

f) la existencia de una declaración del Estado, de un órgano de acreditación o del prestador de servicios de certificación respecto del cumplimiento o la existencia de los factores que anteceden; y

g) cualesquiera otros factores pertinentes.

Artículo 11. Proceder de la parte que confía en el certificado

Serán de cargo de la parte que confía en el certificado las consecuencias jurídicas que entrañe el hecho de que no haya tomado medidas razonables para:

a) verificar la fiabilidad de la firma electrónica; o

b) cuando la firma electrónica esté refrendada por un certificado:

i) verificar la validez, suspensión o revocación del certificado; y

ii) tener en cuenta cualquier limitación en relación con el certificado.

Artículo 12. Reconocimiento de certificados y firmas electrónicas extranjeros

1) Al determinar si un certificado o una firma electrónica produce efectos jurídicos, o en qué medida los produce, no se tomará en consideración:

a) el lugar en que se haya expedido el certificado o en que se haya creado o

utilizado la firma electrónica; ni

b) el lugar en que se encuentre el establecimiento del expedidor o firmante.

2) Todo certificado expedido fuera [del Estado promulgante] producirá los mismos efectos jurídicos en [el Estado promulgante] que todo certificado expedido en [el Estado promulgante] si presenta un grado de fiabilidad sustancialmente equivalente.

3) Toda firma electrónica creada o utilizada fuera [del Estado promulgante] producirá los mismos efectos jurídicos en [el Estado promulgante] que toda firma electrónica creada o utilizada en [el Estado promulgante] si presenta un grado de fiabilidad sustancialmente equivalente.

4) A efectos de determinar si un certificado o una firma electrónica presentan un grado de fiabilidad sustancialmente equivalente para los fines de párrafo 2), o del párrafo 3), se tomarán en consideración las normas internacionales reconocidas y cualquier otro factor pertinente.

5) Cuando, sin perjuicio de lo dispuesto en los párrafos 2), 3) y 4), las partes acuerden entre sí la utilización de determinados tipos de firmas electrónicas y certificados, se reconocerá que ese acuerdo es suficiente a efectos del reconocimiento transfronterizo, salvo que ese acuerdo no sea válido o eficaz conforme al derecho aplicable.