



Asamblea General

Distr. limitada
28 de enero de 2019
Español
Original: inglés

**Comisión de las Naciones Unidas para
el Derecho Mercantil Internacional**
Grupo de Trabajo IV (Comercio Electrónico)
58º período de sesiones
Nueva York, 8 a 12 de abril de 2019

Proyecto de disposiciones sobre el reconocimiento transfronterizo de sistemas de gestión de la identidad y servicios de confianza

Nota de la Secretaría

Índice

	<i>Página</i>
I. Introducción	2
Anexo I. Proyecto de disposiciones sobre el reconocimiento transfronterizo de sistemas de gestión de la identidad y servicios de confianza	3



I. Introducción

1. En el 57º período de sesiones del Grupo de Trabajo, se pidió que en los documentos que preparara la Secretaría en el futuro se presentaran propuestas de disposiciones sobre las cuestiones fundamentales a fin de facilitar el avance de la labor del Grupo de Trabajo sobre las cuestiones jurídicas relacionadas con la gestión de la identidad y los servicios de confianza.
2. En consonancia con esa solicitud, en el anexo I de la presente nota figura un proyecto de disposiciones sobre diversas cuestiones que el Grupo de Trabajo ha examinado hasta la fecha. Las disposiciones se basan, en la medida de lo posible, en las deliberaciones sostenidas por el Grupo de Trabajo en su 57º período de sesiones ([A/CN.9/WG.IV/WP.153](#)). En el documento [A/CN.9/WG.IV/WP.158](#) figuran más observaciones sobre estas y otras cuestiones pertinentes.

Anexo I

Proyecto de disposiciones sobre el reconocimiento transfronterizo de sistemas de gestión de la identidad y servicios de confianza

Capítulo I. Ámbito de aplicación

Artículo 1. Ámbito de aplicación

[Opción A para el texto del párrafo 1

1. El presente [proyecto de instrumento] será aplicable a la utilización de sistemas de gestión de la identidad y servicios de confianza en relación con operaciones comerciales celebradas entre partes que tengan sus establecimientos en Estados diferentes [cuando las normas de derecho internacional privado prevean la aplicación de la ley de una jurisdicción promulgante.]

[Opción B para el texto del párrafo 1

1. El presente [proyecto de instrumento] será aplicable al reconocimiento transfronterizo de [los sistemas de gestión de la identidad] [las credenciales de identidad] y los servicios de confianza que se utilicen en el contexto de actividades comerciales¹.

2. El presente [proyecto de instrumento] será aplicable también a la utilización de sistemas de gestión de la identidad y servicios de confianza en el contexto de servicios públicos relacionados con el comercio².

3. El presente [proyecto de instrumento] será aplicable a la verificación de la identidad de las personas físicas y jurídicas, así como de los objetos físicos y digitales.

Artículo 2. Cuestiones no afectadas por este [proyecto de instrumento]

1. Nada de lo dispuesto en el presente [proyecto de instrumento] obligará a persona alguna a verificar la identidad de un sujeto o a utilizar un servicio de confianza, ni a verificar la identidad de un sujeto o utilizar un servicio de confianza que ofrezca un determinado nivel de fiabilidad.

2. Salvo en los casos previstos en el presente [proyecto de instrumento], nada de lo dispuesto en [él] afectará a la aplicación a [los sistemas de gestión de la identidad y los servicios de confianza] de norma de derecho alguna que sea aplicable a [los sistemas de gestión de la identidad y los servicios de confianza] [, incluidas las normas jurídicas aplicables a la protección de los datos y de la privacidad]³.

¹ En el Grupo de Trabajo se han expresado distintas opiniones en cuanto al “objeto” del reconocimiento jurídico en relación con su labor sobre la gestión de la identidad. En su 57^o período de sesiones, el Grupo de Trabajo analizó los sistemas de gestión de la identidad, las credenciales de identidad y las operaciones de identidad como posibles objetos de reconocimiento jurídico.

² El objetivo de esta disposición es destacar que los sistemas de gestión de la identidad y los servicios de confianza pueden utilizarse fuera de un entorno puramente comercial.

³ Las palabras “incluidas las normas jurídicas aplicables a la protección de los datos y de la privacidad” tienen por objeto responder a las inquietudes del Grupo de Trabajo con respecto a la aplicación de las leyes de protección de los datos y de la privacidad.

Artículo 3. Utilización voluntaria de sistemas de gestión de la identidad y servicios de confianza

1. Nada de lo dispuesto en el presente [proyecto de instrumento] obligará a sujeto alguno a [utilizar un sistema de gestión de la identidad] [aceptar credenciales de identidad] [ni a] utilizar un servicio de confianza sin su consentimiento.
2. A los efectos de lo dispuesto en el párrafo 1, el consentimiento de un sujeto podrá inferirse de su conducta [o de otras circunstancias]⁴.

Capítulo II. Disposiciones generales

Artículo 4. Definiciones

A los efectos del presente [proyecto de instrumento]:

- a) Por “atributo” se entenderá un elemento de información o datos vinculados a un sujeto⁵;
- b) Por “identificación” se entenderá el proceso de reunión, verificación y validación de atributos de identidad de un sujeto que sean suficientes para definir y confirmar su identidad en un contexto en particular⁶;
- c) Por “identidad” se entenderá un conjunto de atributos relativos a un sujeto que [permita distinguirlo suficientemente] [lo describa de un modo singular] dentro de un contexto determinado⁷;
- d) Por “credenciales de identidad” se entenderá [un conjunto de datos que se presenta como prueba de la identidad declarada] [los datos, o el objeto físico en que pueden residir los datos, que un sujeto puede presentar para verificar o autenticar su identidad en un contexto en línea]^{8 9};
- e) Por “gestión de la identidad [electrónica]” se entenderá un conjunto de procesos mediante el cual se gestiona la identificación, autenticación [y autorización] de sujetos en un contexto en línea¹⁰;

⁴ Las palabras “o de otras circunstancias” se refieren a los casos en que el sujeto no es capaz de tener una conducta autónoma, como los objetos físicos o digitales. En esos casos, el consentimiento no será atribuible al sujeto, sino a la persona física o jurídica que sea legalmente responsable de ese sujeto (A/CN.9/965, párr. 109).

⁵ Véase A/CN.9/WG.IV/WP.150, párr. 13.

⁶ Véase A/CN.9/WG.IV/WP.150, párr. 29. El Grupo de Trabajo tal vez desee plantearse si debería incluirse en esta definición la inscripción en un sistema de gestión de la identidad y la emisión de credenciales de identidad.

⁷ Véase A/CN.9/WG.IV/WP.150, párr. 38. Cuando examine la definición de “identidad”, el Grupo de Trabajo tal vez desee plantearse si será necesario exigir la singularidad a los efectos de la labor del Grupo de Trabajo sobre este tema, habida cuenta de que: a) la singularidad es una cualidad de la identidad primaria, y b) la identidad primaria está excluida actualmente del ámbito de su labor (A/CN.9/965, párr. 10).

⁸ Esta definición es una adaptación de la que figura en el artículo 59.1-550 de la Ley de Gestión de la Identidad Electrónica de Virginia (título 59.1, capítulo 50, del Código de Virginia).

⁹ Véase A/CN.9/WG.IV/WP.150, párr. 21. El término “credenciales de identidad” es, en sentido amplio, sinónimo del término “medios de identificación electrónica” que se define en el artículo 3, párr. 2, del Reglamento (UE) núm. 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (reglamento eIDAS), como “una unidad material y/o inmaterial que contiene los datos de identificación de una persona y que se utiliza para la autenticación en servicios en línea”.

¹⁰ Véase A/CN.9/WG.IV/WP.150, párr. 35. En el 57º período de sesiones del Grupo de Trabajo, se dijo que esa definición podría hacer pensar que era necesario mencionar conjuntamente la “identificación”, la “autenticación” y la “autorización”; sin embargo, cualquiera de esos elementos sería suficiente. Por tal motivo, se sostuvo que era preferible la definición de “identificación electrónica” que figuraba en el reglamento eIDAS (A/CN.9/965, párr. 91). El término

f) Por “operador del sistema de gestión de la identidad” se entenderá la persona que gestiona dicho sistema;

g) Por “nivel de garantía” se entenderá una designación del grado de confianza en los procesos de identificación y autenticación, es decir: a) el grado de confianza en el proceso de análisis utilizado para determinar la identidad de un sujeto al que se ha emitido una credencial, y b) el grado de confianza en que el sujeto que utiliza la credencial es el sujeto al que se ha emitido esa credencial. La garantía refleja la fiabilidad de los métodos, procesos y tecnologías empleados¹¹;

h) Por “parte que confía” se entenderá toda persona que pueda actuar sobre la base de sistemas de gestión de la identidad o servicios de confianza;

i) Por “sujeto” se entenderá la persona o el objeto que se identifique en una determinada credencial de identidad y cuya identidad pueda ser autenticada y certificada por un proveedor de identidad¹²;

j) Por “servicio de confianza”¹³ se entenderá un servicio electrónico que ofrezca cierto grado de fiabilidad en cuanto a la calidad de los datos;

k) Por “proveedor de servicios de confianza” se entenderá la persona que preste uno o más servicios de confianza.

Artículo 5. Interpretación

1. La interpretación del presente [instrumento] se regirá por los siguientes principios generales:

- a) no discriminación contra el uso de medios electrónicos;
- b) neutralidad tecnológica;
- c) equivalencia funcional;
- d) [...]

2. En la interpretación del presente [proyecto de instrumento] habrán de tenerse en cuenta su carácter internacional y la necesidad de promover la uniformidad en su aplicación y la observancia de la buena fe.

3. Las cuestiones relativas a las materias que se rigen por el presente [proyecto de instrumento] que no estén expresamente resueltas en él se dirimirán de conformidad con los principios generales en que se basa este [instrumento] [o, a falta de tales principios, de conformidad con la ley aplicable en virtud de las normas del derecho internacional privado]¹⁴.

Artículo 6. No discriminación contra el uso de medios electrónicos

1. No se negarán efectos jurídicos, validez, fuerza ejecutoria ni admisibilidad como prueba a la utilización de [credenciales de identidad] [un sistema de gestión de la identidad] por la sola razón de que [esas credenciales de identidad estén] [los resultados

“identificación electrónica” está definido en el artículo 3, párr. 1, del reglamento eIDAS, como “el proceso de utilizar los datos de identificación de una persona [es decir, las “credenciales de identidad”, tal como se definen en el presente documento] en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica”.

¹¹ Véase [A/CN.9/WG.IV/WP.150](#), párr. 42.

¹² Véase [A/CN.9/WG.IV/WP.150](#), párr. 38.

¹³ El Grupo de Trabajo tal vez desee plantearse si en inglés debería decirse “trusted service” (en lugar de “trust service”) para evitar cualquier ambigüedad en relación con el concepto jurídico firmemente establecido de “trust” en el sentido de “fideicomiso” ([A/CN.9/965](#), párrs. 14 y 101).

¹⁴ La frase “o, a falta de tales principios, de conformidad con la ley aplicable en virtud de las normas del derecho internacional privado”, que se añadió a esta disposición, puede resultar especialmente útil en el contexto transfronterizo.

de la verificación de la identidad estén] [el sistema de gestión de la identidad esté] en forma electrónica¹⁵.

2. No se negarán efectos jurídicos, validez, fuerza ejecutoria ni admisibilidad como prueba a un servicio de confianza por la sola razón de que se preste en forma electrónica.

Artículo 7. Neutralidad tecnológica

Nada de lo dispuesto en el presente [proyecto de instrumento] se aplicará de modo que excluya, restrinja o prive de efectos jurídicos a cualquier [tecnología, método o sistema] utilizado para gestionar la identidad o prestar servicios de confianza que cumpla los requisitos enunciados en el presente [proyecto de instrumento] [, o que cumpla de otro modo los requisitos del derecho aplicable]¹⁶.

Capítulo III. Gestión de la identidad

Artículo 8. Reconocimiento jurídico de un sistema de gestión de la identidad

[Opción A para el texto del artículo 8

Cuando la ley o las partes requieran¹⁷ que se identifique a un sujeto con arreglo a determinado método, ese requisito se dará por cumplido respecto de un sistema de gestión de la identidad si se utiliza un método fiable para verificar los atributos pertinentes del sujeto con el mismo nivel de garantía que proporcione dicho método.]¹⁸

[Opción B para el texto del artículo 8

Cuando las partes, por voluntad propia o por disposición de la ley, deban identificar a un sujeto, la utilización de un sistema de gestión de la identidad con ese propósito surtirá los mismos efectos jurídicos que la aplicación de un procedimiento no electrónico reconocido para ese fin si el sistema de gestión de la identidad emplea un método fiable para verificar los atributos del sujeto que sean pertinentes a esos efectos.]¹⁹

Artículo 9. Normas de fiabilidad para el reconocimiento de un sistema de gestión de la identidad

Para determinar la fiabilidad de un sistema de gestión de la identidad a los efectos del requisito a que se refiere el artículo 8, se tendrán en cuenta todas las circunstancias del caso, incluidas las siguientes:

- a) lo que hubiesen acordado las partes;

¹⁵ La elección entre “credenciales de identidad” y “sistema de gestión de la identidad” depende de si el objeto del reconocimiento jurídico son las credenciales de identidad o los sistemas de gestión de la identidad (véanse la nota 1 *supra* y la sección relativa al reconocimiento jurídico del documento [A/CN.9/WG.IV/WP.158](#)). En cambio, si el objeto del reconocimiento jurídico es el resultado del proceso de identificación (es decir, la “operación de identidad”), la disposición podría referirse a ese proceso.

¹⁶ La frase “o que cumpla de otro modo los requisitos del derecho ley aplicable”, que figura en el artículo 3 de la Ley Modelo de la CNUDMI sobre las Firmas Electrónicas, publicación de las Naciones Unidas, núm. de venta S.02.V.8 (LMFE), se refiere a la posibilidad de que otro régimen legal que no sea el proyecto de instrumento exija, en determinados casos, el cumplimiento de requisitos diferentes de los establecidos en el proyecto de instrumento.

¹⁷ El Grupo de Trabajo tal vez desee plantearse si las disposiciones sobre la equivalencia funcional deberían hacerse extensivas a los casos en que la ley “permita” algo, y confirmar que el uso del verbo “requerir” supone una referencia implícita a las consecuencias jurídicas de la falta de ese algo.

¹⁸ Véase [A/CN.9/965](#), párr. 77. El Grupo de Trabajo tal vez desee aclarar si la referencia a “determinado método” tiene por objeto establecer un vínculo con los medios de identificación en papel.

¹⁹ Véase [A/CN.9/965](#), párr. 78.

- b) cualquier supervisión o certificación que se hubiera realizado con respecto al sistema de gestión de la identidad;
- c) el nivel de garantía vinculado al sistema de gestión de la identidad²⁰;
- d) [...]

Artículo 10. [Presunción] de fiabilidad de los sistemas de gestión de la identidad

1. Un sistema de gestión de la identidad [cumplirá el] [se presumirá fiable a los efectos del cumplimiento del] requisito a que se refiere el artículo 8 si se cumplen las condiciones siguientes:

- a) [descripción del conjunto mínimo de normas adecuadas sobre la forma en que deben funcionar los sistemas de gestión de la identidad, incluidos los aspectos relacionados con la auditoría, los seguros, la certificación, la responsabilidad, la cancelación y demás cuestiones que sean pertinentes para determinar el nivel de garantía];
- b) [descripción de los mecanismos utilizados para asegurar y comprobar que los participantes apliquen las normas]; y
- c) [descripción de los mecanismos utilizados para dar publicidad al cumplimiento por el sistema de gestión de la identidad del conjunto mínimo de normas adecuadas]²¹.

[2. Lo dispuesto en el párrafo 1 se entenderá sin perjuicio de la posibilidad de que una persona:

- a) demuestre de cualquier otra manera, a los efectos de cumplir el requisito a que se refiere el artículo 8, la fiabilidad del sistema de gestión de la identidad; o
- b) aduzca pruebas de que el sistema de gestión de la identidad no es fiable.]²²

Artículo 11. Determinación de la fiabilidad de los sistemas de gestión de la identidad

1. [La persona, el órgano o la entidad, ya sea del sector público o del privado, que el Estado promulgante indique] podrá determinar qué sistemas de gestión de la identidad cumplen el requisito a que se refiere el artículo 8²³.
2. La determinación que se haga con arreglo al párrafo 1 deberá ser congruente con las normas internacionales reconocidas.

Artículo 12. Obligaciones de los operadores de sistemas de gestión de la identidad

1. Todo operador de un sistema de gestión de la identidad deberá:
 - a) atribuir las credenciales de identidad a la persona que corresponda²⁴;
 - b) garantizar la disponibilidad en línea y el funcionamiento correcto de los procesos de gestión de la identidad.

²⁰ Esta disposición tiene por objeto permitir la aplicación de un enfoque *ex post* al reconocimiento.

²¹ Esta disposición es compatible tanto con el enfoque *ex ante* como con el enfoque *ex post* del reconocimiento.

²² Esta disposición se inspira en el artículo 6, párr. 3, de la LMFE. Es aplicable si en el párrafo 1 se establece una presunción de fiabilidad.

²³ Esta disposición, que se basa en el artículo 7 de la LMFE, tiene por objeto permitir la aplicación de un enfoque *ex ante* al reconocimiento.

²⁴ El Grupo de Trabajo tal vez desee plantearse si esta obligación debería hacerse extensiva a la atribución de atributos.

2. Todo operador de un sistema de gestión de la identidad deberá notificar sin demora [y, en todo caso, dentro de los [...] días siguientes a la fecha en que haya tomado conocimiento de ello,] [al órgano de supervisión] [a sus clientes²⁵ y partes que confían que resulten afectados] cualquier falla de seguridad o pérdida de integridad que repercuta [de manera considerable] en las credenciales de identidad o los procesos de autenticación suministrados o los datos personales guardados en el sistema.

3. En caso de que se produzca una falla de seguridad grave o una pérdida de integridad considerable, el operador del sistema de gestión de la identidad deberá suspender la prestación de los servicios afectados [hasta [...]].

4. Todo usuario²⁶ de un sistema de gestión de la identidad deberá notificar al operador de dicho sistema cuando:

a) las credenciales de identidad o los procesos de autenticación hayan quedado comprometidos; o

b) las circunstancias de que tiene conocimiento el usuario dan lugar a un riesgo considerable de que las credenciales de identidad o los procesos de autenticación puedan haber quedado comprometidos²⁷.

Artículo 13. Responsabilidad de los operadores de sistemas de gestión de la identidad

1. Sin perjuicio de la responsabilidad que pudiera estar prevista en la ley, todo operador de un sistema de gestión de la identidad que incumpla las obligaciones que le impone el presente [proyecto de instrumento] [responderá] [deberá asumir las consecuencias jurídicas derivadas] de los daños y perjuicios que dicho incumplimiento cause [deliberadamente o por negligencia] a cualquier persona.

2. Los operadores de sistemas de gestión de la identidad no responderán de los daños y perjuicios derivados de todo uso de los servicios que exceda las limitaciones establecidas [en cuanto a los fines o el valor de las operaciones para las que puede utilizarse el sistema de gestión de la identidad] si han proporcionado medios razonablemente accesibles que permitan [al usuario²⁸ o] a un tercero determinar cuáles son esas limitaciones²⁹.

3. El operador de un sistema de gestión de la identidad no [se presumirá responsable] [incurrirá en responsabilidad] si [la emisión de la credencial de identidad o la asignación de un atributo de identidad] se ajusta a:

a) [las normas aplicables en materia de gestión de la identidad;]

b) [las cláusulas de cualquier contrato que sean aplicables; y]

c) [las normas y principios escritos del marco de confianza de la identidad del que sea miembro el operador].

²⁵ El Grupo de Trabajo tal vez desee considerar la posibilidad de definir los conceptos de “usuario” y “cliente”.

²⁶ El Grupo de Trabajo tal vez desee considerar la posibilidad de definir los conceptos de “usuario” y “cliente”.

²⁷ Esta disposición contiene texto opcional a fin de establecer un plazo dentro del cual deberá hacerse la notificación, indicar las partes a quienes habrá que notificar y determinar de qué magnitud deben ser los efectos en los servicios, las credenciales de identidad o los datos personales para que nazca la obligación de notificar. También es posible establecer la obligación de suspender el funcionamiento del sistema de gestión de la identidad hasta que se contenga la falla o la pérdida o se instituya un nuevo proceso de certificación u otro proceso similar.

²⁸ El Grupo de Trabajo tal vez desee considerar la posibilidad de definir los conceptos de “usuario” y “cliente”.

²⁹ Esta disposición tiene por objeto reconocer la validez de las estipulaciones contractuales por las que se limite la responsabilidad.

[4. El párrafo 3 no es aplicable a los casos en que el operador del sistema de gestión de la identidad haya cometido un acto o una omisión que constituya [negligencia grave o una conducta dolosa].]

Capítulo IV. Servicios de confianza

Artículo 14. Reconocimiento jurídico de un servicio de confianza

Firmas electrónicas³⁰

[Opción A para el texto del párrafo 1

1. Cuando la ley requiera³¹ la firma de una persona, ese requisito se dará por cumplido si se utiliza un método fiable para determinar la identidad de esa persona y para indicar la voluntad que tiene esa persona respecto de la información contenida en [la comunicación electrónica]³².]

[Opción B para el texto del párrafo 1

1. Cuando la ley requiera la firma de una persona, ese requisito se dará por cumplido:
- a) si se utiliza un método para determinar la identidad de esa persona y para indicar la voluntad que tiene esa persona respecto de la información contenida en [la comunicación electrónica]; y
 - b) si el método empleado:
 - i) o bien es tan fiable como sea apropiado para los fines para los que se generó o transmitió [la comunicación electrónica], atendidas todas las circunstancias del caso, incluido todo acuerdo aplicable; o
 - ii) se ha demostrado en la práctica que, por sí solo o con el respaldo de otras pruebas, dicho método ha cumplido las funciones enunciadas en el apartado a) *supra*³³.]

Sellos de tiempo electrónicos

2. Cuando la ley requiera que [determinados documentos, registros o información] estén vinculados a una fecha y hora, ese requisito se dará por cumplido [respecto de una comunicación electrónica] si se utiliza un método fiable para vincular la fecha y hora a [esa comunicación electrónica]³⁴.

³⁰ El Grupo de Trabajo tal vez desee plantearse si los sellos electrónicos deberían considerarse un servicio de confianza diferenciado o si podrían considerarse una subcategoría de las firmas electrónicas.

³¹ El Grupo de Trabajo tal vez desee plantearse si las disposiciones sobre la equivalencia funcional deberían hacerse extensivas a los casos en que la ley “permita” algo, y confirmar que el uso del verbo “requerir” supone una referencia implícita a las consecuencias jurídicas de la falta de ese algo.

³² Esta disposición, que se basa en el artículo 9 de la Ley Modelo de la CNUDMI sobre Documentos Transmisibles Electrónicos, publicación de las Naciones Unidas, número de venta: S.17.V.5 (LMDTE), puede adaptarse para indicar las funciones que se pretenda que cumpla el uso de cada servicio de confianza. Esta disposición no ofrece orientación sobre las normas de fiabilidad, lo que podría hacerse en otra disposición separada, aplicable a todos los servicios de confianza (véase, por ejemplo, el art. 12 de la LMDTE).

³³ Esta opción, que se basa en el artículo 9, párr. 3, de la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales (Nueva York, 2005), ofrece una orientación general sobre las normas de fiabilidad. El apartado b) ii) prevé una cláusula de seguridad para evitar que se rechace una firma electrónica cuando esta ha cumplido efectivamente su función.

³⁴ El Grupo de Trabajo tal vez desee plantearse si debería hacerse referencia a una comunicación electrónica, a mensajes de datos o a algún otro concepto.

Archivado electrónico

3. Cuando la ley requiera que se conserven [determinados documentos, registros o información], ese requisito quedará satisfecho mediante la conservación de los mensajes de datos, siempre que se cumplan las condiciones siguientes:

- a) que sea posible acceder a la información contenida en ellos de manera que pueda consultarse posteriormente;
- b) que el mensaje de datos se conserve con el formato en que se haya generado, enviado o recibido, o con algún formato que pueda demostrarse que reproduce con exactitud la información generada, enviada o recibida; y
- c) que se conserve, de haberla, la información que permita determinar el origen y el destino del mensaje de datos y la fecha y hora en que fue enviado o recibido³⁵.

Servicios de entrega electrónica certificada

4. Cuando la ley requiera la prueba del envío o la recepción de [determinado documento, registro o información], ese requisito se dará por cumplido [respecto de una comunicación electrónica] si se utiliza un método fiable para transmitir [esa comunicación electrónica]³⁶.

Autenticación de sitios web

5. Cuando la ley requiera la identificación del propietario de un sitio web, ese requisito se dará por cumplido si se utiliza un método fiable para determinar la identidad de la persona que es propietaria de ese sitio web y para vincular esa persona al sitio web.

Servicios electrónicos de depósito en garantía

6. Cuando la ley requiera el uso de servicios de depósito en garantía, ese requisito se dará por cumplido si se utiliza un método fiable para [dejar en custodia los bienes depositados en garantía y entregarlos a la parte que tenga derecho a recibirlos].

Artículo 15. Presunción de fiabilidad de los servicios de confianza³⁷

1. Se presumirá que un método es fiable a los efectos del cumplimiento del requisito a que se refiere el artículo 14 si:

- a) los datos de creación de la firma, en el contexto en que son utilizados, están vinculados 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 con posterioridad al momento de la firma; y si,
- d) cuando uno de los objetivos del requisito legal de la firma sea garantizar la integridad de la información a que corresponde, es posible detectar cualquier alteración de esa información hecha después del momento de la firma³⁸.

³⁵ Esta condición no es aplicable a la información que tenga por única finalidad permitir el envío o la recepción del mensaje: véase el párr. 2 del art. 10 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico, publicación de las Naciones Unidas, número de venta: S.99.V.4.

³⁶ El Grupo de Trabajo tal vez desee plantearse si debería hacerse referencia a una comunicación electrónica, a mensajes de datos o a algún otro concepto.

³⁷ En su redacción actual, esta disposición se aplica a las firmas electrónicas, pero puede adaptarse para que sea aplicable a otros servicios de confianza.

³⁸ Esta disposición puede utilizarse cada vez que se exija que un servicio de confianza garantice la integridad.

2. Lo dispuesto en el párrafo 1 se entenderá sin perjuicio de la posibilidad de que una persona:

- a) demuestre de cualquier otra manera, a los efectos de cumplir el requisito a que se refiere el artículo 14, la fiabilidad de la firma electrónica; o
- b) aduzca pruebas de que la firma electrónica no es fiable³⁹.

*Artículo 16. Determinación de la fiabilidad de los servicios de confianza*⁴⁰

1. [La persona, el órgano o la entidad, ya sea del sector público o del privado, que el Estado promulgante indique] podrá determinar qué firmas electrónicas cumplen lo dispuesto en el artículo 14.
2. La determinación que se haga con arreglo al párrafo 1 deberá ser congruente con las normas internacionales reconocidas.

Artículo 17. Obligaciones de los proveedores de servicios de confianza

1. Todo proveedor de servicios de confianza deberá garantizar la disponibilidad y el funcionamiento correcto de los servicios de confianza que preste.
2. Todo proveedor de servicios de confianza deberá notificar sin demora [y, en todo caso, dentro de los [...] días siguientes a la fecha en que haya tomado conocimiento de ello,] [al órgano de supervisión] [a sus clientes⁴¹ y partes que confían que resulten afectados] cualquier falla de seguridad o pérdida de integridad que repercuta [de manera considerable] en los servicios de confianza prestados o los datos personales guardados en ellos.
3. En caso de que se produzca una falla de seguridad grave o una pérdida de integridad considerable, el proveedor de servicios de confianza deberá suspender la prestación de los servicios afectados [hasta [...]].
4. Todo usuario⁴² de un servicio de confianza deberá notificar al proveedor de dicho servicio cuando:
 - a) los datos de creación del servicio de confianza hayan quedado comprometidos; o
 - b) las circunstancias de que tiene conocimiento el usuario dan lugar a un riesgo considerable de que los datos de creación del servicio de confianza puedan haber quedado comprometidos⁴³.

Artículo 18. Responsabilidad de los proveedores de servicios de confianza

1. Sin perjuicio de la responsabilidad que pudiera estar prevista en la ley, todo proveedor de servicios de confianza que incumpla las obligaciones que le impone el

³⁹ Esta disposición se basa en el art. 6, párr. 3, de la LMFE. Contiene una presunción de fiabilidad de las firmas que se ajusten a determinadas normas. Esas normas hacen referencia a la integridad, si el propósito del requisito legal de la firma es garantizar la integridad de la información a que corresponde.

⁴⁰ Esta disposición prevé la posibilidad de realizar una evaluación *ex ante* de la fiabilidad de las firmas electrónicas. En su redacción actual, esta disposición se aplica a las firmas electrónicas, pero podría adaptarse para que fuese aplicable a otros servicios de confianza.

⁴¹ El Grupo de Trabajo tal vez desee considerar la posibilidad de definir los conceptos de “usuario” y “cliente”.

⁴² El Grupo de Trabajo tal vez desee considerar la posibilidad de definir los conceptos de “usuario” y “cliente”.

⁴³ Esta disposición contiene texto opcional a fin de establecer un plazo dentro del cual deberá hacerse la notificación, indicar las partes a quienes habrá que notificar y determinar de qué magnitud deben ser los efectos en los servicios, las credenciales de identidad o los datos personales para que nazca la obligación de notificar. También es posible establecer la obligación de suspender los servicios de confianza hasta que se contenga la falla o la pérdida o se instituya un nuevo proceso de certificación u otro proceso similar.

presente [proyecto de instrumento] [responderá] [deberá asumir las consecuencias jurídicas derivadas] de los daños y perjuicios que dicho incumplimiento cause [deliberadamente o por negligencia] a cualquier persona.

2. Los proveedores de servicios de confianza no responderán de los daños y perjuicios derivados de todo uso de los servicios que exceda las limitaciones establecidas [en cuanto a los fines o el valor para los que puede utilizarse el servicio de confianza] si han proporcionado medios razonablemente accesibles que permitan [al usuario⁴⁴ o] a un tercero determinar cuáles son esas limitaciones⁴⁵.

Capítulo V. Aspectos internacionales

Artículo 19. Reconocimiento jurídico de sistemas de gestión de la identidad y servicios de confianza extranjeros

1. Al determinar si [un sistema de gestión de la identidad] [unas credenciales de identidad] o un servicio de confianza producen efectos jurídicos, o en qué medida los producen, no se tomará en consideración:

a) el lugar en que [se emitan o utilicen las credenciales de identidad] [funcione el sistema de gestión de la identidad] o en que se preste el servicio de confianza;

b) la ubicación del establecimiento del [emisor] [operador del sistema de gestión de la identidad], del proveedor de servicios de confianza o del sujeto.

2. Cuando [el funcionamiento de un sistema de gestión de la identidad] [la emisión de una credencial de identidad] o la prestación de un servicio de confianza tenga lugar fuera [de la jurisdicción promulgante], [dicho sistema] [dicha credencial] o dicho servicio producirá en [la jurisdicción promulgante] los mismos efectos jurídicos que produciría [un sistema de gestión de la identidad que funcionara] [una credencial de identidad que fuese emitida] en [la jurisdicción promulgante] o un servicio de confianza prestado en [dicha jurisdicción promulgante], siempre que ofrecieran [el mismo nivel de fiabilidad] [un nivel de fiabilidad sustancialmente equivalente].

3. Para determinar si [unas credenciales de identidad] [un sistema de gestión de la identidad] o un servicio de confianza ofrece [un] [el mismo] nivel de fiabilidad [sustancialmente equivalente], se tomarán en consideración [las normas internacionales reconocidas]⁴⁶.

Artículo 20. Cooperación

[La persona, el órgano o la entidad, ya sea del sector público o del privado, que el Estado promulgante indique] [deberá] [podrá] cooperar con las entidades extranjeras mediante el intercambio de información, experiencia y buenas prácticas relacionadas con la gestión de la identidad y los servicios de confianza, en particular en lo que respecta a:

a) la certificación de los sistemas de gestión de la identidad y los servicios de confianza;

b) la definición de los niveles de garantía de los sistemas de gestión de la identidad y de los niveles de fiabilidad de los servicios de confianza; y

c) el examen de las novedades pertinentes.

⁴⁴ El Grupo de Trabajo tal vez desee considerar la posibilidad de definir los conceptos de “usuario” y “cliente”.

⁴⁵ Esta disposición tiene por objeto reconocer la validez de las estipulaciones contractuales por las que se limite la responsabilidad.

⁴⁶ El Grupo de Trabajo tal vez desee confirmar que, si esta disposición se incorpora al derecho interno, la consecuencia será que todas las normas de la legislación de la jurisdicción promulgante serán aplicables al sistema de gestión de la identidad o a las credenciales de identidad, incluidas, por ejemplo, las disposiciones legales o contractuales sobre limitación de la responsabilidad.