Naciones Unidas A/CN.9/WG.IV/WP.162

# Asamblea General

Distr. limitada
28 de enero de 2020
Español
Original: inglés

**Comisión de las Naciones Unidas para el Derecho Mercantil Internacional**
**Grupo de Trabajo IV (Comercio Electrónico)**
**60º período de sesiones**
Nueva York, 6 a 9 de abril de 2020

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

### Nota de la Secretaría

## Índice



V.20-00758 (S) 240220 240220

# I. Introducción

1. En la versión revisada del proyecto de disposiciones sobre la utilización y el reconocimiento transfronterizo de sistemas de gestión de la identidad y servicios de confianza que figura en el anexo del presente documento (el “presente proyecto”) se reflejan las deliberaciones mantenidas por el Grupo de Trabajo en su 59º período de sesiones (Viena, 25 a 29 de noviembre de 2019), según se informó en A/CN.9/1005. En las notas de pie de página que acompañan al presente proyecto, se denomina “proyecto anterior” al proyecto de disposiciones que el Grupo de Trabajo examinó en su 59º período de sesiones y que figura en el documento A/CN.9/WG.IV/WP.160.

2. El Grupo de Trabajo tal vez desee observar que en el actual proyecto se han realizado cambios de terminología ante la preocupación de que pudieran surgir diferencias de interpretación. En particular, el término “autenticación” se ha sustituido por “identificación electrónica” y el proceso antes denominado “identificación” se denomina ahora “comprobación de identidad” (art. 1). Así pues, el proceso de la gestión de la identidad se compone ahora de dos etapas (o fases), “comprobación de identidad” e “identificación electrónica”. El término “autenticación” se reserva ahora para el contexto de los servicios de confianza (arts. 21 y 22).

3. En el documento A/CN.9/WG.IV/WP.161, párrafos 6 a 18, figura información de antecedentes sobre la labor que está llevando a cabo el Grupo de Trabajo IV.

# Anexo

## Proyecto de disposiciones[1] sobre la utilización y el reconocimiento transfronterizo de sistemas de gestión de la identidad y servicios de confianza

### Capítulo I. Disposiciones generales

*Artículo 1. Definiciones*

A los efectos del presente [instrumento]:

a) Por “atributo” se entenderá un elemento de información o datos vinculados a [un sujeto][una persona][2];

b) Por “autenticación”, en el contexto de los servicios de confianza, se entenderá un proceso utilizado para atribuir un identificador a un objeto[3];

c) Por “mensaje de datos” se entenderá la información generada, enviada, recibida o archivada por medios electrónicos, magnéticos, ópticos o similares[4];

[1] *Forma del instrumento*: Durante las deliberaciones preliminares sobre esa cuestión que se llevaron a cabo en el 59º período de sesiones del Grupo de Trabajo, se expresó una preferencia clara por que el instrumento se aprobara como una ley modelo, en lugar de una convención (A/CN.9/1005, párr. 123). En el presente proyecto se utiliza el término “[instrumento]” a la espera de que el Grupo de Trabajo tome una decisión al respecto, cuando transmita el instrumento a la Comisión para su aprobación.

[2] *Definiciones*: “*atributo*”: Esta definición se basa en el documento A/CN.9/WG.IV/WP.150, párr. 13. El término se utiliza en las definiciones de “comprobación de identidad” e “identidad”, así como en los arts. 6 y 7.
En cuanto al uso de “sujeto” y “persona”, que dependerá del resultado del examen de la definición de “sujeto” que haga el Grupo de Trabajo, véase la nota 14.

[3] *Definiciones*: “*autenticación*”: Se ha añadido una nueva definición de “autenticación” para designar el proceso de utilización de servicios de confianza con el fin de confirmar la identidad de los objetos. El Grupo de Trabajo tal vez desee examinar la definición junto con las propuestas consistentes en introducir una disposición general sobre la autenticación de objetos (art. 22) y excluir los objetos del ámbito de aplicación de las disposiciones sobre la gestión de la identidad (art. 1, k), definición de “sujetos”).

[4] *Definiciones*: “*mensaje de datos*”: Esta definición está tomada de los textos ya aprobados de la CNUDMI en materia de comercio electrónico, en particular de la Ley Modelo de la CNUDMI sobre Comercio Electrónico (LMCE) (publicación de las Naciones Unidas, núm. de venta S.99.V.4) y de la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales (CCE) (Naciones Unidas, *Treaty Series*, vol. 2898, núm. 50525, pág. 3). El término se utiliza para definir los requisitos que deben cumplir los diversos servicios de confianza que se exponen en el capítulo III. Como se aclara en la definición de “servicios de confianza”, son las propiedades particulares de un mensaje de datos las que constituyen el foco de atención de cada servicio de confianza.

d) Por “identificación electrónica”, en el contexto de los servicios de gestión de la identidad, se entenderá un proceso utilizado para obtener una garantía suficiente de la vinculación entre [un sujeto][una persona] y una identidad[5,6,7];

e) Por “identidad” se entenderá un conjunto de atributos que permiten a [un sujeto][una persona] distinguirse de manera inequívoca en un contexto particular[8];

f) Por “credenciales de identidad” se entenderán los datos, o el objeto físico en que pueden residir los datos, que [un sujeto][una persona] puede presentar para la identificación electrónica de su identidad en forma electrónica[9];

---

[5] *Definiciones*: “*identificación electrónica*”: Como se ha señalado en el párr. 2 *supra*, en el presente proyecto se utiliza el término “identificación electrónica” en lugar de “autenticación” para responder a las preocupaciones que se han suscitado en razón de los múltiples significados que podría tener el término “autenticación”. En el 59º período de sesiones del Grupo de Trabajo se formularon varias preguntas sobre el significado del término “autenticación” y sobre si tenía el mismo significado en los diversos contextos en que se utilizaba (A/CN.9/1005, párrs. 13, 84, 85 y 92). El Grupo de Trabajo solicitó a la Secretaría que se asegurara de que la terminología se utilizara de manera uniforme en todo el documento y en consonancia con la terminología adoptada por la Unión Internacional de Telecomunicaciones (UIT) (véase A/CN.9/1005, párr. 86).
La definición de “identificación electrónica” se ha tomado de la definición de “autenticación” que figura en el documento A/CN.9/WG.IV/WP.150, párr. 15, que a su vez se ha tomado de la Recomendación UIT-T X.1252 de la UIT. En la definición se utiliza el término “garantía” en lugar de “confianza” porque: a) el término “garantía” es el que se emplea en el presente proyecto; y b) la Recomendación UIT-T X.1252 equipara “garantía” y “confianza” en el contexto de la autenticación, como se demuestra al definir “nivel de garantía” como el “nivel de confianza en la vinculación entre una entidad y la información de identidad presentada”.
En el presente proyecto, el concepto de “identificación electrónica”, tal como se encuentra definido, se utiliza en el contexto de la gestión de la identidad en las definiciones de “credenciales de identidad”, “servicios de gestión de la identidad” y “sistema de gestión de la identidad”, así como en los artículos 5, 6, 8 y 9.
En el proyecto de instrumento, el término “autenticación” se refiere a la utilización de servicios de confianza para identificar objetos, y concuerda con el término utilizado en el nombre del servicio de confianza denominado “autenticación de sitios web”.

[6] *Definiciones*: “*factores de identificación electrónica*”: El Grupo de Trabajo tal vez desee examinar si en el proyecto de instrumento debería añadirse la siguiente definición: “Por ‘factores de identificación electrónica’, en el contexto de los servicios de gestión de la identidad, se entenderán los elementos de información o los procesos utilizados para determinar electrónicamente la identidad de un sujeto”. Al proceder a su examen, el Grupo de Trabajo podría tener en cuenta las definiciones de “identificación electrónica” y de “credenciales de identidad”. La definición se basa en la que figura en el documento A/CN.9/WG.IV/WP.150, párr. 17. La expresión “factores de identificación electrónica” se utiliza únicamente en el artículo 6.

[7] *Definiciones*: “*mecanismos de identificación electrónica*”: El Grupo de Trabajo tal vez desee examinar si en el proyecto de instrumento debería insertarse la siguiente definición:
“Por ‘mecanismos de identificación electrónica’, en el contexto de los servicios de gestión de la identidad, se entenderán los mecanismos por los cuales los sujetos emplean credenciales de identidad para identificarse”. La definición se toma del artículo 8, apartado 3, letra c), 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”). Al proceder a su examen, el Grupo de Trabajo podría tener en cuenta las definiciones de “identificación electrónica” y de “credenciales de identidad”. La expresión “mecanismos de identificación electrónica” se utiliza únicamente en el artículo 6.

[8] *Definiciones*: “*identidad*”: Esta definición está tomada del documento A/CN.9/WG.IV/WP.150, párr. 31. En el 59º período de sesiones del Grupo de Trabajo hubo acuerdo general en que se incluyera en la definición el requisito de que la identidad se estableciera “de manera inequívoca” (véase A/CN.9/1005, párr. 108).

[9] *Definiciones*: “*credenciales de identidad*”: Esta definición está tomada del documento A/CN.9/WG.IV/WP.150, párr. 21. El término es, a grandes rasgos, sinónimo de “medios de identificación electrónica”, tal como se define en el artículo 3, apartado 2, del reglamento eIDAS. En la definición se incluyen elementos de la definición que figura en el artículo 59.1-550 de la Ley de Gestión de la Identidad Electrónica de Virginia (título 59.1, cap. 50, del Código de Virginia). En el 59º período de sesiones del Grupo de Trabajo se observó que las credenciales de identidad electrónicas podían utilizarse fuera de línea, por lo que se sugirió que la definición se refiriera más bien a las credenciales de identidad “en forma electrónica” (en lugar de “en un

g) Por “servicios de gestión de la identidad” se entenderán los servicios que consisten en gestionar la comprobación de identidad o la identificación electrónica de [sujetos][personas] en forma electrónica[10];

h) Por “proveedor de servicios de gestión de la identidad” se entenderá una persona que presta servicios de gestión de la identidad[11];

i) Por “sistema de gestión de la identidad” se entenderá un conjunto de funciones y capacidades para gestionar la comprobación de identidad y la identificación electrónica de [sujetos][personas] en forma electrónica[12];

j) Por “comprobación de identidad” se entenderá el proceso de reunión, verificación y validación de atributos que sean suficientes para definir y confirmar la identidad de [un sujeto][una persona] en un contexto en particular[13];

k) Por “sujeto” se entenderá una persona [o un objeto][14];

---

contexto en línea”). El Grupo de Trabajo convino en enmendar la definición en consecuencia (A/CN.9/1005, párr. 110).

[10] *Definiciones*: “*servicios de gestión de la identidad*”: Esta definición está tomada del documento A/CN.9/WG.IV/WP.150, párr. 35, opción a). La definición refleja el entendimiento de que la gestión de la identidad comprende dos etapas (o fases): la “comprobación de identidad” y la “identificación electrónica” (anteriormente denominadas “identificación” y “autenticación”: A/CN.9/1005, párr. 84). Previamente se había expresado cierta preocupación por que se definiera la gestión de la identidad haciendo referencia a estas etapas de forma acumulativa (A/CN.9/965, párr. 91). Teniendo presente esta preocupación, la definición se refiere a “la comprobación de identidad o la identificación electrónica”, y se señala que la conjunción “o” no tiene valor disyuntivo (A/CN.9/1005, párr. 109). La referencia a la “forma electrónica” sigue el acuerdo del Grupo de Trabajo sobre la definición de “credenciales de identidad” (véase la nota 9). Se ha sustituido el término “identificación” por el de “comprobación de identidad” a fin de reflejar el cambio terminológico (véase la nota 13).

[11] *Definiciones*: “*proveedor de servicios de gestión de la identidad*”: Esta definición refleja el acuerdo al que llegó el Grupo de Trabajo en su 59º período de sesiones (A/CN.9/1005, párr. 111).

[12] *Definiciones*: “*sistema de gestión de la identidad*”: En el 59º período de sesiones del Grupo de Trabajo se sugirió que, dado que el proyecto se refería a “servicios de gestión de la identidad”, no era necesario hacer referencia a “sistemas de gestión de la identidad”. Sin embargo, se señaló que, en varias disposiciones del proyecto de instrumento, era más apropiado referirse a “sistemas de gestión de la identidad”, por ejemplo, el artículo 5 sobre la no discriminación (A/CN.9/1005, párrs. 86 y 112) y el artículo 11 sobre la determinación *ex ante* de la fiabilidad (A/CN.9/1005, párr. 102). En consecuencia, el Grupo de Trabajo decidió conservar una definición de sistema de gestión de la identidad (A/CN.9/1005, párr. 112). La definición actual del término refleja el acuerdo al que llegó el Grupo de Trabajo de referirse a “funciones y capacidades”, en consonancia con la terminología de la UIT. A este respecto, en la Recomendación UIT-T X.1252 se define la gestión de identidad como un “conjunto de funciones y capacidades” que se utilizan para i) garantizar la información de identidad; ii) garantizar la identidad de una entidad; y iii) habilitar aplicaciones comerciales y de seguridad.

[13] *Definiciones*: “*comprobación de identidad*”: Como se ha señalado en el párr. 2 supra, en el presente proyecto se utiliza el término “comprobación de identidad” en lugar de “identificación” para responder a las preocupaciones que se habían suscitado por los múltiples significados que podría tener “identificación” (véase A/CN.9/WG.IV/WP.150, párr. 29).

En el 59º período de sesiones del Grupo de Trabajo se señaló que la definición de “identificación” incluía la etapa (o fase) de inscripción del proceso de gestión de la identidad, pero excluía la etapa (o fase) de autenticación, que en el presente proyecto se denomina etapa (o fase) de identificación electrónica (A/CN.9/1005, párr. 84). La “inscripción” puede definirse como el proceso por el que un proveedor de servicios de gestión de la identidad verifica la identidad que declara un sujeto antes de expedirle una credencial (A/CN.9/WG.IV/WP.150, párr. 26).

El término “identificación” no se utiliza en un sentido técnico en el artículo 9.

[14] *Definiciones*: “*sujeto*”: Se ha revisado el uso de los términos “sujeto” y “persona” para mantener la coherencia en todo el proyecto de disposiciones. El término “sujeto” solo se utiliza en el contexto de la gestión de la identidad.

Las palabras “o un objeto” pueden suprimirse si el Grupo de Trabajo está de acuerdo en limitar las disposiciones sobre la gestión de la identidad a las personas físicas y jurídicas. En ese caso, el Grupo de Trabajo quizás desee considerar la posibilidad de suprimir la definición de “sujeto” y sustituir el término “sujeto” por “persona” en todo el proyecto de instrumento.

l) Por “abonado” se entenderá una persona que celebra un contrato de prestación de servicios de gestión de la identidad o servicios de confianza con un proveedor de servicios de gestión de la identidad o un proveedor de servicios de confianza[15];

m) Por “servicio de confianza” se entenderá un servicio electrónico que ofrece garantías de determinadas propiedades de un mensaje de datos e incluye firmas electrónicas, sellos electrónicos, sellos de tiempo electrónicos, autenticación de sitios web, archivado electrónico y servicios de entrega electrónica certificada[16];

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

*Artículo 2. Ámbito de aplicación*

1. El presente [instrumento] será aplicable a la utilización y el reconocimiento transfronterizo de sistemas de gestión de la identidad y servicios de confianza en el contexto de actividades comerciales y servicios relacionados con el comercio[17,18].

2. Nada de lo dispuesto en este [instrumento] exigirá:

a) la identificación de una persona[19];

b) la utilización de un servicio concreto de gestión de la identidad; ni

c) la utilización de un servicio de confianza concreto.

3. Nada de lo dispuesto en el presente [instrumento] afectará a obligación legal alguna de identificar a [un sujeto][una persona] de conformidad con un procedimiento determinado que la ley establezca o exija.

---

[15] *Definiciones*: “*abonado*”: El término “abonado” se utiliza en los artículos 8 y 15, que imponen obligaciones a los abonados en caso de que se produzca una falla de seguridad o de que los servicios queden comprometidos. En el 59º período de sesiones del Grupo de Trabajo se observó que el término “usuario” no estaba claro, ya que podía referirse indistintamente: a) a la persona a la que se prestan los servicios (por ejemplo, la persona que se identifica) y con la cual el proveedor de servicios tenía una relación contractual, o b) a la parte que confía, con la que el proveedor de servicios no tenía una relación contractual (véase A/CN.9/1005, párrs. 28, 39 y 95). Se expresó preferencia por el uso del término “abonado” para hacer referencia a la persona a la que se prestan los servicios (A/CN.9/1005, párrs. 43 y 96).

[16] *Definiciones*: “*servicios de confianza*”: El término “servicios de confianza” procede del reglamento eIDAS, donde se define como “el servicio electrónico prestado habitualmente a cambio de una remuneración” que consiste en uno de los diversos servicios descritos en el capítulo III del reglamento. Por lo tanto, el reglamento eIDAS no establece una definición autónoma de “servicios de confianza”. En el proyecto anterior se propuso que esa definición fuera “un servicio electrónico que ofrezca cierto nivel de fiabilidad en cuanto a las propiedades de los datos”. En el 59º período de sesiones del Grupo de Trabajo se indicó que esa definición no proporcionaba suficiente orientación y que debería adoptarse el enfoque del reglamento eIDAS. Al mismo tiempo, se señaló que una definición más “abstracta” podría adaptarse mejor a lo que sucediera en el futuro. También se observó que los servicios de confianza se preocupaban más por la veracidad y la autenticidad de los datos que por su fiabilidad. La definición actual refleja la decisión del Grupo de Trabajo de incluir una lista no exhaustiva de servicios de confianza (A/CN.9/1005, párr. 18).

[17] *Ámbito de aplicación: utilización nacional y transfronteriza de sistemas de gestión de la identidad y servicios de confianza*: En su 52º período de sesiones, la Comisión señaló que la labor del Grupo de Trabajo debería encaminarse a elaborar un instrumento que pudiera aplicarse a la utilización de la gestión de la identidad y los servicios de confianza tanto a nivel nacional como a través de fronteras (A/74/17, párr. 172).

[18] *Ámbito de aplicación: servicios relacionados con el comercio*: En su 59º período de sesiones, el Grupo de Trabajo convino en que la expresión “servicios relacionados con el comercio” bastaba para abarcar las operaciones realizadas con determinados organismos públicos que participaban en el comercio, como las aduanas con ventanilla única, y que, por consiguiente, no era necesario acotar el significado del término con la palabra “públicos” (A/CN.9/1005, párr. 115).

[19] El Grupo de Trabajo podría también examinar la relación entre esta disposición y el artículo 3, párr. 1.

4. Salvo en los casos previstos en el presente [instrumento], nada de lo dispuesto en [él] afectará a la aplicación a los servicios de gestión de la identidad o los servicios de confianza de norma jurídica alguna incluidas las normas jurídicas aplicables a la privacidad y la protección de datos[20].

*Artículo 3. Utilización voluntaria de sistemas de gestión de la identidad y servicios de confianza*[21]

1. Nada de lo dispuesto en el presente [instrumento] obligará a persona alguna a utilizar un servicio de gestión de la identidad o un servicio de confianza sin su consentimiento.

2. A los efectos de lo dispuesto en el párrafo 1, el consentimiento de una persona podrá inferirse de su conducta.

*Artículo 4. Interpretación*

1. En la interpretación del presente [instrumento] se tendrán en cuenta su carácter internacional y la necesidad de promover la uniformidad en su aplicación y la observancia de la buena fe en el comercio internacional[22].

2. Las cuestiones relativas a las materias que se rigen por el presente [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[23].

[20] La referencia a la privacidad y la protección de datos pone de manifiesto la importancia que el Grupo de Trabajo asigna a estos temas, a la vez que reconoce que estos escapan a su mandato (A/CN.9/965, párr. 125).

[21] *Utilización voluntaria de sistemas de gestión de la identidad y servicios de confianza*: El artículo 3 se basa en el artículo 8, párr. 2, de la CCE. Se ha modificado la redacción para reflejar las decisiones adoptadas por el Grupo de Trabajo en su 59º período de sesiones (véase A/CN.9/1005, párr. 116). En su forma actual, la disposición impide que se imponga una nueva obligación no solo al abonado, sino también al proveedor de servicios y a la parte que confía. El principio de la utilización voluntaria había sido examinado anteriormente por el Grupo de Trabajo en su 57º período de sesiones (A/CN.9/965, párr. 110), en el que se señaló que existía un vínculo con el principio de la autonomía de las partes.

[22] *Interpretación uniforme*: Por lo general, los textos de la CNUDMI contienen una disposición que establece la obligación de interpretar los textos con uniformidad. En su 59º período de sesiones, el Grupo de Trabajo convino en especificar que la referencia a la buena fe era a la buena fe "en el comercio internacional" (A/CN.9/1005, párr. 118). En su forma actual, el artículo 4, párr. 1, refleja lo dispuesto en el artículo 5, párr. 1, de la CCE.

[23] *Principios generales*: En su 59º período de sesiones, el Grupo de Trabajo convino en no enumerar algunos de los principios generales en los que se basaba el instrumento, a saber, los principios de no discriminación contra el uso de medios electrónicos, de neutralidad tecnológica y de equivalencia funcional (A/CN.9/1005, párr. 118). En su forma actual, el artículo 4, párr. 2, refleja lo dispuesto en el artículo 5, párr. 2, de la CCE.

## Capítulo II. Gestión de la identidad

*Artículo 5. Reconocimiento jurídico de un sistema de gestión de la identidad*[24]

No se negarán efectos jurídicos, ni validez, ni fuerza ejecutoria, ni admisibilidad como prueba a la identificación electrónica de [un sujeto][una persona] por la sola razón[25]:

a) de que la comprobación de identidad y la identificación electrónica se hayan hecho en forma electrónica; o[26]

b) de que el sistema de gestión de la identidad no sea uno designado de conformidad con el artículo 11.

*Artículo 6. Obligaciones de los proveedores de servicios de gestión de la identidad*[27]

Todo proveedor de servicios de gestión de la identidad deberá [como mínimo]:

a) inscribir a [los sujetos][las personas], en particular mediante:

i) el registro y la reunión de los atributos de identidad, que correspondan en función del servicio de gestión de la identidad;

ii) la realización de actividades de comprobación y verificación de la identidad; y

iii) la vinculación de las credenciales de identidad [al sujeto][a la persona];

b) actualizar los atributos;

---

[24] *Reconocimiento jurídico de un sistema de gestión de la identidad: generalidades*: El artículo 5, párr. 1, se basa en disposiciones similares de los textos ya aprobados de la CNUDMI en materia de comercio electrónico, como el artículo 5 de la LMCE, el artículo 8, párr. 1, de la CCE y el artículo 7, párr. 1, de la Ley Modelo de la CNUDMI sobre Documentos Transmisibles Electrónicos (LMDTE) (publicación de las Naciones Unidas, eISBN 978-92-1-362736-5). El artículo permite legalmente el uso de la gestión de la identidad y se aplica independientemente de que exista un equivalente fuera de línea (véase el art. 9). La referencia a la "admisibilidad como prueba" proviene del artículo 9 de la LMCE. El párr. 1 b) amplía la disposición que establece el principio de la no discriminación para que incluya la discriminación entre las determinaciones de la fiabilidad *ex ante* y *ex post*. El párr. 1 b) solo trata de la *denegación* de efectos jurídicos al uso de un sistema de gestión de la identidad no designado y, por lo tanto, no afecta al artículo 9, párr. 2, que confiere *mayores* efectos jurídicos a la determinación *ex ante* de la fiabilidad en forma de presunción de fiabilidad *juris tantum*.

[25] *Reconocimiento jurídico de la gestión de la identidad: no discriminación*: En su 59º período de sesiones, el Grupo de Trabajo convino en que el objetivo de la no discriminación, tal como se indicaba en el encabezamiento del artículo 5, párr. 1 (es decir, aquello que era objeto de protección en la disposición sobre la no discriminación), debería ser "la verificación de la identidad" (A/CN.9/1005, párr. 86) y que, en este contexto, "verificación" era sinónimo de "autenticación" (A/CN.9/1005, párr. 85). En consonancia con el enfoque descrito en el párr. 2 del presente documento, se utiliza ahora el término "identificación electrónica".

[26] *Reconocimiento jurídico de la gestión de la identidad: motivos prohibidos*: En su 59º período de sesiones, el Grupo de Trabajo convino en que los motivos de discriminación prohibidos enunciados en el párr. 1 a) deberían ser que la "identificación y verificación" se hubieran hecho en forma electrónica (véase A/CN.9/1005, párr. 86). En consonancia con el enfoque descrito en el párrafo 2 del presente documento, y con la definición de "servicios de gestión de la identidad" que figura en el artículo 1, se utilizan ahora los términos "comprobación de identidad" e "identificación electrónica".

[27] *Obligaciones de los proveedores de servicios de gestión de la identidad*: Las obligaciones del artículo 6 se elaboraron en consulta con expertos a raíz de una solicitud formulada por el Grupo de Trabajo en su 58º período de sesiones (A/CN.9/971, párr. 67). Se ha reformulado la disposición para reflejar la decisión adoptada por el Grupo de Trabajo en su 59º período de sesiones de modificar el inciso i) del apartado a) a fin de consagrar el principio de la minimización de datos (A/CN.9/1005, párr. 93).

c) administrar las credenciales de identidad de conformidad con las normas por las que se rija el sistema de gestión de la identidad, en particular mediante:

i) la emisión, entrega y activación de las credenciales;

ii) la suspensión, revocación y reactivación de las credenciales; y

iii) la renovación y sustitución de las credenciales;

d) gestionar la identificación electrónica de [los sujetos][las personas], en particular mediante:

i) la gestión de los factores de identificación electrónica; y

ii) la administración de los mecanismos de identificación electrónica;

e) garantizar la disponibilidad en línea y el funcionamiento adecuado del sistema de gestión de la identidad; y

f) proporcionar un acceso razonable a las normas por las que se rija el sistema de gestión de la identidad.

### *Artículo 7. Obligaciones de los proveedores de servicios de gestión de la identidad en caso de violación de los datos*[28]

1. En el caso de que se produzca una falla de seguridad o una pérdida de integridad que repercuta de manera considerable en el sistema de gestión de la identidad, incluidos los atributos que en él se gestionan, el proveedor de estos servicios deberá:

a) tomar todas las medidas razonables para contener la falla o la pérdida, incluida, cuando proceda, la suspensión del servicio afectado o la revocación de las credenciales de identidad afectadas;

b) subsanar la falla o la pérdida;

c) notificar la falla o la pérdida de acuerdo con la ley aplicable.

2. Si [un sujeto][una persona] notifica una falla de seguridad o pérdida de integridad al proveedor de servicios de gestión de la identidad, este deberá:

a) investigar la posible falla o pérdida; y

b) adoptar cualquier otra de las medidas previstas en el párrafo 1 que sea apropiada.

### *Artículo 8. Obligaciones de los abonados*[29]

El abonado deberá notificar al proveedor de servicios de gestión de la identidad en los siguientes casos:

a) cuando el abonado tenga conocimiento de que las credenciales de identidad o los mecanismos de identificación electrónica del correspondiente sistema de gestión de la identidad han quedado comprometidos; o

---

[28] *Obligaciones de los proveedores de servicios de gestión de la identidad en caso de violación de los datos*: El artículo 7 ha sido modificado para reflejar las decisiones adoptadas por el Grupo de Trabajo en su 59º período de sesiones (A/CN.9/1005, párr. 94 y párrs. 32 a 36). En particular, el Grupo de Trabajo convino en que las obligaciones de los proveedores de servicios de gestión de la identidad en el caso de una violación de los datos deberían formularse en términos similares a las obligaciones de los proveedores de servicios de confianza en el caso de una violación de los datos, establecidas en el artículo 14, párr. 2. En las notas 43 y 44 figura un análisis más detallado del alcance de esas obligaciones.

[29] *Obligaciones de los abonados*: El artículo 8 ha sido reformulado para reflejar las decisiones adoptadas por el Grupo de Trabajo en su 59º período de sesiones (A/CN.9/1005, párr. 96 y párrs. 37 a 43). En particular, el Grupo de Trabajo convino en que las obligaciones de los abonados a los servicios de gestión de la identidad deberían armonizarse con las obligaciones de los abonados a los servicios de confianza, establecidas en el artículo 14. En las notas 45 y 46 figura un análisis más detallado del alcance de esas obligaciones.

b) cuando las circunstancias de que tenga conocimiento el abonado den lugar a un riesgo considerable de que las credenciales de identidad o los mecanismos de identificación electrónica se hayan podido ver comprometidos.

*Artículo 9. Identificación de [un sujeto][una persona] que utiliza un sistema de gestión de la identidad*[30]

*Opción A*

1. Cuando una norma jurídica requiera o permita que se identifique a [un sujeto] [una persona], esa norma se dará por cumplida respecto de un sistema de gestión de la identidad si se utiliza un método fiable para la identificación electrónica [del sujeto] [de la persona][31].

*Opción B*

1. Un sujeto puede ser identificado mediante el uso de servicios de gestión de la identidad si se utiliza un método fiable para la identificación electrónica [del sujeto] [de la persona][32].

2. Se presumirá que un método es fiable a los efectos del párrafo 1 si se utiliza un sistema de gestión de la identidad designado de conformidad con el artículo 11.

3. Lo dispuesto en el párrafo 2 se entenderá sin perjuicio de la posibilidad de que una persona física o jurídica:

a) demuestre de cualquier otra manera, a los efectos del párrafo 1, la fiabilidad de un método de conformidad con el artículo 10; o

b) aduzca pruebas de que un sistema de gestión de la identidad designado no es fiable[33].

*Artículo 10. Factores pertinentes para la determinación de la fiabilidad*

1. Para determinar la fiabilidad del método a los efectos de lo dispuesto en el artículo 9, deberán tenerse en cuenta todas las circunstancias pertinentes, por ejemplo:

a) el cumplimiento por el proveedor de servicios de gestión de la identidad de las obligaciones que se enumeran en el artículo 6;

---

[30] *Reconocimiento jurídico de la gestión de la identidad: generalidades*: Esta disposición tiene por objeto proporcionar reconocimiento jurídico al uso de la gestión de la identidad con fines de identificación. Se presentan dos opciones al Grupo de Trabajo para que las examine.
La opción A del artículo 9 se ha modificado para que refleje las decisiones adoptadas por el Grupo de Trabajo en su 59º período de sesiones (A/CN.9/1005, párrs. 98, 99 y 101). En ese período de sesiones se señaló que el artículo 9 sería normalmente aplicable cuando las partes hubieran acordado utilizar un servicio de gestión de la identidad para identificarse mutuamente (A/CN.9/1005, párr. 97). En razón de lo establecido en el artículo 2, párr. 2 b), el artículo 9 no deroga ningún requisito legal previsto en la ley aplicable que obligue a identificar a un sujeto de conformidad con un procedimiento definido o prescrito.

[31] *Reconocimiento jurídico de la gestión de la identidad: equivalente fuera de línea*: La opción A del artículo 9 mantiene el enfoque de equivalencia funcional de los proyectos anteriores. Se ha señalado anteriormente que una disposición basada en la equivalencia funcional hace necesario que se identifique un equivalente fuera de línea (A/CN.9/965, párr. 66). En su 59º período de sesiones, el Grupo de Trabajo convino en que el equivalente fuera de línea era la “identificación de un sujeto”, lo cual se refleja en el título del artículo.

[32] *Reconocimiento jurídico de la gestión de la identidad*: La opción B del artículo 9 tiene por objeto afirmar la legalidad del uso de la identificación electrónica sin aplicar un enfoque de equivalencia funcional. El Grupo de Trabajo podría tener presente el artículo 5 al examinar esta opción.

[33] *Presunción de fiabilidad*: En su 59º período de sesiones, el Grupo de Trabajo convino en que el artículo 9 se reformulara en términos similares a los de las disposiciones equivalentes en las que se establecían los requisitos de los servicios de confianza, es decir, los artículos 16 a 22 (A/CN.9/1005, párr. 99). En consecuencia, se han insertado los párrs. 2 y 3, que se basan en los párrs. 2 y 3 del artículo 16 y sustituyen efectivamente a los párrs. 4 y 5 del artículo 11 del proyecto anterior.

b) el ajuste de las reglas de funcionamiento del sistema de gestión de la identidad a cualesquiera normas y procedimientos internacionales reconocidos, incluido el marco normativo relativo a los niveles de garantía, y en particular las reglas sobre:

i) la gobernanza;

ii) la publicación de anuncios y la información que se facilita al usuario;

iii) la gestión de la seguridad de la información;

iv) el mantenimiento de registros;

v) las infraestructuras y el personal;

vi) las inspecciones técnicas; y

vii) las actividades de supervisión y auditoría;

c) toda supervisión o certificación que se hubiera realizado con respecto al sistema de gestión de la identidad; y

d) todo pacto que hubieran acordado las partes.

2. En la determinación relativa a la fiabilidad del método, no se tomará en consideración:

a) el lugar en que funcione el sistema de gestión de la identidad; ni

b) el lugar en que se encuentre el establecimiento del proveedor de servicios de gestión de la identidad.

*Artículo 11. Designación de sistemas de gestión de la identidad fiables*[34]

1. [*La persona, el órgano o la entidad, del sector público o privado, a que el Estado promulgante haya expresamente atribuido competencia*] podrá decidir qué sistemas de gestión de la identidad son fiables a los efectos del artículo 9.

2. [*La persona, el órgano o la entidad, del sector público o privado, a que el Estado promulgante haya expresamente atribuido competencia*] deberá:

a) tener en cuenta todas las circunstancias pertinentes, incluidos los factores enumerados en el artículo 10, para designar un sistema de gestión de la identidad; y

b) publicar una lista de sistemas de gestión de la identidad designados, que incluya detalles del proveedor de servicios de gestión de la identidad.

3. Toda designación que se realice con arreglo a lo dispuesto en el párrafo 1 deberá ajustarse a las normas y procedimientos internacionales reconocidos y pertinentes para determinar la fiabilidad de los sistemas de gestión de la identidad, en particular los marcos normativos relativos a los niveles de garantía.

4. En la designación de un sistema de gestión de la identidad, no se tomará en consideración:

a) el lugar en que funcione el sistema de gestión de la identidad; ni

b) el lugar en que se encuentre el establecimiento del proveedor de servicios de gestión de la identidad.

[34] *Designación de sistemas de gestión de la identidad fiables*: El artículo 11 establece un mecanismo para la determinación *ex ante* de sistemas de gestión de la identidad fiables. El artículo se ha reformulado para reflejar las decisiones adoptadas por el Grupo de Trabajo en su 59º período de sesiones (A/CN.9/1005, párr. 102) y, por lo tanto, se ha reformulado conforme a la disposición correspondiente del capítulo II que trata de la determinación *ex ante* de servicios de confianza fiables (art. 24). Para un examen más detallado de los diversos elementos de esta disposición, véanse las notas 63 y 64.

*Artículo 12. Responsabilidad de los proveedores de servicios de gestión de la identidad*[35]

*Opción A*

[La responsabilidad de los proveedores de servicios de gestión de la identidad se determinará de acuerdo con la ley aplicable[36].]

*Opción B*

Todo proveedor de servicios de gestión de la identidad que incumpla las obligaciones que le correspondan en virtud [del presente instrumento] deberá afrontar las consecuencias jurídicas que entrañe dicho incumplimiento.

*Opción C*

1. Todo proveedor de servicios de gestión de la identidad que incumpla las obligaciones que le correspondan en virtud [del presente instrumento] deberá responder de los daños y perjuicios que dicho incumplimiento cause deliberadamente o por negligencia a cualquier persona[37].

2. El párrafo 1 se aplicará de conformidad con las normas sobre responsabilidad establecidas en la ley aplicable.

3. Sin perjuicio de lo dispuesto en el párrafo 1, el proveedor de servicios de gestión de la identidad no responderá ante el abonado de los daños que sean consecuencia de la utilización de un sistema de gestión de la identidad cuando:

a) esa utilización exceda las limitaciones establecidas en cuanto a los fines o el valor de las operaciones para las que puede utilizarse el servicio de gestión de la identidad; y

b) el proveedor de servicios de gestión de la identidad ha notificado al abonado esas limitaciones de conformidad con la ley aplicable.

[35] *Responsabilidad de los proveedores de servicios de gestión de la identidad*: En su 59º período de sesiones, el Grupo de Trabajo decidió no incluir una disposición de salvaguardia que eximiera de responsabilidad a los proveedores de servicios de gestión de la identidad en determinadas circunstancias (A/CN.9/1005, párr. 104). Por lo demás, el Grupo de Trabajo convino en volver a examinar la responsabilidad de los proveedores de servicios de gestión de la identidad junto con la responsabilidad de los proveedores de servicios de confianza (A/CN.9/1005, párr. 106). En consecuencia, se ha reformulado el artículo 12 para que refleje las opciones presentadas en el artículo 25. Se presentan tres opciones al Grupo de Trabajo para que las examine.

[36] El Grupo de Trabajo podría evaluar si debería mantenerse esta disposición en caso de que el proyecto de instrumento se aprobara como ley modelo, o si la disposición sería superflua dado que sus efectos jurídicos se producirían por aplicación de principios jurídicos generales.

[37] Esta disposición se basa en el texto que acordó el Grupo de Trabajo en su 58º período de sesiones (A/CN.9/971, párr. 101). La disposición se enmendó nuevamente para aclarar el motivo del daño que da lugar a responsabilidad.

## Capítulo III. Servicios de confianza[38]

*Artículo 13. Reconocimiento jurídico de servicios de confianza*[39]

No se negarán efectos jurídicos, ni validez, ni fuerza ejecutoria, ni admisibilidad como prueba[40] a [las propiedades de un mensaje de datos garantizadas[41]] [los datos que se intercambien, verifiquen o autentiquen] mediante la utilización, o con el respaldo, de un servicio de confianza por la sola razón de que:

a) esa información se encuentre en forma electrónica; o

b) no esté respaldada por un servicio de confianza cuya fiabilidad se hubiera establecido de conformidad con el artículo 24.

*Artículo 14. Obligaciones de los proveedores de servicios de confianza*

1. Todo proveedor de servicios de confianza deberá[42]:

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

b) hacer que esas políticas y prácticas sean fácilmente accesibles para los abonados.

2. En el caso de que se produzca una falla de seguridad o una pérdida de integridad que repercuta de manera considerable en un servicio de confianza, el proveedor de ese servicio deberá:

a) tomar todas las medidas razonables para contener la falla o la pérdida, incluida, cuando proceda, la suspensión o la revocación del servicio afectado[43];

---

[38] El capítulo sobre los servicios de confianza consta de una disposición general sobre el reconocimiento jurídico de los servicios de confianza (art. 13), una norma de fiabilidad general acompañada de una cláusula de no discriminación geográfica para facilitar el reconocimiento transfronterizo (art. 23), un mecanismo para la designación *ex ante* de servicios de confianza fiables (art. 24), una disposición sobre la responsabilidad (art. 25) y una lista de servicios de confianza (arts. 16 a 22).

[39] *Reconocimiento jurídico de servicios de confianza: generalidades*: El artículo 13 ha sido reformulado para reflejar las decisiones adoptadas por el Grupo de Trabajo en su 59º período de sesiones (A/CN.9/1005, párr. 26).

[40] Se sugiere que se añadan las palabras “ni admisibilidad como prueba” para armonizar esta disposición con el artículo 5.

[41] Se sugiere la redacción alternativa “las propiedades de un mensaje de datos garantizadas” para armonizar más estrechamente el artículo 13 con la definición de “servicios de confianza”.

[42] *Obligaciones de los proveedores de servicios de confianza: cumplimiento de políticas y prácticas*: El artículo 14, párr. 1, ha sido reformulado para reflejar las decisiones adoptadas por el Grupo de Trabajo en su 59º período de sesiones (A/CN.9/1005, párrs. 31 y 73). Con respecto al párr. 1 b), el Grupo de Trabajo acordó el siguiente texto: “[D]eberá facilitarse el acceso de los abonados a esas políticas y prácticas”, que se ha reformulado en el presente proyecto para aclarar que se trata de una obligación impuesta al proveedor de servicios. El Grupo de Trabajo tal vez desee considerar si esta obligación debería armonizarse con la que incumbe a los proveedores de servicios de gestión de la identidad en el l artículo 6 f) de “proporcionar un acceso razonable a las normas por las que se rija el sistema de gestión de la identidad”.

[43] *Obligaciones de los proveedores de servicios de confianza: contención de fallas de seguridad*: El artículo 14, párr. 2 a) del proyecto anterior imponía la obligación de suspender los servicios de confianza afectados por una falla de seguridad, y establecía un límite opcional a la duración de esa suspensión, que se levantaría, bien cuando se “contuviera” la brecha, bien cuando se emitiera un nuevo certificado o su equivalente (véase también A/CN.9/WG.IV/WP.154, párr. 47). Reconociendo que podría ser conveniente adoptar medidas distintas de la suspensión total, el Grupo de Trabajo convino en su 59º período de sesiones en que el proveedor de servicios de confianza debería estar obligado más bien a “tomar todas las medidas razonables” (A/CN.9/1005, párr. 33). El artículo 14, párr. 2 a) del presente proyecto refleja este acuerdo y especifica que las medidas deben estar orientadas a contener la falla. El Grupo de Trabajo tal vez desee evaluar si la referencia a “contener” la falla serviría para cumplir el objetivo que se desea alcanzar con las medidas que debe adoptar el proveedor de servicios de confianza para responder a una falla de seguridad.

b) subsanar la falla o la pérdida; y

c) notificar la falla o la pérdida de acuerdo con la ley aplicable[44].

*Artículo 15. Obligaciones de los abonados*

Todo abonado[45] deberá notificar al proveedor de servicios de confianza si:

a) el abonado sabe que el servicio de confianza se ha visto comprometido de una manera que afecta a la fiabilidad del servicio[46]; o

b) las circunstancias de que tenga conocimiento el abonado den lugar a un riesgo considerable de que el servicio de confianza se haya podido ver comprometido.

*Artículo 16. Firmas electrónicas*

1. Cuando una norma jurídica requiera o permita la firma de una persona, esa norma se dará por cumplida en relación con un mensaje de datos cuando se utilice un método fiable para:

a) identificar a la persona; y

b) indicar la voluntad que tiene esa persona respecto de la información contenida en el mensaje de datos.

2. Se presumirá que un método es fiable a los efectos del párrafo 1 si se utiliza una firma electrónica designada de conformidad con el artículo 24.

3. Lo dispuesto en el párrafo 2 se entenderá sin perjuicio de la posibilidad de que una persona física o jurídica:

a) demuestre de cualquier otra manera, a los efectos del párrafo 1, la fiabilidad de un método de conformidad con el artículo 23; o

b) aduzca pruebas de que la firma electrónica designada no es fiable[47].

---

[44] *Obligaciones de los proveedores de servicios de confianza: notificación de fallas de seguridad*: El artículo 14, párr. 3 del proyecto anterior imponía al proveedor de servicios de confianza una obligación de notificar, y se especificaba a) quién debía ser notificado y b) el momento en que debía producirse dicha notificación. En su 59º período de sesiones, el Grupo de Trabajo convino en que el instrumento debería hacer referencia a la ley aplicable a estas cuestiones (A/CN.9/1005, párr. 36).

[45] *Obligaciones de los abonados: generalidades*: En su 59º período de sesiones, el Grupo de Trabajo convino en que el instrumento no debería imponer obligaciones a las partes que confían (A/CN.9/1005, párrs. 38 a 40 y 95 a 96).

[46] *Obligaciones de los abonados*: *factor desencadenante*: Mientras que la obligación impuesta a los proveedores de servicios de confianza en el artículo 14, párr. 2, se desencadena por "una falla de seguridad o una pérdida de integridad", la obligación impuesta a los abonados en el artículo 15 surge cuando el servicio de confianza queda "comprometido". En el 59º período de sesiones del Grupo de Trabajo se sugirió que el artículo 15 se refería a la fiabilidad de los servicios de confianza (A/CN.9/1005, párr. 37). En razón de esa sugerencia, en el presente proyecto se ha añadido la expresión "de una manera que afecta a la fiabilidad del servicio". En el artículo 10, apartado 1, del reglamento eIDAS se utiliza una expresión similar.

[47] *Firmas electrónicas*: *presunción de fiabilidad*: En su 59º período de sesiones, el Grupo de Trabajo convino en que los servicios de confianza que se considerasen fiables por aplicación de un enfoque *ex ante* (es decir, de conformidad con lo dispuesto en el art. 24) deberían tener mayores efectos jurídicos y gozar de una presunción de fiabilidad *juris tantum* (A/CN.9/1005, párr. 12). El Grupo de Trabajo convino también en que esta presunción figurase en cada una de las disposiciones en que se establecieran los requisitos de un servicio de confianza (es decir, en los arts. 16 a 22) (A/CN.9/1005, párr. 51). Los párrafos 2 y 3 del artículo 16 reflejan este acuerdo y sustituyen a los párrafos 4 y 5 del artículo 24 del proyecto anterior, respectivamente. El artículo 16, párr. 3, se basa en el artículo 6, párr. 4, de la Ley Modelo sobre las Firmas Electrónicas (LMFE) (publicación de las Naciones Unidas, núm. de venta S.02.V.8).

*Artículo 17. Sellos electrónicos*

1. Cuando una norma jurídica requiera o permita que una persona jurídica estampe un sello, esa norma se dará por cumplida en relación con un mensaje de datos cuando se utilice un método fiable para[48]:

a) proporcionar una garantía fiable del origen del mensaje de datos; y

b) detectar cualquier alteración del mensaje de datos desde su fecha de estampado, distinta de la adición de algún endoso o algún cambio sobrevenido en el curso normal de su transmisión, almacenamiento o presentación[49].

2. Se presumirá que un método es fiable a los efectos del párrafo 1 si se utiliza un sello electrónico designado de conformidad con el artículo 24.

3. Lo dispuesto en el párrafo 2 se entenderá sin perjuicio de la posibilidad de que una persona física o jurídica:

a) demuestre de cualquier otra manera, a los efectos del párrafo 1, la fiabilidad de un método de conformidad con el artículo 23; o

b) aduzca pruebas de que el sello electrónico designado no es fiable[50].

*Artículo 18. Sellos de tiempo electrónicos*

1. Cuando una norma jurídica requiera o permita que determinados documentos, registros, información o datos se vinculen a una fecha y una hora, esa norma se dará por cumplida en relación con un mensaje de datos cuando se utilice un método fiable para:

a) indicar la fecha y la hora, especificando incluso el huso horario utilizado; y

b) vincular dicha fecha y hora al mensaje de datos[51].

2. Se presumirá que un método es fiable a los efectos del párrafo 1 si se utiliza un sello de tiempo electrónico designado de conformidad con el artículo 24.

3. Lo dispuesto en el párrafo 2 se entenderá sin perjuicio de la posibilidad de que una persona física o jurídica:

a) demuestre de cualquier otra manera, a los efectos del párrafo 1, la fiabilidad de un método de conformidad con el artículo 23; o

b) aduzca pruebas de que el sello de tiempo electrónico designado no es fiable[52].

---

[48] *Sellos electrónicos*: *restricción a las personas jurídicas*: En su 59º período de sesiones, el Grupo de Trabajo convino en que los sellos electrónicos solo serían creados por personas jurídicas y que, por consiguiente, el artículo 17 del proyecto anterior (art. 18 del presente proyecto) debería limitarse a los abonados que fueran personas jurídicas (A/CN.9/1005, párrs. 52 y 54).

[49] *Sellos electrónicos*: *función*: En su 59º período de sesiones, el Grupo de Trabajo convino en que la función de un sello electrónico era garantizar el origen y la integridad de los datos a los que estaba vinculado (A/CN.9/1005, párrs. 52 y 54). La garantía de origen se prevé en el apartado a), y la garantía de integridad, en el apartado b). Se ha sugerido que la garantía de origen equivale funcionalmente a la identificación de la persona jurídica que crea el sello (A/CN.9/1005, párr. 52), en cuyo caso es concebible que el origen de los datos pueda garantizarse mediante el uso de una firma electrónica. La previsión en el apartado b) de "la adición de algún endoso o algún cambio sobrevenido en el curso normal de su transmisión, almacenamiento o presentación" refleja el acuerdo a que llegó el Grupo de Trabajo (A/CN.9/1005, párrs. 56 a 58).

[50] *Sellos electrónicos: presunción de fiabilidad*: Véase la nota 47.

[51] *Sellos de tiempo electrónicos: generalidades*: El artículo 18 ha sido reformulado para reflejar las decisiones adoptadas por el Grupo de Trabajo en su 59º período de sesiones (A/CN.9/1005, párr. 55).

[52] *Sellos de tiempo electrónicos: presunción de fiabilidad*: Véase la nota 47.

*Artículo 19. Archivado electrónico*

1. Cuando una norma jurídica requiera o permita la conservación de determinados documentos, registros o información, esa norma se dará por cumplida en relación con el archivado de un mensaje de datos si[53]:

a) es posible acceder a la información contenida en ellos de manera que pueda consultarse posteriormente; y

b) se utiliza un método fiable que permita:

i) indicar la hora y la fecha de archivado y vincular esa hora y esa fecha con el mensaje de datos; y

ii) detectar cualquier alteración del mensaje de datos después de esa hora y fecha, distinta de la adición de algún endoso o algún cambio sobrevenido en el curso normal de su transmisión, almacenamiento o presentación[54];

c) se conserva, 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 recibido[55].

2. Se presumirá que un método es fiable a los efectos del apartado b) del párrafo 1 si se utiliza un servicio de archivado electrónico designado de conformidad con el artículo 24.

3. Lo dispuesto en el párrafo 2 se entenderá sin perjuicio de la posibilidad de que una persona física o jurídica:

a) demuestre de cualquier otra manera, a los efectos del párrafo 1, la fiabilidad de un método de conformidad con el artículo 23; o

b) aduzca pruebas de que el servicio de archivado electrónico designado no es fiable[56].

*Artículo 20. Servicios de entrega electrónica certificada*

1. Cuando una norma jurídica requiera o permita que determinados documentos, registros o información se entreguen mediante correo certificado o un servicio similar[57], esa norma se dará por cumplida en relación con un mensaje de datos cuando se utilice un método fiable para:

a) indicar la hora y la fecha en que el mensaje de datos fue recibido para la entrega; y

---

[53] *Servicios de archivado electrónico: generalidades*: El proyecto anterior se refería al archivado electrónico con las palabras “conservación de mensajes de datos”. A fin armonizar la redacción de esta parte de la disposición con otras disposiciones sobre servicios de confianza y con el resto del párr. 1, así como con el texto utilizado por el Grupo de Trabajo en su 59º período de sesiones (A/CN.9/1005, párr. 59), en el presente proyecto se empleará la expresión “el archivado de un mensaje de datos”.

[54] *Servicios de archivado electrónico*: *función*: En su 59º período de sesiones, el Grupo de Trabajo convino en que una función esencial del archivado electrónico era garantizar la integridad de los datos (A/CN.9/1005, párr. 59). En consonancia con la decisión adoptada por el Grupo de Trabajo, se ha reformulado el inciso ii) del apartado b) para reflejar los criterios de evaluación de la integridad establecidos en el artículo 17, párr. 1 b).

[55] Esta condición no es aplicable a la información que tenga por única finalidad facilitar el envío o la recepción del mensaje; véase el artículo 10, párr. 2, de la LMCE.

[56] *Servicios de archivado electrónico: presunción de fiabilidad*: Véase la nota 47.

[57] *Servicios de entrega electrónica certificada: equivalente fuera de línea*: El proyecto anterior hacía referencia a una norma de derecho que requiriera o permitiera que “se demuestre el envío o la recepción” de un documento, etc. En el 59º período de sesiones del Grupo de Trabajo se propuso que se utilizara un lenguaje más apropiado que hiciera hincapié en la equivalencia funcional entre los servicios de correo certificado y los servicios de entrega electrónica certificada. En consecuencia, se ha reformulado el encabezamiento del párrafo 1 del artículo 20 para hacer referencia a una norma de derecho que requiera que los documentos, etc., “se entreguen mediante correo certificado o un servicio similar”.

b) indicar la hora y la fecha en que el mensaje de datos fue entregado[58].

2. Se presumirá que un método es fiable a los efectos del párrafo 1 si se utiliza un servicio de entrega electrónica certificada designado de conformidad con el artículo 24.

3. Lo dispuesto en el párrafo 2 se entenderá sin perjuicio de la posibilidad de que una persona física o jurídica:

a) demuestre de cualquier otra manera, a los efectos del párrafo 1, la fiabilidad de un método de conformidad con el artículo 23; o

b) aduzca pruebas de que el servicio de entrega electrónica certificada designado no es fiable[59].

*Artículo 21. Autenticación de sitios web*

Cuando una norma jurídica requiera o permita la autenticación de un sitio web, esa norma se dará por cumplida si se utiliza un método fiable para determinar la identidad de la persona que es titular del nombre de dominio de ese sitio web y para vincular esa persona al sitio web correspondiente[60].

*Artículo 22. Autenticación de objetos*

Cuando una norma de derecho requiera o permita que se autentique un objeto, esa norma se dará por cumplida si se utiliza un método fiable para autenticar el objeto[61].

*Artículo 23. Norma de fiabilidad para los servicios de confianza*[62]

1. Para determinar la fiabilidad del método a los efectos de lo dispuesto en los artículos 16 a 22, deberán tenerse en cuenta todas las circunstancias pertinentes, por ejemplo:

a) cualquier norma operacional por la que se rija el servicio de confianza, incluido todo plan destinado a poner fin a la actividad para asegurar la continuidad;

---

[58] *Servicio de entrega electrónica*: *función*: En su 59º período de sesiones, el Grupo de Trabajo convino en que la función esencial de un servicio de entrega electrónica era dar garantías "del momento en que el mensaje de datos fue recibido para la entrega por el servicio de entrega electrónica certificada y del momento en que el mensaje de datos fue entregado por ese sistema al destinatario" (A/CN.9/1005, párr. 64). El artículo 20, párr. 1, del presente proyecto se ha reformulado en consecuencia, aunque la disposición se refiere a una "indicación" de tiempo, en consonancia con la terminología utilizada en el artículo 18, párr. 1. El Grupo de Trabajo tal vez desee evaluar si esta disposición debería exigir expresamente que el servicio de entrega electrónica garantice la integridad del mensaje de datos, confirme la recepción y la entrega e identifique al remitente o al destinatario, o a ambos. Podría decirse que estas funciones ya están contempladas en los apartados a) y b).

[59] *Servicio de entrega electrónica certificada: presunción de fiabilidad*: Véase la nota 47.

[60] *Autenticación de sitios web*: *función*: En su 59º período de sesiones, el Grupo de Trabajo convino en que la función esencial de la autenticación de sitios web era establecer un vínculo entre el sitio web y la persona a la cual se hubiera asignado el nombre de dominio o que tuviera una licencia para usar ese nombre (A/CN.9/1005, párr. 66). En el presente proyecto, la expresión "titular del nombre de dominio" se utiliza para abarcar a las personas a las que un registrador de nombres de dominio ha asignado el nombre de dominio o dado una licencia para utilizarlo. En los debates celebrados hasta la fecha, el Grupo de Trabajo se ha centrado en las circunstancias en que una parte (por ejemplo, el propietario del sitio web) decide libremente autenticar un sitio web, y no en las que lo hace para cumplir una norma de derecho que "requiere" dicha autenticación. En esas circunstancias, la parte actuaría de conformidad con una norma jurídica que "permite" esa autenticación.

[61] *Autenticación de objetos*: *función*: El Grupo de Trabajo tal vez desee considerar si debería añadirse el artículo 23 para hacer referencia a todos los casos de identificación de objetos físicos y digitales. Al proceder a su examen, el Grupo de Trabajo tal vez desee estudiar la definición de "autenticación" que se sugiere y la propuesta de modificar la definición de "sujeto" a fin de excluir los objetos del ámbito de las disposiciones sobre la gestión de la identidad.

[62] *Norma de fiabilidad*: El artículo 23 se ha reformulado para que refleje las decisiones adoptadas por el Grupo de Trabajo en su 59º período de sesiones (A/CN.9/1005, párrs. 67 y 68).

b) cualquier norma o procedimiento internacional reconocido que resulte aplicable;

c) cualquier norma aplicable del sector;

d) la seguridad de los equipos y programas informáticos;

e) los recursos humanos y financieros, incluida la existencia de activos;

f) la periodicidad y el alcance de las auditorías realizadas por un órgano independiente;

g) la existencia de una declaración de un órgano de supervisión, un órgano de acreditación o un mecanismo voluntario respecto de la fiabilidad del método; y

h) cualquier acuerdo pertinente.

2. Se considerará que un método es fiable si se demuestra en la práctica que ha cumplido las funciones a las que se refiere el servicio de confianza correspondiente.

3. En la determinación relativa a la fiabilidad del método, no se tomarán en consideración:

a) el lugar desde el que se presta el servicio de confianza correspondiente; ni

b) el lugar en que se encuentre el establecimiento del proveedor de ese servicio.

*Artículo 24. Designación de servicios de confianza fiables*[63]

1. [*La persona, el órgano o la entidad, del sector público o privado, a que el Estado promulgante haya expresamente atribuido competencia*] podrá decidir qué servicios de confianza son fiables a los efectos de los artículos 16 a 22.

2. [*La persona, el órgano o la entidad, del sector público o privado, a que el Estado promulgante haya expresamente atribuido competencia*] deberá:

a) tener en cuenta todas las circunstancias pertinentes, incluidos los factores enumerados en el artículo 23, para designar un servicio de confianza; y

b) publicar una lista de servicios de confianza designados, que incluya detalles del proveedor de servicios de confianza[64].

3. Toda designación que se realice con arreglo a lo dispuesto en el párrafo 1 deberá ajustarse a las normas y procedimientos internacionales reconocidos y pertinentes para determinar la fiabilidad de los servicios de confianza, en particular los marcos normativos relativos a la fiabilidad.

[63] *Designación de servicios de confianza fiables: generalidades*: El artículo 24 establece un mecanismo para la determinación *ex ante* de los servicios de confianza fiables. Se han reformulado los párrs. 1 y 4 (párr. 3 del proyecto anterior) para reflejar la decisión adoptada por el Grupo de Trabajo en su 59º período de sesiones de que la designación pone el énfasis en el servicio de confianza y no en el método utilizado por ese servicio (A/CN.9/1005, párr. 73). Durante los debates del 59º período de sesiones, se explicó que la designación no se refería a tipos genéricos de servicios de confianza ni a todos los servicios de confianza ofrecidos por un determinado proveedor de servicios de confianza, sino más bien a un servicio de confianza concreto, prestado por un proveedor de servicios identificado.

[64] *Designación de servicios de confianza fiables: obligaciones de la entidad designadora*: Se ha insertado un nuevo párrafo 2 para reflejar la decisión adoptada por el Grupo de Trabajo en su 59º período de sesiones de imponer dos nuevas obligaciones a la entidad designadora (A/CN.9/1005, párr. 73). La finalidad del apartado a) del párrafo 2 es garantizar cierto grado de coherencia entre los servicios de confianza designados como fiables aplicando un enfoque *ex ante* y los que cumplen la norma de fiabilidad del artículo 23 aplicando un enfoque *ex post*. La finalidad del párr. 2 b) es promover la transparencia e informar a los posibles abonados del servicio de confianza pertinente (A/CN.9/1005, párr. 70).

4. En la designación de un servicio de confianza, no se tomarán en consideración:

a) el lugar desde el que se presta el servicio de confianza correspondiente; ni

b) el lugar en que se encuentre el establecimiento del proveedor de ese servicio.

*Artículo 25. Responsabilidad de los proveedores de servicios confianza*[65]

*Opción A*

[La responsabilidad de los proveedores de servicios de confianza se determinará de acuerdo con la ley aplicable[66].]

*Opción B*

Todo proveedor de servicios de confianza que incumpla las obligaciones que le correspondan en virtud [del presente instrumento] deberá afrontar las consecuencias jurídicas que entrañe dicho incumplimiento.

*Opción C*

1. Todo proveedor de servicios de confianza que incumpla las obligaciones que le correspondan en virtud [del presente instrumento] deberá responder de los daños y perjuicios que dicho incumplimiento cause deliberadamente o por negligencia a cualquier persona.

2. El párrafo 1 se aplicará de conformidad con las normas sobre responsabilidad en virtud de la ley aplicable.

3. Sin perjuicio de lo dispuesto en el párrafo 1, el proveedor de servicios de gestión de la identidad no responderá ante el abonado de los daños que sean consecuencia de la utilización de un sistema de gestión de la identidad cuando:

a) esa utilización exceda las limitaciones establecidas en cuanto a los fines o el valor de las operaciones para las que puede utilizarse el servicio confianza; y

b) el proveedor de servicios de confianza haya notificado al abonado esas limitaciones de conformidad con la ley aplicable.

[65] *Responsabilidad de los proveedores de servicios de confianza*: En el 59º período de sesiones del Grupo de Trabajo se expresó apoyo en general a la idea de mantener una disposición sobre la responsabilidad con el fin de proporcionar seguridad jurídica. Se formularon varias propuestas. El Grupo de Trabajo pidió a la Secretaría que reformulara el artículo 25 de modo que reflejara esas propuestas, a fin de examinarlo en el futuro. El artículo 25 del presente proyecto se ha modificado en consecuencia. En la opción A se adopta el enfoque minimalista al recordar que la responsabilidad del proveedor de servicios de confianza, o cualquier limitación de esa responsabilidad, se determinará con arreglo a lo dispuesto en la ley aplicable. En la opción B se sigue el enfoque adoptado en el artículo 9, párr. 2, de la LMFE y, si bien se sigue limitando la responsabilidad en función de lo que establezca la ley aplicable, se especifica que el incumplimiento por el proveedor de servicios de confianza de las obligaciones establecidas en el proyecto de instrumento acarreará consecuencias jurídicas. La opción C es la que ofrece más orientación, ya que se basa en el artículo 25 del proyecto anterior. En esta opción se incluye un nuevo párrafo 2, que se basa en el artículo 11, apartado 4, del reglamento eIDAS. Se ha modificado el párrafo 3 para reflejar las decisiones adoptadas por el Grupo de Trabajo en su 59º período de sesiones (véase A/CN.9/1005, párr. 76).

[66] El Grupo de Trabajo tal vez desee considerar si debería mantenerse esta disposición en caso de que el proyecto de instrumento se aprobara como ley modelo o si sería superflua dado que sus efectos jurídicos se producirían por aplicación de principios jurídicos generales.

## Capítulo IV. Aspectos internacionales

*Artículo 26. Reconocimiento transfronterizo de sistemas de gestión de la identidad y servicios de confianza*[67]

1. Cuando el funcionamiento de un sistema de gestión de la identidad o la prestación de un servicio de confianza tengan lugar fuera [*del Estado promulgante*], dicho sistema o dicho servicio producirán en [*el Estado promulgante*] los mismos efectos jurídicos que produciría un sistema de gestión de la identidad que funcionara en [*el Estado promulgante*] o un servicio de confianza prestado en [*dicho Estado promulgante*], siempre que ofrezcan un nivel de fiabilidad sustancialmente equivalente[68].

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

*Artículo 27. Cooperación*[69]

[*La persona, el órgano o la entidad, del sector público o privado, a que el Estado promulgante haya expresamente atribuido competencia*] [deberá] [podrá] cooperar con 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) al reconocimiento de los efectos jurídicos de los sistemas extranjeros de gestión de la identidad y los servicios de confianza, tanto unilateral como de consuno;

b) a la designación de sistemas de gestión de la identidad y servicios de confianza fiables; y

c) a 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.

---

[67] *Reconocimiento transfronterizo: generalidades*: el artículo 26 se inspira en el artículo 12, párr. 2, de la LMFE. La finalidad de esa disposición es "es dar un criterio general para el reconocimiento transfronterizo de certificados sin el cual los prestadores de servicios de certificación podrían verse enfrentados a la carga irracional de tener que obtener licencias en muchas jurisdicciones" (véase la *Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la Guía para su incorporación al derecho interno 2001*, publicación de las Naciones Unidas, núm. de venta S.02.V.8, segunda parte, párr. 153). El artículo 26 tiene por objeto proporcionar orientación respecto de la aplicación de otras disposiciones del proyecto de instrumento que tratan del reconocimiento transfronterizo, a saber: el artículo 10, párr. 2, (el origen geográfico es irrelevante a los efectos de determinar la fiabilidad de los métodos de gestión de la identidad); el artículo 11, párr. 4, (el origen geográfico es irrelevante a los efectos de designar métodos fiables de gestión de la identidad); el artículo 23, párr. 3 (el origen geográfico es irrelevante a los efectos de determinar la fiabilidad de los servicios de confianza) y el artículo 24, párr. 4 (el origen geográfico es irrelevante a los efectos de designar servicios de confianza fiables). El artículo 10, párr.2; el artículo 11, párr.4; el artículo 23, párr. 3, y el artículo 24, párr. 4, se basan en el artículo 12, párr. 1, de la LMFE, que establece una norma general de no discriminación para determinar la eficacia jurídica de un certificado o una firma electrónica (véase la *Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la Guía para su incorporación al derecho interno 2001*, segunda parte, párr. 152). Para facilitar estas deliberaciones, el Grupo de Trabajo podría volver a examinar su debate sobre la interacción entre los párrafos 1 y 2 del artículo 12 de la LMFE, recogido en el documento A/CN.9/483, párrs. 28 a 36.

[68] *Reconocimiento transfronterizo*: *nivel de equivalencia*: En el 59º período de sesiones del Grupo de Trabajo se expresaron diferentes opiniones sobre el nivel de equivalencia que sería necesario para que un servicio o sistema surtiera efectos jurídicos en otro Estado. El presente proyecto refleja el artículo 12, párr. 2, de la LMFE, en que se exige una equivalencia "sustancial". La alternativa que se había presentado en el proyecto anterior consistía en disponer que la equivalencia fuera exacta (es decir, el servicio extranjero debía ofrecer el "mismo" nivel de fiabilidad).

[69] *Cooperación internacional*: Se ha reformulado el artículo 27 para reflejar las decisiones adoptadas por el Grupo de Trabajo en su 59º período de sesiones (A/CN.9/1005, párr. 122).