Naciones Unidas A/CN.9/WG.IV/WP.167

Asamblea General

Distr. limitada
26 de enero de 2021
Español
Original: inglés

Comisión de las Naciones Unidas para el Derecho Mercantil Internacional
Grupo de Trabajo IV (Comercio Electrónico)
61er período de sesiones
Nueva York (en línea), 5 a 9 de abril de 2021

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

Página

I. Introducción 2

Anexo

Proyecto de disposiciones sobre la utilización y el reconocimiento transfronterizo de sistemas de gestión de la identidad y servicios de confianza 3

V.21-00521 (S) 240221 240221

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 recogen las deliberaciones sostenidas por el Grupo de Trabajo en su 60º período de sesiones (Viena, 19 a 23 de octubre de 2020), de las que se informó en el documento A/CN.9/1045[1].

2. En el documento A/CN.9/WG.IV/WP.166, párrafos 4 a 17, figura información de antecedentes sobre la labor que está llevando a cabo el Grupo de Trabajo IV.

[1] 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 60º período de sesiones y que figura en el documento A/CN.9/WG.IV/WP.162. En el proyecto también se hace referencia a otros textos de la CNUDMI sobre comercio electrónico, a saber, la Ley Modelo de la CNUDMI sobre Comercio Electrónico (“LMCE”), la Ley Modelo de la CNUDMI sobre las Firmas Electrónicas (“LMFE”), la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales (“CCE”) y la Ley Modelo de la CNUDMI sobre Documentos Transmisibles Electrónicos (“LMDTE”).

Anexo

Proyecto de disposiciones[2] 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 una persona;

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

c) Por “identificación electrónica” [“autenticación”], 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 una persona y una identidad[3];

d) Por “identidad” se entenderá un conjunto de atributos que permiten distinguir a una persona de manera inequívoca en un contexto particular;

e) Por “credenciales de identidad” se entenderán los datos, o el objeto físico en que pueden residir los datos, que una persona puede presentar para la identificación electrónica[4];

f) Por “servicios de gestión de la identidad” se entenderán los servicios que consisten en gestionar la comprobación de la identidad o la identificación electrónica de personas en forma electrónica[5];

g) Por “proveedor de servicios de gestión de la identidad” se entenderá una persona que presta servicios de gestión de la identidad[6];

---

[2] *Forma del instrumento*: Durante las deliberaciones preliminares sobre esta 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 adoptara la forma de ley modelo, y no la de 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.

[3] *Definiciones – “identificación electrónica”*: En el presente proyecto se sigue utilizando el término “identificación electrónica” en lugar de “autenticación” para responder a las preocupaciones relacionadas con los múltiples significados del término “autenticación” (A/CN.9/1005, párrs. 13, 84 a 86 y 92). En el 60º período de sesiones del Grupo de Trabajo se expresó apoyo al empleo del término “autenticación” (A/CN.9/1045, párr. 134) y el Grupo de Trabajo convino en colocar entre corchetes las definiciones de “autenticación” e “identificación electrónica” para volver a examinarlas más adelante (*ibid*., párr. 136). Dado que la definición de “autenticación” en el proyecto anterior solo se utilizaba en el contexto de los servicios de confianza (es decir, como “un proceso utilizado para atribuir un identificador a un objeto”), en el presente proyecto el término “autenticación” (y no la definición de dicho término) se colocó entre corchetes.

[4] *Definiciones – “credenciales de identidad”*: El Grupo de Trabajo examinó esta definición en su 60º período de sesiones (A/CN.9/1045, párr. 137). En el presente proyecto, la definición se modificó mediante la sustitución de las palabras “la identificación electrónica de su identidad en forma electrónica” por las palabras “la identificación electrónica” para evitar la redundancia. El Grupo de Trabajo tal vez desee confirmar la versión modificada de la definición.

[5] *Definiciones – “Servicios de gestión de la identidad”*: Esta definición refleja el entendimiento de que la gestión de la identidad comprende dos etapas (o fases): la “comprobación de la identidad” y la “identificación electrónica”. El Grupo de Trabajo tal vez desee analizar si en la definición de “servicios de gestión de la identidad” debería hacerse referencia a las funciones enumeradas en el art. 6 a). En ese caso, se podrían añadir al final de la definición las palabras “, incluidos los servicios enumerados en el art. 6 a)”.

[6] *Definiciones – “proveedor de servicios de gestión de la identidad”*: El Grupo de Trabajo tal vez desee considerar la posibilidad de insertar las palabras “cualquier tipo de” antes de “servicios de

h) Por “sistema de gestión de la identidad” se entenderá un conjunto de funciones y capacidades utilizadas para gestionar la comprobación de la identidad y la identificación electrónica de personas en forma electrónica;

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

j) 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[7];

k) 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[8];

l) Por “proveedor de servicios de confianza” se entenderá una persona que presta 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.

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

a) la identificación de una persona;

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 una persona [o utilizar un servicio de confianza] de conformidad con un procedimiento definido o establecido en la ley[9].

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 a los servicios de

---

gestión de la identidad” a fin de aclarar que no todas las funciones enumeradas en el art. 6 pueden ser pertinentes para todos los sistemas de gestión de la identidad y que, por consiguiente, es posible que un proveedor de servicios de gestión de la identidad no desempeñe todas y cada una de las funciones enumeradas (A/CN.9/1045, párr. 88).

[7] *Definiciones – “abonado”*: En el 59º período de sesiones 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). En su 60º período de sesiones, el Grupo de Trabajo confirmó su apoyo a la definición de “abonado” que figura en el presente proyecto (A/CN.9/1045, párr. 22). Se añadió que el autor de una firma electrónica quedaría comprendido en la definición (*ibid.*) y se propuso que las partes que confiaban quedaran excluidas (*ibid.*, párr. 18).

[8] *Definiciones – “servicios de confianza”*: El Grupo de Trabajo no examinó el término “servicios de confianza” en su 60º período de sesiones. De acuerdo con las deliberaciones sostenidas por el Grupo de Trabajo en su 59º período de sesiones, la definición (que no varía con respecto al proyecto anterior) combina una definición “abstracta” independiente, que se centra en la veracidad y autenticidad de los datos subyacentes, con una lista no exhaustiva de los servicios de confianza comprendidos en el proyecto de instrumento (A/CN.9/1005, párr. 18).

[9] *Preservar la aplicación de las leyes que exigen un procedimiento determinado*: El art. 2, párr. 3, se aplica para limitar el uso de la gestión de la identidad. El Grupo de Trabajo tal vez desee plantearse si esta norma debería hacerse extensiva a la limitación del uso de servicios de confianza y, en caso afirmativo, si debería insertarse el texto que figura entre corchetes. En la LMCE y la LMFE se siguió un criterio diferente, ya que en ellas se limita el uso de los servicios de confianza a su ámbito de aplicación respectivo (por ejemplo, las firmas electrónicas) al instar a las jurisdicciones promulgantes a que especifiquen determinadas excepciones (por ejemplo, remitiéndose a leyes concretas): véanse el art. 7, párr. 3, de la LMCE y el art. 1 de la LMFE (así como las notas correspondientes).

confianza de cualquier [norma jurídica aplicable, incluida cualquier][10] norma jurídica que sea aplicable a la protección y la privacidad de los datos[11].

Artículo 3. Utilización voluntaria de sistemas de gestión de la identidad y servicios de confianza[12]

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.

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 [este] se basa[o, a falta de tales principios, de conformidad con la ley aplicable en virtud de las normas del derecho internacional privado][13].

---

[10] *Preservar la aplicación de otras leyes nacionales*: El art. 2, párr. 4, se redactó antes de que el Grupo de Trabajo deliberara sobre la forma del instrumento. El Grupo de Trabajo tal vez desee considerar la posibilidad de suprimir las palabras que figuran entre corchetes en caso de que el proyecto de disposiciones adopte la forma de ley modelo (véase la nota 2 *supra*). Los textos de la CNUDMI parten de la base de que las disposiciones de una ley modelo se incorporarán al derecho interno de la jurisdicción promulgante como parte de su legislación, y que se les aplicarán las normas vigentes en esa jurisdicción que traten de los conflictos de leyes. Si bien las leyes modelo de la CNUDMI pueden preservar expresamente la aplicación de determinadas leyes (por ejemplo, el art. 1, párr. 2, de la LMDTE), no preservan la aplicación de "cualquier" otra ley que no sea la ley modelo. Además, puede entenderse erróneamente que la referencia a la ley "aplicable" es una remisión a la ley aplicable en virtud de las normas pertinentes del derecho internacional privado. Véase también la nota 19 en lo que respecta a la relación entre el art. 2, párr. 4. y el art. 7.

[11] *Preservar las leyes de protección y privacidad de los datos*: En el 60º período de sesiones del Grupo de Trabajo se sugirió que en el art. 2, párr. 4, se hiciera referencia a "la protección y privacidad de los datos" (y no a "la privacidad y la protección de datos") para reconocer que la disposición se refería únicamente a la "privacidad de los datos" y no a la privacidad en otros contextos. El Grupo de Trabajo tal vez desee confirmar que así se haga, tal como se refleja en el presente proyecto.

[12] *Utilización voluntaria de sistemas de gestión de la identidad y servicios de confianza*: El art. 3 se mantiene sin cambios con respecto al proyecto anterior (véase A/CN.9/1045, párr. 80). Se basa en el art. 8, párr. 2, de la CCE, que trata de la utilización y aceptación voluntarias de las comunicaciones electrónicas. El Grupo de Trabajo convino en que la disposición debería proteger tanto al abonado como a la parte que confía de la imposición de cualquier nueva obligación de utilizar sistemas de gestión de la identidad o servicios de confianza (A/CN.9/1005, párr. 116). En consonancia con el art. 8, párr. 2, de la CCE, el Grupo de Trabajo tal vez desee considerar la posibilidad de añadir las palabras "o aceptar" después de la palabra "utilizar". Quizás desee estudiar también la posibilidad de sustituir "un servicio de gestión de la identidad o un servicio de confianza" por "la identificación electrónica o un servicio de confianza".

[13] *Principios generales*: El art. 4, párr. 2, refleja lo dispuesto en el art. 5, párr. 2, de la CCE. El Grupo de Trabajo tal vez desee estudiar la posibilidad de suprimir el texto que figura entre corchetes. En el 59º período de sesiones se explicó que sería útil hacer referencia a la interpretación con arreglo a la ley aplicable si el instrumento adoptaba la forma de convención (A/CN.9/1005, párr. 117; véase además la explicación que figura en el documento A/CN.9/527, párr. 124). Ninguna de las leyes modelo de la CNUDMI sobre comercio electrónico contiene esta referencia adicional. Como ya se señaló (nota 10), los textos de la CNUDMI parten de la base de que las disposiciones de una ley modelo se incorporarán al derecho interno de la jurisdicción promulgante como parte de su legislación, y que se les aplicarán las normas generales en materia de interpretación que rijan en esa jurisdicción.

Capítulo II. Gestión de la identidad

Artículo 5. Reconocimiento jurídico de sistemas de gestión de la identidad[14]

A reserva de lo dispuesto en el artículo 2, párrafo 3, no se negarán efectos jurídicos, ni validez, ni fuerza ejecutoria, ni admisibilidad como prueba a la identificación electrónica de una persona por la sola razón:

a) de que la comprobación de la identidad y la identificación electrónica se hayan hecho en forma electrónica, o

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[15]

Todo proveedor de servicios de gestión de la identidad deberá [como mínimo][16]:

a) tener en vigor las normas operacionales, procedimientos y prácticas que resulten apropiados, conforme a la finalidad y el diseño[17] del sistema de gestión de la identidad, para establecer [como mínimo][18] los requisitos que deberán cumplirse a los siguientes efectos:

i) inscribir personas, en particular mediante:

a. el registro y la reunión de atributos;

b. la comprobación y verificación de la identidad, y

c. la vinculación de las credenciales de identidad a la persona;

ii) actualizar atributos;

---

[14] *Reconocimiento jurídico de sistemas de gestión de la identidad – generalidades*: Se modificó la redacción del art. 5 para reflejar las decisiones adoptadas por el Grupo de Trabajo en su 60º período de sesiones (A/CN.9/1045, párr. 84).

[15] *Obligaciones de los proveedores de servicios de gestión de la identidad*: Se modificó la redacción del art. 6 para reflejar las decisiones adoptadas por el Grupo de Trabajo en su 60º período de sesiones (A/CN.9/1045, párr. 95). En ese período de sesiones se explicó que, en el caso de los sistemas de gestión de la identidad del sector privado, las funciones enumeradas se regirían normalmente por normas contractuales. Se observó que no todas las funciones enumeradas en el art. 6 serían pertinentes para todos los proveedores de servicios de gestión de la identidad (por ejemplo, los sistemas pluripartitos de gestión de la identidad). También se observó que el art. 6 debería garantizar que el proveedor de los servicios de gestión de la identidad siguiera siendo responsable de todo el conjunto de servicios de gestión de la identidad prestados al abonado (es decir, de todas las funciones enumeradas en el art. 6), y que el art. 6 no impedía que el proveedor de los servicios tercerizara cualquiera de las funciones o distribuyera el riesgo entre sus contratistas (*ibid*., párrs. 90 y 91).

[16] Las palabras “como mínimo” se insertaron para indicar que las funciones enumeradas representan las “obligaciones fundamentales” del proveedor de servicios de gestión de la identidad, que pueden complementarse con obligaciones contractuales estipuladas con arreglo a las normas operacionales (véase A/CN.9/WG.IV/WP.160). El Grupo de Trabajo quizás desee confirmar que también tienen por efecto no dejar margen para ningún apartamiento de esas funciones por la vía del contrato.

[17] En el 60º período de sesiones del Grupo de Trabajo se explicó que las palabras “conforme a la finalidad y el diseño” tenían por objeto otorgar flexibilidad para diseñar los sistemas de gestión de identidad (A/CN.9/1045, párr. 90). El Grupo de Trabajo tal vez desee plantearse si no sería más apropiado hacer referencia a la “estructura” de un sistema de gestión de la identidad (en lugar de a su “diseño”).

[18] Las palabras “como mínimo” se insertaron en el art. 6 a) a raíz de las deliberaciones sostenidas durante el 60º período de sesiones del Grupo de Trabajo y tienen por objeto responder a la preocupación, ya señalada en la nota 15, de que la redacción del nuevo apartado a) pudiera permitir que un proveedor de servicios de gestión de la identidad se eximiera de responsabilidad por el cumplimiento de funciones relacionadas con el servicio de gestión de la identidad que fueran desempeñadas por un contratista (por ejemplo, una entidad independiente en un sistema pluripartito de gestión de la identidad del sector privado) (véase A/CN.9/1045, párr. 90). El Grupo de Trabajo tal vez desee plantearse si las palabras “como mínimo” que figuran en el encabezamiento del art. 6 ya resuelven esa preocupación y si, por lo tanto, se podrían eliminar las palabras del art. 6 a).

iii) gestionar credenciales de identidad, en particular mediante:

a. la emisión, entrega y activación de credenciales;

b. la suspensión, revocación y reactivación de credenciales, y

c. la renovación y sustitución de credenciales;

iv) gestionar la identificación electrónica de personas, en particular mediante:

a. la gestión de factores de identificación electrónica, y

b. la gestión de mecanismos de identificación electrónica;

b) actuar de conformidad con las normas operacionales, procedimientos y prácticas;

c) garantizar la disponibilidad en línea y el correcto funcionamiento del sistema de gestión de la identidad;

d) proporcionar un acceso razonable a las normas operacionales, procedimientos y prácticas, y

e) proporcionar medios razonables para que el abonado notifique de conformidad con el artículo 8.

Artículo 7. Obligaciones de los proveedores de servicios de gestión de la identidad en caso de violación de los datos[19]

1. En el caso de que se produzca una falla de seguridad o una pérdida de integridad que tenga un impacto considerable en el sistema de gestión de la identidad, incluidos los atributos que en él se gestionan, el proveedor de los 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[20,21].

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

a) investigar la posible falla o pérdida, y

[19] *Obligaciones de los proveedores de servicios de gestión de la identidad en caso de violación de los datos*: El Grupo de Trabajo tal vez desee confirmar que el art. 7 establece una norma mínima de la que no pueden apartarse las normas operacionales del sistema de gestión de la identidad ni otros acuerdos contractuales, teniendo en cuenta la opinión predominante del Grupo de Trabajo de que en el art. 14, párr. 2, se establece una norma mínima como la mencionada (A/CN.9/1045, párr. 19). El Grupo de Trabajo tal vez desee también aclarar –a la luz de la salvedad que figura en el art. 2, párr. 4, de que el instrumento no afectará a las leyes sobre protección y privacidad de los datos "salvo en los casos previstos en el presente instrumento"– la relación que existe entre el art. 7 y esas leyes (con respecto a la opinión según la cual el art. 7 sólo sería de aplicación efectiva en las jurisdicciones que no tuvieran leyes sobre protección y privacidad de los datos, véase A/CN.9/1045, párrs. 97 y 98).

[20] *Referencias a la "ley aplicable"*: En consonancia con otras leyes modelo de la CNUDMI sobre comercio electrónico, en el presente proyecto se hace referencia a "la ley" en lugar de a "la ley aplicable".

[21] *Función de otras leyes que rigen el tratamiento de las fallas de seguridad de los datos*: En el 60º período de sesiones del Grupo de Trabajo se indicó que varias de las medidas enumeradas en el art. 7 podían estar comprendidas en las leyes sobre protección y privacidad de los datos, y que, por consiguiente, todas las medidas enumeradas, no solo la notificación, debían ejecutarse de conformidad con la ley aplicable (A/CN.9/1045, párr. 99). El Grupo de Trabajo quizás desee considerar la posibilidad de suprimir las palabras "de acuerdo con la ley en el art. 7, párr. 1 c), y, en consonancia con el criterio esbozado en la nota 20, insertar las palabras ", de conformidad con la ley" al final del encabezamiento del párr. 1 del art. 7.

b) adoptar cualquier otra medida que sea apropiada conforme a lo dispuesto en el párrafo 1.

Artículo 8. Obligaciones de los abonados[22]

El abonado deberá notificar al proveedor de servicios de gestión de la identidad utilizando los medios que este le hubiere proporcionado de conformidad con el artículo 6, o empleando otros medios razonables de notificación, en los siguientes casos:

a) cuando el abonado sepa que sus credenciales de identidad se han visto [o pueden haberse visto] comprometidas, o

[b) cuando las circunstancias de que tenga conocimiento el abonado den lugar a un riesgo considerable de que sus credenciales de identidad puedan haberse visto comprometidas.][23]

Artículo 9. Identificación de personas mediante la gestión de la identidad[24]

1. A reserva de lo dispuesto en el artículo 2, párrafo 3, cuando una norma jurídica requiera o permita que se identifique a una persona [con un fin determinado], esa norma se dará por cumplida respecto de los servicios de gestión de la identidad si se utiliza un método fiable para la identificación electrónica de la persona [con dicho fin][25].

---

[22] *Obligaciones de los abonados*: Se introdujeron cambios en el art. 8 en atención a las decisiones adoptadas por el Grupo de Trabajo en su 60º período de sesiones (A/CN.9/1045, párr. 105). Se volvió a modificar el encabezamiento para destacar que la disposición se refiere principalmente a la notificación y no a algunos medios de notificación en particular. Por consiguiente, se reformuló la frase “utilizar los medios que le hubiere proporcionado el proveedor de servicios de gestión de la identidad de conformidad con el artículo 6 para notificar a dicho proveedor o, en su defecto, deberá emplear medios razonables para notificarlo”.

[23] *Obligaciones de los abonados – conocimiento de que las credenciales se han visto comprometidas*: El apartado b) tiene por objeto contemplar los casos en que se presume que el abonado sabe que las credenciales se han visto comprometidas.

[24] *Reconocimiento jurídico de sistemas de gestión de la identidad – generalidades*: Se modificó la redacción del art. 9 para reflejar las decisiones adoptadas por el Grupo de Trabajo en su 60º período de sesiones (A/CN.9/1045, párr. 117). En ese período de sesiones se explicó que el art. 9 tenía por objeto establecer una norma de equivalencia funcional para la identificación en los casos en que la ley exigiera la identificación, pero no especificara el procedimiento que debía utilizarse para identificar a una persona, o cuando las partes convinieran en identificar. También se explicó que, en consonancia con principios ya establecidos en textos de la CNUDMI, la norma de equivalencia funcional complementaría la norma sobre reconocimiento jurídico prevista en el art. 5. Se añadió que el instrumento no afectaba a la obligación de identificar con arreglo a un método determinado, establecida en el art. 2, párr. 3. Por último, se dijo que la norma se aplicaba solo cuando existía un equivalente fuera de línea, ya que el objetivo de la norma era establecer requisitos de equivalencia entre la identificación fuera de línea y la identificación en línea (*ibid*. párr. 106). Si no existe un equivalente fuera de línea, el art. 5 sigue siendo aplicable para impedir que se niegue el reconocimiento jurídico al uso de la identificación electrónica por la sola razón de que se realice por medios electrónicos (por ejemplo, mediante el intercambio de mensajes de datos).

[25] *Reconocimiento jurídico de sistemas de gestión de la identidad – equivalente fuera de línea*: La inclusión de las palabras entre corchetes que se refieren al fin tiene por objeto disipar una preocupación planteada en el 60º período de sesiones con respecto a la verificación de atributos suficientes (A/CN.9/1045, párrs. 110 y 111). Se explicó que, si no se establecía una correlación entre los atributos necesarios para satisfacer un requisito de identificación fuera de línea y los atributos contenidos en las credenciales de identidad utilizadas para la identificación electrónica, el art. 9 no sería suficiente como norma de equivalencia funcional. Se añadió que la cuestión no se resolvía con la prueba de la fiabilidad, ya que esta se refería a los procesos de gestión de las credenciales de identidad, más que a los atributos contenidos en las credenciales de identidad (*ibid*., párr. 113). En el 60º período de sesiones se cuestionó la necesidad de incluir el texto entre corchetes (*ibid.*, párr. 116). El razonamiento en que se basaba esa opinión era que, si la identificación electrónica implicaba vincular a una persona con una “identidad”, y la “identidad” se definía como un conjunto de atributos que permitían “distinguir a una persona de manera inequívoca en un contexto particular”, el contexto en que se aplicaba el requisito de identificación fuera de línea, incluido el fin que perseguía esa identificación, ya determinaría los atributos exigidos para la identificación electrónica.

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:

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.

Artículo 10. Requisitos para determinar la fiabilidad de los [servicios][sistemas] de gestión de la identidad[26]

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, que podrán ser, entre otras, las siguientes[27]:

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

b) la conformidad de las normas operacionales, políticas y prácticas del proveedor de servicios de gestión de la identidad con cualesquiera normas y procedimientos internacionales reconocidos que sean pertinentes para la prestación de servicios de gestión de la identidad, en particular [el marco de niveles de garantía][los niveles de garantía o marcos similares que proporcionen directrices para designar el grado de confianza en los métodos y procesos utilizados por los sistemas de gestión de la identidad][28], especialmente las normas relativas a los siguientes aspectos:

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) la infraestructura 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;

d) el fin para el que se utilice la identificación, y

e) cualquier acuerdo pertinente entre las partes, incluida cualquier limitación de los fines o el valor de las operaciones para las que pudiera utilizarse el servicio de gestión de la identidad.

---

[26] *Requisitos para determinar la fiabilidad – título*: El título del art. 10 se modificó para reflejar las deliberaciones sostenidas durante el 60º período de sesiones del Grupo de Trabajo (A/CN.9/1045, párr. 124).

[27] *Factores pertinentes para la determinación de la fiabilidad*: Se modificó la redacción del art. 10 para reflejar las decisiones adoptadas por el Grupo de Trabajo en su 60º período de sesiones (A/CN.9/1045, párrs. 118 y 120).

[28] *Niveles de garantía:* Con las palabras “niveles de garantía o marcos similares que proporcionen directrices para designar el grado de confianza en los métodos y procesos utilizados por los sistemas de gestión de la identidad” se trata de abarcar las diversas modalidades posibles de formulación de esos marcos. “Nivel de garantía” es un término definido en el documento A/CN.9/WG.IV/WP.150. El Grupo de Trabajo tal vez desee confirmar si estas palabras son adecuadas para describir el concepto de “marco de niveles de garantía”.

2. A los efectos de determinar la fiabilidad del método, no se tomará en consideración:

a) la ubicación geográfica del lugar en que funcione el sistema de gestión de la identidad, ni

b) la ubicación geográfica del establecimiento del proveedor de servicios de gestión de la identidad.

Artículo 11. Designación de sistemas de gestión de la identidad fiables[29]

1. [*La persona, el órgano o la entidad, del sector público o privado, a que el Estado promulgante haya atribuido competencia expresamente*] podrá designar los sistemas [servicios] de gestión de la identidad que considere 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 atribuido competencia expresamente*] deberá:

a) tener en cuenta todas las circunstancias pertinentes, incluidos los factores enumerados en el artículo 10, al designar un sistema [servicio] de gestión de la identidad[30], y

b) publicar una lista de sistemas [servicios] de gestión de la identidad designados, que incluya detalles del proveedor de servicios de gestión de la identidad [, o informar de otro modo al público][31].

3. Toda designación que se realice con arreglo a lo dispuesto en el párrafo 1 deberá ajustarse a las normas y procedimientos internacionales reconocidos que sean pertinentes para llevar a cabo el proceso de designación, incluidos los marcos de niveles de garantía.

4. A los efectos de designar un sistema [servicio] de gestión de la identidad, no se tomará en consideración:

a) la ubicación geográfica del lugar en que funcione el sistema [servicio] de gestión de la identidad; ni

b) la ubicación geográfica del establecimiento del proveedor de servicios de gestión de la identidad.

[29] *Designación de sistemas de gestión de la identidad fiables*: El art. 11 establece un mecanismo para la determinación *ex ante* de sistemas de gestión de la identidad fiables. Se modificó su redacción para reflejar las decisiones adoptadas por el Grupo de Trabajo en su 60º período de sesiones (A/CN.9/1045, párrs. 125, 126 y 129).

[30] *¿"Sistemas" o "servicios"?*: Conforme a lo acordado por el Grupo de Trabajo en su 60º período de sesiones, se insertó la palabra "servicio" (en singular) junto a la palabra "sistema", ya que los proveedores de servicios de gestión de la identidad ofrecen servicios, no sistemas, de gestión de la identidad a sus abonados. Sin embargo, se observó que el concepto de sistema de gestión de la identidad abarcaba los servicios de gestión de la identidad y que esa designación debería englobar esa idea más amplia (A/CN.9/1045, párr. 126). El Grupo de Trabajo tal vez desee aclarar si se debería hacer referencia a los "servicios de gestión de la identidad" (en plural), habida cuenta de que es el término que se define en el art. 1 f).

[31] *Notificación de los sistemas de gestión de la identidad designados*: En su 60º período de sesiones, el Grupo de Trabajo convino en insertar entre corchetes las palabras "o informar de otro modo al público", para volver a examinarlas más adelante. Con esas palabras se trata de abarcar otros medios de informar al público que no sean la publicación de listas. En el 60º período de sesiones del Grupo de Trabajo, varias delegaciones insistieron en que, si bien se podían utilizar otros medios, era fundamental que se mantuviera la obligación de publicar una lista de sistemas de gestión de la identidad designados (A/CN.9/1045, párr. 128). Si se mantienen esas palabras, el Grupo de Trabajo podría considerar la posibilidad de insertarlas en el art. 23, párr. 2 b).

Artículo 12. Responsabilidad de los proveedores de servicios de gestión de la identidad[32]

Opción A para el artículo 12[33]

La responsabilidad de los proveedores de servicios de gestión de la identidad se determinará de acuerdo con la ley.

Opción B para el artículo 12[34]

1. Sin perjuicio de la responsabilidad que le atribuya la ley por el incumplimiento de otras obligaciones, el proveedor de servicios de gestión de la identidad responderá de los daños que cause a cualquier persona por el incumplimiento intencional o culposo de las obligaciones que le impone [el presente instrumento].

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 se deriven de la utilización de un sistema de gestión de la identidad:

a) en la medida en que 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, ni

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

Capítulo III. Servicios de confianza

Artículo 13. Reconocimiento jurídico de servicios de confianza[35]

No se negarán efectos jurídicos, ni validez, ni fuerza ejecutoria, ni admisibilidad como prueba al resultado de la utilización de un servicio de confianza por la sola razón:

a) de que esa información se encuentre en forma electrónica, o

b) de que no esté respaldada por un servicio de confianza designado de conformidad con el artículo 23.

Artículo 14. Obligaciones de los proveedores de servicios de confianza

1. Todo proveedor de servicios de confianza deberá[36]:

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

b) facilitar el acceso de los abonados y los terceros a esas políticas y prácticas, y

[32] *Responsabilidad de los proveedores de servicios de gestión de la identidad*: Se modificó la redacción del art. 12 a fin de reflejar las opciones presentadas en el art. 24 (A/CN.9/1045, párr. 131).

[33] Véase la nota 53 *infra*.

[34] Véase la nota 54 *infra*.

[35] *Reconocimiento jurídico de servicios de confianza – generalidades:* Se modificó la redacción del art. 13 para reflejar las decisiones adoptadas por el Grupo de Trabajo en su 60º período de sesiones (A/CN.9/1045, párr. 16).

[36] *Obligaciones de los proveedores de servicios de confianza – cumplimiento de políticas y prácticas*: Se modificó la redacción del párr. 1 del art. 14 para reflejar las decisiones adoptadas por el Grupo de Trabajo en su 60º período de sesiones (A/CN.9/1045, párrs. 18 y 21).

c) proporcionar y poner a disposición del público los medios que el abonado deberá utilizar para cumplir la obligación de notificar las fallas de seguridad de conformidad con el artículo 15[37].

2. En el caso de que se produzca una falla de seguridad o una pérdida de integridad que tenga un impacto considerable[38] en un servicio de confianza, el proveedor de ese servicio deberá[39]:

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

b) subsanar la falla o la pérdida, y

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

Artículo 15. Obligaciones de los abonados[40]

Todo abonado[41] deberá notificar al proveedor de servicios de confianza en los siguientes casos:

a) cuando el abonado sepa que el servicio de confianza se ha visto comprometido de una manera que afecta a la fiabilidad del servicio, o

b) cuando 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[42]

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:

a) para identificar a la persona, y

---

[37] *Obligaciones de los proveedores de servicios de confianza – obligación de proporcionar medios de notificación*: El Grupo de Trabajo tal vez desee estudiar si la naturaleza de la obligación prevista en el art. 14, párr. 1 c), debería ser la misma que la de la obligación establecida en el art. 6 d) y, en caso afirmativo, si debería armonizarse la redacción de esas dos obligaciones.

[38] Se invitó al Grupo de Trabajo, en su 60º período de sesiones, a que proporcionara orientación sobre el significado de la frase “que tenga un impacto considerable” (en el proyecto anterior: “que repercuta de manera considerable”). Al respecto, el Grupo de Trabajo tal vez desee tener en cuenta que en el art. 19, párr. 2, del Reglamento eIDAS (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) se exige a los proveedores de servicios de confianza que notifiquen “cualquier violación de la seguridad o pérdida de la integridad que tenga un impacto significativo en el servicio de confianza prestado”. Varios factores pueden contribuir a la evaluación del impacto. Los formularios de notificación de incidentes previstos en el Reglamento eIDAS ayudan a evaluar el impacto de los incidentes, aclarando su duración, el tipo de datos y el porcentaje de abonados afectados, así como otra información de interés. La Agencia de la Unión Europea para la Ciberseguridad dispone de directrices técnicas para la notificación de incidentes con arreglo al art. 19 del Reglamento eIDAS, así como de un informe anual sobre dichos incidentes de seguridad, que los interesados pueden consultar.

[39] En el 60º período de sesiones del Grupo de Trabajo prevaleció la opinión de que el art. 14, párr. 2, establecía una norma mínima de aplicación obligatoria, de la que, por ende, no era posible apartarse por la vía del contrato (A/CN.9/1045, párr. 19). Véase también la nota 19 *supra*.

[40] *Obligaciones de los abonados – generalidades*: El Grupo de Trabajo tal vez desee considerar la posibilidad de modificar la redacción del art. 15 para armonizarlo con el art. 8, tomando en cuenta la propuesta formulada en la nota 37 *supra*.

[41] *Obligaciones de los abonados – definición de “abonado”*: En su 59º período de sesiones, el Grupo de Trabajo convino en que el instrumento no debía imponer obligaciones a las partes que confiaban (A/CN.9/1005, párrs. 38 a 40, 95 y 96). Como se señaló en la nota 7 *supra*, en el 60º período de sesiones se explicó que el autor de una firma electrónica quedaría comprendido en la definición de “abonado” (A/CN/9/1045, párr. 22).

[42] *Firmas electrónicas*: En su 60º período de sesiones, el Grupo de Trabajo convino en mantener el texto del art. 16 tal como figuraba en el proyecto anterior para volver a examinarlo más adelante (A/CN.9/1045, párr. 34).

b) para 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 23.

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

a) demuestre de cualquier otra manera, a los efectos del párrafo 1, la fiabilidad de un método de conformidad con el artículo 22, o

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

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:

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

b) para detectar cualquier alteración del mensaje de datos que sea posterior a su fecha de estampado y que no consista en la adición de algún endoso o algún cambio sobrevenido en el curso normal de su transmisión, almacenamiento o presentación.

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 23.

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

a) demuestre de cualquier otra manera, a los efectos del párrafo 1, la fiabilidad de un método de conformidad con el artículo 22, o

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

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 hora, esa norma se dará por cumplida en relación con un mensaje de datos cuando se utilice un método fiable:

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

b) para vincular dicha fecha y hora al mensaje de datos.

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 23.

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

a) demuestre de cualquier otra manera, a los efectos del párrafo 1, la fiabilidad de un método de conformidad con el artículo 22, o

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

Artículo 19. Archivado electrónico[43]

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 se cumplen las condiciones siguientes:

[43] *Archivado electrónico*: Se introdujeron cambios en el art. 19 para reflejar las decisiones adoptadas por el Grupo de Trabajo en su 60º período de sesiones (A/CN.9/1045, párr. 39). Entre otras cosas, el Grupo de Trabajo convino en que el término “mensaje de datos” abarcaba los datos que no se enviaban ni recibían (A/CN.9/1045, párr. 41).

a) que sea posible acceder a la información contenida en el mensaje de datos de manera que pueda consultarse posteriormente, y

b) que se utilice un método fiable:

i) para indicar la fecha y hora de archivado y vincular esa fecha y hora al mensaje de datos, y

ii) para conservar el mensaje de datos en el formato en que se haya generado, enviado o recibido, o en otro formato que pueda demostrarse que es capaz de detectar cualquier alteración del mensaje de datos que se produzca con posterioridad a esa fecha y hora y que no consista en la adición de algún endoso o algún cambio sobrevenido en el curso normal de su transmisión, almacenamiento o presentación;

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 recibido.

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 23.

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

a) demuestre de cualquier otra manera, a los efectos del párrafo 1, la fiabilidad de un método de conformidad con el artículo 22, o

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

Artículo 20. [Servicios de] entrega electrónica certificada[44]

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

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

b) para indicar la fecha y hora en que el mensaje de datos fue entregado;

c) para garantizar la integridad del mensaje de datos, y

d) para identificar al remitente y al destinatario.

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 23.

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

a) demuestre de cualquier otra manera, a los efectos del párrafo 1, la fiabilidad de un método de conformidad con el artículo 22, o

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

[44] *Entrega electrónica - funciones*: Se introdujeron cambios en el art. 20 para reflejar las decisiones adoptadas por el Grupo de Trabajo en su 60º período de sesiones, a fin de exigir expresamente que el servicio de entrega electrónica garantizara la integridad del mensaje de datos e identificara al remitente y al destinatario (A/CN.9/1045, párr. 44).

Artículo 21. Autenticación de sitios web[45]

1. 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 identificar a la persona que es titular del nombre de dominio[46] de ese sitio web y para vincular a esa persona al sitio web correspondiente[47].

2. Se presumirá que un método es fiable a los efectos del párrafo 1 si se utiliza un servicio de autenticación de sitios web designado de conformidad con el artículo 23.

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

a) demuestre de cualquier otra manera, a los efectos del párrafo 1, la fiabilidad de un método de conformidad con el artículo 22, o

b) aduzca pruebas de que el servicio de autenticación de sitios web designado no es fiable.

Artículo 22. Requisitos para determinar la fiabilidad de los servicios de confianza[48]

1. Para determinar la fiabilidad del método a los efectos de lo dispuesto en los artículos 16 a 21 deberán tenerse en cuenta todas las circunstancias pertinentes, que podrán ser, entre otras, las siguientes:

a) cualesquiera normas operacionales, políticas o prácticas del proveedor de servicios de confianza, incluido cualquier plan destinado a poner fin a la actividad para asegurar la continuidad;

b) cualquier norma o procedimiento internacional reconocido que resulte aplicable y sea pertinente para la prestación de servicios de confianza;

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;

---

[45] *Autenticación de sitios web – generalidades:* Se introdujeron cambios en el art. 21 para reflejar las decisiones adoptadas por el Grupo de Trabajo en su 60º período de sesiones (A/CN.9/1045, párr. 48).

[46] *Autenticación de sitios web – titular del nombre de dominio*: 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 ha dado una licencia para utilizarlo. En las deliberaciones que ha sostenido hasta la fecha, el Grupo de Trabajo ha centrado la atención en las circunstancias en que una parte (por ejemplo, el propietario de un sitio web) acepta libremente autenticar un sitio web, y no en los casos en que lo hace para cumplir una norma jurídica que “requiere” dicha autenticación. En esas circunstancias, la parte actuaría de conformidad con una norma jurídica que “permite” esa autenticación.

[47] *Autenticación de sitios web – funciones*: 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 quien se hubiera asignado el nombre de dominio o a quien se hubiera otorgado una licencia para usar ese nombre (A/CN.9/1005, párr. 66). En el 60º período de sesiones del Grupo de Trabajo se indicó que la autenticación de un sitio web comprendía dos elementos: la identificación del titular del nombre de dominio y la vinculación de esa persona al sitio web. Por consiguiente, el objeto del servicio de confianza era la fiabilidad del sitio web y no la identidad del propietario. Se hizo hincapié en que la finalidad de la autenticación de sitios web era identificar personas, no objetos (A/CN.9/1045, párr. 47). En ese período de sesiones también se indicó que cualquier examen de los objetos que se hiciera en el marco del proyecto de instrumento debía limitarse a su vinculación con una persona (*ibid*., párr. 49). El art. 21 es la única disposición que trata de los objetos.

[48] *Requisitos para determinar la fiabilidad*: Se modificó la redacción del art. 22 (art. 23 del proyecto anterior) a fin de reflejar las decisiones adoptadas por el Grupo de Trabajo en su 60º período de sesiones (A/CN.9/1045, párrs. 56, 57 y 61). El nivel de fiabilidad del método utilizado puede variar según la función que se persiga con ese método.

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;

h) la función para la que se utiliza el servicio de confianza[49], y

i) cualquier acuerdo pertinente entre las partes, incluida cualquier limitación que estipulen en cuanto a los fines o el valor de las operaciones para las que podría utilizarse el servicio de confianza.

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. A los efectos de determinar la fiabilidad del método, no se tomará en consideración:

a) la ubicación geográfica del lugar en que funcione el servicio de confianza, ni

b) la ubicación geográfica del establecimiento del proveedor del servicio de confianza.

Artículo 23. Designación de servicios de confianza fiables[50]

1. [*La persona, el órgano o la entidad, del sector público o privado, a que la jurisdicción promulgante haya atribuido competencia expresamente*] podrá designar los servicios de confianza que sean fiables a los efectos de los artículos 16 a 21.

[1 *bis*. Se presumirá que un método es fiable a los efectos de los artículos 16 a 21 si se utiliza un servicio de confianza designado de conformidad con el párrafo 1.

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

a) demuestre de cualquier otra manera la fiabilidad de un método, o

b) aduzca pruebas de que un servicio de confianza designado no es fiable.][51]

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

a) tener en cuenta todas las circunstancias pertinentes, incluidos los factores enumerados en el artículo 22, al designar un servicio de confianza, y

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

3. Toda designación que se realice con arreglo a lo dispuesto en el párrafo 1 deberá ajustarse a las normas y procedimientos internacionales reconocidos que sean pertinentes para llevar a cabo el proceso de designación.

4. A los efectos de designar un servicio de confianza, no se tomarán en consideración:

a) la ubicación geográfica del lugar en que se presta el servicio de confianza, ni

---

[49] El art. 22, párr. 1 h), refleja una decisión adoptada por el Grupo de Trabajo en su 60º período de sesiones (A/CN.9/1045, párr. 56). El Grupo de Trabajo tal vez desee observar que este factor difiere del que figura en el art. 10, párr. 1 d).

[50] *Designación de servicios de confianza fiables – generalidades*: Se introdujeron cambios en el art. 23 (art. 24 del proyecto anterior) para reflejar las decisiones adoptadas por el Grupo de Trabajo en su 60º período de sesiones (A/CN.9/1045, párr. 61). En este artículo se establece un mecanismo para la determinación *ex ante* de servicios de confianza fiables. En el marco de las deliberaciones sostenidas durante el 59º período de sesiones del Grupo de Trabajo, 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 (A/CN.9/1005, párr. 69).

[51] *Designación de servicios de confianza fiables – efectos*: El Grupo de Trabajo tal vez desee estudiar la posibilidad de insertar los párrs. 1 *bis* y 1 *ter* en el art. 23 y, en consecuencia, suprimir los correspondientes párrs. 2 y 3 de los arts. 16, 17, 18, 19, 20 y 21. Del mismo modo, el Grupo de Trabajo quizás desee considerar la posibilidad de trasladar los párrs. 2 y 3 del art. 9 al art. 11.

b) la ubicación geográfica del establecimiento del proveedor del servicio de confianza.

Artículo 24. Responsabilidad de los proveedores de servicios de confianza[52]

Opción A[53]

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

Opción B[54]

1. Sin perjuicio de la responsabilidad que le atribuya la ley por el incumplimiento de otras obligaciones, el proveedor de servicios de confianza responderá de los daños que cause a cualquier persona por el incumplimiento intencional o culposo de las obligaciones que le impone [el presente instrumento].

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

3. Sin perjuicio de lo dispuesto en el párrafo 1, el proveedor de servicios de confianza no responderá ante el abonado de los daños que se deriven de la utilización de los servicios de confianza:

a) en la medida en que 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 confianza, ni

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

Capítulo IV. Aspectos internacionales

Artículo 25. Reconocimiento transfronterizo de [sistemas][servicios] de gestión de la identidad y servicios de confianza

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

---

[52] *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 conservar en el proyecto una disposición sobre la responsabilidad con el fin de proporcionar seguridad jurídica. En su 60º período de sesiones, el Grupo de Trabajo examinó varias opciones presentadas por la Secretaría. Se introdujeron modificaciones en el art. 24 para reflejar las decisiones adoptadas por el Grupo de Trabajo en ese período de sesiones (A/CN.9/1045, párr. 66).

[53] En la opción A se adopta un enfoque minimalista al reconocer que la responsabilidad del proveedor de servicios de confianza, incluida cualquier limitación de esa responsabilidad, se determinará con arreglo a lo dispuesto en la ley aplicable y con independencia del instrumento. El Grupo de Trabajo tal vez desee analizar si esta disposición debería conservarse en el caso de que el proyecto de instrumento adoptara la forma de ley modelo o si sería superflua dado que sus efectos jurídicos se producirían por aplicación de principios generales del derecho.

[54] En la opción B se adopta un enfoque similar al utilizado en el art. 13 del Reglamento eIDAS. En el párr. 1 se establece un principio general de responsabilidad por el incumplimiento intencional o culposo de cualquiera de las obligaciones que emanan del instrumento. La norma prevista en cuanto a la culpa (*negligence*) es la común, es decir, ni leve ni grave. La culpa leve y la culpa grave son conceptos jurídicos cuyo contenido puede variar de un ordenamiento jurídico a otro y que pueden no existir en todos ellos. El párr. 2 remite al derecho interno en lo que respecta a cuestiones conexas, como los elementos constitutivos de la culpa, la carga de la prueba y otras cuestiones probatorias, y aspectos como la culpa concurrente y la responsabilidad por hecho ajeno. En el párr. 3 se establecen las condiciones para limitar la responsabilidad.

2. Para determinar si [unas credenciales de identidad] [un sistema de gestión de la identidad] [un servicio 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][55].

[3. Se presumirá la equivalencia si la persona, órgano o entidad designada por [la jurisdicción promulgante] de conformidad con los artículos 11 y 23 ha determinado la equivalencia a los efectos de lo dispuesto en este párrafo.][56]

Artículo 26. Cooperación

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

a) el reconocimiento de los efectos jurídicos de sistemas de gestión de la identidad y servicios de confianza extranjeros, haya sido otorgado unilateralmente o de común acuerdo;

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

c) 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.

---

[55] *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 debería exigirse para que se produjeran efectos jurídicos transfronterizos (A/CN.9/1005, párr. 120). El presente proyecto refleja lo dispuesto en el art. 12, párr. 2, de la LMFE, en el que se requiere una equivalencia "sustancial". La alternativa propuesta en el proyecto anterior era que se exigiera una equivalencia exacta (es decir, que el servicio extranjero ofreciera el "mismo" nivel de fiabilidad). Las deliberaciones al respecto continuaron en el 60º período de sesiones (A/CN.9/1045, párr. 69).

[56] *Reconocimiento transfronterizo – presunción de equivalencia*: El párr. 3 tiene por objeto vincular el art. 25 con los arts. 11 y 23 (véase A/CN.9/1045, párr. 71), en particular con respecto a la designación *ex ante*. El Grupo de Trabajo tal vez desee analizar los casos en que una entidad designadora se ampararía en el párr. 3 en lugar de designar el sistema de gestión de la identidad o servicio de confianza extranjero, especialmente a la luz de lo dispuesto en el art. 11, párr. 4, y el art. 23, párr. 4. Además, el Grupo de Trabajo quizás desee considerar la posibilidad de añadir una nueva disposición al art. 25 para facultar a la entidad designadora a determinar que un sistema de gestión de la identidad o un servicio de confianza designado por una entidad extranjera se considerará, en la jurisdicción promulgante, un sistema de gestión de la identidad o un servicio de confianza designado de conformidad con el art. 11, párr. 1, o el art. 23, párr. 1, respectivamente.