



# Asamblea General

Distr. limitada  
7 de septiembre de 2021  
Español  
Original: inglés

**Comisión de las Naciones Unidas para  
el Derecho Mercantil Internacional**  
**Grupo de Trabajo IV (Comercio Electrónico)**  
**62º período de sesiones**  
Viena, 22 a 26 de noviembre de 2021

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

**Nota de la Secretaría**

### Índice

	<i>Página</i>
I. Introducción .....	2
II. Cuestiones que se someten a examen .....	2
A. Terminología .....	2
B. Modificaciones introducidas en el proyecto de disposiciones .....	3
C. Responsabilidad .....	4
<b>Anexo</b>	
Proyecto de disposiciones sobre la utilización y el reconocimiento transfronterizo de la gestión de la identidad y los servicios de confianza .....	6



## I. Introducción

1. En la versión revisada del proyecto de disposiciones sobre la utilización y el reconocimiento transfronterizo de la gestión de la identidad y los servicios de confianza que figura en el anexo del presente documento (el “presente proyecto”) se reflejan los resultados de las deliberaciones sostenidas por el Grupo de Trabajo en su 61<sup>er</sup> período de sesiones (6 a 9 de abril de 2021), de las que se informa en el documento [A/CN.9/1051](#)<sup>1</sup>.

2. En el documento [A/CN.9/WG.IV/WP.169](#), párrafos 4 a 20, figura información sobre los antecedentes de la labor que está llevando a cabo el Grupo de Trabajo IV. Al proyecto de disposiciones que el Grupo de Trabajo examinó en su 61<sup>er</sup> período de sesiones, que figura en el anexo del documento [A/CN.9/WG.IV/WP.167](#), se hace referencia con el nombre de “proyecto anterior”.

## II. Cuestiones que se someten a examen

3. En las deliberaciones que sostuvo durante su 61<sup>er</sup> período de sesiones, el Grupo de Trabajo centró la atención en las cuestiones relativas a la terminología, los servicios de confianza, la responsabilidad y el reconocimiento transfronterizo. Se hicieron avances importantes en el examen de esas cuestiones. En esta sección, la secretaria formula algunas observaciones complementarias para ayudar al Grupo de Trabajo a seguir analizando esas cuestiones.

### A. Terminología

4. En el Grupo de Trabajo se ha reconocido que la gestión de la identidad comprende dos etapas. En períodos de sesiones anteriores del Grupo de Trabajo se ha utilizado diferente terminología para hacer referencia a las dos etapas. No se ha decidido aún qué términos utilizar. Además, en algunos casos aún falta decidir si se hará referencia a la gestión de la identidad como “sistema” o como “servicios”:

a) En el presente proyecto (al igual que en el proyecto anterior), la primera etapa se denomina “comprobación de identidad”. Sin embargo, en el Grupo de Trabajo se ha señalado que, de acuerdo con la terminología técnica, esta etapa puede denominarse “identificación”<sup>2</sup>. También se ha aludido a ella con el nombre de “inscripción”<sup>3</sup> y, de hecho, en el presente proyecto (al igual que en el proyecto anterior) se reconoce que la comprobación de la identidad forma parte de la inscripción (véase el art. 6 a) i));

b) En el presente proyecto (del mismo modo que en el proyecto anterior) se utiliza el término “identificación electrónica” para hacer referencia a la segunda etapa, aunque en el Grupo de Trabajo se han empleado también los términos “autenticación” y “verificación”<sup>4</sup>. En el Grupo de Trabajo se ha sugerido asimismo que se utilice el término “autenticación” para hacer referencia a la “comprobación de la identidad” (es decir, la primera etapa)<sup>5</sup>. Además, se ha observado que la palabra “identificación” se utiliza en la segunda etapa para hacer referencia a la aseveración de una identidad (que

<sup>1</sup> En las notas de pie de página que acompañan al presente proyecto se hace referencia al proyecto de disposiciones que el Grupo de Trabajo examinó en su 60<sup>o</sup> período de sesiones (que figura en el documento [A/CN.9/WG.IV/WP.162](#)) con el nombre de “proyecto anterior”. 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”).

<sup>2</sup> [A/CN.9/1005](#), párr. 84.

<sup>3</sup> *Ibid.*

<sup>4</sup> *Ibid.*

<sup>5</sup> [A/CN.9/1051](#), párr. 67.

después es necesario “autenticar” o “verificar”)<sup>6</sup>. A estas diferencias terminológicas se suma el término “autenticación electrónica”, que se ha utilizado en los capítulos sobre comercio electrónico de algunos acuerdos comerciales regionales celebrados últimamente<sup>7</sup>; si bien no se asigna un significado uniforme al término en todos esos acuerdos, en general corresponde a la segunda etapa de la gestión de la identidad<sup>8</sup>. En el 61<sup>er</sup> período de sesiones del Grupo de Trabajo se expresó amplio apoyo a que se utilizara “identificación electrónica” para hacer referencia a la segunda etapa, aunque también se expresó cierto apoyo al uso del término “autenticación”<sup>9</sup>;

c) En el proyecto de disposiciones se hace referencia a los sistemas y los servicios de gestión de la identidad. Ambos términos se definen en el artículo 1. En la mayoría de los casos, en el presente proyecto se hace referencia a los servicios de gestión de la identidad. Sin embargo, en algunas disposiciones del presente proyecto se alude a los sistemas de gestión de la identidad: i) como algo distinto de los servicios de gestión de la identidad (véanse, p. ej., los arts. 6, 7, 12 y 25), o ii) como otra forma posible de hacer referencia a los servicios de gestión de la identidad (véanse, p. ej., los arts. 5, 10 y 11, que se refieren a la fiabilidad y la designación de “sistemas de gestión de la identidad” y “servicios de gestión de la identidad”). Si bien en períodos de sesiones anteriores se examinó la interacción entre los sistemas y los servicios de gestión de la identidad<sup>10</sup>, el Grupo de Trabajo tal vez desee confirmar si, en las disposiciones antes citadas, se debería utilizar el término “sistema de gestión de la identidad” en lugar de “servicios de gestión de la identidad” o viceversa.

## B. Modificaciones introducidas en el proyecto de disposiciones

5. Los artículos 16 a 21 del proyecto de instrumento se reformularon para reflejar las deliberaciones del Grupo de Trabajo. En particular:

a) *Cuando la ley “permita”*: En el proyecto de disposiciones ya no se hace referencia a una norma jurídica que “permita” la práctica correspondiente en papel. Esto significa que se ha vuelto a la formulación utilizada en la Ley Modelo de la CNUDMI sobre Comercio Electrónico (“LMCE”) y en la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales (“CCE”)<sup>11</sup>;

b) *Presunción de fiabilidad*: Para evitar repeticiones, las normas comunes que establecen la presunción de fiabilidad de los métodos utilizados por un servicio de confianza designado, prevista en los párrafos 2 y 3 de los artículos 16 a 21 del proyecto anterior, se unificaron en el artículo 22<sup>12</sup>;

c) *Grado de fiabilidad relativo*: Se modificó el artículo 22, que establece los requisitos de fiabilidad, insertando un apartado a) en el párrafo 1 a fin de reconocer que la fiabilidad de los métodos utilizados por un servicio de confianza es relativa y no absoluta<sup>13</sup>. La disposición se basa en el artículo 9, párrafo 3 b) i), de la CCE, según el cual la fiabilidad se determina en función de “los fines” del mensaje de datos de que se trate (es decir, la comunicación electrónica a la que se aplica la firma electrónica).

<sup>6</sup> *Ibid.*

<sup>7</sup> Véase, por ejemplo, el Tratado Integral y Progresista de Asociación Transpacífico, artículo 14.1; el Tratado entre los Estados Unidos Mexicanos, los Estados Unidos de América y Canadá, artículo 19.1; la Asociación Económica Integral Regional, artículo 12.1 c).

<sup>8</sup> En algunos acuerdos comerciales regionales, el término “autenticación” abarca también la acción de garantizar la integridad de los mensajes de datos, que es una función prevista en el presente proyecto en relación con los servicios de confianza.

<sup>9</sup> A/CN.9/1051, párr. 67.

<sup>10</sup> Véanse A/CN.9/1045, párr. 126, y A/CN.9/1051, párr. 59. Véase también el análisis que figura en A/CN.9/WG.IV/WP.171.

<sup>11</sup> A/CN.9/1051, párrs. 42 a 44.

<sup>12</sup> *Ibid.*, párrs. 31 a 34.

<sup>13</sup> *Ibid.*, párr. 45.

Se modificaron las disposiciones correspondientes del capítulo II, sobre gestión de la identidad, (es decir, los arts. 9 y 10) para reflejar esos cambios.

6. Además, las disposiciones del capítulo III, relativas a los servicios de confianza, se armonizaron con las del capítulo II, que se refieren a la gestión de la identidad, en los casos en que esas disposiciones cumplen la misma función<sup>14</sup>. En particular:

a) *Obligaciones de los proveedores de servicios de confianza*: En el artículo 14, párrafo 1 a), se introdujo una nueva obligación de tener en vigor normas operacionales, políticas y prácticas. Se basa en la obligación de los proveedores de servicios de gestión de la identidad prevista en el artículo 6 a). Se reformuló la obligación prevista actualmente en el artículo 14, párrafo 1 b), para armonizarla con la obligación prevista respecto de los proveedores de servicios de gestión de la identidad en el artículo 6 b). En consecuencia, tanto los proveedores de servicios de confianza como los proveedores de servicios de gestión de la identidad están obligados ahora a actuar de conformidad con sus normas operacionales, políticas y prácticas y de acuerdo con las declaraciones que hayan hecho respecto de dichas normas, políticas y prácticas. Las obligaciones previstas en el artículo 6, apartados d) y e), también se reformularon para armonizarlas con las del artículo 14, párrafo 1, apartados c) y d);

b) *Obligaciones de los usuarios*: Se modificó el artículo 15 a fin de incorporar la redacción utilizada para formular la obligación correspondiente en el artículo 8.

### C. Responsabilidad

7. Se reformularon las normas de responsabilidad previstas en los artículos 12 y 24 del proyecto de instrumento para reflejar las deliberaciones sostenidas por el Grupo de Trabajo en su 61<sup>er</sup> período de sesiones<sup>15</sup>.

8. En el presente proyecto se retuvo la “opción B” del proyecto anterior, que recibió amplio apoyo y por la que se expresó preferencia, en lugar de la “opción A” de dicho proyecto. Se eliminó la referencia a los elementos de culpa (“negligencia” y “deliberadamente”) y se utilizó el término “pérdidas” en lugar de “daños”<sup>16</sup>. De este modo, el presente proyecto establece un nuevo fundamento de la responsabilidad, distinto del fundamento de la responsabilidad contractual<sup>17</sup>.

9. Todavía no se ha llegado a un consenso sobre el fondo de las normas relativas a la responsabilidad. Durante el 61<sup>er</sup> período de sesiones se plantearon varias cuestiones que el Grupo de Trabajo tal vez desee seguir examinando en su 62<sup>o</sup> período de sesiones, entre ellas las siguientes:

a) *Relación con el contrato*<sup>18</sup>: Según el presente proyecto, la responsabilidad del proveedor de servicios nace cuando este incumple la obligación prevista en el proyecto de instrumento de actuar de conformidad con sus normas operacionales, políticas y prácticas. Por lo general, esas normas, políticas y prácticas estarán incorporadas al contrato celebrado entre el usuario y el proveedor de servicios. En consecuencia, el incumplimiento del contrato puede hacer incurrir en responsabilidad al proveedor de servicios tanto en virtud del proyecto de instrumento como por aplicación del derecho de los contratos. A su vez, la legislación nacional podría repercutir en la capacidad del proveedor de servicios para limitar o excluir su responsabilidad de acuerdo con los artículos 12, párrafo 3, y 24, párrafo 3. Por consiguiente, el Grupo de Trabajo tal vez desee plantearse hasta qué punto el proveedor de servicios puede limitar su responsabilidad por la vía del contrato de conformidad con el proyecto de instrumento, en otros casos que no sean los previstos en los artículos 12, párrafo 3, y 24, párrafo 3;

<sup>14</sup> *Ibid.*, párr. 52.

<sup>15</sup> *Ibid.*, párrs. 13 a 29.

<sup>16</sup> *Ibid.*, párr. 21.

<sup>17</sup> *Ibid.*, párr. 24.

<sup>18</sup> *Ibid.*, párr. 16.

b) *Otras consecuencias jurídicas*: Según el presente proyecto, la responsabilidad por pérdidas no es la única consecuencia jurídica que emana del incumplimiento por el proveedor de servicios de una obligación establecida en el proyecto de instrumento. Ese incumplimiento puede afectar no solo a la fiabilidad del método utilizado por el proveedor de servicios (véanse los arts. 10, párr. 2 a), y 22, párr. 2 a)), sino también a la designación del proveedor de servicios (véanse los arts. 11, párr. 2 a), y 23, párr. 2 a)).

10. Una cuestión conexas que se planteó en el 61<sup>er</sup> período de sesiones del Grupo de Trabajo en el contexto de la responsabilidad fue la relación entre las obligaciones establecidas en el proyecto de instrumento y las obligaciones estipuladas en el contrato. La opinión predominante expresada en el Grupo de Trabajo es que, al menos respecto de algunas de esas obligaciones, no hay posibilidad de apartamiento contractual<sup>19</sup>. El Grupo de Trabajo también ha escuchado sugerencias en el sentido de que, si se formula la disposición pertinente de modo que establezca requisitos “mínimos”, esas obligaciones podrían complementarse, aunque no excluirse, por la vía del contrato. En otras palabras, el proyecto de disposiciones establece un límite mínimo obligatorio. El Grupo de Trabajo tal vez desee analizar esta cuestión en mayor detalle.

---

<sup>19</sup> [A/CN.9/1045](#), párr. 19.

## Anexo

# Proyecto de disposiciones sobre la utilización y el reconocimiento transfronterizo de la gestión de la identidad y los 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<sup>20</sup>;
- 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 el que pueden residir los datos, que una persona puede presentar para la identificación electrónica;
- 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<sup>21</sup>;
- g) Por “proveedor de servicios de gestión de la identidad” se entenderá una persona que presta servicios de gestión de la identidad<sup>22</sup>;
- 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<sup>23</sup>;
- 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 particular;
- j) Por “usuario” 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;
- k) Por “servicio de confianza” se entenderá un servicio electrónico que ofrece garantías de determinadas propiedades de un mensaje de datos e incluye los métodos para crear y gestionar firmas electrónicas, sellos electrónicos, sellos de tiempo

<sup>20</sup> Véase más arriba el párrafo 4.

<sup>21</sup> El Grupo de Trabajo tal vez desee considerar la posibilidad de suprimir las palabras “de personas en forma electrónica” en vista de las definiciones de “comprobación de la identidad” y de “identificación electrónica”.

<sup>22</sup> El Grupo de Trabajo tal vez desee estudiar la conveniencia de insertar las palabras “cualquier tipo de” antes de “servicios de gestión de la identidad” a fin de aclarar que no todas las funciones enumeradas en el artículo 6 pueden ser pertinentes para todos los sistemas de gestión de la identidad y que, por consiguiente, cabría la posibilidad de que un proveedor de servicios de gestión de la identidad no desempeñara todas y cada una de las funciones enumeradas (A/CN.9/1045, párr. 88).

<sup>23</sup> Véase la nota 21 *supra*.

electrónicos, autenticación de sitios web, archivado electrónico y servicios de entrega electrónica certificada<sup>24</sup>;

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 la gestión de la identidad y los servicios de confianza en el contexto de actividades comerciales y servicios relacionados con el comercio.

2. Nada de lo dispuesto en este [instrumento] impondrá la obligación<sup>25</sup>:

- a) de identificar a una persona;
- b) de utilizar un determinado servicio de gestión de la identidad, o
- c) de utilizar un determinado servicio de confianza.

[cuando ni la ley aplicable ni el contrato celebrado por las partes exijan identificar a la persona o utilizar un determinado servicio de gestión de la identidad o servicio de confianza]<sup>26</sup>.

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<sup>27</sup>.

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 confianza de cualquier ley que sea aplicable a la protección y la privacidad de los datos<sup>28</sup>.

<sup>24</sup> Se modificó la definición de “servicio de confianza” para reflejar las deliberaciones sostenidas por el Grupo de Trabajo en su 61<sup>er</sup> período de sesiones (A/CN.9/1051, párrs. 35 y 36).

<sup>25</sup> La finalidad del párrafo 2 del artículo 2 es preservar la neutralidad de la tecnología y del modelo, mientras que el párrafo 1 del artículo 3 tiene por objeto preservar la autonomía de las partes. El Grupo de Trabajo quizás desee considerar la posibilidad de trasladar los párrafos 2 y 3 del artículo 2, que se refieren al funcionamiento de las disposiciones, al artículo 3. En ese caso, el artículo 2 solo delimitaría las materias que quedan comprendidas en el ámbito de aplicación del instrumento. Como alternativa, el Grupo de Trabajo podría estudiar la posibilidad de trasladar únicamente los apartados b) y c) del párrafo 2 al párrafo 1 del artículo 3 (véase la nota 30 *infra*).

<sup>26</sup> La finalidad del texto entre corchetes es indicar que el párrafo 2 no afecta a ninguna ley o acuerdo contractual que imponga la obligación de identificar o de utilizar determinados servicios de gestión de la identidad o de confianza.

<sup>27</sup> El párrafo 3 del artículo 2 se aplica para limitar el uso de la gestión de la identidad. El Grupo de Trabajo tal vez desee plantearse si esta disposición 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 Ley Modelo de la CNUDMI sobre las Firmas Electrónicas (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 (p. ej., las firmas electrónicas) al instar a las jurisdicciones promulgantes a que especifiquen determinadas excepciones (p. ej., remitiéndose a leyes concretas): véanse el artículo 7, párrafo 3, de la LMCE y el artículo 1 de la LMFE (y las notas que las acompañan).

<sup>28</sup> En consonancia con las leyes modelo que ya ha aprobado la CNUDMI (como se explica en la nota 10 de pie de página del documento A/CN.9/WG.IV/WP.167), se modificó el párrafo 4 del artículo 2 para eliminar la referencia a la preservación en general de “cualquier norma jurídica aplicable” y conservar la referencia a la preservación en particular de las leyes aplicables a la privacidad y la protección de los datos.

*Artículo 3. Utilización voluntaria de la gestión de la identidad y los servicios de confianza*<sup>29</sup>

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 [o a utilizar un determinado servicio de gestión de la identidad o un determinado servicio de confianza]<sup>30</sup> 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 origen 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<sup>31</sup>.

## Capítulo II. Gestión de la identidad

*Artículo 5. Reconocimiento jurídico de la gestión de la identidad*

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

- a) de que la comprobación de la identidad y la identificación electrónica estén en forma electrónica, o
- b) de que el sistema de gestión de la identidad no haya sido designado de conformidad con el artículo 11.

*Artículo 6. Obligaciones de los proveedores de servicios de gestión de la identidad*<sup>32</sup>

Todo proveedor de servicios de gestión de la identidad deberá[, como mínimo]<sup>33</sup>:

<sup>29</sup> El artículo 3 se basa en el artículo 8, párrafo 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 usuario como a la parte que confía de la imposición de cualquier obligación nueva de utilizar la gestión de la identidad o servicios de confianza (A/CN.9/1005, párr. 116). En consonancia con el artículo 8, párrafo 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”.

<sup>30</sup> La finalidad del texto entre corchetes es aplicar la sugerencia de incorporar al artículo 3 los apartados b) y c) del párrafo 2 del artículo 2 (véase la nota 25 *supra*).

<sup>31</sup> Se modificó el párrafo 2 del artículo 4 para reflejar la decisión adoptada por el Grupo de Trabajo en su 61<sup>er</sup> período de sesiones (A/CN.9/1051, párr. 56).

<sup>32</sup> Véanse más arriba el párrafo 6 a) (en lo que respecta a la armonización de las obligaciones de estos proveedores con las de los proveedores de servicios de confianza) y el párrafo 10 (en cuanto a la relación con las obligaciones contractuales).

<sup>33</sup> Las palabras “como mínimo” figuran en el encabezamiento del artículo 6 y en el apartado a). Esas palabras se insertaron en el apartado a) a raíz de las deliberaciones sostenidas durante el 60<sup>o</sup> período de sesiones del Grupo de Trabajo y tienen por objeto responder a la preocupación de que, de lo contrario, ese apartado 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 (p. ej., 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 artículo 6 ya resuelven esa preocupación y si, por lo tanto, se podrían eliminar en el apartado a) de ese artículo.

a) tener en vigor normas operacionales, políticas y prácticas que resulten apropiadas para los fines<sup>34</sup> y el diseño del sistema de gestión de la identidad y que permitan definir[, como mínimo,]<sup>35</sup> 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;
- 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 sus normas operacionales, políticas y prácticas y de acuerdo con las declaraciones que haya hecho al respecto;
- c) garantizar la disponibilidad en línea y el correcto funcionamiento del sistema de gestión de la identidad;
- d) facilitar el acceso de los usuarios y los terceros a sus normas operacionales, políticas y prácticas, y
- e) proporcionar y poner a disposición del público los medios que puede emplear un usuario para notificar una falla de seguridad al proveedor de servicios de gestión de la identidad 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*

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[, de conformidad con la ley]<sup>36</sup>:

- a) tomar todas las medidas razonables para contener la falla o la pérdida, entre ellas, cuando proceda, la suspensión del servicio afectado o la revocación de las credenciales de identidad afectadas;
- b) subsanar la falla o la pérdida, y
- c) notificar la falla o la pérdida [de conformidad con la ley]<sup>37</sup>.

<sup>34</sup> El Grupo de Trabajo tal vez desee estudiar si esta disposición debería hacer referencia a la “función” en lugar de a los “fines”, en vista del uso que se hace de los términos “función” y “fines” en el artículo 10, párrafo 1, que se basa en terminología establecida de la CNUDMI.

<sup>35</sup> Véase la nota 33 *supra*.

<sup>36</sup> En el 60º período de sesiones del Grupo de Trabajo se indicó que varias de las medidas enumeradas en el artículo 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 conformidad con la ley” en el artículo 7, párrafo 1 c), e insertar esas mismas palabras al final del encabezamiento del párrafo 1 del artículo 7, como se indica entre corchetes.

<sup>37</sup> Véase la nota 36 *supra*.

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

*Artículo 8. Obligaciones de los usuarios*<sup>38</sup>

El usuario deberá notificar al proveedor de servicios de gestión de la identidad utilizando alguno de 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 usuario sepa que sus credenciales de identidad se han visto [o pueden haberse visto] comprometidas, o
- [b) cuando las circunstancias de que tenga conocimiento el usuario den lugar a un riesgo considerable de que sus credenciales de identidad puedan haberse visto comprometidas.]

*Artículo 9. Identificación de personas mediante la gestión de la identidad*<sup>39</sup>

A reserva de lo dispuesto en el artículo 2, párrafo 3, cuando la ley requiera la identificación de una persona [con un fin determinado]<sup>40</sup>, o prevea consecuencias para el caso de que falte la identificación, ese requisito se dará por cumplido respecto de los servicios de gestión de la identidad si se utiliza un método para realizar la identificación electrónica de la persona [con ese fin].

*Artículo 10. Requisitos de fiabilidad de los [servicios][sistemas] de gestión de la identidad*

1. A los efectos de lo dispuesto en el artículo 9, el método deberá:

- a) ser tan fiable como resulte apropiado para los fines para los que se utiliza el servicio de gestión de la identidad, o
- b) haber demostrado en la práctica que ha cumplido la función que se describe en el artículo 9<sup>41</sup>.

2. Para determinar la fiabilidad del método deberán tenerse en cuenta todas las circunstancias pertinentes, que podrán ser, entre otras, las siguientes:

- 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 aplicables y que resulten pertinentes para la prestación de los servicios de gestión de la identidad, en particular

<sup>38</sup> Se introdujeron cambios en el artículo 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. El Grupo de Trabajo no examinó en más detalle esta disposición en su 61º período de sesiones, por lo que se mantienen los corchetes en los apartados a) y b).

<sup>39</sup> El artículo 9 refleja las decisiones adoptadas por el Grupo de Trabajo en su 60º período de sesiones (A/CN.9/1045, párr. 117). También se le introdujeron algunos cambios más, como se explica más arriba en el párrafo 5.

<sup>40</sup> Véase la nota 34 *supra*.

<sup>41</sup> El Grupo de Trabajo tal vez desee analizar si el apartado b) del párrafo 1 del artículo 10 (y la disposición correspondiente del artículo 22) debería mantenerse o si podría suprimirse a la luz de lo dispuesto en el párrafo 5 a) del artículo 10, que ya puede prever ese efecto cuando en la práctica el método haya cumplido su función.

[el marco de niveles de garantía][los marcos de niveles de garantía u otros marcos similares que proporcionen directrices para designar el grado de confianza en los sistemas de gestión de la identidad]<sup>42</sup>, 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 que estipulen en cuanto a los fines o el valor de las operaciones para las que pudiera utilizarse el servicio de gestión de la identidad.

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 sistema de gestión de la identidad][se preste el servicio de gestión de la identidad], ni
- b) la ubicación geográfica del establecimiento del proveedor de servicios de gestión de la identidad.

4. Se presumirá que el método utilizado por un sistema [servicio] de gestión de la identidad designado de conformidad con el artículo 11 es fiable.

5. Lo dispuesto en el párrafo 4 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 método utilizado por un sistema de gestión de la identidad designado de conformidad con el artículo 11 no es fiable.

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

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 sistemas [servicios] de gestión de la identidad que se presuman fiables<sup>43</sup>.

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

<sup>42</sup> Con las palabras “los marcos de niveles de garantía u otros marcos similares que proporcionen directrices para designar el grado de confianza en los sistemas de gestión de la identidad” se trata de abarcar las diversas modalidades que pueden utilizarse para formular 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”.

<sup>43</sup> Véase más arriba el párrafo 4 c). El Grupo de Trabajo tal vez desee plantearse si el artículo 11 debería referirse a la designación de sistemas o servicios, teniendo en cuenta que el artículo 23 se refiere a la designación de servicios. Véase [A/CN.9/1045](#), párrafo 126, con respecto a las deliberaciones más recientes del Grupo de Trabajo sobre esta cuestión.

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, 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]<sup>44</sup>.

3. Toda designación que se realice de conformidad con 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<sup>45</sup>.

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 [se preste el servicio] de gestión de la identidad, ni

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

*Artículo 12. Responsabilidad de los proveedores de servicios de gestión de la identidad*<sup>46</sup>

1. Todo proveedor de servicios de gestión de la identidad que incumpla las obligaciones que le impone [el presente instrumento] deberá responder de las pérdidas que dicho incumplimiento cause [a cualquier persona].

2. El párrafo 1 se aplicará de conformidad con las normas de responsabilidad establecidas en la ley y sin perjuicio de las circunstancias siguientes:

a) la existencia de cualquier otro fundamento de la responsabilidad previsto en la ley, incluida la responsabilidad por incumplimiento de las obligaciones contractuales, o

b) cualquier otra consecuencia jurídica que, con arreglo a [este instrumento], se derive del incumplimiento por el proveedor de servicios de gestión de la identidad de las obligaciones que le impone [el presente instrumento].

3. Sin perjuicio de lo dispuesto en el párrafo 1, el proveedor de servicios de gestión de la identidad no responderá ante el usuario de las pérdidas que se deriven de la utilización de un sistema de gestión de la identidad:

a) en la medida en que dicha 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;

[b) cuando esas limitaciones hayan sido acordadas por el proveedor de servicios de gestión de la identidad con el usuario,]<sup>47</sup> ni

<sup>44</sup> 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, 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). El Grupo de Trabajo no analizó las palabras en su 61º período de sesiones. Si se mantienen las palabras, el Grupo de Trabajo podría considerar la posibilidad de insertarlas también en el artículo 23, párrafo 2 b).

<sup>45</sup> La referencia al "marco de niveles de garantía" se reformulará en función del resultado de las deliberaciones sobre el artículo 10, párrafo 2 b).

<sup>46</sup> Véanse más arriba los párrafos 7 a 10.

<sup>47</sup> El apartado b) del párrafo 3 del artículo 12 se añadió para reflejar el entendimiento del Grupo de Trabajo de que se pueden reconocer limitaciones de la responsabilidad siempre que se hayan acordado.

c) cuando el proveedor de servicios de gestión de la identidad haya notificado [informado de]<sup>48</sup> esas limitaciones al usuario de conformidad con la ley.

### Capítulo III. Servicios de confianza

#### *Artículo 13. Reconocimiento jurídico de los servicios de confianza*

No se negarán efectos jurídicos, validez, 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 esté en forma electrónica, o
- b) de que el servicio de confianza no haya sido 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<sup>49</sup>:

- a) tener en vigor normas operacionales, políticas y prácticas que resulten apropiadas para los fines y el diseño [funciones]<sup>50</sup> del servicio de confianza, incluido un plan para garantizar la continuidad en caso de cese de la actividad;
- b) actuar de conformidad con sus normas operacionales, políticas y prácticas y de acuerdo con las declaraciones que haya hecho al respecto;
- c) facilitar el acceso de los usuarios y los terceros a esas normas operacionales, políticas y prácticas, y
- d) proporcionar y poner a disposición del público los medios que puede emplear un usuario para notificar una falla de seguridad al proveedor de servicios de confianza de conformidad con el artículo 15.

2. En el caso de que se produzca una falla de seguridad o una pérdida de integridad que tenga un impacto considerable en un servicio de confianza, el proveedor de ese servicio deberá [de conformidad con la ley]<sup>51</sup>:

- 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 conformidad con la ley]<sup>52</sup>.

#### *Artículo 15. Obligaciones de los usuarios*<sup>53</sup>

El usuario deberá notificar al proveedor de servicios de confianza utilizando alguno de los medios que este le hubiere proporcionado de conformidad con el artículo 14, párrafo 1, o empleando otros medios razonables de notificación, en los siguientes casos:

- a) cuando el usuario sepa que el servicio de confianza se ha visto comprometido, o

<sup>48</sup> El objetivo del apartado c) del párrafo 3 del artículo 12 no es introducir una nueva obligación, sino remitir a las obligaciones ya previstas en la ley aplicable. Para evitar dudas, el Grupo de Trabajo podría estudiar si la palabra “informado” es más apropiada que la palabra “notificado” a esos efectos.

<sup>49</sup> Véanse más arriba el párrafo 6 a) (en lo que respecta a la armonización de las obligaciones de estos proveedores con las de los proveedores de servicios de gestión de la identidad) y el párrafo 10 (en cuanto a la relación con las obligaciones contractuales).

<sup>50</sup> Véase la nota 34 *supra*.

<sup>51</sup> Véase la nota 33 *supra*.

<sup>52</sup> *Ibid.*

<sup>53</sup> Véase más arriba el párrafo 6 b). La disposición se reformulará a la luz de los resultados de las deliberaciones sobre el artículo 8.

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

*Artículo 16. Firmas electrónicas*

Cuando la ley requiera la firma de una persona, o prevea consecuencias para el caso de que falte una firma, ese requisito se dará por cumplido en relación con un mensaje de datos si se utiliza un método:

- a) para identificar a la persona, y
- b) para indicar la voluntad que tiene esa persona respecto de la información contenida en el mensaje de datos.

*Artículo 17. Sellos electrónicos*

Cuando la ley requiera que una persona jurídica estampe un sello, o prevea consecuencias para el caso de que falte un sello, ese requisito se dará por cumplido en relación con un mensaje de datos si se utiliza un método:

- a) para proporcionar una garantía fiable del origen del mensaje de datos, y
- b) para detectar cualquier alteración del mensaje de datos que se haya producido después de la fecha [y hora] en que fue estampado el sello y que no consista en la adición de algún endoso o algún cambio sobrevenido en el curso normal de su transmisión, almacenamiento o presentación.

*Artículo 18. Sellos de tiempo electrónicos*

Cuando la ley requiera que un documento en papel o electrónico o cierta información o datos se vinculen a una fecha y hora, o prevea consecuencias para el caso de que falte la fecha y hora, ese requisito se dará por cumplido en relación con un mensaje de datos si se utiliza un método:

- 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.

*Artículo 19. Archivado electrónico*

Cuando la ley requiera que se conserve un documento en papel o electrónico o cierta información, o prevea consecuencias para el caso de que no se conserven, ese requisito se dará por cumplido en relación con un mensaje de datos si se utiliza un método:

- a) para hacer accesible la información contenida en el mensaje de datos a fin de que pueda consultarse posteriormente;
- b) para indicar la fecha y hora de archivado y vincular esa fecha y hora al mensaje de datos;
- c) 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, y
- d) para conservar, si la hubiera, 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.

*Artículo 20. Servicios de entrega electrónica certificada*

Cuando la ley requiera que un documento en papel o electrónico o cierta información se entreguen mediante correo certificado u otro servicio similar, o prevea consecuencias

para el caso de que no se entreguen, ese requisito se dará por cumplido en relación con un mensaje de datos si se utiliza un método:

- a) para indicar la fecha y hora en que el mensaje de datos fue recibido para la entrega, y la fecha y hora en que fue entregado;
- b) para detectar cualquier alteración del mensaje de datos que se haya producido después de la fecha y hora en que el mensaje de datos fue recibido para la entrega, hasta la fecha y hora en que fue entregado, y que no consista en la adición de algún endoso o de la información exigida en el presente artículo ni en un cambio sobrevenido en el curso normal de su transmisión, almacenamiento o presentación, y
- c) para identificar al remitente y al destinatario.

#### *Artículo 21. Autenticación de sitios web*

Cuando la ley requiera la autenticación de un sitio web, o prevea consecuencias para el caso de falta de autenticación de un sitio web, ese requisito se dará por cumplido si se utiliza un método:

- a) para identificar a la persona que es titular del nombre de dominio de ese sitio web, y
- b) para vincular a esa persona al sitio web.

#### *Artículo 22. Requisitos de fiabilidad de los servicios de confianza*

1. A los efectos de lo dispuesto en los artículos 16 a 21, el método deberá:

- a) ser tan fiable como resulte apropiado para los fines<sup>54</sup> para los que se utiliza el servicio de confianza, o
- b) haber demostrado en la práctica que ha cumplido las funciones que se describen en el artículo.

2. Para determinar la fiabilidad del método deberán tenerse en cuenta todas las circunstancias pertinentes, que podrán ser, entre otras, las siguientes:

- a) el cumplimiento por el proveedor de servicios de confianza de las obligaciones que se enumeran en el artículo 14;
- b) la conformidad de las normas operacionales, políticas y prácticas del proveedor de servicios de confianza con cualesquiera normas y procedimientos internacionales reconocidos que sean aplicables y que resulten pertinentes para la prestación de los 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;
- 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<sup>55</sup> para la que se utiliza el servicio de confianza<sup>56</sup>, y

<sup>54</sup> Véase la nota 34 *supra*.

<sup>55</sup> Véase la nota 34 *supra*.

<sup>56</sup> El artículo 22, párrafo 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 previsto en el artículo 10, párrafo 2 d).

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 pudiera utilizarse el servicio de confianza.

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

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

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

4. Se presumirá que el método utilizado por un servicio de confianza designado de conformidad con el artículo 23 es fiable.

5. Lo dispuesto en el párrafo 4 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 método utilizado por un servicio de confianza designado de conformidad con el artículo 23 no es fiable.

#### *Artículo 23. Designación de servicios de confianza fiables*

1. [La persona, el órgano o la entidad, del sector público o privado, a que la jurisdicción promulgante haya atribuido competencia expresamente] podrá designar servicios de confianza que se presuman fiables.

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, 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.

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

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

#### *Artículo 24. Responsabilidad de los proveedores de servicios de confianza*

1. Todo proveedor de servicios de confianza que incumpla las obligaciones que le impone [el presente instrumento] deberá responder de las pérdidas que dicho incumplimiento cause [a cualquier persona].

2. El párrafo 1 se aplicará de conformidad con las normas de responsabilidad establecidas en la ley y sin perjuicio de las circunstancias siguientes:

a) la existencia de cualquier otro fundamento de la responsabilidad previsto en la ley, incluida la responsabilidad por incumplimiento de las obligaciones contractuales, o

b) cualquier otra consecuencia jurídica que, con arreglo a [este instrumento], se derive del incumplimiento por el proveedor de servicios de confianza de las obligaciones que le impone [el presente instrumento].

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

a) en la medida en que dicha 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;

[b) cuando esas limitaciones hayan sido acordadas por el proveedor de servicios de confianza con el usuario,]<sup>57</sup> ni

c) cuando el proveedor de servicios de confianza haya notificado<sup>58</sup> esas limitaciones al usuario de conformidad con la ley.

## Capítulo IV. Aspectos internacionales

### *Artículo 25. Reconocimiento transfronterizo*<sup>59</sup>

1. Cuando el funcionamiento de un sistema de gestión de la identidad, la emisión de una credencial de identidad o la prestación de un servicio de gestión de la identidad o servicio de confianza tengan lugar fuera de [la jurisdicción promulgante], dicho sistema, credencial o servicio producirá en [la jurisdicción promulgante] los mismos efectos jurídicos que produciría si funcionara, se emitiera o se prestara, respectivamente, en [la jurisdicción promulgante], siempre y cuando ofrezca un nivel de fiabilidad [sustancialmente equivalente] [que sea como mínimo equivalente].

2. Para determinar si un sistema de gestión de la identidad, un servicio de gestión de la identidad o una credencial de identidad, según corresponda, o un servicio de confianza ofrecen un nivel de fiabilidad [sustancialmente equivalente] [que sea como mínimo equivalente], se tomarán en consideración las normas internacionales reconocidas.

[3. Se presumirá la equivalencia si [la persona, el órgano o la entidad designados 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.]<sup>60</sup>

### *Artículo 26. Cooperación*

[La persona, el órgano o la entidad a que la jurisdicción 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.

<sup>57</sup> Véase la nota 47 *supra*.

<sup>58</sup> Véase la nota 48 *supra*.

<sup>59</sup> Los párrafos 1 y 2 del artículo 25 se modificaron para reflejar las deliberaciones sostenidas por el Grupo de Trabajo en su 61<sup>er</sup> período de sesiones (A/CN.9/1051, párrs. 60 y 61).

<sup>60</sup> El Grupo de Trabajo examinó el párrafo 3 del artículo 25 en su 61<sup>er</sup> período de sesiones (A/CN.9/1051, párrs. 63 a 66). El Grupo de Trabajo acordó conservar el párrafo para seguir analizándolo, aunque decidió modificarlo levemente para corregir la referencia a la entidad designadora (*ibid.*, párr. 66).