



Asamblea General

Distr. limitada
1 de febrero de 2019
Español
Original: inglés

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

Observaciones explicativas relativas al proyecto de disposiciones sobre el reconocimiento transfronterizo de sistemas de gestión de la identidad y servicios de confianza

Nota de la Secretaría

Índice

	<i>Página</i>
I. Introducción	2
II. Principales objetivos de política del proyecto de disposiciones	2
III. Observaciones explicativas sobre el proyecto de disposiciones	3
A. Capítulo I – Ámbito de aplicación (artículos 1 a 3)	3
B. Capítulo II – Disposiciones generales (artículos 4 a 7)	4
C. Capítulo III – Gestión de la identidad (artículos 8 a 13)	6
D. Capítulo IV – Servicios de confianza (artículos 14 a 18)	11
E. Capítulo V – Aspectos internacionales (artículos 19 a 20)	14



I. Introducción

1. La presente nota contiene observaciones relativas al proyecto de disposiciones sobre el reconocimiento transfronterizo de sistemas de gestión de la identidad y servicios de confianza que figura en el documento [A/CN.9/WG.IV/WP.157](#). En el documento [A/CN.9/WG.IV/WP.156](#), párrafos 6 a 15, se proporciona información sobre los antecedentes de la labor del Grupo de Trabajo en lo que respecta a las cuestiones jurídicas relacionadas con los sistemas de gestión de la identidad y los servicios de confianza.

II. Principales objetivos de política del proyecto de disposiciones

2. En los últimos 20 años se ha observado un crecimiento exponencial de las actividades en línea. El aumento de las actividades comerciales en línea (es decir, las operaciones electrónicas entre empresas, entre empresas y consumidores, y entre empresas y el Estado) es particularmente importante en cuanto al valor que representa. El comercio electrónico mundial aumentó de 64.000 millones de dólares de los Estados Unidos en 1999, a más de 25 billones en 2015¹. Este crecimiento coincide con un aumento del acceso de las personas y las empresas a Internet. Por ejemplo, el porcentaje de hogares con acceso a Internet se elevó de 35 % en 2002 a 83,6 % en 2017². Se ha observado un incremento similar en la disponibilidad de servicios de gobierno electrónico (incluidos los relacionados con el comercio), banca electrónica y pagos electrónicos.

3. Es necesario que ese crecimiento sea respaldado por una sensación de confianza en el entorno en línea. Un aspecto importante de la confianza en línea es la capacidad de identificar de manera fiable a cada una de las partes, especialmente cuando no ha existido una interacción personal previa. A lo largo de los años se han sugerido diversas soluciones para responder a la necesidad de identificación en línea. Como consecuencia de ello, han proliferado los métodos, tecnologías y dispositivos utilizados para la gestión de la identidad. El debate de los aspectos jurídicos de la gestión de la identidad a nivel mundial puede permitir no solo conciliar esas soluciones diferentes, sino también fomentar la interoperabilidad entre los sistemas de gestión de la identidad, independientemente de que se trate de operaciones entre particulares o con el Estado.

4. Existen varios obstáculos que se oponen a una utilización más amplia de los sistemas de gestión de la identidad y los servicios de confianza. Algunos de ellos son de carácter jurídico, e incluyen: 1) la falta de leyes que confieran efectos jurídicos a los sistemas de gestión de la identidad y los servicios de confianza; 2) la existencia de leyes y criterios divergentes en materia de gestión de la identidad, entre los que cabe mencionar las leyes que imponen la necesidad de utilizar determinadas tecnologías; 3) la existencia de leyes que exigen el uso de documentos de identidad en papel para poder realizar operaciones comerciales en línea; y 4) la falta de mecanismos que permitan obtener el reconocimiento jurídico transfronterizo de los sistemas de gestión de la identidad y los servicios de confianza ([A/CN.9/965](#), párr. 52).

5. El objetivo principal de la labor del Grupo de Trabajo es eliminar esos obstáculos mediante la elaboración de normas jurídicas uniformes. Son varios los fines de esas normas, a saber: aumentar la eficiencia; reducir el costo de las operaciones; aumentar la seguridad en general y la seguridad jurídica de las operaciones electrónicas, estableciendo así un marco de confianza; y cerrar la brecha digital.

¹ Fuente: Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD), Informe sobre comercio electrónico y desarrollo 2001, UNCTAD/SDTE/ECB/1, pág. 44; UNCTAD, Informe sobre la economía de la información 2017, UNCTAD/IER/2017, pág. 28.

² Fuente: Unión Internacional de Telecomunicaciones (UIT), estadísticas de las TIC, desarrollo de las TIC a nivel mundial, 2001 a 2018, que puede consultarse en <https://www.itu.int/es/ITU-D/Statistics/Pages/default.aspx>.

6. De este modo, la labor del Grupo de Trabajo contribuye al cumplimiento de los Objetivos de Desarrollo Sostenible. En particular, la importancia de la identidad se reconoce en el Objetivo de Desarrollo Sostenible 16, cuya meta 9 es que se proporcione una identidad jurídica a todos los seres humanos. En la economía digital, esto se traduce en el derecho a una identidad digital. La creación de un marco jurídico que regule los sistemas de gestión de la identidad y los servicios de confianza promoverá la implementación de la identidad digital en condiciones de seguridad. Al fomentar la confianza en el entorno en línea, ese marco jurídico también contribuirá al desarrollo sostenible y a la inclusión social, en consonancia con el Objetivo de Desarrollo Sostenible 9, que se refiere a impulsar la innovación (entre otras cosas).

III. Observaciones explicativas sobre el proyecto de disposiciones

A. Capítulo I – Ámbito de aplicación (artículos 1 a 3)

1. Finalidad de la utilización de sistemas de gestión de la identidad (artículo 1, párrafo 1)

7. La identificación puede exigirse con diferentes propósitos, a saber: para dar cumplimiento a la normativa, determinar la validez de un documento comercial o cumplir obligaciones contractuales (A/CN.9/965, párrs. 82 a 83; véase también el documento A/CN.9/WG.IV/WP.153, párrs. 32 a 34). **El Grupo de Trabajo tal vez desee plantearse cómo debería aplicarse el proyecto de disposiciones a los efectos de dar cumplimiento a la normativa.**

2. Reconocimiento jurídico interno y transfronterizo (artículo 1, párrafo 1)

8. El reconocimiento de los sistemas de gestión de la identidad y los servicios de confianza extranjeros se beneficia con la existencia de un marco jurídico interno. Ello se debe a que en dicho marco se establecen los conceptos jurídicos que resultan pertinentes para el mecanismo de reconocimiento. El reconocimiento transfronterizo se facilita aún más en los que casos en que la legislación interna, si bien no contiene disposiciones idénticas, establece normas armonizadas que recogen principios generales comunes. Además, el reconocimiento de sistemas de gestión de la identidad a través de fronteras tiene cierto grado de similitud con el reconocimiento entre distintos sistemas de gestión de la identidad, con independencia de cualquier elemento transfronterizo o extranjero. Por estas razones, el proyecto de disposiciones se ha elaborado con miras a ofrecer una base para la incorporación al derecho interno tanto de un acuerdo internacional como de un texto legislativo modelo.

3. Entidades pertinentes (artículo 1, párrafos 2 y 3)

a) Entidades públicas

9. Si bien la labor del Grupo de Trabajo se centra en las operaciones entre empresas, también deberían tenerse en cuenta los sistemas de gestión de la identidad establecidos en otros ámbitos que son pertinentes para las operaciones comerciales, especialmente en el contexto de los servicios públicos relacionados con el comercio, como las ventanillas únicas para actividades aduaneras (A/CN.9/965, párr. 83). Por estas razones, se justifica incluir a las entidades públicas entre las entidades a las que puede aplicarse el proyecto.

10. **El Grupo de Trabajo tal vez desee analizar si la participación de entidades públicas en operaciones de gestión de la identidad o en servicios de confianza plantea problemas específicos**, teniendo en cuenta la aplicación de los principios de neutralidad tecnológica (véase el párr. 23 *infra*) y autonomía de las partes (véase el párr. 24 *infra*).

b) Identificación de los objetos

11. Se ha señalado que la labor del Grupo de Trabajo debería facilitar la identificación fiable de ambas clases de sujetos (es decir, las personas físicas y jurídicas) y ambos tipos de objetos (es decir, los objetos físicos y digitales) en las operaciones, y que la identificación de un objeto podría ser útil para identificar a los sujetos de una operación. En cualquier caso, habría que distinguir claramente entre los sujetos y los objetos, ya que los objetos carecen de personalidad jurídica y no pueden asumir responsabilidad (A/CN.9/965, párr. 11).

12. La referencia que se hace en el párrafo 3 a la “verificación de la identidad” refleja la decisión del Grupo de Trabajo de centrar su labor en las cuestiones relacionadas con la identidad secundaria (o identidad vinculada a las operaciones) y, dentro de ese contexto, en las cuestiones relativas al reconocimiento (es decir, la verificación de la identidad) y no a la atribución de la identidad (A/CN.9/965, párr. 10). La identidad vinculada a las operaciones (o identidad secundaria) y la identidad básica (o identidad primaria) se describen más detalladamente en el documento A/CN.9/WG.IV/WP.153, párrafos 7 a 10.

4. No imposición de nuevas obligaciones de identificar (artículo 2, párrafo 1)

13. Un principio general común a todos los textos de la CNUDMI sobre comercio electrónico es que esos textos no afectan al derecho sustantivo, por ejemplo, al derecho aplicable en general a las operaciones comerciales.

14. En el contexto de los sistemas de gestión de la identidad y los servicios de confianza, este principio implica que la legislación relativa a la gestión de la identidad no debe introducir ninguna obligación nueva de identificar; que la legislación sobre servicios de confianza no debe introducir ninguna obligación nueva de utilizar algún tipo de servicio de confianza en particular, y que las obligaciones existentes deben mantenerse inalteradas.

15. Se ha dicho que existe un estrecho vínculo entre el principio de no imponer nuevas obligaciones de identificar y el principio de la autonomía de las partes (A/CN.9/965, párr. 110). Asimismo, se ha señalado que podrían surgir obligaciones de identificar en razón de la utilización de algún servicio de confianza en particular, pero que, de todos modos, la utilización de ese servicio de confianza debería ser voluntaria (*ibidem*).

5. Referencia a las leyes de protección de los datos y de la privacidad (artículo 2, párrafo 2)

16. El Grupo de Trabajo ha subrayado la importancia de los regímenes de protección de los datos para la gestión de la identidad y los servicios de confianza. En el artículo 2, párrafo 2, se hace referencia expresamente a las leyes de protección de los datos y de la privacidad, con el fin de reflejar la importancia que el Grupo de Trabajo asigna a esas leyes.

B. Capítulo II – Disposiciones generales (artículos 4 a 7)**1. Definiciones (artículo 4)**

17. Las definiciones que figuran en el artículo 4 se han formulado sobre la base de la terminología empleada en los textos de la CNUDMI sobre comercio electrónico.

18. En su 57º período de sesiones, el Grupo de Trabajo pidió a la Secretaría que incluyera varias de las definiciones extraídas del artículo 3 del reglamento eIDAS³ en la lista de definiciones esenciales, a fin de poder consultarlas en el futuro. Esas definiciones son las siguientes:

³ 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.

a) Por “identificación electrónica” se entiende el proceso de utilizar los datos de identificación de una persona en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica;

b) Por “medios de identificación electrónica” se entiende una unidad material y/o inmaterial que contiene los datos de identificación de una persona y que se utiliza para la autenticación en servicios en línea;

c) Por “datos de identificación de la persona” se entiende un conjunto de datos que permite establecer la identidad de una persona física o jurídica, o de una persona física que representa a una persona jurídica;

d) Por “sistema de identificación electrónica” se entiende un régimen para la identificación electrónica en virtud del cual se expiden medios de identificación electrónica a las personas físicas o jurídicas o a una persona física que representa a una persona jurídica;

e) Por “autenticación” se entiende un proceso electrónico que posibilita la identificación electrónica de una persona física o jurídica, o del origen y la integridad de datos en formato electrónico;

f) Por “fuente fidedigna” se entiende cualquier fuente que, independientemente de su forma, sea fiable para obtener datos, información o elementos probatorios exactos que puedan utilizarse para demostrar la identidad;

g) Por “parte que confía” (“parte usuaria” en el reglamento eIDAS) se entiende la persona física o jurídica que confía en la identificación electrónica o el servicio de confianza.

19. El Grupo de Trabajo tal vez desee plantearse si estas definiciones, que no se corresponden con los términos definidos por la CNUDMI, deberían reemplazar o complementar las definiciones que figuran en el artículo 4 del proyecto de disposiciones.

2. Principios generales e interpretación uniforme (artículos 5 a 7)

20. Por lo general, los textos de la CNUDMI contienen una disposición que alude al origen uniforme de dichos textos y al deber de interpretarlos de manera uniforme. El propósito plasmado en el artículo 5, párrafo 2, es garantizar que se mantenga la uniformidad en el momento de la interpretación y aplicación del texto legislativo.

21. El Grupo de Trabajo determinó que los siguientes principios generales eran pertinentes para su labor sobre los aspectos jurídicos de los sistemas de gestión de la identidad y los servicios de confianza: 1) no discriminación contra el uso de medios electrónicos; 2) equivalencia funcional; 3) neutralidad tecnológica; y 4) autonomía de las partes ([A/CN.9/936](#), párr. 67).

22. Si bien esos principios generales han sido recogidos en los textos de la CNUDMI sobre comercio electrónico para su aplicación en el plano nacional (véanse, por ejemplo, los arts. 3, 5 y 6 de la LMFE⁴), resultan igualmente aplicables a nivel transfronterizo por cuanto establecen en el plano nacional el fundamento jurídico que permitirá a la jurisdicción receptora reconocer y preservar los efectos jurídicos de los sistemas de gestión de la identidad y los servicios de confianza extranjeros.

23. La importancia del principio de neutralidad tecnológica para la gestión de la identidad ha sido plenamente reconocida. Con respecto a los países en desarrollo, se ha señalado que la aplicación de dicho principio podría evitar que se adoptaran requisitos técnicos demasiado costosos o complejos para los comerciantes ([A/CN.9/965](#), párr. 38). La aplicación del principio de neutralidad tecnológica en el contexto de los sistemas de gestión de la identidad puede exigir que estos reúnan determinados requisitos mínimos,

⁴ *Ley Modelo de la CNUDMI sobre las Firmas Electrónicas* (publicación de las Naciones Unidas, núm. de venta S.02.V.8).

referidos a las propiedades de los sistemas y no a determinadas tecnologías (A/CN.9/936, párr. 69).

24. La autonomía de las partes es un principio fundamental del derecho mercantil. Sin embargo, la aplicación de dicho principio está sujeta a las limitaciones que emanen de normas jurídicas imperativas (A/CN.9/936, párr. 72). Esas limitaciones son particularmente importantes debido a que los requisitos legales que se cumplen mediante el uso de sistemas de gestión de la identidad o servicios de confianza suelen ser obligatorios. A medida que avance en su labor, **el Grupo de Trabajo quizás desee determinar las normas básicas que las partes no podrán modificar ni excluir, a fin de dar mayor certeza y previsibilidad al reconocimiento transfronterizo de los sistemas de gestión de la identidad y los servicios de confianza** (A/CN.9/965, párr. 109). Por ese motivo, no se incluyó en el proyecto una disposición relativa a la autonomía de las partes (por ejemplo, basada en el art. 5 de la LMFE). No obstante, los elementos del principio de la autonomía de las partes se recogieron en el artículo 3.

25. El principio de la autonomía de las partes también contribuye a reforzar el cumplimiento de los acuerdos contractuales, como las normas de los sistemas de gestión de la identidad y los marcos y las normas de los sistemas de los servicios de confianza. Las normas de los sistemas pueden ser especialmente pertinentes en el contexto de los sistemas federados de gestión de la identidad (véase A/CN.9/WG.IV/WP.154, párr. 39).

C. Capítulo III – Gestión de la identidad (artículos 8 a 13)

1. Reconocimiento jurídico de un sistema de gestión de la identidad sobre la base de la equivalencia funcional (artículo 8)

26. El principio de equivalencia funcional exige determinar los requisitos que debe reunir un documento, método o proceso electrónico para cumplir las mismas funciones que el concepto análogo basado en el papel. Se ha observado que una disposición sobre equivalencia funcional solo será aplicable en la medida en que la identificación basada en el papel sea pertinente (A/CN.9/965, párr. 69) y que puede ser necesario establecer en la disposición un vínculo con los procesos de gestión de la identidad fuera de línea (A/CN.9/965, párr. 66).

27. En su 57º período de sesiones, el Grupo de Trabajo resaltó algunos elementos que debería tener una disposición sobre equivalencia funcional para conferir efectos jurídicos a la gestión de la identidad: la referencia a un elemento de identificación física utilizado fuera de línea (ya sea un documento, un registro u otra fuente fidedigna); la referencia a todas las etapas del proceso de gestión de la identidad (es decir, la identificación y la autenticación); y la referencia a los niveles de garantía u otra norma que permita evaluar la confianza en la correcta identificación (A/CN.9/965, párrs. 70 a 78).

28. Se han expresado distintas opiniones en el Grupo de Trabajo en cuanto al objeto del reconocimiento jurídico (A/CN.9/965, párr. 25), que a su vez determina el enfoque que tendrá una disposición sobre equivalencia funcional. En el contexto de la gestión de la identidad, pueden ser objeto de reconocimiento jurídico: a) el sistema de gestión de la identidad; b) las credenciales de identidad emitidas por un sistema de gestión de la identidad; o c) el resultado del proceso de identificación realizado mediante el uso de un sistema de gestión de la identidad (es decir, la operación de identidad) (A/CN.9/965, párr. 24).

29. La opinión predominante es que el Grupo de Trabajo debería concentrarse en el reconocimiento de los procesos (es decir, los sistemas), así como en el reconocimiento de los resultados tanto con respecto a los sistemas de gestión de la identidad como a los servicios de confianza (A/CN.9/965, párrs. 94 a 99). En ese sentido, también se explicó que el reconocimiento jurídico de los sistemas de gestión de la identidad, de las credenciales y del resultado del proceso de identificación se complementaban (A/CN.9/965, párr. 26). Por consiguiente, si se reconocen los sistemas de gestión de la identidad, también se reconocen las credenciales utilizadas para la identificación,

así como el resultado del proceso de identificación. Las dos opciones para el texto del artículo 8, que se examinaron en el 57º período de sesiones del Grupo de Trabajo, reflejan este enfoque.

30. Puede haber casos en que la identificación se lleve a cabo exclusivamente en línea y no sea posible aplicar el principio de equivalencia funcional (A/CN.9/965, párr. 62). A fin de contemplar todos los casos, se sugirió que el Grupo de Trabajo analizara las características de un método de identificación aceptable en lugar de tratar de elaborar disposiciones sobre equivalencia funcional (A/CN.9/965, párr. 69).

2. Normas de fiabilidad (artículo 9)

31. Entre los elementos pertinentes para determinar la fiabilidad del método que deberían figurar en una disposición sobre equivalencia funcional cabe mencionar los siguientes: a) acuerdos contractuales, si están permitidos con arreglo a la ley aplicable; b) certificación y supervisión; y c) niveles de garantía.

a) Certificación

32. La certificación de los proveedores de servicios de gestión de la identidad y de servicios de confianza puede contribuir en gran medida a fomentar la confianza en esos proveedores y en los servicios que prestan. Entre las opciones de certificación cabe citar las siguientes: la autocertificación; la certificación por un tercero independiente; la certificación por un tercero independiente acreditado; y la certificación por un órgano del Estado. La decisión sobre la forma más apropiada de certificación depende del tipo de servicio de que se trate, su costo y el nivel de confianza deseado. En el contexto de las operaciones entre empresas, resulta conveniente ofrecer todas las opciones de certificación, incluida la no certificación, ya que los socios comerciales deberían poder elegir la opción más adecuada a sus necesidades, teniendo en cuenta que cada opción producirá efectos jurídicos diferentes (A/CN.9/965, párr. 112).

33. Sin embargo, se señaló que cualquier solución que entrañara la intervención de un órgano central de certificación, acreditación o supervisión podría no ser apropiada en los casos en que se utilizara la tecnología de registro descentralizado, debido a las dificultades que habría, entre otras cosas, para determinar cuáles eran el órgano habilitado para solicitar la certificación y el órgano encargado de realizar la evaluación y adoptar medidas correctivas y de ejecución (A/CN.9/965, párrs. 114 y 129).

34. En los mecanismos de reconocimiento jurídico existentes (véase A/CN.9/WG.IV/WP.153, párrs. 61 a 73 y 76 a 79) que aplican el método *ex ante* (véanse los párrs. 47 a 49 *infra*), la certificación (incluida la autocertificación) es un elemento necesario para evaluar los sistemas de gestión de la identidad utilizando normas basadas en los resultados.

35. La certificación también puede ser pertinente para el reconocimiento jurídico *ex post* (véanse los párrs. 44 a 45 *infra*). Por ejemplo, los apartados e) y f) del artículo 10 de la LMFE mencionan, aunque no exigen, la acreditación, las auditorías y la autocertificación como elementos a tener en cuenta para determinar si los sistemas utilizados por un proveedor de servicios de certificación son fiables.

36. Se han expresado diferentes puntos de vista sobre la conveniencia de que participen organismos públicos en el proceso de certificación. Por una parte, se ha dicho que la certificación voluntaria no implica necesariamente la intervención de organismos públicos, sino que puede llevarse a cabo una certificación independiente (A/CN.9/965, párr. 112).

37. Por otra parte, se ha indicado que la supervisión por el Estado de las actividades de las entidades de certificación del sector privado es esencial para prevenir el riesgo de menoscabo de la competencia y las arbitrariedades, en particular con respecto a los pequeños agentes del mercado (A/CN.9/965, párrs. 115 y 128). Además, se ha observado que la acreditación de las entidades de certificación ante organismos estatales tiene por objeto garantizar la independencia, la imparcialidad y la equidad en las actividades de dichas entidades. En respuesta a esa observación, se ha señalado que un organismo

independiente podría estar en mejores condiciones de alcanzar esos objetivos (A/CN.9/965, párr. 115).

38. El criterio adoptado en el artículo 10 de la LMFE es producto del principio de neutralidad del modelo. La inserción de disposiciones imperativas con respecto a la supervisión puede percibirse como un impedimento para la adopción de un modelo de mercado basado en la autorregulación de los servicios de confianza.

b) Supervisión

39. Es habitual que se supervisen los sistemas de gestión de la identidad, ya que la supervisión se considera útil, o incluso necesaria, para fomentar la confianza en los proveedores de servicios y en los servicios que estos prestan. No obstante, la creación de un órgano con ese cometido tiene consecuencias administrativas y financieras. La utilización de mecanismos alternativos o complementarios, como la certificación por terceros, puede contribuir al logro de los objetivos de la supervisión y, al mismo tiempo, reducir los costos conexos.

40. Se ha observado un aumento de la participación de organismos públicos no solo en las actividades de supervisión, sino también en la creación e implementación de sistemas de gestión de la identidad y en la prestación de servicios de gestión de la identidad y servicios de confianza, lo cual exige separar las funciones de supervisión de otras funciones que desempeñan esos organismos (A/CN.9/965, párr. 128).

c) Niveles de garantía y cuadro comparativo

41. El nivel de garantía es una medida del grado de confianza en los procesos de identificación y autenticación y, por lo tanto, es esencial para determinar la fiabilidad del sistema de gestión de la identidad utilizado (A/CN.9/965, párr. 61). Se han expresado diferentes puntos de vista sobre la conveniencia de referirse al concepto de niveles de garantía (véase A/CN.9/965, párrs. 63 a 68).

42. Es posible hacer referencia a los niveles de garantía en una disposición sobre equivalencia funcional (es decir, el art. 8), o en una disposición que establezca normas relativas a la fiabilidad del sistema de gestión de la identidad (es decir, el art. 9). **El Grupo de Trabajo tal vez desee sopesar si, en los casos en que se haga referencia a niveles de garantía, bastaría con una referencia genérica, o si sería necesario mencionar distintos niveles de garantía** y, en este último caso, si debería atribuirse a cada nivel de garantía un efecto jurídico distinto (véase A/CN.9/965, párrs. 59 y 60).

43. En su 57º período de sesiones, el Grupo de Trabajo analizó el mecanismo del “cuadro comparativo” como método para verificar si un sistema de gestión de la identidad se ajustaba a la descripción genérica de un nivel de garantía (véase A/CN.9/965, párrs. 43 a 48 y 54). Un ejemplo práctico de la forma en que podría funcionar el cuadro comparativo figura en el documento A/CN.9/WG.IV/WP.153, párrafo 80.

3. Determinación de la fiabilidad *ex post* (artículo 9)

44. El artículo 9 tiene por objeto aplicar un método *ex post* para determinar la fiabilidad de los sistemas de gestión de la identidad. Con el método *ex post* se evalúa un sistema de gestión de la identidad solo en el caso de que se plantee efectivamente una controversia y siempre que se cumplan determinadas condiciones definidas con anterioridad. En algunos textos de la CNUDMI se ha adoptado este método con respecto a los servicios de confianza (véase, por ejemplo, el art. 9, párr. 3, de la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales).

45. En los documentos A/CN.9/965 (párrs. 40 a 45) y A/CN.9/WG.IV/WP.153 (párrs. 74 a 75) figuran otras consideraciones sobre el método *ex post*.

4. Presunción de fiabilidad (artículo 10)

46. El artículo 10 se basa en el artículo 6, párrafo 3, de la LMFE, según el cual se presume la fiabilidad de las firmas electrónicas que cumplan determinados requisitos. El artículo 10 puede ser aplicable tanto *ex post* como *ex ante*. Si se aplica *ex post*, respalda la aplicación del artículo 9 al enunciar criterios técnicos objetivos que permiten determinar más fácilmente la fiabilidad. Sin embargo, los mismos criterios pueden ser evaluados *ex ante* por un órgano determinado. En este último caso, el artículo 10 se aplica en combinación con el artículo 11.

5. Determinación de la fiabilidad *ex ante* (artículo 11)

47. El artículo 11 tiene por objeto aplicar un método *ex ante* para determinar la fiabilidad de los sistemas de gestión de la identidad.

48. La aplicación de este método exige que se definan previamente las condiciones que debe reunir un sistema de gestión de la identidad para figurar en una “lista blanca” de sistemas de gestión de la identidad reconocidos. Se ha expresado la opinión de que es preferible aplicar el método *ex ante* cuando se utilizan los niveles de garantía superiores (A/CN.9/965, párr. 47).

49. Las deliberaciones del Grupo de Trabajo sobre este método han puesto de relieve dos cuestiones: 1) la necesidad de que los sistemas de gestión de la identidad sean evaluados por un mecanismo institucional centralizado; y 2) la participación de organismos públicos. En los documentos A/CN.9/965 (párrs. 40 a 45) y A/CN.9/WG.IV/WP.153 (párrs. 61 a 73) se proporciona más información sobre los mecanismos institucionales que pueden utilizarse para aplicar el método *ex ante*. En el documento A/CN.9/965 (párrs. 49 a 50) figuran otras consideraciones sobre la participación de organismos públicos.

6. Obligaciones de los operadores de sistemas de gestión de la identidad (artículo 12)

50. En el artículo 12, párrafo 1, se establecen los elementos iniciales para determinar las obligaciones fundamentales de los operadores de sistemas de gestión de la identidad. Dicho párrafo se inspira en las disposiciones correspondientes del reglamento eIDAS.

a) Obligación de notificar las fallas de seguridad

51. En el artículo 12, párrafo 2, se establece la obligación de notificar las fallas de seguridad. Esta obligación es uno de los aspectos del principio de la transparencia (A/CN.9/936, párr. 88).

52. Las fallas de seguridad pueden afectar tanto a los sistemas como a las operaciones. Se ha determinado que es importante contar con un mecanismo adecuado de notificación de las fallas de seguridad para mejorar la calidad de los servicios y acrecentar el nivel de confianza en los sistemas de gestión de la identidad y los servicios de confianza (A/CN.9/965, párr. 123).

53. La notificación de las fallas de seguridad tiene elementos en común con la notificación de violaciones de los datos, pero también diferencias importantes. En el documento A/CN.9/WG.IV/WP.154 (párrs. 43 y 44) se recogen ejemplos de leyes vigentes que establecen un régimen para la comunicación de las fallas de seguridad.

b) Obligación de divulgar los servicios ofrecidos

54. En sus deliberaciones sobre el principio de la transparencia, el Grupo de Trabajo ha examinado la obligación de divulgar los servicios ofrecidos (A/CN.9/965, párr. 121). La transparencia de los servicios ofrecidos es importante no solo para los usuarios (para permitirles tomar una decisión fundamentada), sino también para los competidores y otras entidades interesadas (por ejemplo, a efectos de vigilar la competencia en el mercado) (A/CN.9/965, párr. 121). El párrafo 1 del artículo 12, en su redacción actual, no establece una obligación autónoma de divulgar los servicios ofrecidos.

55. Es probable que los operadores de sistemas de gestión de la identidad que participan en federaciones o que obtienen de algún otro modo una certificación para prestar sus servicios divulguen una cantidad considerable de información. Con respecto a otros proveedores, se pueden establecer ciertas obligaciones mínimas de divulgación de información. Por ejemplo, el artículo 9, párrafo 1, de la LMFE contiene una lista de los datos que el proveedor de servicios de certificación debe proporcionar a la parte que confía en el certificado.

7. Responsabilidad de los operadores de sistemas de gestión de la identidad (artículo 13)

56. Se ha afirmado que, en la medida en que la labor del Grupo de Trabajo abarque normas aplicables a nivel nacional, es necesario contemplar la cuestión de la asignación de responsabilidad (A/CN.9/965, párr. 116), ya que el régimen de responsabilidad aplicable puede tener repercusiones importantes en el fomento de la utilización de sistemas de gestión de la identidad y servicios de confianza para fines comerciales y no comerciales.

57. En ese sentido, el Grupo de Trabajo ha decidido examinar las siguientes cuestiones: la determinación de las entidades responsables, teniendo en cuenta los regímenes de responsabilidad especiales aplicables a las entidades públicas; la posibilidad de limitar la responsabilidad de las partes que cumplan ciertos requisitos previamente determinados; los mecanismos legales que permiten limitar la responsabilidad, por ejemplo, mediante la exención de responsabilidad o la inversión de la carga de la prueba); y las limitaciones contractuales de la responsabilidad (A/CN.9/936, párr. 85). El documento A/CN.9/WG.IV/WP.154 (párrs. 23 a 30) contiene una breve descripción de la legislación relativa a la responsabilidad de los operadores de sistemas de gestión de la identidad.

58. En el artículo 13, párrafo 1, se consagra el principio general de que un operador de sistemas de gestión de la identidad debería ser considerado responsable de las consecuencias que se deriven de la falta de prestación de los servicios en la forma convenida o, en defecto de acuerdo al respecto, conforme a lo exigido por la ley (A/CN.9/965, párr. 117). Sin embargo, en algunos casos puede no ser fácil identificar al operador del sistema de gestión de la identidad (por ejemplo, cuando se emplea la tecnología de registro descentralizado).

59. Con arreglo al texto actual de dicha disposición, una entidad pública puede ser considerada responsable cuando actúa como proveedora de servicios. La responsabilidad de la entidad pública puede ser diferente según si desempeña funciones de supervisión o si emite credenciales de identidad primaria.

60. En el artículo 13, tal como está redactado actualmente, solo se asigna responsabilidad a los operadores de sistemas de gestión de la identidad. **El Grupo de Trabajo tal vez desee sopesar si las normas relativas a la responsabilidad deberían aplicarse también a otras entidades interesadas** (por ejemplo, los usuarios y los terceros que confían) o si, en cambio, deberían aplicarse a tales entidades las normas de responsabilidad general. El Grupo de Trabajo quizás desee plantearse también si, en aras de la transparencia, debería ser obligatorio poner en conocimiento de los usuarios y otras entidades interesadas el régimen de responsabilidad aplicable.

61. En el artículo 13 se hace referencia al dolo y la negligencia como fundamento de la responsabilidad. En la publicación *Fomento de la confianza en el comercio electrónico* figura un análisis de las normas en materia de diligencia, incluidas la negligencia simple, la negligencia presunta y la responsabilidad objetiva, con respecto a la responsabilidad de los operadores de infraestructura de clave pública⁵.

⁵ *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónicas* (publicación de las Naciones Unidas, núm. de venta S.09.V.4), párrs. 179 a 201.

62. **El Grupo de Trabajo quizás desee estudiar si convendría establecer más normas con respecto a la carga de la prueba y a la definición de los daños y perjuicios** o si, en cambio, tales normas deberían estar contempladas en el derecho interno aplicable.

63. En el artículo 13, párrafo 2, se limita la responsabilidad de los operadores de sistemas de gestión de la identidad por los daños y perjuicios derivados de cualquier uso de los servicios que exceda las limitaciones dadas a conocer por el operador de sistemas de gestión de la identidad. Esta disposición complementa la obligación de divulgar los servicios ofrecidos, que es uno de los aspectos del principio de la transparencia. En la publicación *Fomento de la confianza en el comercio electrónico* se analiza la capacidad de los operadores de infraestructura de clave pública de limitar su responsabilidad o eximirse de ella por la vía del contrato⁶.

64. En el artículo 13, párrafo 3, se establece un mecanismo que alienta a los operadores de sistemas de gestión de la identidad a adoptar determinadas normas al exigir que se apliquen dichas normas como condición para obtener la exención de responsabilidad. Otra posibilidad sería que la disposición se refiriera a la utilización de niveles de garantía más altos.

65. El párrafo 3 del artículo 13 está supeditado a lo dispuesto en el párrafo 4 de ese artículo. La norma de “negligencia grave o conducta dolosa” está recogida en la Ley de Gestión de la Identidad Electrónica de Virginia (véase [A/CN.9/WG.IV/WP.154](#), párr. 29).

66. Un medio alternativo de resolver las cuestiones relativas a la responsabilidad consiste en establecer un mecanismo basado en seguros, en virtud del cual el asegurador indemniza por los daños y perjuicios derivados del uso de un sistema de gestión de la identidad. Otro mecanismo al que puede recurrirse prevé la aplicación automática de una cláusula de indemnización fijada convencionalmente o de una cláusula penal de cuantía fija si se cumplen determinadas condiciones.

D. Capítulo IV – Servicios de confianza (artículos 14 a 18)

67. Como cuestión preliminar, **el Grupo de Trabajo tal vez desee reflexionar sobre si debería crearse una lista abierta de servicios de confianza basada en una definición común de “servicio de confianza” o si convendría en cambio establecer normas comunes aplicables a todos los servicios de confianza y normas específicas aplicables a cada uno de ellos.** En una lista abierta de servicios de confianza podrían figurar los siguientes: firmas electrónicas; sellos electrónicos; sellos de tiempo electrónicos; servicios de entrega electrónica certificada; autenticación de sitios web; archivado electrónico; servicios electrónicos de depósito en garantía; y prueba electrónica de la presencia.

1. Reconocimiento jurídico de un servicio de confianza sobre la base del principio de equivalencia funcional (artículo 14)

68. Para poder redactar una disposición sobre equivalencia funcional que resulte adecuada para los servicios de confianza, es necesario determinar las funciones específicas que pretende cumplir ese servicio de confianza. El artículo 14 contiene disposiciones básicas sobre equivalencia funcional adaptadas a cada uno de los servicios de confianza enumerados en él. **El Grupo de Trabajo tal vez desee plantearse si una disposición sobre la equivalencia funcional de los servicios de confianza debería prever: a) normas de fiabilidad generales o específicas; b) la presunción de fiabilidad; c) la evaluación de la fiabilidad *ex ante*; y d) una cláusula de seguridad que impida el rechazo.**

⁶ *Ibid.*, párrs. 202 a 210.

a) Firmas electrónicas

69. El artículo 14, párrafo 1, se refiere a las firmas electrónicas, que son una modalidad habitual de servicios de confianza. Todos los textos de la CNUDMI sobre comercio electrónico contienen disposiciones sobre el uso de firmas electrónicas.

70. Algunos tipos de firma electrónica y otros servicios de confianza, como los archivos electrónicos, pueden ofrecer garantías de la integridad del mensaje de datos. En los textos de la CNUDMI, la integridad de un mensaje de datos es un requisito necesario para lograr la equivalencia funcional con la noción de “original” que se atribuye a los documentos en papel. **El Grupo de Trabajo tal vez desee examinar si la garantía de integridad debería preverse como un servicio de confianza diferenciado.**

b) Sellos electrónicos

71. Los sellos electrónicos están previstos en el reglamento eIDAS como un medio de prueba del origen y la integridad de un documento electrónico expedido por una persona jurídica (reglamento eIDAS, considerando 59). Además, “los sellos electrónicos pueden utilizarse para autenticar cualquier activo digital de la persona jurídica, por ejemplo, programas informáticos o servidores” (reglamento eIDAS, considerando 65).

72. Los textos de la CNUDMI sobre los servicios de confianza son aplicables tanto a las personas físicas como a las personas jurídicas. Además, se ha indicado que la labor actual del Grupo de Trabajo debería aplicarse también a los objetos físicos y digitales y, de ese modo, abarcar también los programas informáticos o servidores.

73. El artículo 8 de la LMCE⁷ exige la integridad para establecer la equivalencia funcional de la noción de “original” que se atribuye a los documentos en papel. El artículo 6, párrafo 3, de la LMFE se refiere al concepto de “integridad” cuando uno de los objetivos del requisito legal de la firma consiste en dar seguridades en cuanto a la integridad de la información a que corresponde.

74. A la luz de lo que antecede, **el Grupo de Trabajo tal vez desee plantearse si los sellos electrónicos deberían preverse como un servicio de confianza diferenciado o si pueden considerarse una subcategoría de las firmas electrónicas.**

c) Archivado electrónico

75. El artículo 14, párrafo 3, trata de los servicios de archivado electrónico, que a su vez están relacionados con la conservación de los documentos electrónicos. Los documentos electrónicos que se desea conservar pueden haber sido generados por primera vez en forma electrónica o pueden contener información consignada inicialmente en papel. Los servicios de archivado electrónico también pueden proporcionar una garantía de la integridad de los documentos electrónicos archivados, así como del momento en que se archivaron.

76. El archivado electrónico tiene la función de proporcionar seguridad jurídica respecto de la validez de los documentos electrónicos archivados, tanto en caso de litigio como en otros casos en que sea necesario. Se ha sugerido que el mecanismo de reconocimiento jurídico del archivado electrónico se limite a garantizar el cumplimiento de los requisitos legales de la jurisdicción en la que tengan que utilizarse los documentos archivados (A/CN.9/965, párr. 126). Si el Grupo de Trabajo desea considerar la posibilidad de elaborar una disposición sobre el archivado electrónico, se sugiere utilizar como base del debate el artículo 10 de la LMCE, que trata de la conservación de los mensajes de datos.

⁷ *Ley Modelo de la CNUDMI sobre Comercio Electrónico* (publicación de las Naciones Unidas, núm. de venta S.99.V.4).

77. Además, la ley puede exigir que sea posible migrar los documentos electrónicos archivados de manera tal que se pueda acceder a ellos, independientemente de la evolución tecnológica. Ese resultado puede obtenerse mediante la aplicación del principio de neutralidad tecnológica y de los requisitos de equivalencia funcional con el concepto de “integridad”, a saber: que cuando sea necesario presentar información, esta pueda mostrarse a la persona a quien se deba presentar (art. 8, párr. 1 b), de la LMCE).

d) Otros servicios de confianza

78. Los sellos de tiempo electrónicos, que están previstos en el artículo 14, párrafo 2, tienen por objeto aportar prueba de la fecha y hora en que el sello se vinculó a los datos. También pueden aportar prueba de la integridad de los datos a los que están vinculadas la fecha y hora.

79. Los servicios de entrega electrónica certificada, que están previstos en el artículo 14, párrafo 4, tienen por objeto aportar prueba del envío de una comunicación electrónica por el remitente identificado y de su recepción por el destinatario identificado. También pueden aportar prueba de la integridad de los datos transmitidos y del momento de envío y recepción de los datos.

80. El artículo 14, párrafo 5, se refiere a la autenticación de sitios web. Según el reglamento eIDAS, “los servicios de autenticación de sitios web proporcionan un medio por el que puede garantizarse a la persona que visita un sitio web que existe una entidad auténtica y legítima que respalda la existencia del sitio web” (reglamento eIDAS, considerando 67). **El Grupo de Trabajo tal vez desee estudiar si la autenticación de sitios web debería preverse como un servicio de confianza diferenciado** o si puede considerarse una subcategoría de las firmas electrónicas.

81. El artículo 14, párrafo 6, trata de los servicios electrónicos de depósito en garantía, que consisten en asumir la custodia de los bienes depositados en garantía y entregarlos a la persona que tenga derecho a recibirlos, una vez cumplidas las condiciones establecidas en el contrato de depósito en garantía. Los servicios electrónicos de depósito en garantía se utilizan para el pago de sumas de dinero y la comunicación del código fuente de programas informáticos. Por ejemplo, el pago del precio de las mercaderías puede postergarse hasta que los compradores reciban las mercaderías; al mismo tiempo, el vendedor recibe la confirmación de que el dinero para pagar el precio está disponible y será liberado en el momento de la entrega y aceptación de las mercaderías.

82. Los servicios de prueba electrónica de la presencia tienen por objeto demostrar que un sujeto se encontraba en un lugar determinado en un momento en particular. Este servicio de confianza se ha analizado en relación con los testamentos electrónicos. También puede ser pertinente para la inscripción en línea, por ejemplo, para acceder a servicios bancarios. **El Grupo de Trabajo tal vez desee examinar la cuestión de si debería redactarse una disposición que trate concretamente de los servicios de prueba electrónica de la presencia.**

2. Presunción de fiabilidad de los servicios de confianza (artículo 15)

83. En la LMFE y en varias leyes nacionales sobre las firmas electrónicas se hace una distinción entre los servicios de confianza sobre la base del nivel de fiabilidad que ofrecen. Concretamente, esas leyes atribuyen consecuencias jurídicas a las firmas electrónicas que satisfagan determinados requisitos, por lo que se considera que ofrecen un mayor nivel de fiabilidad. Para evitar cualquier confusión, se recomienda que en la labor del Grupo de Trabajo se haga referencia a “niveles de fiabilidad” cuando se analicen los servicios de confianza y que la expresión “niveles de garantía” se utilice únicamente cuando se aluda a los sistemas de gestión de la identidad.

84. **El Grupo de Trabajo quizás desee plantearse si el concepto de nivel de garantía debería aplicarse al reconocimiento de los servicios de confianza,** o si debería aplicarse algún otro concepto para determinar la fiabilidad de un determinado servicio de confianza. Se ha señalado que podrían utilizarse credenciales de identidad que ofrezcan un alto nivel de garantía para servicios de confianza que tengan distintos niveles de fiabilidad (A/CN.9/965, párr. 106). Por lo tanto, no hay correlación alguna entre los niveles de garantía de la identificación electrónica y los niveles de fiabilidad de un servicio de confianza.

3. Responsabilidad de los proveedores de servicios de confianza (artículo 18)

85. Como principio general, los proveedores de servicios de confianza deberían ser considerados responsables de las consecuencias que se deriven de la falta de prestación de los servicios en la forma convenida o, en defecto de acuerdo al respecto, conforme a lo exigido por la ley (A/CN.9/965, párr. 117). El tipo de servicio de confianza prestado determinará el alcance de esa responsabilidad.

86. La LMFE contiene disposiciones relativas a la responsabilidad derivada del proceder del firmante (art. 8), del prestador de servicios de certificación (art. 9) y de la parte que confía (art. 11). En esas disposiciones se establecen las obligaciones de cada una de las entidades que haya participado en el ciclo de vida de la firma electrónica. Además, la LMFE reconoce la posibilidad de que los proveedores de servicios de certificación limiten el alcance o el grado de su responsabilidad.

87. El documento A/CN.9/WG.IV/WP.154 (párrs. 33 a 35) contiene una breve descripción de la legislación relativa a la responsabilidad de los proveedores de servicios de confianza.

E. Capítulo V – Aspectos internacionales (artículos 19 a 20)

1. Reconocimiento jurídico transfronterizo (artículo 19)

88. El reconocimiento jurídico transfronterizo puede entenderse de diferentes maneras (véase A/CN.9/WG.IV/WP.153, párr. 55). En el 57º período de sesiones del Grupo de Trabajo se observó que la concesión del trato nacional era el criterio preferible para el reconocimiento jurídico transfronterizo (A/CN.9/965, párr. 30). El artículo 19 se ha redactado teniendo presente dicha observación.

89. El régimen de responsabilidad aplicable puede ser pertinente para evaluar la equivalencia de un sistema de gestión de la identidad extranjero. En consecuencia, se ha dicho que, para facilitar el reconocimiento transfronterizo de sistemas de gestión de la identidad, es preciso determinar cuál es la ley aplicable al régimen de responsabilidad (A/CN.9/965, párr. 116). Para ello puede ser necesario elaborar una norma de derecho internacional privado que prevea concretamente la cuestión, o hacer remisión a normas jurídicas ya existentes. **El Grupo de Trabajo tal vez desee plantearse si el reconocimiento jurídico transfronterizo supondría la aplicación del régimen de responsabilidad nacional a los sistemas de gestión de la identidad y los servicios de confianza extranjeros.**

90. En el artículo 19 no se contempla expresamente la limitación de la responsabilidad. Pueden resultar aplicables otras normas, entre ellas normas jurídicas imperativas, que pueden limitar la validez de esas cláusulas contractuales.

91. En el artículo 19, párrafo 2, se establece el nivel de fiabilidad como criterio para evaluar la equivalencia de un sistema de gestión de la identidad extranjero o de una credencial de identidad extranjera. En dicha disposición se plantean dos alternativas: que el sistema de gestión de la identidad extranjero proporcione el mismo nivel de fiabilidad, o que ofrezca un nivel de fiabilidad sustancialmente equivalente. El concepto de “nivel de fiabilidad sustancialmente equivalente” se extrajo del artículo 12 de la LMFE. **El Grupo de Trabajo quizás desee estudiar si, con respecto al reconocimiento de los sistemas de gestión de la identidad, convendría ofrecer más**

orientación sobre la referencia al concepto de niveles de garantía y el uso de cuadros comparativos.

2. Mecanismos de cooperación institucional (artículo 20)

92. Los mecanismos de cooperación institucional pueden contribuir a lograr el reconocimiento jurídico recíproco y la interoperabilidad de los sistemas de gestión de la identidad y los servicios de confianza.

93. El artículo 20 se refiere a la cooperación institucional en el sentido de cooperación entre Estados. La cooperación puede consistir en el intercambio de información, experiencia y buenas prácticas, en particular en lo que respecta a los requisitos técnicos y los niveles de garantía, la revisión por pares de los sistemas de gestión de la identidad y el examen de las novedades pertinentes. En una decisión de ejecución del reglamento eIDAS⁸ figuran más detalles sobre el intercambio de información y la revisión por pares y se indica, en particular, que el Estado miembro no estará obligado a facilitar la información que se le solicite si la divulgación de esa información pudiera poner en peligro cuestiones de seguridad pública o seguridad nacional o secretos comerciales, profesionales o empresariales.

94. Se puede lograr otra forma de cooperación mediante la federación de sistemas de gestión de la identidad. Aunque normalmente la federación se basa en acuerdos contractuales, las disposiciones legales pueden contribuir a promoverla. Para más información sobre la federación de sistemas de gestión de la identidad, véase el documento [A/CN.9/WG.IV/WP.154](#), párrafo 39.

95. Las federaciones de sistemas de gestión de la identidad funcionan sobre la base de la interoperabilidad técnica y de un marco jurídico común definido por un conjunto de normas del sistema. La armonización de los contratos y las normas legales puede contribuir al establecimiento de ese marco jurídico común ([A/CN.9/965](#), párr. 120).

96. Se ha mencionado que la adopción de un mecanismo *ex ante* para el reconocimiento jurídico también puede dar lugar a una forma de cooperación institucional.

⁸ Decisión de Ejecución (UE) 2015/296 de la Comisión, de 24 de febrero de 2015, por la que se establecen las modalidades de procedimiento para la cooperación entre los Estados miembros en materia de identificación electrónica.