Naciones Unidas A/CN.9/WG.IV/WP.154

Asamblea General

Distr. limitada
12 de septiembre de 2018
Español
Original: inglés

Comisión de las Naciones Unidas para el Derecho Mercantil Internacional
Grupo de Trabajo IV (Comercio Electrónico)
57º período de sesiones
Viena, 19 a 23 de noviembre de 2018

Cuestiones jurídicas relacionadas con la gestión de la identidad y los servicios de confianza

Nota de la Secretaría

Índice

V.18-05929 (S) 111018 111018

I. Introducción

1. En la presente nota se exponen determinados aspectos de algunos de los temas que el Grupo de Trabajo consideró pertinentes para su examen de las cuestiones jurídicas relacionadas con la gestión de la identidad y los servicios de confianza (A/CN.9/936, párr. 58) a fin de facilitar la continuación de los debates. El propósito de esta nota es, en particular, poner de relieve las cuestiones fundamentales que se plantean y sugerir posibles soluciones, sin restringir la posibilidad de que se analicen otros temas o de que algunos temas se examinen en forma conjunta, según proceda. En el documento A/CN.9/WG.IV/WP.153 se describen algunos aspectos de otros temas que el Grupo de Trabajo consideró pertinentes para su examen de las cuestiones jurídicas relacionadas con la gestión de la identidad y los servicios de confianza.

2. En el documento A/CN.9/WG.IV/WP.152, párrafos 6 a 17, se proporciona información sobre los antecedentes de la labor del Grupo de Trabajo en lo que respecta a las cuestiones jurídicas relacionadas con la gestión de la identidad y los servicios de confianza. En el documento A/CN.9/WG.IV/WP.152, párrafo 18, figura una lista de otros documentos pertinentes.

II. Cuestiones de interés para la labor futura sobre los aspectos jurídicos de la gestión de la identidad y los servicios de confianza

A. Certificación de los proveedores de gestión de la identidad y los proveedores de servicios de confianza

3. La certificación, incluida la autocertificación, así como la acreditación y las auditorías independientes pueden contribuir considerablemente a fomentar la confianza en los proveedores de gestión de la identidad y los proveedores de servicios de confianza. La decisión sobre la forma más apropiada de certificación puede depender del tipo de servicio de que se trate, su costo y el nivel de seguridad deseado.

4. El reglamento eIDAS prevé un sistema global de supervisión y certificación de los servicios de confianza. Su artículo 17 dispone que los Estados miembros designarán un organismo que se encargará de supervisar periódicamente a los prestadores cualificados de servicios de confianza y de adoptar otras medidas, en caso necesario, en relación con otros prestadores de servicios de confianza. En el artículo 17, párrafo 4, se enumeran las funciones concretas que ha de desempeñar el organismo de supervisión.

5. Cabe señalar que, de conformidad con el reglamento eIDAS, para considerar cualificado a un prestador de servicios de confianza es necesario que exista un organismo de supervisión. En particular, conforme al artículo 20, los prestadores cualificados de servicios de confianza deben ser auditados al menos cada 24 meses por un organismo de evaluación de la conformidad, y el consiguiente informe de evaluación de la conformidad debe enviarse al organismo de supervisión. Cuando el organismo de supervisión requiera a un prestador de servicios de confianza que corrija su incumplimiento y el prestador no actúe en consecuencia, el organismo de supervisión podrá retirar la cualificación al prestador o al servicio que este presta.

6. A su vez, en el marco del reglamento eIDAS, solo los prestadores cualificados de servicios de confianza pueden ofrecer servicios de confianza cualificados que entrañen determinados efectos jurídicos, como las presunciones. Por ejemplo, conforme al artículo 25, párrafo 2, una firma electrónica cualificada tendrá un efecto jurídico equivalente al de una firma manuscrita. En resumen, la existencia del organismo de supervisión hace posible la prestación de servicios de confianza cualificados que entrañen efectos jurídicos.

7. Con respecto a los servicios de confianza, en el artículo 10, apartados e) y f), de la Ley Modelo sobre Firmas Electrónicas (LMFE) se hace referencia a la existencia de acreditación, auditorías y autocertificación como un elemento que podría tenerse en

cuenta para determinar si los sistemas utilizados por un prestador de servicios de certificación son fiables. Por tanto, según ese enfoque, la existencia de un órgano de supervisión y de sistemas de acreditación es opcional y la apreciación de su existencia, discrecional.

8. En los modelos de reconocimiento jurídico recíproco que utilizan listas de confianza (véase A/CN.9/WG.IV/WP.153, párrs. 61 a 73 y 76 a 79), la certificación (incluida la autocertificación) es un elemento necesario para evaluar los sistemas de gestión de la identidad utilizando normas basadas en los resultados. Podría ser necesario establecer un conjunto predefinido de perfiles que hayan de utilizarse para la evaluación.

9. El Grupo de Trabajo tal vez desee sopesar si la existencia de la certificación, incluida la autocertificación, de la acreditación y de las auditorías independientes debería estar vinculada a determinados efectos jurídicos, y, en caso afirmativo, a qué efectos, o si más bien debería incluirse entre los elementos que podrían ser pertinentes para evaluar la fiabilidad o alguna otra cualidad de los proveedores de gestión de la identidad y de servicios de confianza. En sus deliberaciones, el Grupo de Trabajo tal vez desee también indicar si el uso de la certificación, incluida la autocertificación, y de la acreditación y las auditorías independientes debería ser obligatorio u opcional.

B. Niveles de seguridad

1. Gestión de la identidad

10. El nivel de seguridad es una medida de la fiabilidad de una aseveración de identidad que se basa en los procesos utilizados. Existen diferentes definiciones del concepto de niveles de seguridad, utilizadas por distintas entidades públicas y privadas. Su formulación se actualiza periódicamente a medida que evolucionan la tecnología y los procesos institucionales. Habida cuenta de la adopción del principio de neutralidad tecnológica, solo se toman en consideración los niveles de seguridad definidos de manera tecnológicamente neutra.

11. El Instituto Nacional de Normas y Tecnología (NIST) de los Estados Unidos de América ha definido tres niveles diferentes de seguridad relacionados con la identidad: el nivel relativo a la identidad (“IAL”), el relativo al autenticador (“AAL”) y el relativo a la federación (“FAL”)[1]. El primer nivel mencionado se refiere al proceso de comprobación de identidad, el segundo, al proceso de autenticación, y el tercero, al protocolo de aseveración utilizado en un entorno federado para comunicar información sobre la autenticación y los atributos (si procede) a una parte que confía.

12. Más precisamente, el nivel IAL tiene que ver con la solidez del proceso de comprobación de identidad para determinar con certeza la identidad de una persona; el AAL se refiere a la solidez del proceso de autenticación en sí y a los vínculos entre el autenticador y el identificador de una persona concreta; y el FAL se refiere a la solidez del protocolo de aseveración que utiliza la federación para comunicar información sobre la autenticación y los atributos a una parte que confía, si se utiliza una estructura de identidad federada[2].

13. Cada nivel de seguridad relacionado con la identidad tiene sus propios grados de solidez en función de determinados requisitos. Por ejemplo, en el grado IAL1, los atributos, si los hubiere, los asevera la propia entidad o debería darse por supuesto que los asevera la propia entidad. En el IAL2, se requiere comprobar la identidad, ya sea en persona o a distancia. Además, en relación con ese grado se exige que los atributos de identificación hayan sido verificados en persona o a distancia utilizando, como mínimo, unos procedimientos establecidos. En el grado IAL3 se requiere la comprobación de identidad en persona y la verificación de los atributos de identificación por un

[1] NIST, Special Publication 800-63-3, *Digital Identity Guidelines*, junio de 2017, sección 2. Se puede consultar en https://doi.org/10.6028/NIST.SP.800-63-3.

[2] NIST, *Digital Identity Guidelines*, cit., sección 5.2.

representante autorizado del prestador de servicios de certificación mediante el examen de la documentación física de conformidad con unos procedimientos establecidos.

14. En el artículo 8 del reglamento eIDAS se establecen tres niveles de seguridad para la gestión de la identidad: bajo, sustancial y alto, así como los criterios correspondientes a cada nivel. En particular, el nivel de seguridad bajo refleja un grado limitado de confianza en la identidad pretendida o declarada de una persona; el nivel de seguridad sustancial corresponde a un grado sustancial de confianza en la identidad pretendida o declarada de una persona; y el nivel de seguridad alto se refiere a un grado de confianza en la identidad pretendida o declarada de una persona superior al que correspondería al nivel sustancial.

15. En un acto de ejecución del reglamento eIDAS[3] se establecen las especificaciones y procedimientos técnicos mínimos que se utilizarán para determinar la fiabilidad y la calidad de la inscripción, la gestión de los medios de identificación electrónica, la autenticación y la gestión y organización de los proveedores que presten un servicio relacionado con la gestión de la identidad en un contexto transfronterizo. Esas especificaciones y procedimientos técnicos se describen de una forma tecnológicamente neutra.

16. A la luz de lo que antecede, el Grupo de Trabajo tal vez desee estudiar si el concepto de niveles de seguridad debería utilizarse para cumplir requisitos legales o determinar efectos jurídicos. De ser así, tal vez desee también examinar, en particular, la relación entre los niveles de seguridad, por un lado, y los requisitos y mecanismos de reconocimiento jurídico, por el otro. El Grupo de Trabajo quizás podría deliberar también sobre si debería examinar las características de los niveles de seguridad, y, en caso afirmativo, cuál debería ser el alcance de ese examen.

2. Servicios de confianza

17. Una cuestión fundamental en relación con los servicios de confianza es si debería aplicarse también a ellos el concepto de niveles de seguridad. Varias leyes nacionales sobre las firmas electrónicas reconocen dos niveles de firmas electrónicas. El primero abarca todas las formas de firma electrónica. El segundo asocia determinadas consecuencias jurídicas, como la presunción de origen e integridad, a las firmas electrónicas que satisfagan ciertos requisitos. Esto puede interpretarse en el sentido de que se introducen distintos niveles de seguridad con respecto a las firmas electrónicas.

18. En lo que respecta a los servicios de confianza, el artículo 24, párrafo 1, del reglamento eIDAS ofrece un ejemplo de utilización de los niveles de seguridad en el contexto del cumplimiento de un requisito de identificación para la expedición de un certificado cualificado. Concretamente, para satisfacer el requisito de que el prestador cualificado de servicios de confianza verifique la identidad de la persona a la que se expida un certificado cualificado, el reglamento eIDAS permite que dicha verificación se haga a distancia utilizando medios de identificación electrónica que cumplan los requisitos establecidos con respecto a los niveles de seguridad “sustancial” o “alto”.

19. El Grupo de Trabajo tal vez desee examinar si el concepto de niveles de seguridad debería aplicarse a los servicios de confianza y, en caso afirmativo, de qué manera.

C. Responsabilidad

20. El régimen de responsabilidad aplicable puede tener repercusiones importantes en la promoción de la utilización de servicios de gestión de la identidad y servicios de confianza para fines comerciales y no comerciales. En ese sentido, cabe señalar que, si bien en los casos de identificación indebida en las operaciones comerciales se suele disponer de recursos legales, los casos de atribución indebida de la identidad básica en

[3] Reglamento de Ejecución (UE) 2015/1502 de la Comisión, de 8 de septiembre de 2015, sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica.

documentos en papel pueden no dar lugar a responsabilidad si la legislación nacional no hace responsables de ese servicio a las entidades públicas.

21. El Grupo de Trabajo ya ha identificado algunas cuestiones pertinentes para sus deliberaciones sobre la responsabilidad de participantes en la gestión de la identidad y los servicios de confianza, a saber: qué entidades deberían ser responsables (los emisores, los proveedores, otras partes), teniendo en cuenta los regímenes de responsabilidad especiales aplicables a las entidades públicas; la posibilidad de limitar la responsabilidad de las partes que cumplieran unos requisitos previamente determinados; mecanismos legales que permitieran 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).

22. En algunos casos, podría no ser fácil determinar cuál es la entidad responsable, por ejemplo, cuando se trata de datos sobre atributos en los que se confía proporcionados por un servicio de confianza, cuando se emplea la tecnología de registro descentralizado para el estampado de fecha y hora (A/CN.9/936, párr. 86). En otros casos, podría utilizarse un mecanismo basado en seguros para las operaciones comerciales, en virtud del cual la utilización indebida del sistema de identificación electrónica o el servicio de confianza podría dar lugar a una indemnización por parte del asegurador. Otro mecanismo prevé la aplicación automática de una cláusula de indemnización fijada convencionalmente o de una cláusula penal de cuantía fija si se cumplen determinadas condiciones.

1. Gestión de la identidad

23. El artículo 9 del reglamento eIDAS dispone que, en el momento de efectuar la notificación de un sistema de gestión de la identidad, se transmita información sobre el régimen de responsabilidades aplicable a la parte que expida los medios de identificación electrónica y la parte que utilice el procedimiento de autenticación.

24. El artículo 11 del reglamento eIDAS dispone que el Estado miembro que efectúa la notificación será responsable de los perjuicios causados en caso de incumplimiento de sus obligaciones de garantizar que los datos de identificación de la persona que representan en exclusiva a la persona en cuestión se atribuyen a la persona adecuada, y garantizar la disponibilidad de la autenticación en línea de la información utilizada para confirmar los datos de identificación de la persona. También dispone que la parte que expida los medios de identificación electrónica será responsable de los perjuicios causados en caso de incumplimiento de la obligación de garantizar que los medios de identificación electrónica se atribuyan a la persona representada en exclusiva por los datos de identificación. Por último, el artículo dispone que la parte que realice el procedimiento de autenticación será responsable en caso de incumplimiento de la obligación de garantizar el correcto funcionamiento del procedimiento de autenticación en línea utilizado para confirmar los datos de identificación de la persona.

25. El artículo 11 del reglamento eIDAS se aplica únicamente a las operaciones transfronterizas, y siempre y cuando el incumplimiento sea deliberado o por negligencia. Se aplica en consonancia con las normas nacionales en lo que respecta a cuestiones como la definición de daños y perjuicios y la asignación de la carga de la prueba, y sin perjuicio de la responsabilidad adicional derivada de las normas nacionales de las partes que participen en las operaciones en que se utilicen los sistemas de gestión de la identidad.

26. En resumen, el reglamento eIDAS asigna responsabilidad a los participantes en el sistema de gestión de la identidad si estos incumplen determinadas obligaciones citadas, si ese incumplimiento es deliberado o por negligencia, siempre y cuando se trate de una operación transfronteriza, y sin perjuicio de la responsabilidad adicional que pueda derivarse en virtud de las normas nacionales.

27. En el artículo 281 de la Ley 2017-20 de Benin se indica que el operador del sistema de gestión de la identidad será responsable de los perjuicios causados a los usuarios de los sistemas de gestión de la identidad si dichos perjuicios fueran causados de forma deliberada o negligente.

28. El artículo 1-552 de la Ley de Gestión de la Identidad Electrónica de Virginia exime de responsabilidad al proveedor de marco de confianza de identidad o proveedor de identidad si la credencial de identidad se ha expedido o el atributo de identidad o sello de confianza se han asignado de conformidad con las normas de gestión de la identidad aprobadas por la Secretaría de Tecnología del Commonwealth de Virginia, las estipulaciones contractuales, y las normas y reglas escritas del marco de confianza de identidad del que sea miembro el proveedor de identidad. De conformidad con el artículo 1-550, un sello de confianza es un sello oficial de lectura mecánica, medio de autenticación, certificación, licencia, o logotipo que el operador de un marco de confianza de identidad puede proporcionar a proveedores de identidad certificados dentro de su marco de confianza para indicar que el proveedor de identidad cumple las normas y reglas escritas del marco de confianza de identidad.

29. En resumen, la Ley de Gestión de la Identidad Electrónica de Virginia exime de responsabilidad a los operadores de marcos de confianza de identidad y los proveedores de identidad que cumplan las normas establecidas por un organismo público, las estipulaciones contractuales y el reglamento de la federación. Se determina si se han cumplido las especificaciones y normas mínimas establecidas por el Commonwealth de Virginia recurriendo a autoridades de certificación independientes que efectúan exámenes del cumplimiento de objetivos, coherentes y sujetos a inspección, sobre la base de unos criterios de certificación claramente definidos[4]. La exención no se aplica si el operador del marco de confianza de identidad o el proveedor de identidad ha cometido un acto u omisión con negligencia grave o una falta deliberada de conducta.

30. El artículo 1-555 de la Ley de Gestión de la Identidad Electrónica de Virginia establece que ninguna disposición de dicha ley o acto u omisión de una entidad pública relacionados con la gestión de la identidad ha de interpretarse como una renuncia a la inmunidad soberana de dicha entidad pública.

31. El Grupo de Trabajo podría examinar a qué entidades se debe exigir responsabilidad, en virtud de qué régimen de responsabilidad, y si debería establecerse un régimen especial de responsabilidad para las entidades públicas.

32. Al examinar el régimen de responsabilidad, el Grupo de Trabajo tal vez desee tener en cuenta: a) la posibilidad de limitar la responsabilidad de las partes que cumplan unos requisitos predeterminados, por ejemplo, eximiéndolas o invirtiendo la carga de la prueba; b) si deberían vincularse los distintos niveles de seguridad con distintos regímenes de responsabilidad; c) la posibilidad de limitar la responsabilidad mediante contrato; y d) si se debería obligar a suministrar metadatos que describan el régimen de responsabilidad, incluidas las limitaciones del caso.

2. Servicios de confianza

33. El artículo 13 del reglamento eIDAS dispone que los prestadores de servicios de confianza serán responsables de los perjuicios causados de forma deliberada o por negligencia a cualquier persona física o jurídica en razón del incumplimiento de las obligaciones establecidas en el reglamento. En otras palabras, a los prestadores de servicios de confianza que cumplen las obligaciones establecidas en el reglamento no se les exige responsabilidad.

34. Además, el artículo 13 introduce una presunción rebatible de intencionalidad o negligencia en el caso de un prestador cualificado de servicios de confianza, mientras que la carga de la prueba de la intencionalidad o la negligencia de un prestador no cualificado de servicios de confianza corresponderá a la persona que alegue los perjuicios. Esta disposición tiene por objeto fomentar la confianza de los usuarios en los prestadores cualificados, habida cuenta de que, en caso de perjuicios, la presunción facilita la obtención de una reparación. Por último, en el artículo 13 se reconoce la posibilidad de que los prestadores de servicios de confianza limiten su responsabilidad,

[4] Commonwealth of Virginia Identity Management Standards Advisory Council, *Guidance Document 5: Certification of Identity Trust Framework Operators* (draft), Section 7: Certification of Identity Trust Framework Operators.

siempre que informen con antelación a sus clientes de esas limitaciones y que esas limitaciones sean reconocibles para un tercero.

35. La LMFE contiene disposiciones relativas a la responsabilidad dimanante del proceder del firmante (art. 8), del prestador de servicios de certificación (art. 9) y de la parte que confía en el certificado (art. 11). Esas disposiciones estipulan las obligaciones de cada entidad que haya participado en el ciclo de vida de la firma electrónica. La LMFE reconoce la posibilidad de que los proveedores de servicios de certificación limiten el alcance o el grado de su responsabilidad.

D. Mecanismos de cooperación institucional

36. 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. Pueden ser de carácter público o privado.

37. El artículo 12 del reglamento eIDAS ofrece un ejemplo de mecanismo de cooperación institucional, al indicar que los Estados miembros cooperarán con respecto a la interoperabilidad y la seguridad de los sistemas de gestión de la identidad. La cooperación podrá consistir en un intercambio de información, experiencia y prácticas idóneas, en particular sobre los requisitos técnicos y los niveles de seguridad, la revisión por pares de los sistemas de identificación electrónica, y el examen de las novedades pertinentes.

38. En el acto de ejecución del reglamento eIDAS[5] figuran detalles adicionales sobre el intercambio de información y la revisión por pares, y se indica, en particular, que el Estado miembro no tendrá obligación de facilitar la información que se le solicite si su divulgación pudiera poner en peligro asuntos de seguridad pública o seguridad nacional o secretos comerciales, profesionales o empresariales. También se establece una red de cooperación para facilitar la realización de actividades de cooperación. Cabe señalar que, si bien el sistema de revisión por pares del sistema de gestión de la identidad que ha de notificarse es opcional, lo cierto es que sus resultados podrían aportar información importante sobre si el sistema podría ajustarse a las normas exigidas, y, por lo tanto, constituye un paso importante en el mecanismo de notificación sobre el que se basa la estructura institucional del reglamento eIDAS.

39. Se puede lograr un tipo diferente de cooperación entre los sistemas de gestión de la identidad mediante la federación de esos sistemas. Conforme a ese modelo, la información sobre la identidad verificada por un sistema de gestión de la identidad se facilita de manera convenida y controlada a diversas partes en un sistema diferente de gestión de la identidad que tienen necesidad de esa información sobre la identidad con distintos propósitos (véase también A/CN.9/WG.IV/WP.153, párr. 47). La federación de sistemas de gestión de la identidad logra la interoperabilidad entre sus participantes utilizando un marco técnico y jurídico común definido por un conjunto de normas del sistema. La federación puede contribuir, por tanto, a aumentar el número de usuarios y de aplicaciones y a frenar los costos por concepto de gestión de la identidad. Aunque las federaciones se basan en acuerdos contractuales, las disposiciones legales pueden contribuir a promover la federación (véase, por ejemplo, el uso de sellos de confianza en la Ley de Gestión de la Identidad de Virginia, citada en el párr. 28 *supra*).

E. Transparencia

40. El Grupo de Trabajo determinó que el principio de transparencia era pertinente para las deliberaciones futuras sobre la gestión de la identidad y los servicios de confianza (A/CN.9/936, párr. 8). Al hacerlo, destacó dos obligaciones relativas a ese principio: el deber de revelar qué servicios de gestión de la identidad y de confianza se

[5] 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.

ofrecen y cuál es la calidad de esos servicios; y el deber de notificar las fallas de los mecanismos de seguridad.

41. Con respecto a los servicios ofrecidos y su calidad, cabe señalar que los proveedores de entidad y los proveedores de confianza que participan en federaciones o que obtienen de algún otro modo una certificación para prestar sus servicios divulgarían una cantidad considerable de información. Se pueden establecer unas obligaciones mínimas en cuanto a la divulgación de información para otros proveedores. Por ejemplo, el artículo 9, párrafo 1, de la LMFE contiene una lista de la información que el prestador de servicios de certificación debe proporcionar a la parte que confía en el certificado.

42. Con respecto a la obligación de notificar las fallas de seguridad, se señaló que esa notificación tenía elementos en común con la notificación de violaciones de los datos, pero también diferencias importantes. Se añadió que existían algunos ejemplos útiles de mecanismos que iban más allá de la mera notificación en los casos en que se produjesen fallas en los mecanismos de seguridad (A/CN.9/936, párr. 89). Pueden tenerse en cuenta otras consideraciones relacionadas con la posible utilización de inteligencia sobre amenazas cibernéticas para mitigar riesgos.

43. En el artículo 10 del reglamento eIDAS se hace referencia a la obligación de los Estados miembros de notificar los casos de violación o puesta en peligro que afecten a la fiabilidad del sistema de autenticación transfronteriza. El Estado miembro que efectúa la notificación también debe suspender o revocar sin dilaciones la autenticación que haya sido puesta en peligro o las partes afectadas de esa autenticación.

44. De modo similar, el artículo 19, párrafo 2, del reglamento eIDAS obliga a los prestadores de servicios de confianza a notificar al organismo de supervisión y otros organismos pertinentes, como la autoridad de protección de datos, cualquier violación de la seguridad o pérdida de la integridad que tenga un impacto significativo en el servicio de confianza prestado o en los datos personales correspondientes. La notificación deberá realizarse sin demoras indebidas y, en cualquier caso, en un plazo de 24 horas tras tener conocimiento de la violación de la seguridad o pérdida de la integridad.

45. El artículo 8, párrafo 1 b), de la LMFE establece un mecanismo de notificación opcional que el firmante puede utilizar en caso de que los datos de creación de la firma hayan quedado en entredicho o de que exista un riesgo considerable de que hayan quedado en entredicho.

46. Una posible disposición sobre el deber de divulgar las fallas de seguridad podría formularse de la siguiente manera:

> Los proveedores de identidad y los proveedores de servicios de confianza notificarán sin demora [y, en todo caso, dentro de los ... días después de tener conocimiento de ello], [al órgano de supervisión] [a sus clientes y partes que confían afectados] toda falla de seguridad o pérdida de la integridad que tenga repercusiones [considerables] en los servicios, credenciales de identidad o procesos de autenticación prestados o en los datos personales correspondientes.
>
> En caso de que la falla de seguridad o pérdida de la integridad sean considerables, los proveedores de identidad y los proveedores de servicios de confianza deberán suspender la prestación de los servicios afectados [hasta ...].
>
> Los usuarios de servicios de identidad y usuarios de servicios de confianza deberán notificar al proveedor de servicios en caso de que las credenciales de identidad, los procesos de autenticación o los datos de creación de servicios de confianza hayan quedado en entredicho, o en caso de que las circunstancias de que tenga conocimiento el usuario den lugar a un riesgo sustancial de que las credenciales de identidad, los procesos de autenticación o los datos de creación de servicios de confianza hayan quedado en entredicho.

47. El proyecto de disposición contiene texto opcional para establecer un plazo dentro del cual debe hacerse la notificación, a fin de identificar a las partes a quienes habrá que

notificar y determinar el grado de repercusión en los servicios, credenciales de identidad o datos personales que desencadena la obligación de notificar. También es posible establecer la obligación de suspender el sistema de gestión de la identidad y los servicios de confianza hasta que se contenga la falla o la pérdida o se entable un nuevo proceso de certificación o un proceso similar.

F. Conservación de los datos

48. El Grupo de Trabajo ya ha puesto de relieve la importancia para el comercio transfronterizo de la armonización e interoperabilidad de los regímenes de conservación de datos (A/CN.9/936, párr. 91). Al hacerlo, ha destacado al menos dos posibles aspectos de interés. El primero se refiere a la protección de los datos; el segundo, al almacenamiento y archivo de los datos.

49. La protección de datos es un tema que puede plantear cuestiones particularmente complejas. El Grupo de Trabajo tal vez desee confirmar que, en consonancia con el principio general de que los textos de la CNUDMI sobre comercio electrónico no afectan al derecho sustantivo (véase A/CN.9/WG.IV/WP.153, párr. 48), las normas relativas a la protección de datos y cuestiones conexas, como la privacidad, deberían seguir siendo aplicables en su totalidad, y tal vez desee también, por tanto, determinar si hay especificaciones o aclaraciones adicionales que resultarían útiles.

50. El almacenamiento y archivo de documentos es una función que puede cumplirse utilizando medios electrónicos, como ya indica el artículo 10 de la Ley Modelo sobre Comercio Electrónico (LMCE), que establece los requisitos para la equivalencia funcional entre los mensajes de datos y los documentos en papel con respecto a la conservación. La obligación de conservar los documentos deriva del derecho sustantivo y se refiere al tiempo necesario para la prescripción de las distintas medidas.

51. La prestación de servicios de almacenamiento y archivo de datos puede ser objeto de un servicio de confianza concreto (véanse los párrs. 64 y 65 *infra*). En el marco de la interoperabilidad de los servicios de confianza, el Grupo de Trabajo tal vez desee examinar las cuestiones relativas a la portabilidad de los archivos electrónicos.

G. Supervisión de los proveedores de servicios

52. En caso de que el Grupo de Trabajo determine que sería apropiado examinar los sistemas de gestión de la identidad y los sistemas de servicios de confianza en lugar de las operaciones conexas (véase A/CN.9/WG.IV/WP.153, párrs. 57 a 59), crear un organismo de supervisión podría ser útil, o incluso necesario, para fomentar la confianza en los proveedores de servicios y en los servicios prestados. No obstante, la creación de un organismo de ese tipo entraña varias consecuencias administrativas y financieras. Unos mecanismos alternativos o complementarios, como la certificación por terceros, pueden contribuir a lograr los objetivos de supervisión de los proveedores de servicios y, al mismo tiempo, reducir los costos conexos.

53. Las leyes de Vermont y de Virginia otorgan la autoridad de supervisión de los proveedores de servicios de identidad a organismos públicos. Del mismo modo, el artículo 97 de la Ley 2017-07 del Togo asigna funciones de supervisión de los proveedores de servicios de confianza a la autoridad nacional de certificación. En virtud del artículo 283 de la Ley 2017-20 de Benin, los proveedores de servicios de identidad son nombrados por una autoridad pública. El sistema de notificación previsto por el reglamento eIDAS también conlleva un mecanismo de supervisión de la gestión y prestación de servicios de identidad.

54. Con respecto a los proveedores de servicios de confianza, varias leyes asignan a un organismo de supervisión la facultad de otorgar el reconocimiento como cualificado o de supervisar la forma en que se otorga ese reconocimiento por terceros. El reglamento eIDAS exige a los Estados miembros que designen un organismo nacional de supervisión competente en lo que respecta a los proveedores de servicios de confianza.

55. La LMFE contiene una referencia opcional a la existencia de organismos de supervisión, dado que adopta el principio de neutralidad del modelo, ya que insertar disposiciones imperativas sobre la existencia de organismos de supervisión puede entenderse en el sentido de que impide la adopción de un modelo de mercado basado en la autorregulación de los servicios de confianza.

H. Cuestiones específicamente relacionadas con los servicios de confianza

56. La labor sobre las cuestiones jurídicas relativas a los servicios de confianza está estrechamente relacionada con la labor sobre la gestión de la identidad. Por consiguiente, las observaciones sobre los servicios de confianza en el contexto del principio de equivalencia funcional (A/CN.9/WG.IV/WP.153, párrs. 36 y 37), el reconocimiento jurídico (A/CN.9/WG.IV/WP.153, párrs. 93 a 98), y los niveles de seguridad (párrs. 17 a 19 *supra*) y de responsabilidad (párrs. 33 a 35 *supra*) se han formulado de manera conjunta con el examen de esas mismas cuestiones en lo que respecta a la gestión de la identidad.

57. No obstante, el tratamiento jurídico de los servicios de confianza también puede plantear dificultades particulares. Una cuestión fundamental es el hecho de que cada servicio de confianza es diferente y, por lo tanto, plantea un conjunto diferente de cuestiones que examinar. Además, se plantea la cuestión de si el tratamiento jurídico de los servicios de confianza debería consistir en establecer una lista abierta de servicios de confianza basada una definición común de "servicio de confianza" o más bien en proporcionar normas comunes aplicables a todos los servicios de confianza y normas específicas aplicables a cada uno de ellos.

58. Además, tal vez sea posible referirse a disposiciones sobre equivalencia funcional para describir las funciones que se desea cumplir con la utilización de cada servicio de confianza de una manera similar a las disposiciones de la CNUDMI sobre las firmas electrónicas y la conservación de documentos (véase A/CN.9/WG.IV/WP.153, párr. 36). La existencia de un importante acervo legislativo sobre las firmas electrónicas[6] y la experiencia adquirida en la aplicación de esa legislación pueden ser útiles al estudiar esta sugerencia.

59. El reglamento eIDAS constituye un ejemplo de norma amplia sobre los servicios de confianza. Contiene disposiciones generales sobre la responsabilidad y la carga de la prueba (art. 13; véanse los párrs. 23 a 26 *supra*), la supervisión (art. 17; véase el párr. 53 *supra*) y los requisitos de seguridad (art.19; véase el párrafo 44 *supra*, en lo que respecta al deber de notificar las fallas de seguridad o la pérdida de datos), entre otros.

60. El reglamento eIDAS contiene una sección específica aplicable a todos los servicios de confianza cualificados. Los servicios de confianza cualificados son reconocibles porque se incluyen en una lista de confianza que mantienen los Estados miembros de la Unión Europea. Al respecto, el Grupo de Trabajo tal vez desee examinar si debería hacerse una distinción entre servicios de confianza en función del nivel de seguridad relacionado con cada servicio de confianza y, en caso de establecer esa distinción, determinar el mecanismo institucional que debería utilizarse para distinguir entre los servicios de confianza.

61. El reglamento eIDAS también contiene disposiciones específicas relativas a los siguientes servicios de confianza: las firmas electrónicas; los sellos electrónicos; los sellos de tiempo electrónicos; los servicios de entrega electrónica certificada y la autenticación de sitios web[7]. Cada servicio de confianza puede prestarse de forma

[6] El Global Cyberlaw Tracker de la UNCTAD indica que 145 Estados, o sea el 78% del total, han aprobado leyes sobre operaciones electrónicas, que suelen incluir disposiciones sobre firmas electrónicas.

[7] Se puede consultar una definición de esos servicios de confianza en el documento A/CN.9/WG.IV/WP.150.

cualificada. Las firmas electrónicas y los sellos electrónicos también pueden tener formato avanzado.

62. La Ley 045-2009/AN de Burkina Faso contiene un artículo sobre las disposiciones aplicables a todos los proveedores de servicios de confianza, así como disposiciones sobre la forma de lograr la acreditación, lo cual es pertinente para alcanzar la condición de proveedor cualificado de servicios de confianza. Esa ley también contiene disposiciones específicas sobre los certificados electrónicos cualificados, los archivos electrónicos, los sellos de tiempo electrónicos y los servicios de entrega electrónica certificada. También incluye un capítulo específico sobre las firmas electrónicas.

63. La Ley 2017-20 de Benin contiene una parte general aplicable a todos los proveedores de servicios de confianza y disposiciones específicas sobre los siguientes servicios de confianza: las firmas electrónicas; los sellos electrónicos; los sellos de tiempo electrónicos y los archivos electrónicos.

64. El artículo 301 de dicha ley dispone que los archivos electrónicos garantizan la autenticidad e integridad de los documentos, los datos y la información que se almacenan de ese modo. Además, contiene una disposición sobre la equivalencia funcional similar a la del artículo 10 de la LMCE.

65. El artículo 302 de la Ley 2017-20 de Benin indica además que el propósito de los archivos electrónicos es conservar los documentos, los datos y la información para su uso ulterior, y que los datos pertinentes deberían estructurarse, indizarse y almacenarse de manera de posibilitar su conservación y migración (véase también el párr. 51 *supra*). Debería ser posible el acceso independientemente de la evolución tecnológica. La disposición se aplica tanto a los documentos originados electrónicamente como a los originados en papel y digitalizados posteriormente.

66. La Ley 2017-07 del Togo contiene también un artículo sobre las disposiciones aplicables a todos los proveedores de servicios de confianza, y sobre los procedimientos para alcanzar la condición de proveedor cualificado de servicios de confianza. Esa ley también contiene disposiciones específicas sobre los certificados electrónicos, los archivos electrónicos, los sellos de tiempo electrónicos y los servicios de entrega electrónica certificada. También incluye un capítulo específico sobre las firmas electrónicas.

67. La Ley 2017-07 del Togo se complementa con el Decreto 2018-062/PR, que establece las obligaciones comunes a todos los proveedores de servicios de confianza. Esas obligaciones tienen que ver con la seguridad y confidencialidad de los datos, la responsabilidad, los recursos financieros, la accesibilidad, la protección de los datos, la transparencia y la gestión de riesgos. Además, el decreto contiene disposiciones relativas a cada uno de los servicios de confianza señalados en la Ley 2017-07.

68. Otros servicios de confianza que se han identificado, pero aún no han recibido un tratamiento legislativo específico, son las cuentas de seguridad bloqueada electrónicas y los sistemas electrónicos de demostración de la presencia. Este último servicio de confianza se ha examinado en relación con los testamentos electrónicos[8].

69. El Grupo de Trabajo tal vez desee considerar si debería utilizarse el mismo mecanismo para el tratamiento jurídico de la gestión de la identidad y los servicios de confianza o si debería haber mecanismos distintos. Además, podría examinar si el tratamiento jurídico de los servicios de confianza debería consistir en establecer una lista abierta de servicios de confianza sobre la base de una definición común de “servicio de confianza” o más bien en proporcionar normas comunes aplicables a todos los servicios de confianza y normas específicas aplicables a cada uno de esos servicios. En particular, el Grupo de Trabajo tal vez desee examinar si se deben formular normas de equivalencia funcional para cada servicio de confianza y si también debería hacerse referencia a los niveles de seguridad en el contexto de los servicios de confianza.

[8] Véase, por ejemplo, el artículo 8 del proyecto de ley de testamentos electrónicos que está preparando la National Conference of Commissioners on Uniform State Laws.