Naciones Unidas A/CN.9/WG.IV/WP.155

Asamblea General

Distr. limitada
13 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

Proyecto de instrumento sobre el reconocimiento jurídico transfronterizo de la gestión de la identidad y los servicios de confianza — Propuesta de Alemania

Nota de la Secretaría

Alemania presentó un documento a la Secretaría para que se examinara en el 57º período de sesiones del Grupo de Trabajo. El texto que figura en el anexo de la presente nota es traducción al español del documento recibido en inglés por la Secretaría.

V.18-06087 (S) 021118 021118

Anexo

Proyecto de instrumento sobre el reconocimiento jurídico transfronterizo de la gestión de la identidad y los servicios de confianza

Reafirmando su convicción de que el desarrollo de la tecnología de la información y las comunicaciones es una condición *sine qua non* del crecimiento económico sostenible y la mejora de la calidad de vida en general;

Observando que las comunicaciones electrónicas aumentan la eficiencia de la gestión pública y de las actividades comerciales, fortalecen las relaciones económicas exteriores y permiten que partes y mercados anteriormente considerados remotos accedan a nuevas oportunidades, desempeñando así un papel fundamental en el desarrollo económico, tanto a nivel nacional como internacional;

Dado que la incertidumbre acerca de la regulación tecnológica y el régimen jurídico de la circulación de documentos electrónicos en la interacción entre los órganos estatales y municipales, las personas físicas y las organizaciones de los Estados Partes en el [proyecto de instrumento][1] constituye un obstáculo para el desarrollo de la interacción electrónica;

Convencidos de que el logro de la confianza entre todos los participantes en la interacción electrónica es una condición necesaria del desarrollo de dicha interacción;

Considerando que las normas uniformes deben basarse en el respeto del derecho de las partes a escoger medios, tecnologías y servicios de identificación y de confianza apropiados, teniendo en cuenta los principios de neutralidad tecnológica y equivalencia funcional, siempre y cuando los métodos elegidos por las partes estén en consonancia con los objetivos de las normas jurídicas vigentes;

Reconociendo que es oportuno y viable que los sistemas de confianza centralizados y descentralizados y su utilización aceleren el progreso y la economía digital, en particular basando en la confianza las actividades de comercio electrónico y transporte, la solución de controversias por medios electrónicos, la creación del gobierno electrónico y servicios públicos electrónicos, la preparación de cursos de capacitación en línea, los servicios electrónicos de atención de la salud, diversos registros electrónicos y los servicios financieros electrónicos;

Han convenido en lo siguiente:

Capítulo I. Ámbito de aplicación

Artículo 1. Ámbito de aplicación

1. En el presente [proyecto de instrumento] se definen las características básicas del entorno de confianza transfronterizo, que es un conjunto de condiciones normativas, institucionales y técnicas necesarias para que exista confianza en el intercambio transfronterizo de información entre organismos públicos, personas físicas y empresas en forma electrónica.

2. A los efectos de determinar el ámbito de aplicación de este [proyecto de instrumento] no se tendrán en cuenta el Estado de pertenencia, el estado civil ni la situación jurídica de los participantes en la interacción electrónica transfronteriza, ni tampoco la índole de los documentos o mensajes electrónicos que intercambien.

3. El entorno de confianza transfronterizo se compone de los siguientes segmentos:

[1] El [proyecto de instrumento] es un espacio reservado para el nombre del texto, cuya forma definitiva será decidida por la CNUDMI.

1) el segmento centralizado, que abarca las condiciones normativas, institucionales y técnicas necesarias para que exista confianza en el intercambio de documentos electrónicos, lo que supone establecer requisitos obligatorios en relación con el control que ejercen las Partes de las actividades de los operadores de servicios de confianza, los programas y equipos informáticos utilizados por esos operadores en la interacción electrónica transfronteriza, los servicios de confianza, los procedimientos de verificación de la conformidad de los operadores de servicios de confianza con los requisitos establecidos, y los programas y equipos informáticos;

2) el segmento autorregulado, que abarca las condiciones normativas, institucionales y técnicas necesarias para que exista confianza en el intercambio de mensajes electrónicos por conducto de bases de datos descentralizadas y la creación de unidades de datos que indican el carácter autorregulador de la interacción electrónica transfronteriza.

4. El entorno de confianza transfronterizo es utilizado por los participantes para garantizar el nivel de confianza necesario entre las partes de la interacción electrónica. La elección de un determinado segmento del entorno de confianza transfronterizo, o una combinación de sus segmentos, de conformidad con el artículo 1, párrafo 3, del presente [proyecto de instrumento], depende de la índole de cada uno de los servicios digitales que exigen que el entorno de confianza transfronterizo les proporcione confianza.

Capítulo II. Disposiciones generales

Artículo 2. Definiciones

1. A los efectos del presente [proyecto de instrumento]:

1) Se entenderá que la expresión “participantes en el entorno de confianza transfronterizo” comprende a organismos públicos, el Consejo de Coordinación, operadores de servicios de confianza, operadores de bases de datos descentralizadas, personas físicas y organizaciones;

2) Por “mensaje electrónico” se entenderá la información generada, enviada, recibida o archivada utilizando redes de información y telecomunicaciones;

3) Por “documento electrónico” se entenderá todo mensaje electrónico que reúna los requisitos necesarios y suficientes para que se reconozcan sus efectos jurídicos y cuya veracidad y autenticidad sean confirmadas por un operador de servicios de confianza con arreglo a lo dispuesto en el presente [proyecto de instrumento];

4) Por “registros de operaciones” se entenderán los mensajes electrónicos autenticados por operadores de bases de datos descentralizadas e incorporados por esos operadores a un bloque de datos (válidos) significativo;

5) Por “bloque de datos (válidos) significativo” se entenderá un conjunto de registros de operaciones generados de conformidad con las normas establecidas por el operador de la base de datos descentralizada, que no admiten alteración ni adición alguna;

6) Por “servicios de confianza” se entenderán los servicios que confirman la veracidad y autenticidad de los documentos electrónicos y/o sus detalles, entre ellos, por ejemplo, los servicios relacionados con la creación y el uso de firmas electrónicas, sellos electrónicos y sellos de tiempo electrónicos, la entrega electrónica y la autenticación de sitios web;

7) Por “interacción electrónica transfronteriza” se entenderá un intercambio de mensajes electrónicos y/o documentos electrónicos a través de los sistemas de información entre los participantes del entorno de confianza transfronterizo;

8) El “Consejo Coordinador” es el órgano creado de conformidad con el presente [proyecto de instrumento] que establece los requisitos generales, obligatorios para los Miembros, aplicables a las actividades de los operadores de servicios de confianza, a los equipos y programas informáticos utilizados por los operadores de

servicios de confianza para llevar a cabo la interacción electrónica transfronteriza, y a los procedimientos de verificación de la conformidad de los operadores de servicios de confianza y los equipos y programas informáticos con los requisitos; y que desempeña otras funciones establecidas en el presente [proyecto de instrumento];

9) Por "ubicación" se entenderá el lugar indicado como su domicilio por una parte en el entorno de confianza transfronterizo, o, en su defecto, el lugar de residencia de una persona física o el lugar de constitución de una persona jurídica;

10) Por "operador de servicios de confianza" se entenderá una persona física o jurídica que cumpla los requisitos establecidos por el Consejo de Coordinación, que haya obtenido una confirmación del cumplimiento mediante un procedimiento establecido por el Consejo de Coordinación y que preste servicios de confianza en el segmento centralizado del entorno de confianza transfronterizo;

11) Por "operadores de bases de datos descentralizadas ("mineros")" se entenderán las personas físicas o jurídicas (incluidas las que actúan de manera anónima) que utilicen los programas y equipos informáticos necesarios para participar en el segmento autorregulado del entorno de confianza transfronterizo registrando las operaciones y comprobando su autenticidad, formando bloques de datos en bases de datos descentralizadas y verificando su integridad;

12) Por "usuario" se entenderá un organismo público, una persona física o una organización que envíe o reciba mensajes electrónicos y/o documentos electrónicos, incluidos los enviados a través de los servicios prestados en el segmento autorregulado del entorno de confianza transfronterizo;

13) Por "sistemas de información" se entenderá la suma de las tecnologías y equipos informáticos diseñados y utilizados para crear, enviar, recibir, almacenar o procesar de alguna otra manera mensajes electrónicos, entre ellos documentos electrónicos, en la interacción electrónica transfronteriza;

14) Por "firma o sello electrónico" se entenderán los datos electrónicos, adjuntados o lógicamente asociados a otros datos electrónicos, que sean utilizados por el firmante para firmar y que documenten una determinada relación entre el firmante y esos otros datos electrónicos de modo tal que un tercero pueda verificar la existencia de esa relación posteriormente;

15) Por "firmante" se entenderá la persona física (si se trata de una firma electrónica) o jurídica (si se trata de un sello electrónico) que firma un documento electrónico con su firma o sello electrónico;

16) Por "certificado cualificado de firma o sello electrónico" se entenderá una confirmación electrónica que vincule determinados datos a una persona física (si se trata de una firma electrónica) o a una persona jurídica (si se trata de un sello electrónico) para verificar la firma o sello electrónico y que confirme al menos su identidad; que sea emitido por el operador de servicios de confianza cuya conformidad con los requisitos haya sido comprobada con arreglo al procedimiento previsto en el artículo 8, párrafo 6, del presente [proyecto de instrumento] y que reúna los requisitos establecidos por el Consejo de Coordinación;

17) Por "sello de tiempo electrónico" se entenderán los datos electrónicos que vinculen otros datos electrónicos a una fecha y hora determinadas y que registre la existencia de esos datos electrónicos en ese momento, de modo tal que los participantes en la interacción electrónica o un tercero puedan verificar ese hecho posteriormente;

18) Por "servicio de entrega electrónica certificada" se entenderá un servicio que permita transmitir datos electrónicos entre terceros y aportar pruebas del procesamiento de los datos transmitidos, incluida la prueba del envío y la recepción de los datos, y que proteja los datos transmitidos, evitando su pérdida, hurto, alteración o modificación no autorizada;

19) Por "certificado cualificado de autenticación de sitios web" se entenderá una confirmación electrónica que permita autenticar un sitio web mediante la vinculación

de ese sitio web a la persona física o jurídica a la que se haya emitido esa confirmación por un operador de servicios de confianza cuya conformidad con los requisitos haya sido comprobada con arreglo al procedimiento previsto en el artículo 8, párrafo 6, del presente [proyecto de instrumento] y que reúna los requisitos establecidos por el Consejo de Coordinación;

20) Por "identidad" se entenderá la información relativa a un sujeto determinado (el usuario) expresada en forma de uno o más atributos que permitan distinguir suficientemente a ese sujeto en un contexto en particular;

21) Por "medio de identificación" se entenderá un elemento material o inmaterial que contiene la identidad de un sujeto determinado (el usuario);

22) Por "gestión de la identidad" se entenderá un conjunto de funciones y competencias (por ejemplo, administración, gestión y mantenimiento, presentación de pruebas, intercambio de comunicaciones, correlación y vinculación, cumplimiento de políticas, autenticación y aseveración) utilizadas para: i) garantizar la información de identidad (por ejemplo, identificadores, credenciales, atributos); ii) garantizar la identidad de una entidad; y iii) habilitar aplicaciones de negocios y de seguridad;

23) Por "identificación primaria (fundamental)" se entenderá el proceso de reunión, verificación y validación de información sobre atributos de identidad suficientes acerca de un sujeto determinado (el usuario) para definir y confirmar su identidad con independencia del contexto.

Por lo general, la identificación primaria es realizada por el organismo que expide el certificado de identidad primaria correspondiente (por ejemplo, partida de nacimiento, documento nacional de identidad, pasaporte, etc.).

24) Por "identificación secundaria (vinculada a una operación)" se entenderá el proceso de reunión, verificación y validación de información sobre atributos de identidad suficientes acerca de un sujeto determinado (el usuario) para definir y confirmar su identidad en un contexto determinado.

La identificación secundaria es realizada por un operador de servicios de confianza y puede consistir en: a) la identificación del solicitante en el momento en que se registra como usuario del (o los) servicio(s) de confianza ofrecido(s) por ese operador, o b) la identificación del usuario para utilizar un servicio de confianza en particular.

a) A los efectos de la identificación del solicitante en el momento en que se registra, el operador del servicio de confianza utiliza normalmente un certificado de identidad primaria o el resultado de una identificación anterior del solicitante. Una vez identificado el solicitante, el operador del servicio de confianza crea o emite su propio registro de la identidad secundaria del usuario (certificado de identidad secundaria);

b) A los efectos de la identificación del usuario para utilizar un determinado servicio de confianza, el operador del servicio exige al usuario, que ya tiene su identidad de usuario conforme al apartado a) de esta definición, que se identifique utilizando su certificado de identidad secundaria (ya sea por conocimiento o por posesión (incluidos los datos biométricos)).

25) Por "sistema de identificación" se entenderá un entorno (en línea) utilizado para operaciones de identificación y regido por un conjunto de normas del sistema, en el que puede existir confianza recíproca entre personas físicas o jurídicas porque fuentes autorizadas han establecido y autenticado sus identidades respectivas. Un sistema de identificación comprende: a) un conjunto de reglas, métodos, procedimientos y rutinas, tecnologías, normas, políticas y procesos, b) aplicable a un grupo de entidades participantes, c) que rige la reunión, verificación, almacenamiento, intercambio y autenticación de información sobre los atributos de identidad de una persona física o jurídica, así como la fiabilidad de esa información; d) con el fin de facilitar operaciones de identificación;

26) Por “operación de identificación” se entenderá toda operación en la que intervengan dos o más participantes y que implique establecer, verificar, emitir, aseverar, revocar o comunicar información de identidad o fiarse de ella;

27) Por “proveedor de identificación” se entenderá: a) una entidad encargada de identificar a las personas físicas o jurídicas, emitir los medios de identificación correspondientes y conservar y administrar esa información de identidad;

28) Por “sistema de identificación autorizado” se entenderá un sistema de identificación que: a) cumpla los requisitos establecidos por el Consejo de Coordinación, y b) haya sido notificado al Consejo de Coordinación por el proveedor de identificación que gestione ese sistema de identificación en la forma dispuesta en el artículo 5, párrafo 2, del presente [proyecto de instrumento];

29) Por “nivel de garantía de un sistema de identificación autorizado” se entenderá un atributo (una característica) de un sistema de identificación autorizado determinado por el proveedor de identificación que gestione ese sistema de identificación de conformidad con los requisitos establecidos por el Consejo de Coordinación en el artículo 5, párrafo 2, del presente [proyecto de instrumento];

30) Por “Miembro” (del Consejo de Coordinación) se entenderá una persona jurídica: i) que posea las facultades jurídicas y la potestad de otorgar el reconocimiento jurídico de la gestión de la identidad y los servicios de confianza en el contexto de la legislación nacional en la materia, y ii) que haya reconocido oficialmente todas las disposiciones del presente [proyecto de instrumento].

Artículo 3. Interpretación

1. En la interpretación del presente [proyecto de instrumento] se tendrán en cuenta su carácter internacional y la necesidad de promover la uniformidad en su aplicación, la observancia de la buena fe en la interacción electrónica transfronteriza y el cumplimiento de los principios establecidos en el artículo 5 de este [proyecto de instrumento].

2. Las cuestiones relativas a las materias que se rigen por el presente [proyecto de instrumento] que no estén expresamente resueltas en él se dirimirán de conformidad con los principios generales en que se basa este instrumento o, en su defecto, con arreglo a la ley aplicable en virtud de las normas del derecho internacional privado.

Artículo 4. Principios

La interacción electrónica transfronteriza en el entorno de confianza transfronterizo se basa en los principios siguientes, que se aplican a ambos segmentos de dicho entorno:

1) Neutralidad tecnológica;

2) Equivalencia funcional con respecto a la gestión de la identidad y los servicios de confianza prestados;

3) Protección de la información reservada, es decir, la información protegida por el derecho internacional y la legislación nacional de los Estados Partes, incluidos los secretos comerciales y los datos personales, en la interacción electrónica transfronteriza;

4) El uso de cualquier tipo de información, documentos y mensajes, incluidos los bloques de datos existentes en bases de datos descentralizadas, solo se permite para fines que no sean contrarios al derecho internacional o a la legislación nacional de los Estados Partes;

5) Neutralidad económica, que contribuye a la eficiencia en función de los costos y evita las distorsiones en el ámbito de la gestión de la identidad y los servicios de confianza prestados;

6) Proporcionalidad, que significa que el contenido y la forma de las acciones deben estar en consonancia con el objetivo que se persigue;

7) Autonomía de las partes, que es el derecho de los participantes a elegir libremente los soportes, las tecnologías y los servicios de identificación y de confianza que consideren apropiados para sus necesidades empresariales concretas;

8) No discriminación.

Capítulo III. El Consejo de Coordinación

Artículo 5. Funciones del Consejo de Coordinación

1. El Consejo de Coordinación es el órgano que cumple las funciones de organismo rector en el segmento centralizado del entorno de confianza transfronterizo y de facilitador en el segmento autorregulado de dicho entorno.

2. En el segmento centralizado del entorno de confianza transfronterizo, el Consejo de Coordinación aprobará como mínimo el siguiente conjunto de requisitos, procedimientos, políticas y condiciones cuyo cumplimiento evidente por los participantes permitirá el reconocimiento recíproco de los resultados de la identificación y los medios de identificación, así como de los resultados de la utilización de servicios de confianza:

A. Gestión de la identidad

1) Requisitos relativos a las propiedades y características de los sistemas de identificación utilizados para realizar la identificación primaria que podrán ser autorizados.

Conforme a estos requisitos, los sistemas de identificación deberán establecerse y funcionar en el contexto nacional de los Estados Partes y respetar la legislación nacional pertinente, incluidas las disposiciones nacionales aplicables a la certificación de los sistemas de identificación.

Estos requisitos tendrán en cuenta la posibilidad de los sistemas de identificación autorizados de definir distintos niveles de garantía;

2) Alcance de la responsabilidad por pérdidas de los proveedores de identificación de los sistemas de identificación autorizados;

3) Procedimientos de reconocimiento recíproco de los resultados de operaciones de identificación obtenidos y de los medios de identificación expedidos por los proveedores de identificación de los sistemas de identificación autorizados;

4) Determinación, a los fines del presente [proyecto de instrumento], de los efectos jurídicos derivados de la utilización de sistemas de identificación autorizados, entre ellos el reconocimiento recíproco de los resultados de operaciones de identificación obtenidos y de los medios de identificación expedidos por los proveedores de identificación de los sistemas de identificación autorizados; para ello se tendrán en cuenta los diferentes niveles de garantía ofrecidos por los sistemas de identificación autorizados;

5) Condiciones básicas exigidas para la utilización de sistemas de identificación autorizados;

6) Requisitos relativos a las propiedades y características que deben tener los sistemas de identificación utilizados para que los operadores de servicios de confianza puedan realizar la identificación secundaria de los usuarios;

7) Normas aplicables a la solución de controversias.

B. Servicios de confianza

1) Requisitos aplicables a los procedimientos operacionales de los operadores de servicios de confianza, en particular el seguro de responsabilidad civil y la auditoría de los operadores de servicios de confianza;

2) Requisitos relativos a los programas y equipos informáticos utilizados en la interacción electrónica transfronteriza;

3) Procedimientos de verificación de la conformidad de los operadores de servicios de confianza con los requisitos establecidos, incluida la verificación de la conformidad de los sistemas de identificación utilizados para la identificación secundaria de los usuarios y de la conformidad de los equipos y programas informáticos (auditoría);

4) Alcance de la responsabilidad por pérdidas de los operadores de servicios de confianza;

5) Normas aplicables a la solución de controversias;

6) Requisitos exigidos a las personas físicas y (o) jurídicas que se dedican a confirmar el cumplimiento de los operadores de servicios de confianza, así como a verificar la conformidad de los sistemas de identificación utilizados para realizar la identificación secundaria de los usuarios y la conformidad de los equipos y programas informáticos (auditoría);

7) Condiciones básicas exigidas para la utilización de los servicios de confianza definidos en los artículos 15, 16, 17, 18, 19 y 20 de este [proyecto de instrumento].

C. Otros documentos previstos en el presente [proyecto de instrumento]

3. En virtud del presente [proyecto de instrumento], los Miembros convienen en hacer cumplir o respetar los requisitos aprobados por el Consejo de Coordinación de conformidad con el párrafo 2 del presente artículo por los organismos públicos y los gobiernos autónomos locales, los usuarios, los operadores y los servicios de confianza comprendidos en su jurisdicción.

4. En el segmento autorregulado del entorno de confianza transfronterizo, el Consejo de Coordinación:

1) Aprobará un procedimiento recomendado para confirmar la incorporación de los operadores de bases de datos descentralizadas a las bases de datos correspondientes;

2) Aprobará el procedimiento de notificación al Consejo de Coordinación de los incidentes relacionados con la información contenida en bases de datos descentralizadas, es decir, los casos en que se utilicen mensajes electrónicos, registros de operaciones o bloques de datos contenidos en bases de datos descentralizadas en contravención de las normas del derecho internacional o la legislación nacional de los Miembros;

3) Organizará el procedimiento de notificación mediante el cual los operadores de bases de datos descentralizadas comunicarán al Consejo de Coordinación que asumen voluntariamente el compromiso contraído por este último de hacer cumplir los requisitos previstos en el presente [proyecto de instrumento] para garantizar que el uso de cualquier tipo de información, documentos o mensajes, incluidos los bloques de datos contenidos en bases de datos descentralizadas, se haga únicamente con fines que no sean contrarios al derecho internacional o a la legislación nacional de los Miembros; y para informar al Consejo de Coordinación de los incidentes relacionados con la información contenida en bases de datos descentralizadas.

5. Las decisiones y los documentos aprobados por el Consejo de Coordinación con respecto al segmento autorregulado del entorno de confianza transfronterizo son de carácter consultivo.

Artículo 6. Creación y procedimientos del Consejo de Coordinación

1. El Consejo de Coordinación estará compuesto por sus Miembros, que serán elegidos por un período de cuatro años. Cada Miembro podrá designar a un representante autorizado.

2. El Consejo de Coordinación podrá crear los órganos subsidiarios que estime necesarios para el desempeño de sus funciones.

3. Cada miembro del Consejo de Coordinación tendrá un voto.

4. Las decisiones del Consejo de Coordinación sobre la reglamentación de sus actividades se adoptarán por el voto favorable de no menos de dos tercios de sus miembros.

5. Las decisiones del Consejo de Coordinación por las que se aprueben los actos a que se refiere el artículo 5, párrafo 2, deberán adoptarse por unanimidad.

6. El Consejo de Coordinación aprobará su reglamento interno, incluido el procedimiento de elección de su presidente, el procedimiento para mantener la confianza mutua entre los representantes competentes de los Miembros en el entorno de confianza transfronterizo y el procedimiento de adopción de decisiones relativo a la aprobación de los documentos especificados en el artículo 5 del presente [proyecto de instrumento].

Capítulo IV. Participantes en el entorno de confianza transfronterizo

Artículo 7. Organismos públicos y gobiernos autónomos locales de los Estados Partes

1. Los organismos públicos participarán en la interacción electrónica transfronteriza para el ejercicio de las funciones públicas que les impone la legislación nacional de los Estados Partes de conformidad con las normas establecidas en el presente [proyecto de instrumento] y los actos aprobados por el Consejo de Coordinación con arreglo a lo dispuesto en este [proyecto de instrumento].

2. Los organismos públicos tendrán derecho a tomar sus propias decisiones con respecto a su participación en el segmento autorregulado del entorno de confianza transfronterizo.

3. En los casos que determine el Consejo de Coordinación, los organismos públicos tendrán derecho a exigir, para que se entable una interacción electrónica, otros requisitos además de los establecidos en el presente [proyecto de instrumento] y en los actos aprobados por el Consejo de Coordinación de conformidad con este [proyecto de instrumento], siempre que esos requisitos adicionales no sean incompatibles con los ya establecidos.

Artículo 8. Operadores de servicios de confianza

1. Los operadores de servicios de confianza participarán en el segmento centralizado del entorno de confianza transfronterizo.

2. Los operadores de servicios de confianza podrán prestar esos servicios dentro de las fronteras de un determinado Miembro y/o en todo el territorio de todos los Estados Partes.

3. Los operadores de servicios de confianza estarán obligados a cumplir con los requisitos establecidos por el Consejo de Coordinación, dependiendo de la zona (la totalidad o una parte del territorio de los Estados Partes) en que esos operadores presten sus servicios, y deberán comprobar que cumplen los requisitos en la forma establecida por el Consejo de Coordinación.

4. Los operadores de servicios de confianza tendrán la obligación de publicar en Internet la información relacionada con su adquisición de la calidad de operadores de servicios de confianza o con la modificación de su calidad de tales. Los operadores de servicios de confianza estarán obligados a notificar a las autoridades competentes del Miembro responsable de cualquier cambio que se produzca en la prestación del servicio de confianza o en su calidad de operadores de servicios de confianza. Los operadores

de servicios de confianza tendrán la obligación de comunicar a las autoridades competentes de los Miembros y al Consejo de Coordinación cualquier información que se refiera a incidentes ocurridos en la interacción electrónica transfronteriza. El Consejo de Coordinación establecerá el procedimiento y las condiciones aplicables a la comunicación de información relacionada con incidentes ocurridos en la interacción electrónica transfronteriza.

5. Los operadores de servicios de confianza estarán obligados a contratar un seguro de responsabilidad civil o a tener un respaldo económico suficiente de conformidad con los requisitos establecidos por el Consejo de Coordinación.

6. Los operadores de servicios de confianza deberán someterse a un procedimiento de evaluación (auditoría independiente) destinado a comprobar si ellos mismos, los servicios de confianza que prestan, incluidos los sistemas de identificación utilizados para determinar la identidad secundaria de los usuarios, y los programas y equipos informáticos, cumplen los requisitos exigidos por el Consejo de Coordinación en la forma establecida por este.

Artículo 9. Auditoría de cumplimiento independiente. Seguro

1. Solo los operadores de servicios de confianza cuya conformidad con los requisitos haya sido comprobada mediante una auditoría de cumplimiento independiente tendrán derecho a prestar servicios de confianza.

2. Los organismos o instituciones autorizados con arreglo al procedimiento establecido por el Consejo de Coordinación podrán llevar a cabo auditorías de cumplimiento.

3. Los operadores de servicios de confianza deberán contratar un seguro de responsabilidad civil de conformidad con los requisitos establecidos por el Consejo de Coordinación.

Artículo 10. Operadores de bases de datos descentralizadas

1. Los operadores de bases de datos descentralizadas participarán en el segmento autorregulado del entorno de confianza transfronterizo.

2. Los operadores de bases de datos descentralizadas organizarán la interacción electrónica transfronteriza entre sí y con los usuarios sobre la base de los principios de la autorregulación, y velarán por el cumplimiento del presente [proyecto de instrumento] en lo que respecta a la utilización de cualquier tipo de información, documento o mensaje, incluidos los bloques de datos existentes en las bases de datos descentralizadas, únicamente con fines que no sean incompatibles con el derecho internacional y la legislación nacional de los Estados Partes, y en lo que respecta a la comunicación al Consejo de Coordinación de los incidentes de información ocurridos en las bases de datos descentralizadas.

3. La presentación voluntaria al Consejo de Coordinación de la notificación del cumplimiento voluntario de estos requisitos por parte del operador de una base de datos descentralizada tendrá por efecto que se reconozca que dicho operador cumple los requisitos establecidos en el presente [proyecto de instrumento] en lo que respecta al uso de cualquier tipo de información, documento o mensaje, incluidos los bloques de datos existentes en las bases de datos descentralizadas, únicamente con fines que no sean incompatibles con el derecho internacional y la legislación nacional de los Miembros y en lo que respecta a la comunicación al Consejo de Coordinación de los incidentes de información ocurridos en las bases de datos descentralizadas. El Consejo de Coordinación establecerá el procedimiento de presentación de esas notificaciones y la forma en que deberá llevarse una lista de los operadores de bases de datos descentralizadas de los Miembros en el entorno de confianza transfronterizo.

El Consejo de Coordinación tendrá derecho a rechazar la notificación de un operador de bases de datos descentralizadas que figure en la lista si dispone de información que indique que ese operador ha infringido el derecho internacional o la legislación nacional de los Estados Partes.

4. La interacción entre los operadores de bases de datos descentralizadas y el Consejo de Coordinación, así como la interacción entre esos operadores y los usuarios, podrá llevarse a cabo sin necesidad de identificar a las personas físicas o jurídicas que gestionan y utilizan las bases de datos descentralizadas.

5. Si el Consejo de Coordinación recibe información de que un operador de bases de datos descentralizadas ha actuado en contravención de lo dispuesto en el párrafo 2 del presente artículo del [proyecto de instrumento], dicho operador de bases de datos descentralizadas podrá ser excluido de la lista publicada de proveedores de bases de datos descentralizadas que sean partes en el entorno de confianza transfronterizo.

Artículo 11. Usuarios

1. Los usuarios participarán en los dos segmentos del entorno de confianza transfronterizo.

2. En función del segmento del entorno de confianza transfronterizo en que participen, los usuarios intercambiarán mensajes electrónicos o documentos electrónicos de conformidad con las normas establecidas por el Consejo de Coordinación y los operadores de servicios de confianza, o con arreglo a las normas establecidas por los operadores de bases de datos descentralizadas, respectivamente.

Capítulo V. El entorno transfronterizo de la infraestructura de confianza

Artículo 12. Programas y equipos informáticos de los operadores de servicios de confianza

1. Los operadores de servicios de confianza solo utilizarán programas y equipos informáticos que hayan demostrado satisfactoriamente, con arreglo a los procedimientos de evaluación previstos en el artículo 8, párrafo 6, y el artículo 9, párrafo 1, que cumplen los requisitos exigidos para la prestación de sus servicios.

2. El Consejo de Coordinación, de conformidad con lo dispuesto en el artículo 8, párrafo 6, y en el artículo 9, párrafos 1 y 2, establecerá los requisitos de funcionamiento aplicables a los programas y equipos informáticos de los operadores de servicios de confianza, así como los requisitos relativos al procedimiento de verificación de la conformidad de los programas y equipos informáticos con los requisitos de funcionamiento establecidos en consonancia con el principio de neutralidad tecnológica.

Artículo 13. Programas y equipos informáticos de los operadores de bases de datos descentralizadas

Los operadores de bases de datos descentralizadas determinarán de manera independiente los requisitos que deberán reunir los programas y equipos informáticos para la verificación de la autenticidad e integridad de los registros de operaciones, así como para la creación, el almacenamiento y la verificación de la integridad de los bloques de datos.

Artículo 14. Programas y equipos informáticos de los usuarios

Los usuarios deberán adoptar sus propias medidas para asegurarse de que los programas y equipos informáticos que utilicen en la interacción electrónica transfronteriza cumplan los requisitos exigidos por los operadores de servicios de confianza.

Capítulo VI. Prestación de servicios de confianza en el segmento centralizado del entorno de confianza transfronterizo

Artículo 15. Firma electrónica

1. No se negarán efectos jurídicos, ni admisibilidad como medio de prueba en un proceso judicial, a una firma electrónica por la sola razón de que esté en forma electrónica o porque no reúna los requisitos necesarios para que se le considere una firma electrónica cualificada.

2. Una firma electrónica avanzada deberá cumplir los siguientes requisitos:

a) estar vinculada de manera exclusiva al firmante;

b) permitir la identificación del firmante;

c) haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar bajo su control exclusivo;

d) estar vinculada a los datos firmados por ella de modo tal que cualquier modificación ulterior de esos datos sea detectable.

3. Una firma electrónica cualificada es una firma electrónica avanzada basada en un certificado cualificado de la firma electrónica y creada con programas y equipos informáticos que hayan sido certificados de conformidad con el artículo 8, párrafo 6. Una firma electrónica cualificada surtirá efectos jurídicos equivalentes a los de una firma manuscrita.

Una firma electrónica avanzada que no sea una firma electrónica cualificada surtirá efectos jurídicos equivalentes a los de una firma manuscrita en los casos en que las partes determinen, de común acuerdo, que podrá utilizarse ese tipo de firma, o cuando así lo dispongan las normas legales o reglamentarias de los Estados Partes.

4. Toda firma electrónica cualificada que se base en un certificado cualificado expedido dentro de la jurisdicción de un Miembro será reconocida como firma electrónica cualificada por todos los demás Miembros.

Artículo 16. Sello electrónico

1. No se negarán efectos jurídicos, ni admisibilidad como medio de prueba en un proceso judicial, a un sello electrónico por la sola razón de que esté en forma electrónica o porque no reúna los requisitos necesarios para que se le considere un sello electrónico cualificado.

2. Un sello electrónico avanzado deberá cumplir los siguientes requisitos:

a) estar vinculado de manera exclusiva al creador del sello;

b) permitir la identificación del creador del sello;

c) haber sido creado utilizando los datos de creación del sello electrónico que el creador del sello puede utilizar bajo su control exclusivo;

d) estar vinculado a los datos a que se refiere de modo tal que cualquier modificación ulterior de esos datos sea detectable.

3. Un sello electrónico cualificado es un sello electrónico avanzado basado en un certificado cualificado del sello electrónico y creado utilizando programas y equipos informáticos que hayan sido certificados de conformidad con el artículo 8, párrafo 6. Un sello electrónico cualificado gozará de la presunción de integridad de los datos y de exactitud del origen de los datos a los que esté vinculado ese sello electrónico cualificado.

Un sello electrónico avanzado que no sea un sello electrónico cualificado gozará de la presunción de integridad de los datos y de exactitud del origen de los datos a los que esté vinculado ese sello electrónico cualificado en los casos en que las partes

determinen, de común acuerdo, que podrá utilizarse ese tipo de sello, o cuando así lo dispongan las normas legales o reglamentarias de los Estados Partes.

4. Todo sello electrónico cualificado que se base en un certificado cualificado expedido dentro de la jurisdicción de un Miembro será reconocido como sello electrónico cualificado por todos los demás Miembros.

Artículo 17. Sello de tiempo electrónico

1. No se negarán efectos jurídicos, ni admisibilidad como medio de prueba en un proceso judicial, a un sello de tiempo electrónico por la sola razón de que esté en forma electrónica o porque no reúna los requisitos necesarios para que se le considere un sello cualificado de tiempo electrónico.

2. Un sello cualificado de tiempo electrónico creará una presunción de exactitud de la fecha y hora especificadas y de la integridad de los datos que dicho sello cualificado de tiempo electrónico certifica.

3. Un sello cualificado de tiempo electrónico deberá cumplir los siguientes requisitos:

a) vincular la fecha y la hora a los datos de manera que se excluya razonablemente la posibilidad de que los datos se modifiquen de una forma que no pueda detectarse;

b) basarse en una fuente de información exacta sobre la hora, vinculada al Tiempo Universal Coordinado;

c) haber sido firmado mediante el uso de una firma electrónica avanzada, o haber sido sellado con un sello electrónico avanzado de un operador de servicios de confianza cuya conformidad con los requisitos haya sido comprobada con arreglo al procedimiento previsto en el artículo 8, párrafo 6.

4. Todo sello cualificado de tiempo electrónico que haya sido emitido dentro de la jurisdicción de un Miembro será reconocido como sello cualificado de tiempo electrónico por todos los demás Miembros.

Artículo 18. Servicio de entrega electrónica certificada

1. No se negarán efectos jurídicos, ni admisibilidad como medio de prueba en un proceso judicial, a los datos enviados y recibidos a través de un servicio de entrega electrónica certificada por la sola razón de que estén en forma electrónica o no cumplan los requisitos necesarios para que se les considere un servicio cualificado de entrega electrónica certificada.

2. Los datos enviados y recibidos utilizando un servicio cualificado de entrega electrónica certificada crearán una presunción de integridad de los datos, de envío de dichos datos por un remitente identificado, de recepción de dichos datos por un destinatario identificado, de la exactitud de la fecha y hora de envío y recepción indicadas por el servicio cualificado de entrega electrónica certificada.

3. Todo servicio cualificado de entrega electrónica certificada deberá cumplir los siguientes requisitos:

a) Deberá ser prestado por uno o más operadores de servicios de confianza cuya conformidad con los requisitos haya sido comprobada con arreglo al procedimiento previsto en el artículo 8, párrafo 6, del presente [proyecto de instrumento];

b) Deberá garantizar la identidad del remitente con un alto grado de confianza;

c) Deberá garantizar la identidad del destinatario antes de la entrega de los datos;

d) El envío y la recepción de los datos deberán garantizarse mediante una firma electrónica avanzada o un sello electrónico avanzado de un operador cualificado de servicios de confianza de manera tal que se excluya la posibilidad de que los datos se modifiquen de una forma que no pueda detectarse;

e) Cualquier modificación de los datos que sea necesaria para enviar o recibir esos datos deberá indicarse claramente al remitente y al destinatario de dichos datos;

f) La fecha y la hora de envío, recepción y cualquier modificación de los datos deberán indicarse con un sello cualificado de tiempo electrónico.

4. Los resultados de la utilización de un servicio cualificado de entrega electrónica certificada que hayan sido obtenidos dentro de la jurisdicción de un Miembro serán reconocidos por los demás Miembros como el resultado de la utilización de un servicio cualificado de entrega electrónica certificada.

Artículo 19. Autenticación de sitios web

1. Todo certificado cualificado de autenticación de un sitio web deberá contener:

a) una indicación, formulada de un modo que permita al menos su procesamiento automatizado, de que el certificado ha sido emitido como un certificado cualificado de autenticación de sitios web;

b) un conjunto de datos que distingan de manera inequívoca al operador de servicios de confianza que emitió el certificado cualificado;

c) en el caso de personas físicas: por lo menos el nombre, o un seudónimo, de la persona a la cual se emitió el certificado; en el caso de personas jurídicas: por lo menos el nombre de la persona jurídica a la cual se emitió el certificado y, en su caso, el número de inscripción que figure en el registro oficial;

d) datos sobre la dirección, que incluyan al menos la ciudad y el Estado, de la persona física o jurídica a la cual se emitió el certificado y, en su caso, la dirección que figure en el registro oficial;

e) el nombre o nombres de dominio utilizados por la persona física o jurídica a la cual se emitió el certificado;

f) los detalles relativos al comienzo y el final del período de vigencia del certificado;

g) el código de identidad del certificado, que debe ser un código exclusivo del operador de servicios de confianza;

h) la firma electrónica avanzada o el sello electrónico avanzado del operador de servicios de confianza cuya conformidad con los requisitos haya sido comprobada con arreglo al procedimiento previsto en el artículo 8, párrafo 6, del presente [proyecto de instrumento];

i) la ubicación de los servicios de consulta sobre la vigencia del certificado que puedan utilizarse para averiguar si el certificado cualificado está vigente.

2. Los resultados de la utilización de un servicio de confianza que autentique sitios web sobre la base de un certificado cualificado de autenticación de sitios web emitido dentro de la jurisdicción de un Miembro serán reconocidos por todos los demás Miembros como el resultado de la utilización de un servicio de confianza de autenticación de sitios web basado en un certificado cualificado de autenticación de sitios web.

Artículo 20. Otros servicios de confianza

1. El Consejo de Coordinación podrá incluir en su ámbito de regulación otros servicios de confianza además de los especificados en los artículos 15 a 19 del presente [proyecto de instrumento].

2. La reglamentación de esos otros servicios de confianza deberá ser similar a la de los servicios de confianza a que se refieren los artículos 15 a 19 del presente [proyecto de instrumento].

3. A fin de contribuir al uso transfronterizo general de los servicios de confianza, se debería permitir su utilización como medio de prueba en procesos judiciales incoados

en todos los Estados Partes. Corresponderá a la legislación nacional definir los efectos jurídicos de los servicios de confianza, a menos que se disponga otra cosa en el presente [proyecto de instrumento].

Artículo 21. Reconocimiento de los servicios de confianza prestados por terceros países y organizaciones internacionales

1. Los servicios de confianza ofrecidos por operadores autorizados de conformidad con la legislación de terceros países o las normas de organizaciones internacionales podrán ser reconocidos como jurídicamente equivalentes a los servicios de confianza ofrecidos por operadores cuya conformidad con los requisitos haya sido comprobada con arreglo al procedimiento previsto en el artículo 8, párrafo 6, del presente [proyecto de instrumento], si así se estipula en un acuerdo celebrado entre el Consejo de Coordinación y un órgano autorizado de un tercer país o de una organización internacional con arreglo a lo dispuesto en el párrafo 2 del presente artículo.

2. En los acuerdos a que se hace referencia en el párrafo 1 del presente artículo deberá estipularse, entre otras cosas, que:

1) Los requisitos exigidos a los operadores de servicios de confianza de terceros países u organizaciones internacionales no podrán ser inferiores a los requisitos aplicables a los operadores de servicios de confianza que presten esos servicios de conformidad con el presente [proyecto de instrumento];

2) Los terceros países u organizaciones internacionales que sean parte en esos acuerdos deberán reconocer en su territorio (dentro de su jurisdicción) la equivalencia jurídica entre los servicios prestados por los operadores de servicios de confianza cuya conformidad con los requisitos haya sido comprobada con arreglo al procedimiento previsto en el artículo 8, párrafo 6, del presente [proyecto de instrumento] y los servicios prestados por los operadores de servicios de confianza autorizados con arreglo a la legislación del tercer país o la organización internacional que haya firmado el acuerdo.

Capítulo VII. Protección de los derechos e intereses de los participantes en la interacción electrónica transfronteriza

Artículo 22. Protección judicial

1. Los documentos y mensajes electrónicos, incluidos los que sean resultado de la utilización de los servicios de confianza que se describen en los artículos 15 a 20 del presente [proyecto de instrumento], se admitirán como medio de prueba en todos los órganos jurisdiccionales y tribunales arbitrales de los Miembros.

2. Los derechos tutelados por la ley que estén certificados por un documento electrónico tendrán la misma eficacia que los derechos certificados mediante un documento en papel.

Artículo 23. Solución de controversias

1. El Consejo de Coordinación reglamentará el procedimiento administrativo de solución de las controversias derivadas de la interacción electrónica transfronteriza en el segmento centralizado del entorno de confianza transfronterizo.

2. Los participantes en la interacción electrónica transfronteriza tendrán derecho a celebrar acuerdos bilaterales y multilaterales sobre el procedimiento de solución de controversias derivadas de la interacción electrónica transfronteriza.