►B REGLAMENTO (UE) Nº 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 ►C2 y por el que se deroga la Directiva 1999/93/CE ◄

(DO L 257 de 28.8.2014, p. 73)

Modificado por:

		Diario Oficial		
		nº	página	fecha
►M1	Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo de 11 de abril de 2024	L 1183	1	30.4.2024

Rectificado por:

►C1 Rectificación, DO L 296 de 1.11.2016, p. 25 (910/2014)
►C2 Rectificación, DO L 104 de 20.4.2017, p. 28 (910/2014)

▼B

REGLAMENTO (UE) Nº 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 ►C2 y por el que se deroga la Directiva 1999/93/CE ◄

CAPÍTULO I

DISPOSICIONES GENERALES

▼M1

Artículo 1

Objeto

El presente Reglamento tiene por objeto garantizar el correcto funcionamiento del mercado interior y la existencia de un nivel de seguridad adecuado de los medios de identificación electrónica y los servicios de confianza utilizados en toda la Unión, a fin de permitir y facilitar que las personas físicas y jurídicas ejerzan el derecho a participar en la sociedad digital de forma segura y a acceder a los servicios públicos y privados en línea en toda la Unión. A tales efectos, el presente Reglamento:

a) establece las condiciones en las cuales los Estados miembros reconocerán los medios de identificación electrónica de las personas físicas y jurídicas pertenecientes a un sistema de identificación electrónica notificado de otro Estado miembro y en las que proporcionarán y reconocerán las carteras europeas de identidad digital;

b) establece normas para los servicios de confianza, en particular para las transacciones electrónicas;

c) establece un marco jurídico para las firmas electrónicas, los sellos electrónicos, los sellos de tiempo electrónicos, los documentos electrónicos, los servicios de entrega electrónica certificada, los servicios certificados para la autenticación de sitios web, el archivo electrónico, la declaración electrónica de atributos, los dispositivos de creación de firmas electrónicas y de sellos electrónicos, y los libros mayores electrónicos.

▼B

Artículo 2

Ámbito de aplicación

▼M1

1. El presente Reglamento se aplica a los sistemas de identificación electrónica notificados por los Estados miembros, a las carteras europeas de identidad digital proporcionadas por los Estados miembros y a los prestadores de servicios de confianza establecidos en la Unión.

▼B

2. El presente Reglamento no se aplica a la prestación de servicios de confianza utilizados exclusivamente dentro de sistemas cerrados resultantes del Derecho nacional o de acuerdos entre un conjunto definido de participantes.

▼M1

3. El presente Reglamento no afecta al Derecho de la Unión o nacional relacionado con la celebración y validez de los contratos, otras obligaciones jurídicas o de procedimiento de índole formal o requisitos sectoriales de índole formal.

▼M1

4. El presente Reglamento se entiende sin perjuicio del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo ([1]).

▼B

Artículo 3

Definiciones

A efectos del presente Reglamento, se aplicarán las siguientes definiciones:

▼M1

1) «identificación electrónica», proceso consistente en utilizar los datos de identificación de la persona en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a otra persona física o a una persona jurídica;

2) «medios de identificación electrónica», unidad material yo inmaterial que contiene los datos de identificación de la persona y que se utiliza para la autenticación en servicios en línea o, cuando proceda, en servicios fuera de línea;

3) «datos de identificación de la persona», conjunto de datos que se emite de conformidad con el Derecho de la Unión o nacional y permite establecer la identidad de una persona física o jurídica, o de una persona física que representa a otra persona física o a una persona jurídica;

4) «sistema de identificación electrónica», régimen para la identificación electrónica en virtud del cual se expiden medios de identificación electrónica a personas físicas o jurídicas o a personas físicas que representan a otras personas físicas o personas jurídicas;

5) «autenticación», proceso electrónico que permite la confirmación de la identificación electrónica de una persona física o jurídica, o la confirmación del origen y la integridad de datos en formato electrónico;

5 *bis*) «usuario», persona física o jurídica, o persona física que representa a otra persona física o a una persona jurídica, que utiliza servicios de confianza o medios de identificación electrónica prestados de conformidad con el presente Reglamento;

6) «parte usuaria», persona física o jurídica que confía en la identificación electrónica, las carteras europeas de identidad digital u otros medios de identificación electrónica, o en un servicio de confianza;

▼B

7) «organismo del sector público», las autoridades estatales, regionales o locales, los organismos de Derecho público y las asociaciones formadas por una o varias de estas autoridades o uno o varios de estos organismos de Derecho público, o las entidades privadas mandatarias de al menos una de estas autoridades, organismos o asociaciones para prestar servicios públicos actuando en esa calidad;

([1]) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DO L 119 de 4.5.2016, p. 1).

▼B

8) «organismo de Derecho público», el definido en el artículo 2, apartado 1, punto 4, de la Directiva 2014/24/UE del Parlamento Europeo y del Consejo ([1]);

9) «firmante», una persona física que crea una firma electrónica;

10) «firma electrónica», los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar;

11) «firma electrónica avanzada», la firma electrónica que cumple los requisitos contemplados en el artículo 26;

12) «firma electrónica cualificada», una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica;

13) «datos de creación de la firma electrónica», los datos únicos que utiliza el firmante para crear una firma electrónica;

14) «certificado de firma electrónica», una declaración electrónica que vincula los datos de validación de una firma con una persona física y confirma, al menos, el nombre o el seudónimo de esa persona;

15) «certificado cualificado de firma electrónica», un certificado de firma electrónica que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo I;

▼M1

16) «servicio de confianza», servicio electrónico prestado habitualmente a cambio de una remuneración, consistente en cualquiera de las actividades siguientes:

   a) la expedición de certificados de firma electrónica, certificados de sello electrónico, certificados de autenticación de sitios web o certificados para la prestación de otros servicios de confianza;

   b) la validación de certificados de firma electrónica, certificados de sello electrónico, certificados de autenticación de sitios web o certificados para la prestación de otros servicios de confianza;

   c) la creación de firmas electrónicas o sellos electrónicos;

   d) la validación de firmas electrónicas o sellos electrónicos;

   e) la conservación de firmas electrónicas, sellos electrónicos, certificados de firma electrónica o certificados de sello electrónico;

   f) la gestión de dispositivos de creación de firma electrónica a distancia o dispositivos de creación de sello electrónico a distancia;

   g) la expedición de declaraciones electrónicas de atributos;

   h) la validación de declaraciones electrónicas de atributos;

([1]) Directiva 2014/24/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, sobre contratación pública y por la que se deroga la Directiva 2004/18/CE (DO L 94 de 28.3.2014, p. 65).

▼M1

i) la creación de sellos de tiempo electrónicos;

j) la validación de sellos de tiempo electrónicos;

k) la prestación de servicios de entrega electrónica certificada;

l) la validación de los datos transmitidos a través de servicios de entrega electrónica certificada y las pruebas correspondientes;

m) el archivo electrónico de datos y documentos electrónicos;

n) la actividad de registro de datos electrónicos en un libro mayor electrónico.

▼B

17) «servicio de confianza cualificado», un servicio de confianza que cumple los requisitos aplicables establecidos en el presente Reglamento;

▼M1

18) «organismo de evaluación de la conformidad», organismo de evaluación de la conformidad definido en el artículo 2, punto 13, del Reglamento (CE) n.º 765/2008, cuya competencia para realizar una evaluación de la conformidad de un prestador cualificado de servicios de confianza y de los servicios de confianza cualificados que este presta, o cuya competencia para certificar carteras europeas de identidad digital o medios de identificación electrónica, esté acreditada en virtud de dicho Reglamento;

▼B

19) «prestador de servicios de confianza», una persona física o jurídica que presta uno o más servicios de confianza, bien como prestador cualificado o ►C2 como prestador no cualificado de servicios de confianza ◄;

20) «prestador cualificado de servicios de confianza», un prestador de servicios de confianza que presta uno o varios servicios de confianza cualificados y al que el organismo de supervisión ha concedido la cualificación;

▼M1

21) «producto», equipo o programa informático o sus componentes correspondientes, destinado a ser utilizado para la prestación de servicios de identificación electrónica y servicios de confianza;

▼B

22) «dispositivo de creación de firma electrónica», un equipo o programa informático configurado que se utiliza para crear una firma electrónica;

23) «dispositivo cualificado de creación de firma electrónica», un dispositivo de creación de firmas electrónicas que cumple los requisitos enumerados en el anexo II;

▼M1

23 *bis*) «dispositivo cualificado de creación de firma electrónica a distancia», dispositivo cualificado de creación de firmas electrónicas que está gestionado por un prestador cualificado de servicios de confianza, de conformidad con el artículo 29 *bis*, en nombre de un firmante;

▼M1

23 *ter*) «dispositivo cualificado de creación de sello electrónico a distancia», dispositivo cualificado de creación de sellos electrónicos que está gestionado por un prestador cualificado de servicios de confianza, de conformidad con el artículo 39 *bis*, en nombre de un creador de sellos;

▼B

24) «creador de un sello», una persona jurídica que crea un sello electrónico;

25) «sello electrónico», datos en formato electrónico anejos a otros datos en formato electrónico, o asociados de manera lógica con ellos, para garantizar el origen y la integridad de estos últimos;

26) «sello electrónico avanzado», un sello electrónico que cumple los requisitos contemplados en el artículo 36;

27) «sello electrónico cualificado», un sello electrónico avanzado que se crea mediante un dispositivo cualificado de creación de sellos electrónicos y que se basa en un certificado cualificado de sello electrónico;

28) «datos de creación del sello electrónico», los datos únicos que utiliza el creador del sello electrónico para crearlo;

29) «certificado de sello electrónico», una declaración electrónica que vincula los datos de validación de un sello con una persona jurídica y confirma el nombre de esa persona;

30) «certificado cualificado de sello electrónico», un certificado de sellos electrónicos que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo III;

31) «dispositivo de creación de sello electrónico», un equipo o programa informático configurado que se utiliza para crear un sello electrónico;

32) «dispositivo cualificado de creación de sello electrónico», un dispositivo de creación de sellos electrónicos que cumple *mutatis mutandis* los requisitos enumerados en el anexo II;

33) «sello de tiempo electrónico», datos en formato electrónico que vinculan otros datos en formato electrónico con un instante concreto, aportando la prueba de que estos últimos datos existían en ese instante;

34) «sello cualificado de tiempo electrónico», un sello de tiempo electrónico que cumple los requisitos establecidos en el artículo 42;

35) «documento electrónico», todo contenido almacenado en formato electrónico, en particular, texto o registro sonoro, visual o audiovisual;

36) «servicio de entrega electrónica certificada», un servicio que permite transmitir datos entre partes terceras por medios electrónicos y aporta pruebas relacionadas con la gestión de los datos transmitidos, incluida la prueba del envío y la recepción de los datos, y que protege los datos transmitidos frente a los riesgos de pérdida, robo, deterioro o alteración no autorizada;

▼B

37) «servicio cualificado de entrega electrónica certificada», un servicio de entrega electrónica certificada que cumple los requisitos establecidos en el artículo 44;

▼M1

38) «certificado de autenticación de sitio web», declaración electrónica que permite autenticar un sitio web y vincula el sitio web con la persona física o jurídica a quien se ha expedido el certificado;

▼B

39) «certificado cualificado de autenticación de sitio web», un certificado de autenticación de sitio web expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo IV;

40) «datos de validación», los datos utilizados para validar una firma electrónica o un sello electrónico;

▼M1

41) «validación», proceso consistente en verificar y confirmar que los datos en formato electrónico son válidos de conformidad con el presente Reglamento;

42) «cartera europea de identidad digital», medio de identificación electrónica que permite al usuario almacenar, gestionar y validar de forma segura datos de identificación de la persona y declaraciones electrónicas de atributos con el fin de proporcionarlos a las partes usuarias y a otros usuarios de carteras europeas de identidad digital, así como firmar por medio de firmas electrónicas cualificadas o sellar por medio de sellos electrónicos cualificados;

43) «atributo», característica, cualidad, derecho o permiso de una persona física o jurídica o de un objeto;

44) «declaración electrónica de atributos», declaración en formato electrónico que permite la autenticación de atributos;

45) «declaración electrónica cualificada de atributos», declaración electrónica de atributos expedida por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo V;

46) «declaración electrónica de atributos expedida por un organismo del sector público responsable de una fuente auténtica, o en nombre de este», declaración electrónica de atributos expedida por un organismo del sector público que sea responsable de una fuente auténtica o por un organismo del sector público que sea designado por el Estado miembro para expedir dichas declaraciones de atributos en nombre de los organismos del sector público responsables de las fuentes auténticas de conformidad con el artículo 45 *septies* y con el anexo VII;

47) «fuente auténtica», repositorio o sistema, mantenido bajo la responsabilidad de un organismo del sector público o de una entidad privada, que contiene y proporciona atributos acerca de una persona física o jurídica, o de un objeto, y que se considera una fuente principal de dicha información, o que está reconocido como auténtico de conformidad con el Derecho de la Unión o nacional, incluidas las prácticas administrativas;

▼M1

48) «archivo electrónico», servicio que garantiza la recepción, el almacenamiento, la recuperación y la eliminación de datos electrónicos y documentos electrónicos para asegurar su durabilidad y legibilidad, así como para preservar su integridad, confidencialidad y prueba de origen durante todo el período de conservación;

49) «servicio cualificado de archivo electrónico», servicio de archivo electrónico prestado por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el artículo 45 *undecies*;

50) «etiqueta de confianza de la UE para la cartera de identidad digital», indicación verificable, sencilla y reconocible formulada de manera clara, de que la cartera europea de identidad digital de que se trate se ha proporcionado de conformidad con el presente Reglamento;

51) «autenticación reforzada de usuario», autenticación basada en la utilización de al menos dos factores de identificación de diferentes categorías, ya sea conocimiento (algo que solo conoce el usuario), posesión (algo que solo posee el usuario) o inherencia (algo que es el usuario), que son independientes —es decir, que la vulneración de uno no compromete la fiabilidad de los demás—, y concebida de manera que se proteja la confidencialidad de los datos de autenticación;

52) «libro mayor electrónico», secuencia de registros electrónicos de datos que garantiza la integridad de dichos registros y la exactitud de su orden cronológico;

53) «libro mayor electrónico cualificado», libro mayor electrónico proporcionado por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el artículo 45 *terdecies*;

54) «datos personales», toda información en el sentido del artículo 4, punto 1, del Reglamento (UE) 2016/679;

55) «correspondencia de la identidad», proceso por el cual se establece una correspondencia o vínculo entre los datos o medios de identificación electrónica y una cuenta existente perteneciente a esa misma persona;

56) «registro de datos», datos electrónicos registrados con metadatos relacionados que respaldan el tratamiento de los datos;

57) «modo fuera de línea», en lo que respecta al uso de las carteras europeas de identidad digital, interacción entre un usuario y un tercero que tiene lugar en una ubicación física utilizando tecnologías de proximidad inmediata, sin necesidad de que la cartera europea de identidad digital acceda a sistemas a distancia a través de redes de comunicaciones electrónicas a efectos de la interacción.

▼B

Artículo 4

Principio del mercado interior

1. No se impondrá restricción alguna a la prestación de servicios de confianza en el territorio de un Estado miembro por un prestador de servicios de confianza establecido en otro Estado miembro por razones que entren en los ámbitos cubiertos por el presente Reglamento.

▼B

2. Se permitirá la libre circulación en el mercado interior de los productos y servicios de confianza que se ajusten al presente Reglamento.

▼M1

Artículo 5

Seudónimos en transacciones electrónicas

Sin perjuicio de las normas específicas del Derecho de la Unión o nacional que exijan a los usuarios identificarse o de los efectos jurídicos que el Derecho nacional contemple para los seudónimos, no se prohibirá la utilización de seudónimos escogidos por los usuarios.

▼B

CAPÍTULO II

IDENTIFICACIÓN ELECTRÓNICA

▼M1

SECCIÓN 1

cartera europea de identidad digital

Artículo 5 bis

Carteras europeas de identidad digital

1. A los efectos de garantizar que todas las personas físicas y jurídicas dispongan de un acceso transfronterizo seguro, de confianza y sin incidencias a servicios públicos y privados en la Unión, manteniendo al mismo tiempo el pleno control sobre sus datos, cada Estado miembro proporcionará al menos una cartera europea de identidad digital en los veinticuatro meses siguientes a la entrada en vigor de los actos de ejecución a que se refieren el apartado 23 del presente artículo y el artículo 5 *quater*, apartado 6.

2. Las carteras europeas de identidad digital se proporcionarán de una o varias de las maneras siguientes:

a) directamente por un Estado miembro;

b) con arreglo a un mandato de un Estado miembro;

c) de manera independiente de un Estado miembro, pero con el reconocimiento de dicho Estado miembro.

3. El código fuente de los componentes de programas informáticos de las carteras europeas de identidad digital tendrá licencia de código abierto. Los Estados miembros podrán disponer que, por razones debidamente justificadas, no se divulgue el código fuente de componentes específicos distintos de los instalados en los dispositivos de los usuarios.

4. Las carteras europeas de identidad digital permitirán al usuario, de manera intuitiva, transparente y rastreable por el usuario:

a) solicitar, obtener, seleccionar, combinar, almacenar, eliminar, compartir y presentar de forma segura, bajo el control exclusivo del usuario, datos de identificación de la persona y, cuando proceda, en combinación con declaraciones electrónicas de atributos, autenticarse ante partes usuarias en línea y, en su caso, en modo fuera de línea, con el fin de acceder a servicios públicos y privados, velando al mismo tiempo por que sea posible divulgar los datos selectivamente;

▼**M1**

b) generar seudónimos y almacenarlos cifrados y localmente en la cartera europea de identidad digital;

c) autenticar de forma segura la cartera europea de identidad digital de otra persona, así como recibir y compartir datos de identificación de la persona y declaraciones electrónicas de atributos de manera segura entre las dos carteras europeas de identidad digital;

d) acceder a un registro de todas las transacciones realizadas a través de la cartera europea de identidad digital mediante un panel común que permita al usuario:

i) ver una lista actualizada de las partes usuarias con las que ha establecido una conexión y, en su caso, todos los datos intercambiados,

ii) solicitar fácilmente a una parte usuaria que suprima los datos personales en virtud del artículo 17 del Reglamento (UE) 2016/679,

iii) notificar fácilmente una parte usuaria a la autoridad nacional de protección de datos en los casos en los que se reciba una solicitud de datos presuntamente ilícita o sospechosa;

e) firmar por medio de firmas electrónicas cualificadas o sellar por medio de sellos electrónicos cualificados;

f) descargar, en la medida en que sea técnicamente viable, los datos, la declaración electrónica de atributos y las configuraciones del usuario;

g) ejercer los derechos del usuario a la portabilidad de los datos.

5. En particular, las carteras europeas de identidad digital:

a) admitirán protocolos e interfaces comunes:

i) para expedir datos de identificación de la persona, declaraciones electrónicas cualificadas y no cualificadas de atributos o certificados cualificados y no cualificados para la cartera europea de identidad digital,

ii) para que las partes usuarias soliciten y validen datos de identificación de la persona y declaraciones electrónicas de atributos,

iii) para compartir con las partes usuarias, y presentarles, datos de identificación de la persona, una declaración electrónica de atributos o datos conexos divulgados selectivamente, en línea y, cuando proceda, en modo fuera de línea,

iv) para que el usuario permita la interacción con la cartera europea de identidad digital y muestre una etiqueta de confianza de la UE para la cartera de identidad digital,

v) para incorporar al usuario de manera segura utilizando un medio de identificación electrónica de conformidad con el artículo 5 *bis*, apartado 24,

vi) para permitir la interacción entre las carteras europeas de identidad digital de dos personas a fin de recibir, validar y compartir datos de identificación de la persona y declaraciones electrónicas de atributos de manera segura,

▼**M1**

vii) para autenticar e identificar a partes usuarias aplicando mecanismos de autenticación de conformidad con el artículo 5 *ter*,

viii) para que las partes usuarias verifiquen la autenticidad y la validez de las carteras europeas de identidad digital,

ix) para solicitar a una parte usuaria que suprima los datos personales en virtud del artículo 17 del Reglamento (UE) 2016/679,

x) para denunciar a una parte usuaria ante la autoridad nacional competente de protección de datos cuando se reciba una solicitud de datos presuntamente ilícita o sospechosa,

xi) para crear firmas electrónicas o sellos electrónicos cualificados mediante dispositivos cualificados de creación de firma electrónica o sello electrónico;

b) no facilitarán información alguna a los prestadores de servicios de confianza de declaraciones electrónicas de atributos sobre el uso de dichas declaraciones electrónicas;

c) garantizarán que la identidad de las partes usuarias pueda autenticarse e identificarse mediante la aplicación de mecanismos de autenticación de conformidad con el artículo 5 *ter*;

d) cumplirán los requisitos establecidos en el artículo 8 en lo referente al nivel de seguridad alto, en particular en lo que sea aplicable a los requisitos de acreditación y verificación de la identidad, así como a la gestión y autenticación de medios de identificación electrónica;

e) en el caso de las declaraciones electrónicas de atributos con políticas de divulgación incorporadas, aplicarán el mecanismo adecuado para informar al usuario de que la parte usuaria o el usuario de la cartera europea de identidad digital solicitante de la declaración electrónica de atributos tiene permiso para acceder a dicha declaración;

f) garantizarán que los datos de identificación personal disponibles a través del sistema de identificación electrónica en virtud del cual se proporciona la cartera europea de identidad digital correspondan de forma única, a la persona física, la persona jurídica o la persona física que representa a la persona física o jurídica y estén asociados con esa cartera europea de identidad digital;

g) ofrecerán a todas las personas físicas la posibilidad de firmar, por defecto y de forma gratuita, mediante firmas electrónicas cualificadas.

No obstante lo dispuesto en el párrafo primero, letra g), los Estados miembros podrán establecer medidas proporcionadas para garantizar que el uso gratuito de las firmas electrónicas cualificadas por parte de las personas físicas se limite a fines no profesionales.

6. Los Estados miembros informarán a los usuarios, sin demora, de toda violación de la seguridad que pueda haber comprometido total o parcialmente sus carteras europeas de identidad digital o su contenido, en particular si sus carteras europeas de identidad digital han sido suspendidas o revocadas en virtud del artículo 5 *sexies*;

▼M1

7. Sin perjuicio de lo dispuesto en el artículo 5 *septies*, los Estados miembros podrán contemplar, de conformidad con el Derecho nacional, funcionalidades adicionales de las carteras europeas de identidad digital, como la interoperabilidad con los medios nacionales de identificación electrónica existentes. Dichas funcionalidades adicionales cumplirán lo dispuesto en el presente artículo.

8. Los Estados miembros proporcionarán mecanismos de validación gratuitos a fin de:

a) garantizar que se pueda verificar la autenticidad y validez de las carteras europeas de identidad digital;

b) permitir que los usuarios verifiquen la autenticidad y validez de la identidad de las partes usuarias registradas de conformidad con el artículo 5 *ter*.

9. Los Estados miembros velarán por que la validez de la cartera europea de identidad digital pueda revocarse en las siguientes circunstancias:

a) a petición expresa del usuario;

b) cuando la seguridad de la cartera europea de identidad digital se haya visto comprometida;

c) en caso de fallecimiento del usuario o cese de actividad de la persona jurídica.

10. Los proveedores de carteras europeas de identidad digital garantizarán que los usuarios puedan solicitar fácilmente apoyo técnico y notificar problemas técnicos o cualquier otro incidente que afecte negativamente al uso de las carteras europeas de identidad digital.

11. Las carteras europeas de identidad digital se proporcionarán en el marco de un sistema de identificación electrónica con nivel de seguridad alto.

12. Las carteras europeas de identidad digital respetarán el principio de seguridad desde el diseño.

13. La expedición, el uso y la revocación de las carteras europeas de identidad digital serán gratuitos para todas las personas físicas.

14. Los usuarios tendrán pleno control sobre el uso de su cartera europea de identidad digital y sobre los datos que consten en ella. El proveedor de la cartera europea de identidad digital no recopilará información sobre el uso de la cartera europea de identidad digital que no sea necesaria para la prestación de los servicios de esta, ni combinará datos de identificación de la persona u otros datos personales almacenados o relativos al uso de la cartera europea de identidad digital con datos personales obtenidos a través de otros servicios ofrecidos por dicho proveedor o a través de servicios de terceros que no sean necesarios para la prestación de los servicios de la cartera europea de identidad digital, a menos que el usuario haya solicitado expresamente lo contrario. Se establecerá una separación lógica entre los datos personales relacionados con la provisión de carteras europeas de identidad digital y cualesquier otros datos que obren en poder del proveedor de las carteras europeas de identidad digital. Si la cartera europea de identidad digital ha sido proporcionada por entidades privadas de conformidad con lo dispuesto en el apartado 2, letras b) y c), se aplicarán *mutatis mutandis* las disposiciones del artículo 45 *nonies*, apartado 3.

▼**M1**

15. La utilización de las carteras europeas de identidad digital será voluntaria. El acceso a los servicios públicos y privados, el acceso al mercado laboral y la libertad de empresa no se restringirán de ninguna manera ni perjudicarán a las personas físicas o jurídicas que no utilicen las carteras europeas de identidad digital. Seguirá siendo posible acceder a los servicios públicos y privados mediante los otros medios de identificación y autenticación existentes.

16. El marco técnico de la cartera europea de identidad digital:

a) no permitirá que, tras la expedición de la declaración de atributos, los prestadores de declaraciones electrónicas de atributos o cualquier otra parte obtengan datos que permitan que se rastree, vincule o correlacione, u obtener de cualquier otra manera, conocimiento de las transacciones o del comportamiento del usuario a menos que este lo autorice explícitamente;

b) permitirá tecnologías de protección de la privacidad que garanticen la no vinculación, cuando la declaración de atributos no requiera la identificación del usuario.

17. Todo tratamiento de datos personales realizado por los Estados miembros o en su nombre por organismos o partes responsables de la provisión de carteras europeas de identidad digital como medio de identificación electrónica se llevará a cabo de conformidad con medidas adecuadas y efectivas de protección de datos. Se demostrará que dicho tratamiento cumple el Reglamento (UE) 2016/679. Los Estados miembros podrán introducir disposiciones nacionales para especificar en más detalle la aplicación de dichas medidas.

18. Sin dilación indebida, los Estados miembros comunicarán a la Comisión información sobre:

a) el organismo responsable de establecer y mantener la lista de partes usuarias registradas que utilizan las carteras europeas de identidad digital de conformidad con el artículo 5 *ter*, apartado 5, y la localización de dicha lista;

b) los organismos responsables de la provisión de carteras europeas de identidad digital de conformidad con el artículo 5 *bis*, apartado 1;

c) los organismos responsables de garantizar que los datos de identificación de la persona estén asociados a la cartera europea de identidad digital de conformidad con el artículo 5 *bis*, apartado 5, letra f);

d) el mecanismo que permite validar los datos de identificación de la persona a que se refiere el artículo 5 *bis*, apartado 5, letra f), y la identidad de las partes usuarias;

e) el mecanismo para validar la autenticidad y la validez de las carteras europeas de identidad digital.

La Comisión pondrá a disposición del público la información notificada en virtud del párrafo primero, a través de un canal seguro, la información a que se refiere el presente apartado en una forma firmada o sellada electrónicamente que sea apropiada para el tratamiento automático.

▼M1

19. Sin perjuicio del apartado 22 del presente artículo, el artículo 11 se aplicará *mutatis mutandis* a la cartera europea de identidad digital.

20. El artículo 24, apartado 2, letras b) y d) a h), se aplicará *mutatis mutandis* a los proveedores de carteras europeas de identidad digital.

21. Se garantizará la accesibilidad de las carteras europeas de identidad digital para las personas con discapacidad, en igualdad de condiciones que el resto de los usuarios, conforme a los requisitos de accesibilidad previstos en la Directiva (UE) 2019/882 del Parlamento Europeo y del Consejo ([1]).

22. A efectos de la provisión de las carteras europeas de identidad digital, ni estas ni los sistemas de identificación electrónica con arreglo a los cuales se proporcionan estarán sujetos a los requisitos establecidos en los artículos 7, 9, 10, 12 y 12 *bis*.

23. A más tardar el 21 de noviembre de 2024, la Comisión establecerá, mediante actos de ejecución, una lista de normas de referencia y, en su caso, las especificaciones y los procedimientos aplicables a los requisitos a que se refieren los apartados 4, 5, 8 y 18 del presente artículo sobre la implantación de las carteras europeas de identidad digital. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

24. La Comisión establecerá, mediante actos de ejecución, una lista de normas de referencia y, cuando proceda, especificaciones y procedimientos, con el fin de facilitar la incorporación de los usuarios a la cartera europea de identidad digital utilizando bien medios de identificación electrónica conformes con el nivel de seguridad alto, bien medios de identificación electrónica conformes con el nivel de seguridad sustancial junto con procedimientos adicionales de incorporación a distancia, de modo que, en conjunto, cumplan los requisitos del nivel de seguridad alto. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 48, apartado 2.

Artículo 5 ter

Partes usuarias de las carteras europeas de identidad digital

1. Cuando una parte usuaria tenga previsto utilizar carteras europeas de identidad digital para prestar servicios públicos o privados mediante una interacción digital, se registrará en el Estado miembro en el que esté establecida.

2. El proceso de registro tendrá un coste razonable y proporcional al riesgo. La parte usuaria proporcionará, como mínimo:

a) la información necesaria para autenticarse en las carteras europeas de identidad digital, lo que como mínimo incluye:

   i) el Estado miembro en el que la parte usuaria tiene su sede, y

([1]) Directiva (UE) 2019/882 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre los requisitos de accesibilidad de los productos y servicios (DO L 151 de 7.6.2019, p. 70).

▼M1

ii) el nombre de la parte usuaria y, en su caso, su número de registro tal como figura en un registro oficial, junto con los datos de identificación de dicho registro oficial;

b) los datos de contacto de la parte usuaria;

c) el uso previsto de las carteras europeas de identidad digital, incluida una mención de los datos que la parte usuaria solicitará a los usuarios.

3. Las partes usuarias no solicitarán a los usuarios datos distintos de los mencionados en virtud del apartado 2, letra c).

4. Los apartados 1 y 2 se entenderán sin perjuicio del Derecho de la Unión o nacional aplicable a la prestación de servicios específicos.

5. Los Estados miembros publicarán la información a que se refiere el apartado 2 en línea en una forma firmada o sellada electrónicamente que sea apropiada para el tratamiento automático.

6. Las partes usuarias registradas de conformidad con el presente artículo informarán sin demora a los Estados miembros sobre cualquier cambio en la información facilitada en el registro en virtud del apartado 2.

7. Los Estados miembros facilitarán un mecanismo común para permitir la identificación y autenticación de las partes usuarias, tal como prevé el artículo 5 *bis*, apartado 5, letra c).

8. Cuando las partes usuarias tengan previsto utilizar carteras europeas de identidad digital, se identificarán respecto al usuario.

9. Las partes usuarias serán responsables de llevar a cabo el procedimiento de autenticación y validación de los datos de identificación personal y de las declaraciones electrónicas de atributos solicitados por las carteras europeas de identidad digital. Las partes usuarias no rechazarán el uso de seudónimos, cuando el Derecho de la Unión o nacional no exija la identificación del usuario.

10. Los intermediarios que actúen en nombre de las partes usuarias se considerarán partes usuarias y no almacenarán datos sobre el contenido de la transacción.

11. A más tardar el 21 de noviembre de 2024, la Comisión establecerá especificaciones técnicas y procedimientos para los requisitos mencionados en los apartados 2, 5 y 6 a 9 del presente artículo, mediante actos de ejecución relativos a la implantación de las carteras europeas de identidad digital, tal como prevé el artículo 5 *bis*, apartado 23. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 48, apartado 2.

Artículo 5 quater

Certificación de las carteras europeas de identidad digital

1. La conformidad de las carteras europeas de identidad digital y el sistema de identificación electrónica con arreglo al cual se proporcionan los requisitos establecidos en el artículo 5 *bis*, apartados 4, 5 y 8, el requisito de separación lógica establecido en el artículo 5 *bis*, apartado 14, y, cuando proceda, con las normas y especificaciones técnicas previstas en el artículo 5 *bis*, apartado 24, será certificada por organismos de evaluación de la conformidad designados por los Estados miembros.

▼M1

2. La certificación de conformidad de las carteras europeas de identidad digital con los requisitos pertinentes de ciberseguridad previstos en el apartado 1 del presente artículo, o partes de ellos, que sean pertinentes para la ciberseguridad, será realizada de conformidad con los esquemas de certificación de la ciberseguridad adoptados en virtud del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo ([1]) e indicados en los actos de ejecución mencionados en el apartado 6 del presente artículo.

3. Para los requisitos a que se refiere el apartado 1 del presente artículo que no sean pertinentes para la ciberseguridad y para los requisitos a que se refiere el apartado 1 del presente artículo que sean pertinentes para la ciberseguridad, en la medida en que los esquemas de certificación de la ciberseguridad a que se refiere el apartado 2 del presente artículo no incluyan los requisitos de ciberseguridad pertinentes, o solo lo hagan parcialmente, los Estados miembros establecerán también para dichos requisitos esquemas nacionales de certificación con arreglo a los requisitos establecidos en los actos de ejecución a los que se refiere el apartado 6 del presente artículo. Los Estados miembros transmitirán sus proyectos de esquemas nacionales de certificación al Grupo de Cooperación sobre la Identidad Digital Europea establecido en virtud del artículo 46 *sexies*, apartado 1, (en lo sucesivo, "Grupo de Cooperación"). El Grupo de Cooperación podrá emitir dictámenes y recomendaciones.

4. La certificación en virtud del apartado 1 tendrá una validez máxima de cinco años, siempre que se realice una evaluación de la vulnerabilidad cada dos años. Cuando se detecte una vulnerabilidad y no se subsane oportunamente, se cancelará la certificación.

5. El cumplimiento de los requisitos establecidos en el artículo 5 *bis* del presente Reglamento para las operaciones de tratamiento de datos personales podrá ser certificado con arreglo al Reglamento (UE) 2016/679.

6. A más tardar el 21 de noviembre de 2024, la Comisión establecerá, mediante actos de ejecución, una lista de normas de referencia y, en su caso, las especificaciones y los procedimientos para la certificación de las carteras europeas de identidad digital a que se refieren los apartados 1, 2 y 3 del presente artículo. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

7. Los Estados miembros comunicarán a la Comisión los nombres y direcciones de los organismos de evaluación de la conformidad a que se refiere el apartado 1. La Comisión pondrá dicha información a disposición de todos los Estados miembros.

8. La Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 47 por los que se establezcan los criterios específicos que deben satisfacer los organismos de evaluación de la conformidad designados a que se refiere el apartado 1 del presente artículo.

([1]) Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.º 526/2013 ("Reglamento sobre la Ciberseguridad") (DO L 151 de 7.6.2019, p. 15).

▼M1

Artículo 5 quinquies

Publicación de una lista de carteras europeas de identidad digital certificadas

1. Los Estados miembros informarán a la Comisión y al Grupo de Cooperación establecido en virtud del artículo 46 *sexies*, apartado 1, sin dilación indebida, de las carteras europeas de identidad digital que se hayan proporcionado de conformidad con el artículo 5 *bis* y que hayan sido certificadas por los organismos de evaluación de la conformidad a que se refiere el artículo 5 *quater*, apartado 1. Informarán a la Comisión y al Grupo de Cooperación establecido en virtud del artículo 46 *sexies*, apartado 1, sin dilación indebida cuando se cancele alguna certificación y expondrán los motivos de la cancelación.

2. Sin perjuicio de lo dispuesto en el artículo 5 *bis*, apartado 18, la información facilitada por los Estados miembros mencionada en el apartado 1 del presente artículo incluirá, como mínimo:

a) el certificado y el informe de evaluación de la certificación de la cartera europea de identidad digital certificada;

b) una descripción del sistema de identificación electrónica en virtud del cual se proporciona la cartera europea de identidad digital;

c) el régimen de supervisión aplicable y la información sobre el régimen de responsabilidades respecto de la parte que proporciona la cartera europea de identidad digital;

d) la autoridad o autoridades responsables del sistema de identificación electrónica;

e) disposiciones relativas a la suspensión o revocación del sistema de identificación electrónica de la autenticación o de las partes afectadas.

3. A tenor de la información recibida en virtud del apartado 1, la Comisión establecerá, publicará en el *Diario Oficial de la Unión Europea* y mantendrá en un formato legible por máquina una lista de carteras europeas de identidad digital certificadas.

4. Todo Estado miembro podrá presentar a la Comisión una solicitud de suprimir de la lista a la que se refiere el apartado 3 una cartera europea de identidad digital y el sistema de identificación electrónica en virtud del cual se proporciona.

5. Cuando se produzcan cambios en la información facilitada en virtud del apartado 1, el Estado miembro facilitará a la Comisión información actualizada.

6. La Comisión mantendrá actualizada la lista a que se refiere el apartado 3 mediante la publicación en el *Diario Oficial de la Unión Europea* de las modificaciones correspondientes de la lista en el plazo de un mes a partir de la recepción de una solicitud con arreglo al apartado 4 o de información actualizada con arreglo al apartado 5.

7. A más tardar el 21 de noviembre de 2024, la Comisión establecerá los formatos y procedimientos aplicables a efectos de los apartados 1, 4 y 5 del presente artículo, mediante actos de ejecución relativos a la implantación de las carteras europeas de identidad digital, tal como prevé el artículo 5 *bis*, apartado 23. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 48, apartado 2.

▼M1

Artículo 5 sexies

Violación de la seguridad de las carteras europeas de identidad digital

1. Cuando se viole o quede parcialmente comprometida la seguridad de las carteras europeas de identidad digital proporcionadas en virtud del artículo 5 *bis*, de los mecanismos de validación a que se refiere el artículo 5 *bis*, apartado 8, o del sistema de identificación electrónica en virtud del cual se proporcionan las carteras europeas de identidad digital de un modo que afecte a su fiabilidad o a la de otras carteras europeas de identidad digital, el Estado miembro que haya proporcionado las carteras europeas de identidad digital suspenderá, sin dilación indebida, la provisión y el uso de dichas carteras.

Cuando la gravedad de la violación o el compromiso de seguridad a que se refiere párrafo primero lo justifique, el Estado miembro retirará sin dilación indebida las carteras europeas de identidad digital.

El Estado miembro informará de ello a los usuarios afectados, a los puntos de contacto únicos designados con arreglo al artículo 46 *quater*, apartado 1, a las partes usuarias y a la Comisión.

2. Si la violación o el compromiso de seguridad a que se refiere el apartado 1, párrafo primero, del presente artículo no se subsana en un plazo de tres meses desde la suspensión, el Estado miembro que haya proporcionado las carteras europeas de identidad digital las retirará y revocará su validez. El Estado miembro informará, en consecuencia, de la retirada a los usuarios afectados, a los puntos de contacto únicos designados en virtud del artículo 46 *quater*, apartado 1, a las partes usuarias y a la Comisión.

3. Cuando se haya subsanado la violación o el compromiso de seguridad a que se refiere el apartado 1, párrafo primero, del presente artículo, el Estado miembro proveedor restablecerá la provisión y el uso de las carteras europeas de identidad digital e informará sin dilación indebida a los usuarios y partes usuarias afectados, a los puntos únicos de contacto designados en virtud del artículo 46 *quater*, apartado 1, y a la Comisión.

4. La Comisión publicará en el *Diario Oficial de la Unión Europea* las modificaciones correspondientes de la lista a que se refiere el artículo 5 *quinquies*, sin dilación indebida.

5. A más tardar el 21 de noviembre de 2024, la Comisión establecerá, mediante actos de ejecución, una lista de normas de referencia y, en su caso, establecerá las especificaciones y los procedimientos relativos a las medidas a que se refieren los apartados 1, 2 y 3 del presente artículo. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 48, apartado 2.

Artículo 5 septies

Uso transfronterizo de las carteras europeas de identidad digital

1. Cuando los Estados miembros exijan una identificación y una autenticación electrónicas para acceder a un servicio en línea prestado por un organismo del sector público, también aceptarán las carteras europeas de identidad digital proporcionadas de conformidad con el presente Reglamento.

▼M1

2. Cuando el Derecho de la Unión o nacional exija que las partes usuarias privadas que prestan servicios —con la excepción de las microempresas y pequeñas empresas según se definen en el artículo 2 del anexo de la Recomendación 2003/361/CE de la Comisión ([1])— utilicen una autenticación reforzada de usuario para la identificación en línea, o cuando se requiera una autenticación reforzada de usuario para la identificación en línea en virtud de una obligación contractual, en particular en los ámbitos del transporte, la energía, la banca, los servicios financieros, la seguridad social, la sanidad, el agua potable, los servicios postales, la infraestructura digital, la educación o las telecomunicaciones, dichas partes usuarias privadas también aceptarán, a más tardar treinta y seis meses a partir de la fecha de entrada en vigor de los actos de ejecución a que se refieren el artículo 5 *bis*, apartado 23, y el artículo 5 *quater*, apartado 6, y únicamente a petición voluntaria del usuario, las carteras europeas de identidad digital proporcionadas de conformidad con el presente Reglamento.

3. Cuando los prestadores de plataformas en línea de muy gran tamaño a que se refiere el artículo 33 del Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo ([2]) exijan la autenticación del usuario para acceder a servicios en línea, también aceptarán y facilitarán el uso de las carteras europeas de identidad digital proporcionadas con arreglo al presente Reglamento para la autenticación del usuario, únicamente a petición voluntaria del usuario y en lo que respecta a los datos mínimos necesarios para el servicio en línea específico para el que se solicita la autenticación.

4. En cooperación con los Estados miembros, la Comisión facilitará la elaboración de códigos de conducta en estrecha colaboración con todas las partes interesadas pertinentes, en particular la sociedad civil, para contribuir a la amplia disponibilidad y la facilidad de uso de las carteras europeas de identidad digital contempladas en el ámbito de aplicación del presente Reglamento y alentar a los prestadores de servicios a ultimar la elaboración de códigos de conducta.

5. En un plazo de veinticuatro meses a partir de la implantación de las carteras europeas de identidad digital, la Comisión evaluará la demanda, disponibilidad y facilidad de uso de las carteras europeas de identidad digital, teniendo en cuenta criterios como la adopción por los usuarios, la presencia transfronteriza de prestadores de servicios, el desarrollo tecnológico, la evolución de los patrones de uso y la demanda de los usuarios.

▼M1

SECCIÓN 2

sistemas de identificación electrónica

▼B

Artículo 6

Reconocimiento mutuo

1. Cuando sea necesaria una identificación electrónica utilizando un medio de identificación electrónica y una autenticación en virtud de la normativa o la práctica administrativa nacionales para acceder a un

([1]) Recomendación 2003/361/CE de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas (DO L 124 de 20.5.2003, p. 36).

([2]) Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales) (DO L 277 de 27.10.2022, p. 1).

▼B

servicio prestado en línea por un organismo del sector público en un Estado miembro, se reconocerá en dicho Estado miembro, a efectos de la autenticación transfronteriza en dicho servicio en línea, el medio de identificación electrónica expedido en otro Estado miembro, siempre que:

a) este medio de identificación electrónica haya sido expedido en virtud de un sistema de identificación electrónica incluido en la lista publicada por la Comisión de conformidad con el artículo 9;

b) el nivel de seguridad de este medio de identificación electrónica corresponda a un nivel de seguridad igual o superior al nivel de seguridad requerido por el organismo del sector público para acceder a dicho servicio en línea en el primer Estado miembro, siempre que el nivel de seguridad de dicho medio de identificación electrónica corresponda a un nivel de seguridad sustancial o alto;

c) el organismo público en cuestión utilice un nivel de seguridad sustancial o alto en relación con el acceso a ese servicio en línea.

Este reconocimiento se producirá a más tardar 12 meses después de que la Comisión publique la lista a que se refiere la letra a) del párrafo primero.

2. Un medio de identificación electrónica expedido por un sistema de identificación electrónica incluido en la lista publicada por la Comisión de conformidad con el artículo 9 y que corresponda al nivel de seguridad bajo podrá ser reconocido por los órganos del sector público a efectos de la autenticación transfronteriza del servicio prestado en línea por dichos órganos.

Artículo 7

Condiciones para la notificación de los sistemas de identificación electrónica

Un sistema de identificación electrónica podrá ser objeto de notificación con arreglo al artículo 9, apartado 1, si se cumplen la totalidad de las condiciones siguientes:

a) que los medios de identificación electrónica en virtud del sistema de identificación electrónica hayan sido expedidos:

   i) por el Estado miembro que efectúa la notificación,

   ii) por mandato del Estado miembro que efectúa la notificación, o

   iii) independientemente del Estado miembro que efectúa la notificación y reconocidos por dicho Estado miembro;

b) que los medios de identificación electrónica en virtud del sistema de identificación electrónica puedan usarse para acceder al menos a un servicio prestado por un organismo del sector público que exija la identificación electrónica en el Estado miembro que efectúa la notificación;

c) que tanto el sistema de identificación electrónica como los medios de identificación electrónicos en su virtud expedidos cumplan los requisitos de al menos uno de los niveles de seguridad previstos en el acto de ejecución a que hace referencia el artículo 8, apartado 3;

▼B

d) que el Estado miembro que efectúa la notificación garantice que los datos de identificación de la persona que representan en exclusiva a la persona en cuestión se atribuyen de conformidad con las especificaciones técnicas, las normas y los procedimientos del nivel de seguridad pertinente establecido en el acto de ejecución a que se refiere el artículo 8, apartado 3, a la persona física o jurídica a la que se refiere el artículo 3, punto 1, en el momento de expedición de los medios de identificación electrónica previstos en este sistema;

e) que la parte que expide los medios de identificación electrónica previstos en este sistema garantice que los medios de identificación electrónica se atribuyan a la persona a que se refiere la letra d) del presente artículo de conformidad con las especificaciones técnicas, las normas y los procedimientos del nivel de seguridad pertinente establecidos en el acto de ejecución a que se refiere el artículo 8, apartado 3;

f) el Estado miembro que efectúa la notificación garantiza la disponibilidad de la autenticación en línea de manera que cualquier parte usuaria establecida en el territorio de otro Estado miembro pueda confirmar los datos de identificación de la persona recibidos en formato electrónico.

Para las partes usuarias distintas de los organismos del sector público, el Estado miembro que efectúa la notificación podrá definir las condiciones de acceso a esa autenticación. La autenticación transfronteriza deberá ser gratuita cuando se realice en relación con un servicio en línea prestado por un organismo del sector público.

Los Estados miembros no impondrán requisitos técnicos específicos desproporcionados a las partes usuarias que tengan intención de llevar a cabo tal autenticación, cuando esos requisitos impidan u obstaculicen significativamente la interoperabilidad de los sistemas de identificación electrónica notificados;

▼M1

g) al menos seis meses antes de la notificación a la que se refiere el artículo 9, apartado 1, el Estado miembro que efectúa la notificación presentará a los demás Estados miembros, a efectos del artículo 12, apartado 5, una descripción de este sistema, de conformidad con las modalidades de procedimiento establecidas en los actos de ejecución adoptados en virtud del artículo 12, apartado 6;

▼B

h) el sistema de identificación electrónica cumple los requisitos del acto de ejecución a que se refiere el artículo 12, apartado 8.

Artículo 8

Niveles de seguridad de los sistemas de identificación electrónica

1. Un sistema de identificación electrónica notificado en virtud del artículo 9, apartado 1, deberá especificar los niveles de seguridad bajo, sustancial y alto para los medios de identificación electrónica expedidos en virtud del mismo.

2. Los niveles de seguridad bajo, sustancial y alto cumplirán los siguientes criterios, respectivamente:

▼B

a) el nivel de seguridad bajo se referirá a un medio de identificación electrónica, en el contexto de un sistema de identificación electrónica, que establece un grado limitado de confianza en la identidad pretendida o declarada de una persona y se describe en referencia a las especificaciones técnicas, las normas y los procedimientos del mismo, entre otros los controles técnicos, y cuyo objetivo es reducir el riesgo de uso indebido o alteración de la identidad;

b) el nivel de seguridad sustancial se referirá a un medio de identificación electrónica, en el contexto de un sistema de identificación electrónica, que establece un grado sustancial de confianza en la identidad pretendida o declarada de una persona y se describe en referencia a las especificaciones técnicas, las normas y los procedimientos del mismo, entre otros los controles técnicos, y cuyo objetivo es reducir sustancialmente el riesgo de uso indebido o alteración de la identidad;

c) el nivel de seguridad alto se referirá a un medio de identificación electrónica, en el contexto de un sistema de identificación electrónica, que establece un grado de confianza en la identidad pretendida o declarada de una persona superior al medio de identificación electrónica con un nivel de seguridad sustancial, y se describe en referencia a las especificaciones técnicas, las normas y los procedimientos del mismo, entre otros los controles técnicos, cuyo objetivo es evitar el uso indebido o alteración de la identidad.

▼M1

3. A más tardar el 18 de septiembre de 2015, teniendo en cuenta las normas internacionales pertinentes, y en los términos del apartado 2, la Comisión establecerá, mediante actos de ejecución, las especificaciones técnicas mínimas, las normas y los procedimientos con referencia a los cuales se especificarán los niveles de seguridad bajo, sustancial y alto de los medios de identificación electrónica..

▼B

Estas especificaciones técnicas mínimas, normas y procedimientos se establecerán en referencia a la fiabilidad y la calidad de los siguientes elementos:

a) el procedimiento para demostrar y comprobar la identidad de las personas físicas o jurídicas que solicitan la expedición de los medios de identificación electrónica;

b) el procedimiento para expedir los medios de identificación electrónica solicitados;

c) el mecanismo de autenticación mediante el cual la persona física o jurídica utiliza los medios de identificación electrónica para confirmar su identidad a una parte usuaria;

d) la entidad que expide los medios de identificación electrónica;

e) cualquier otro organismo que intervenga en la solicitud de expedición de los medios de identificación electrónica, y

f) las especificaciones técnicas y de seguridad de los medios de identificación electrónica.

Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

▼B

Artículo 9

Notificación

1. El Estado miembro que efectúa la notificación transmitirá a la Comisión la siguiente información y, sin dilaciones indebidas, cualquier modificación posterior de la misma:

a) una descripción del sistema de identificación electrónica, que incluya sus niveles de seguridad y el emisor o emisores de los medios de identificación electrónica en virtud de este sistema;

b) el régimen de supervisión aplicable y la información sobre el régimen de responsabilidades respecto de:

i) la parte que expida los medios de identificación electrónica, y

ii) la parte que utilice el procedimiento de autenticación;

c) la autoridad o autoridades responsables del sistema de identificación electrónica;

d) información sobre la o las entidades que gestionan el registro de los datos únicos de identificación de la persona;

e) una descripción de cómo se cumplen los requisitos de los actos de ejecución a los que se hace referencia en el artículo 12, apartado 8;

f) una descripción de la autenticación a la que se refiere la letra f) del artículo 7;

g) disposiciones relativas a la suspensión o revocación del sistema de identificación electrónica, o autenticación notificados o de las partes interesadas.

▼M1

2. La Comisión publicará en el *Diario Oficial de la Unión Europea*, sin dilación indebida, la lista de los sistemas de identificación electrónica notificados de conformidad con el apartado 1 junto con información básica sobre dichos sistemas.

3. La Comisión publicará en el *Diario Oficial de la Unión Europea* las modificaciones de la lista a que se hace referencia en el apartado 2 en el plazo de un mes desde la fecha en que se reciba la citada notificación.

▼B

4. Todo Estado miembro podrá presentar a la Comisión la solicitud de suprimir un sistema de identificación electrónica notificado por dicho Estado miembro de la lista a la que se refiere el apartado 2. La Comisión publicará en el *Diario Oficial de la Unión Europea* las modificaciones correspondientes de la lista en el plazo de un mes a partir de la fecha de recepción de la solicitud del Estado miembro.

▼B

5. La Comisión podrá, mediante actos de ejecución, definir las circunstancias, formatos y procedimientos relativos a la notificación a que se refiere el apartado 1. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

Artículo 10

▼M1

Violación de la seguridad de los sistemas de identificación electrónica

▼B

1. En caso de que el sistema de identificación electrónica notificado con arreglo al artículo 9, apartado 1, o la autenticación a que se refiere el artículo 7, letra f), hayan sido violados o puestos parcialmente en peligro de una forma que afecte a la fiabilidad de la autenticación transfronteriza de dicho sistema, el Estado miembro que efectúa la notificación suspenderá o revocará sin dilaciones indebidas dicha autenticación transfronteriza o las partes afectadas, e informará al respecto a los demás Estados miembros y a la Comisión.

2. Cuando se haya subsanado la violación o la puesta en peligro a que se refiere el apartado 1, el Estado miembro que efectúa la notificación restablecerá la autenticación transfronteriza e informará sin dilaciones indebidas a los demás Estados miembros y a la Comisión.

3. Si la violación o la puesta en peligro a que se refiere el apartado 1 no se corrige en un plazo de tres meses a partir de la suspensión o revocación, el Estado miembro que efectúa la notificación comunicará la retirada del sistema de identificación electrónica a los demás Estados miembros y a la Comisión.

La Comisión publicará en el *Diario Oficial de la Unión Europea* las modificaciones correspondientes de la lista a que se refiere el artículo 9, apartado 2, sin dilaciones indebidas.

Artículo 11

Responsabilidad

1. El Estado miembro que efectúa la notificación será responsable de los perjuicios causados de forma deliberada o por negligencia a cualquier persona física o jurídica en caso de incumplimiento de sus obligaciones en virtud de las letras d) y f) del artículo 7 en una transacción transfronteriza.

2. La parte que expida los medios de identificación electrónica será responsable de los perjuicios causados de forma deliberada o por negligencia a cualquier persona física o jurídica en caso de incumplimiento de sus obligaciones en virtud de la letra e) del artículo 7 en una transacción transfronteriza.

3. La parte que realice el procedimiento de autenticación será responsable de los perjuicios causados de forma deliberada o por negligencia a cualquier persona física o jurídica en caso de incumplimiento de sus obligaciones en virtud de la letra f) del artículo 7 en una transacción transfronteriza.

4. Los apartados 1, 2 y 3 se aplicarán con arreglo a las normas nacionales sobre responsabilidad.

▼B

5. Los apartados 1, 2 y 3 se entenderán sin perjuicio de la responsabilidad de las partes de acuerdo con la legislación nacional en relación con una transacción en la que se utilicen medios de identificación electrónica incluidos en el sistema de identificación electrónica notificado en virtud del artículo 9, apartado 1.

▼M1

Artículo 11 bis

Correspondencia transfronteriza de la identidad

1. Cuando actúen como partes usuarias de servicios transfronterizos, los Estados miembros garantizarán una correspondencia inequívoca de la identidad para las personas físicas que utilicen medios de identificación electrónica notificados o carteras europeas de identidad digital.

2. Los Estados miembros establecerán medidas técnicas y organizativas para garantizar un elevado nivel de protección de los datos personales utilizados para la correspondencia de la identidad y para evitar la elaboración de perfiles de usuarios.

3. A más tardar el 21 de noviembre de 2024, la Comisión establecerá una lista de normas de referencia y, en su caso, establecerá las especificaciones y los procedimientos relativos a los requisitos a que se refiere el apartado 1 del presente artículo por medio de actos de ejecución. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 48, apartado 2.

▼B

Artículo 12

▼M1

Interoperabilidad

▼B

1. Los sistemas nacionales de identificación electrónica notificados de conformidad con el artículo 9, apartado 1, serán interoperables.

2. A efectos del apartado 1, se establecerá un marco de interoperabilidad.

3. El marco de interoperabilidad debe cumplir los criterios siguientes:

a) aspirar a ser neutro desde un punto de vista tecnológico y no discriminar entre soluciones técnicas nacionales específicas para la identificación electrónica dentro del Estado miembro;

b) ajustarse a las normas internacionales y europeas, siempre que sea posible;

▼M1

c) facilitarla aplicación de la privacidad y la seguridad desde el diseño;

———————

▼B

4. El marco de interoperabilidad consistirá en lo siguiente:

a) una referencia a los requisitos técnicos mínimos relativos a los niveles de seguridad contemplados en el artículo 8;

▼B

b) una correlación entre los niveles de seguridad nacionales de los sistemas de identificación electrónica y los niveles de seguridad contemplados en el artículo 8;

c) una referencia a los requisitos técnicos mínimos para la interoperabilidad;

▼M1

d) una referencia a un conjunto mínimo de datos de identificación de la persona necesarios para representar de manera única a una persona física o jurídica o a una persona física que representa a otra persona física o a una persona jurídica y que está disponible en los sistemas de identificación electrónica;

▼B

e) reglas de procedimiento;

f) acuerdos para la resolución de litigios, y

g) normas comunes de seguridad operativa.

▼M1

5. Los Estados miembros llevarán a cabo revisiones *inter pares* de los sistemas de identificación electrónica incluidos en el ámbito de aplicación del presente Reglamento y que habrán de notificarse en virtud del artículo 9, apartado 1, letra a).

6. A más tardar el 18 de marzo de 2025, la Comisión fijará, mediante actos de ejecución, las modalidades de procedimiento necesarias para las revisiones *inter pares* mencionadas en el apartado 5 del presente artículo, con vistas a fomentar un alto grado de confianza y seguridad que corresponda al nivel de riesgo. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

———————

8. A más tardar el 18 de septiembre de 2025, a efectos de establecer condiciones uniformes para la ejecución de los requisitos del apartado 1 del presente artículo, la Comisión, sin perjuicio de los criterios establecidos en el apartado 3 del presente artículo y teniendo en cuenta los resultados de la cooperación entre Estados miembros, adoptará actos de ejecución sobre el marco de interoperabilidad tal como se establece en el apartado 4 del presente artículo. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

▼B

9. Los actos de ejecución a que se refieren los apartados 7 y 8 del presente artículo se adoptarán de conformidad con el procedimiento de examen contemplado en el artículo 48, apartado 2.

▼M1

Artículo 12 bis

Certificación de los sistemas de identificación electrónica

1. La certificación de la conformidad de los sistemas de identificación electrónica que vayan a notificarse con los requisitos de ciberseguridad establecidos en el presente Reglamento, incluida la conformidad con los requisitos pertinentes en materia de ciberseguridad establecidos en el artículo 8, apartado 2, en relación con los niveles de seguridad de los sistemas de identificación electrónica, correrá a cargo de organismos de evaluación de la conformidad designados por los Estados miembros.

▼M1

2. La certificación en virtud del apartado 1 del presente artículo se realizará con arreglo a un esquema de certificación de la ciberseguridad en virtud del Reglamento (UE) 2019/881 o partes de dicho esquema, en la medida en que el certificado de ciberseguridad o partes de este abarquen dichos requisitos de ciberseguridad.

3. La certificación en virtud del apartado 1 tendrá una validez de hasta cinco años, siempre que se realice una evaluación de la vulnerabilidad cada dos años. Cuando se detecte una vulnerabilidad y no se subsane en un plazo de tres meses desde dicha detección, se cancelará la certificación.

4. No obstante lo dispuesto en el apartado 2, los Estados miembros podrán solicitar, de conformidad con dicho apartado, información adicional al Estado miembro que efectúa la notificación sobre los sistemas de identificación electrónica, o parte de ellos, certificados.

5. La revisión *inter pares* de los sistemas de identificación electrónica a que se refiere el artículo 12, apartado 5, no se aplicará a sistemas de identificación electrónica, ni a partes de ellos, certificados de conformidad con el apartado 1 del presente artículo. Los Estados miembros podrán utilizar un certificado o una declaración de conformidad, expedida con arreglo a un esquema de certificación pertinente o partes de dichos esquemas, con los requisitos que no estén relacionados con la ciberseguridad establecidos en el artículo 8, apartado 2, en relación con el nivel de seguridad de los sistemas de identificación electrónica.

6. Los Estados miembros comunicarán a la Comisión los nombres y direcciones de los organismos de evaluación de la conformidad a que se refiere el apartado 1. La Comisión pondrá dicha información a disposición de todos los Estados miembros.

Artículo 12 ter

Acceso a características de equipo y programa informático

Cuando los proveedores de carteras europeas de identidad digital y los emisores de los medios de identificación electrónica notificados que actúen a título comercial o profesional y utilicen servicios básicos de plataforma según se definen en el artículo 2, punto 2, del Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo ([1]), con el fin de ofrecer servicios de cartera europea de identidad digital y medios de identificación electrónica a usuarios finales, o en el marco de tal prestación, sean usuarios profesionales según se define en el artículo 2, apartado 21, de dicho Reglamento, los guardianes de acceso les permitirán, en particular, la interoperabilidad efectiva con las mismas características de sistema operativo, de equipo y o programa informático, así como el acceso a dichas características a efectos de interoperabilidad. La interoperabilidad efectiva y el acceso se permitirán de forma gratuita y con independencia de que las características de equipo y programa informático formen parte del sistema operativo, a las que puede acceder o que utiliza el guardián de acceso cuando presta tales servicios, en el sentido del artículo 6, apartado 7, del Reglamento (UE) 2022/1925. El presente artículo se entenderá sin perjuicio de lo dispuesto en el artículo 5 *bis*, apartado 14, del presente Reglamento.

([1]) Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo, de 14 de septiembre de 2022, sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento de Mercados Digitales) (DO L 265 de 12.10.2022, p. 1).

▼B

CAPÍTULO III

SERVICIOS DE CONFIANZA

SECCIÓN 1

Disposiciones generales

Artículo 13

Responsabilidad y carga de la prueba

▼M1

1. No obstante lo dispuesto en el apartado 2 del presente artículo y sin perjuicio del Reglamento (UE) 2016/679, los prestadores de servicios de confianza serán responsables de los perjuicios causados de forma intencional o por negligencia a cualquier persona física o jurídica debido al incumplimiento de las obligaciones establecidas en el presente Reglamento. Toda persona física o jurídica que haya sufrido perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento por parte de un prestador de servicios de confianza tendrá derecho a solicitar una indemnización de conformidad con el Derecho de la Unión y nacional.

La carga de la prueba de la intencionalidad o la negligencia de un prestador no cualificado de servicios de confianza corresponderá a la persona física o jurídica que alegue los perjuicios a que se refiere el párrafo primero.

Se presumirá la intencionalidad o la negligencia de un prestador cualificado de servicios de confianza salvo cuando ese prestador cualificado de servicios de confianza demuestre que los perjuicios a que se refiere el párrafo primero se produjeron sin intencionalidad ni negligencia por su parte.

▼B

2. Cuando un prestador de servicios informe debidamente a sus clientes con antelación sobre las limitaciones de la utilización de los servicios que presta y estas limitaciones sean reconocibles para un tercero, el prestador de servicios de confianza no será responsable de los perjuicios producidos por una utilización de los servicios que vaya más allá de las limitaciones indicadas.

3. Los apartados 1 y 2 se aplicarán con arreglo a las normas nacionales sobre responsabilidad.

▼M1

Artículo 14

Aspectos internacionales

1. Los servicios de confianza prestados por prestadores de servicios de confianza establecidos en un tercer país o por una organización internacional serán reconocidos como legalmente equivalentes a los servicios de confianza cualificados prestados por prestadores cualificados de servicios de confianza establecidos en la Unión si los servicios de confianza originarios del tercer país o los de la organización internacional son reconocidos mediante actos de ejecución o un acuerdo celebrado entre la Unión y el tercer país o la organización internacional en virtud del artículo 218 del TFUE.

Los actos de ejecución a que se refiere el párrafo primero se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 48, apartado 2.

▼M1

2. Los actos de ejecución y los acuerdos a que se refiere el apartado 1 garantizarán que los prestadores de servicios de confianza del tercer país de que se trate o las organizaciones internacionales y los servicios de confianza que prestan cumplen los requisitos aplicables a los prestadores cualificados de servicios de confianza establecidos en la Unión y a los servicios de confianza cualificados que prestan. En particular, los terceros países y las organizaciones internacionales establecerán, mantendrán y publicarán una lista de confianza de los prestadores reconocidos de servicios de confianza.

3. Los acuerdos a que se refiere el apartado 1 garantizarán que los servicios de confianza cualificados prestados por prestadores cualificados de servicios de confianza establecidos en la Unión sean reconocidos como legalmente equivalentes a los servicios de confianza prestados por prestadores de servicios en el tercer país o por la organización internacional con los que se celebra el acuerdo.

Artículo 15

Accesibilidad para las personas con discapacidad y necesidades especiales

La provisión de medios de identificación electrónica, así como la prestación de servicios de confianza y los productos destinados a los usuarios finales empleados en la prestación de dichos servicios, deberán estar disponibles en un lenguaje claro y comprensible, de conformidad con la Convención de las Naciones Unidas sobre los Derechos de las Personas con Discapacidad y con los requisitos de accesibilidad de la Directiva (UE) 2019/882, beneficiando así también a las personas que experimentan limitaciones funcionales, como las personas de edad avanzada y las personas con un acceso limitado a las tecnologías digitales.

Artículo 16

Sanciones

1. Sin perjuicio de lo dispuesto en el artículo 31 de la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo ([1]), los Estados miembros establecerán el régimen de sanciones aplicables a las infracciones del presente Reglamento. Dichas sanciones serán efectivas, proporcionadas y disuasorias.

2. Los Estados miembros garantizarán que el incumplimiento del presente Reglamento por parte de prestadores cualificados y no cualificados de servicios de confianza se sancione con multas administrativas de un máximo de, al menos:

a) 5 000 000 EUR cuando el prestador de servicios de confianza sea una persona física, o

b) 5 000 000 EUR o una cuantía equivalente al 1 % del volumen de negocios anual total a nivel mundial de la empresa a la que perteneciera el prestador de servicios de confianza durante el ejercicio financiero anterior al año en que se haya producido el incumplimiento, optándose por la de mayor cuantía, cuando el prestador de servicios de confianza sea una persona jurídica.

([1]) Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2) (DO L 333 de 27.12.2022, p. 80).

▼M1

3. En función del ordenamiento jurídico de los Estados miembros, las normas relativas a las multas administrativas podrán aplicarse de tal modo que la incoación de la multa corresponda al organismo de supervisión competente, y su imposición a los órganos jurisdiccionales nacionales competentes. La aplicación de tales normas en estos Estados miembros garantizará que estas vías de recurso sean efectivas y tengan un efecto equivalente a las multas administrativas impuestas directamente por las autoridades de control.

▼B

SECCIÓN 2

▼M1

Servicios de confianza no cualificados

———————

▼B

Artículo 19

Requisitos de seguridad aplicables a los prestadores de servicios de confianza

1. Los prestadores cualificados y no cualificados de servicios de confianza adoptarán las medidas técnicas y organizativas adecuadas para gestionar los riesgos para la seguridad de los servicios de confianza que prestan. Habida cuenta de los últimos avances tecnológicos, dichas medidas garantizarán un nivel de seguridad proporcionado al grado de riesgo. En particular, se adoptarán medidas para evitar y reducir al mínimo el impacto de los incidentes de seguridad e informar a los interesados de los efectos negativos de cualquiera de tales incidentes.

2. Los prestadores cualificados y no cualificados de servicios de confianza, sin demoras indebidas pero en cualquier caso en un plazo de 24 horas tras tener conocimiento de ellas, notificarán al organismo de supervisión y, en caso pertinente, ►C2 a otros organismos relevantes ◄ como el organismo nacional competente en materia de seguridad de la información, o 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.

Cuando la violación de seguridad o la pérdida de integridad puedan atentar contra una persona física o jurídica a la que se ha prestado el servicio de confianza, el prestador de servicios de confianza notificará también a la persona física o jurídica, sin demora indebida, la violación de seguridad o la pérdida de integridad.

Cuando proceda, en particular si una violación de la seguridad o pérdida de la integridad afecta a dos o más Estados miembros, el organismo de supervisión notificado informará al respecto a los organismos de supervisión de los demás Estados miembros de que se trate y a la ENISA.

El organismo de supervisión notificado informará al público o exigirá al prestador de servicios de confianza que lo haga, en caso de considerar que la divulgación de la violación de seguridad o la pérdida de integridad reviste interés público.

▼B

3. El organismo de supervisión facilitará a la ENISA anualmente un resumen de las notificaciones de violación de la seguridad y pérdida de la integridad recibidas de los prestadores de servicios de confianza.

4. La Comisión podrá, mediante actos de ejecución, establecer:

a) una mayor especificación de las medidas a que se refiere el apartado 1, y

b) la definición de los formatos y procedimientos, incluidos los plazos, aplicables a efectos del apartado 2.

Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

▼M1

Artículo 19 bis

Requisitos aplicables a los prestadores no cualificados de servicios de confianza

1. Los prestadores no cualificados de servicios de confianza que prestan servicios de confianza no cualificados:

a) contarán con políticas adecuadas y adoptarán las medidas que procedan para gestionar los riesgos jurídicos, empresariales, operativos y otros riesgos directos o indirectos para la prestación del servicio de confianza no cualificado que, no obstante lo dispuesto en el artículo 21de la Directiva (UE) 2022/2555, deberá incluir, como mínimo, las medidas relacionadas con:

   i) procedimientos de registro para un servicio de confianza e incorporación a este,

   ii) controles administrativos o de procedimiento necesarios para prestar servicios de confianza,

   iii) gestión e implantación de servicios de confianza;

b) notificarán al organismo de supervisión, a las personas afectadas identificables, al público si es de interés público y, cuando proceda, a otras autoridades competentes pertinentes cualquier violación de la seguridad o interrupción en la prestación del servicio o en la aplicación de las medidas a que se refiere la letra a), incisos i), ii) o iii), que tenga un impacto significativo en el servicio de confianza prestado o en los datos personales mantenidos en él, sin dilación indebida y, en cualquier caso, a más tardar a las veinticuatro horas de haber tenido conocimiento de cualquier violación de la seguridad o interrupción.

2. A más tardar el 21 de mayo de 2025, la Comisión establecerá, mediante actos de ejecución, una lista de normas de referencia y, en su caso, establecerá las especificaciones y los procedimientos para el apartado 1, letra a), del presente artículo. Se presumirá el cumplimiento de los requisitos establecidos en el presente artículo cuando se observen dichos procedimientos, especificaciones y normas. Los actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

▼B

SECCIÓN 3

Servicios de confianza cualificados

Artículo 20

Supervisión de los prestadores cualificados de servicios de confianza

▼M1

1. Los prestadores cualificados de servicios de confianza serán auditados al menos cada veinticuatro meses, corriendo con los gastos que ello genere, por un organismo de evaluación de la conformidad. La auditoría confirmará que tanto los prestadores cualificados de servicios de confianza como los servicios de confianza cualificados que prestan cumplen los requisitos establecidos en el presente Reglamento y en el artículo 21 de la Directiva (UE) 2022/2555. Los prestadores cualificados de servicios de confianza enviarán el informe de evaluación de la conformidad correspondiente al organismo de supervisión en el plazo de tres días hábiles tras su recepción.

1 *bis*. Los prestadores cualificados de servicios de confianza informarán al organismo de supervisión al menos un mes antes de cualquier auditoría prevista y permitirán la participación del organismo de supervisión en calidad de observador.

1 *ter*. Los Estados miembros notificarán a la Comisión, sin dilación indebida, los nombres, direcciones y datos de acreditación de los organismos de evaluación de la conformidad a que se refiere el apartado 1, así como cualquier modificación posterior de los mismos. La Comisión pondrá dicha información a disposición de todos los Estados miembros.

2. Sin perjuicio de lo dispuesto en el apartado 1, el organismo de supervisión podrá en cualquier momento auditar o solicitar a un organismo de evaluación de la conformidad que realice una evaluación de la conformidad de prestadores cualificados de servicios de confianza, con cargo a dichos prestadores cualificados de servicios de confianza, para confirmar que estos y los servicios de confianza cualificados prestados cumplen los requisitos establecidos en el presente Reglamento. En caso de posible vulneración de las normas sobre protección de datos personales, el organismo de supervisión informará, sin dilación indebida, a las autoridades de control competentes establecidas en virtud del artículo 51 del Reglamento (UE) 2016/679.

3. Cuando el prestador cualificado de servicios de confianza incumpla cualquiera de los requisitos que se establecen en el presente Reglamento, el organismo de supervisión le exigirá subsanar dicho incumplimiento dentro de un plazo determinado, si procede.

Si el prestador no subsanase el incumplimiento, en su caso, dentro del plazo fijado por el organismo de supervisión, este, cuando esté justificado en particular por el alcance, la duración y las consecuencias del incumplimiento, retirará la cualificación a dicho prestador o al servicio en cuestión que este presta.

3 *bis*. Cuando las autoridades competentes designadas o establecidas en virtud del artículo 8, apartado 1, de la Directiva (UE) 2022/2555 informen al organismo de supervisión de que el prestador cualificado de servicios de confianza incumple alguno de los requisitos establecidos en el artículo 21 de dicha Directiva, el organismo de supervisión, cuando esté justificado en particular por el alcance, la duración y las consecuencias del incumplimiento, retirará la cualificación a dicho prestador o al servicio en cuestión que este presta.

▼M1

3 *ter*. Cuando las autoridades de control establecidas en virtud del artículo 51 del Reglamento (UE) 2016/679 informen al organismo de supervisión de que el prestador cualificado de servicios de confianza incumple alguno de los requisitos establecidos en dicho Reglamento, el organismo de supervisión, cuando esté justificado en particular por el alcance, la duración y las consecuencias del incumplimiento, retirará la cualificación a dicho prestador o al servicio en cuestión que este presta.

3 *quater*. El organismo de supervisión comunicará al prestador cualificado de servicios de confianza la retirada de su cualificación o de la cualificación del servicio de que se trate. El organismo de supervisión informará al organismo notificado con arreglo al artículo 22, apartado 3, del presente Reglamento a efectos de actualizar las listas de confianza a que se refiere el apartado 1 de dicho artículo y a la autoridad competente designada o establecida en virtud del artículo 8, apartado 1, de la Directiva (UE) 2022/2555.

4. A más tardar el 21 de mayo de 2025, la Comisión establecerá, mediante actos de ejecución, una lista de normas de referencia y, en su caso, especificaciones y procedimientos para lo siguiente:

a) la acreditación de los organismos de evaluación de la conformidad y el informe de evaluación de la conformidad a que se refiere el apartado 1;

b) los requisitos de auditoría con arreglo a los cuales los organismos de evaluación de la conformidad realizarán la evaluación de la conformidad, incluida la evaluación compuesta, de los prestadores cualificados de servicios de confianza a que se refiere el apartado 1;

c) los sistemas de evaluación de la conformidad que utilizarán los organismos de evaluación de la conformidad para evaluar la conformidad de los prestadores cualificados de servicios de confianza y para proporcionar el informe a que se refiere el apartado 1.

Los actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

▼B

Artículo 21

Inicio de un servicio de confianza cualificado

▼M1

1. Cuando los prestadores de servicios de confianza tengan intención de iniciar la prestación de un servicio de confianza cualificado, notificarán al organismo de supervisión su intención junto con un informe de evaluación de la conformidad expedido por un organismo de evaluación de la conformidad que confirme el cumplimiento de los requisitos establecidos en el presente Reglamento y en el artículo 21 de la Directiva (UE) 2022/2555.

2. El organismo de supervisión verificará si el prestador de servicios de confianza y los servicios de confianza que presta cumplen los requisitos establecidos en el presente Reglamento, y en particular, los requisitos aplicables a los prestadores cualificados de servicios de confianza y a los servicios de confianza cualificados que estos prestan.

▼M1

Con el fin de verificar que el prestador de servicios de confianza cumple los requisitos establecidos en el artículo 21 de la Directiva (UE) 2022/2555, el organismo de supervisión solicitará a las autoridades competentes designadas o establecidas en virtud del artículo 8, apartado 1, de dicha Directiva que emprendan acciones de supervisión en ese sentido y que proporcionen información sobre los resultados de dichas acciones sin dilación indebida y en cualquier caso en el plazo de dos meses desde la recepción de dicha solicitud. Si la verificación no ha concluido en el plazo de dos meses desde la notificación, dichas autoridades competentes informarán al organismo de supervisión especificando los motivos de la dilación y el plazo previsto para concluir la verificación.

Si el organismo de supervisión concluye que el prestador de servicios de confianza y los servicios de confianza que este presta cumplen los requisitos establecidos en el presente Reglamento, el organismo de supervisión concederá la cualificación al prestador de servicios de confianza y a los servicios de confianza que este presta y lo comunicará al organismo a que se refiere el artículo 22, apartado 3, a efectos de actualizar las listas de confianza previstas en el artículo 22, apartado 1, a más tardar tres meses después de la notificación efectuada de conformidad con el apartado 1 del presente artículo.

Si la verificación no ha concluido en el plazo de tres meses desde la notificación, el organismo de supervisión informará al prestador de servicios de confianza especificando los motivos de la dilación y el plazo previsto para concluir la verificación.

▼B

3. Los prestadores cualificados de servicios de confianza podrán comenzar a prestar el servicio de confianza cualificado una vez que la cualificación haya sido indicada en las listas de confianza a que se refiere el artículo 22, apartado 1.

▼M1

4. A más tardar el 21 de mayo de 2025, la Comisión establecerá, mediante actos de ejecución, los formatos y procedimientos de la notificación y la verificación a efectos de lo dispuesto en los apartados 1 y 2 del presente artículo. Los actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

▼B

Artículo 22

Listas de confianza

1. Cada Estado miembro establecerá, mantendrá y publicará listas de confianza con información relativa a los prestadores cualificados de servicios de confianza con respecto a los cuales sea responsable, junto con la información relacionada con los servicios de confianza cualificados prestados por ellos.

2. Los Estados miembros establecerán, mantendrán y publicarán, de manera segura, las listas de confianza firmadas o selladas electrónicamente a que se refiere el apartado 1 en una forma apropiada para el tratamiento automático.

3. Los Estados miembros notificarán a la Comisión, sin retrasos indebidos, información sobre el organismo responsable del establecimiento, mantenimiento y publicación de las listas de confianza nacionales, y detalles relativos al lugar en que se publican dichas listas, los certificados utilizados para firmar o sellar las listas de confianza y cualquier modificación de los mismos.

▼B

4. La Comisión pondrá a disposición del público, a través de un canal seguro, la información a que se refiere el apartado 3 en una forma firmada o sellada electrónicamente apropiada para el tratamiento automático.

5. A más tardar el 18 de septiembre de 2015 la Comisión, mediante actos de ejecución, especificará la información a que se refiere el apartado 1 y definirá las especificaciones técnicas y formatos de las listas de confianza, aplicables a efectos de los apartados 1 a 4. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

Artículo 23

Etiqueta de confianza «UE» para servicios de confianza cualificados

1. Una vez que la cualificación a que se refiere el artículo 21, apartado 2, párrafo segundo, se haya incluido en la lista de confianza a que se refiere el artículo 22, apartado 1, los prestadores cualificados de los servicios de confianza podrán usar la etiqueta de confianza «UE» para indicar de manera simple, reconocible y clara los servicios de confianza cualificados que prestan.

2. Al utilizar la etiqueta de confianza «UE» para los servicios de confianza cualificados a que se refiere el apartado 1, los prestadores de los servicios de confianza garantizarán que en su sitio web exista un enlace a la lista de confianza pertinente.

3. A más tardar el 1 de julio de 2015 la Comisión, por medio de actos de ejecución, elaborará especificaciones relativas a la forma y en particular la presentación, composición, tamaño y diseño de la etiqueta de confianza «UE» para servicios de confianza cualificados. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

Artículo 24

Requisitos para los prestadores cualificados de servicios de confianza

▼M1

1. Al expedir un certificado cualificado o una declaración electrónica cualificada de atributos, el prestador cualificado de servicios de confianza verificará la identidad y, si procede, cualquier atributo específico de la persona física o jurídica a la que se expida el certificado cualificado o la declaración electrónica cualificada de atributos.

1 *bis*. La verificación de la identidad a que se refiere el apartado 1 se llevará a cabo por los medios adecuados, por el prestador cualificado de servicios de confianza, bien directamente o bien por medio de un tercero, sobre la base de uno de los siguientes métodos o de una combinación de los mismos cuando sea necesario de conformidad con los actos de ejecución a que se refiere el apartado 1 *quater*:

a) a través de la cartera europea de identidad digital o de un medio de identificación electrónica notificado que satisfaga los requisitos establecidos en el artículo 8 con respecto al nivel de seguridad alto;

b) por medio de un certificado de una firma electrónica cualificada o de un sello electrónico cualificado expedido de conformidad con la letra a), c) o d);

▼M1

c) utilizando otros métodos de identificación que garanticen la identificación de la persona con un nivel alto de confianza, cuya conformidad será confirmada por un organismo de evaluación de la conformidad;

d) a través de la presencia física de la persona física o de un representante autorizado de la persona jurídica, mediante pruebas y procedimientos adecuados, de conformidad con el Derecho nacional.

1 *ter*. La verificación de los atributos a que se refiere el apartado 1 se llevará a cabo, por los medios adecuados, por el prestador cualificado de servicios de confianza, bien directamente o bien por medio de un tercero, sobre la base de uno de los siguientes métodos o, cuando sea necesario, de una combinación de estos, de conformidad con los actos de ejecución a que se refiere el apartado 1 *quater*:

a) a través de la cartera europea de identidad digital o de un medio de identificación electrónica notificado que satisfaga los requisitos establecidos en el artículo 8 con respecto al nivel de seguridad alto;

b) por medio de un certificado de una firma electrónica cualificada o de un sello electrónico cualificado expedido de conformidad con el apartado 1 *bis*, letra a), c) o d);

c) por medio de una declaración electrónica cualificada de atributos;

d) utilizando otros métodos que garanticen la verificación de los atributos con un nivel alto de confianza, cuya conformidad será confirmada por un organismo de evaluación de la conformidad;

e) mediante la presencia física de la persona física o de un representante autorizado de la persona jurídica, mediante pruebas y procedimientos adecuados, de conformidad con el Derecho nacional.

«1 *quater*. A más tardar el 21 de mayo de 2025, la Comisión establecerá, mediante actos de ejecución, una lista de normas de referencia y, en su caso, establecerá las especificaciones y los procedimientos para la verificación de la identidad y los atributos de conformidad con los apartados 1, 1 *bis* y 1 *ter* del presente artículo. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 48, apartado 2.»;

▼B

2. Los prestadores cualificados de servicios de confianza que prestan servicios de confianza cualificados:

▼M1

a) informarán al organismo de supervisión de cualquier cambio en la prestación de servicios de confianza cualificados al menos un mes antes de llevarlo a cabo, y con una antelación de al menos tres meses en caso de que tengan intención de cesar tales actividades;

▼B

b) contarán con personal y, si procede, con subcontratistas, que posean los conocimientos especializados, la fiabilidad, la experiencia y las cualificaciones necesarios y hayan recibido la formación adecuada en materia de seguridad y normas de protección de datos personales y que apliquen procedimientos administrativos y de gestión que correspondan a normas europeas o internacionales;

c) con respecto al riesgo de la responsabilidad por daños y perjuicios de conformidad con el artículo 13, mantendrán recursos financieros suficientes u obtendrán pólizas de seguros de responsabilidad adecuadas, de conformidad con la legislación nacional;

▼M1

d) antes de entrar en una relación contractual, informarán, de manera clara, comprensible y fácilmente accesible, en un espacio públicamente accesible y de forma individual, a cualquier persona que desee utilizar un servicio de confianza cualificado acerca de las condiciones precisas relativas a la utilización de dicho servicio, incluidas las limitaciones de su utilización;

e) utilizarán sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad y la fiabilidad técnicas de los procesos que sustenten, en particular utilizando técnicas criptográficas adecuadas;

▼B

f) utilizarán sistemas fiables para almacenar los datos que se les faciliten de forma verificable, de modo que:

i) estén a disposición del público para su recuperación solo cuando se haya obtenido el consentimiento de la persona a la que corresponden los datos,

ii) solo personas autorizadas puedan hacer anotaciones y modificaciones en los datos almacenados,

iii) pueda comprobarse la autenticidad de los datos;

▼M1

f *bis*) No obstante lo dispuesto en el artículo 21 de la Directiva (UE) 2022/2555, contarán con políticas adecuadas y adoptarán las medidas que procedan para gestionar los riesgos jurídicos, empresariales, operativos y otros riesgos directos o indirectos para la prestación del servicio de confianza cualificado, en particular al menos medidas relacionadas con lo siguiente:

i) procedimientos de registro en un servicio e incorporación a este,

ii) controles administrativos o de procedimiento,

iii) gestión e implantación de servicios;

f *ter*) notificarán al organismo de supervisión, a las personas afectadas identificables, a otros organismos competentes pertinentes cuando proceda y, a solicitud del organismo de supervisión, al público si es de interés público, cualquier violación de la seguridad o interrupción en la prestación del servicio o en la aplicación de las medidas a que se refiere la letra f *bis*), incisos i), ii) o iii), que tenga un impacto significativo en el servicio de confianza prestado o en los datos personales mantenidos en él, sin dilación indebida y, en cualquier caso, a más tardar veinticuatro horas después de haberse producido el incidente;

g) adoptarán medidas adecuadas contra la falsificación, el robo o la apropiación indebida de datos o contra la eliminación, alteración o bloqueo de dichos datos sin tener derecho a ello;

h) registrarán y mantendrán accesible, durante el tiempo que sea necesario cuando hayan cesado las actividades del prestador cualificado de servicios de confianza, toda la información pertinente referente a los datos expedidos y recibidos por el prestador cualificado de servicios de confianza, al objeto de que sirvan de prueba en los procedimientos legales y para garantizar la continuidad del servicio. Esta actividad de registro podrá realizarse por medios electrónicos;

▼M1

i) contarán con un plan de cese actualizado para garantizar la continuidad del servicio de conformidad con las disposiciones que sean verificadas por el organismo de supervisión en virtud del artículo 46 *ter*, apartado 4, letra i);

———————

▼B

k) en caso de los prestadores cualificados de servicios de confianza que expidan certificados cualificados, establecerán y mantendrán actualizada una base de datos de certificados.

▼M1

El organismo de supervisión podrá solicitar información adicional a la información notificada en virtud del párrafo primero, letra a), o el resultado de una evaluación de la conformidad y podrá condicionar la concesión de la autorización para aplicar los cambios previstos a los servicios de confianza cualificados. Si la verificación no ha concluido en el plazo de tres meses desde la notificación, el organismo de supervisión informará al prestador de servicios de confianza especificando los motivos de la dilación y el plazo previsto para concluir la verificación.

▼B

3. Cuando los prestadores cualificados de servicios de confianza que expidan certificados cualificados decidan revocar un certificado, registrarán su revocación en su base de datos de certificados y publicarán el estado de revocación del certificado oportunamente y, en todo caso, en un plazo de 24 horas después de la recepción de la solicitud. La revocación será efectiva inmediatamente después de su publicación.

4. Con respecto a lo dispuesto en el apartado 3, los prestadores cualificados de servicios de confianza que expidan certificados cualificados proporcionarán a cualquier parte usuaria información sobre el estado de validez o revocación de los certificados cualificados expedidos por ellos. Esta información deberá estar disponible al menos por cada certificado en cualquier momento y con posterioridad al período de validez del certificado en una forma automatizada que sea fiable, gratuita y eficiente.

▼M1

4 *bis*. Los apartados 3 y 4 se aplicarán, en consecuencia, a la revocación de declaraciones electrónicas cualificadas de atributos.

4 *ter*. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 47 por el que se establecen las medidas adicionales mencionadas en el apartado 2, punto f *bis*) del presente artículo.

5. A más tardar el 21 de mayo de 2025, la Comisión establecerá, mediante actos de ejecución, una lista de normas de referencia y, en su caso, establecerá las especificaciones y los procedimientos aplicables a los requisitos a que se refiere el apartado 2, del presente artículo. Se presumirá el cumplimiento de los requisitos establecidos en el presente apartado cuando se observen dichas normas, especificaciones y procedimientos. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

Artículo 24 bis

Reconocimiento de servicios de confianza cualificados

1. Las firmas electrónicas cualificadas basadas en un certificado cualificado expedido en un Estado miembro y los sellos electrónicos cualificados basados en un certificado cualificado expedido en un

▼M1

Estado miembro serán reconocidos, respectivamente, como firmas electrónicas cualificadas y sellos electrónicos cualificados en todos los demás Estados miembros.

2. Los dispositivos cualificados de creación de firma electrónica y los dispositivos cualificados de creación de sello electrónico certificados en un Estado miembro serán reconocidos, respectivamente, como dispositivos cualificados de creación de firma electrónica y dispositivos cualificados de creación de sello electrónico en todos los demás Estados miembros.

3. Un certificado cualificado de firma electrónica, un certificado cualificado de sello electrónico, un servicio de confianza cualificado para la gestión de dispositivos cualificados de creación de firma electrónica a distancia y un servicio de confianza cualificado para la gestión de dispositivos cualificados de creación de sello electrónico a distancia proporcionados en un Estado miembro serán reconocidos, respectivamente, como certificado cualificado de firma electrónica, certificado cualificado de sello electrónico, servicio de confianza cualificado para la gestión de dispositivos cualificados de creación de firma electrónica a distancia y servicio de confianza cualificado para la gestión de dispositivos cualificados de creación de sello electrónico a distancia en todos los demás Estados miembros.

4. Un servicio de validación cualificado de firmas electrónicas cualificadas y un servicio de validación cualificado de sellos electrónicos cualificados prestado en un Estado miembro serán reconocidos, respectivamente, como servicio de validación cualificado de firmas electrónicas cualificadas y servicio de validación cualificado de sellos electrónicos cualificados en todos los demás Estados miembros.

5. Un servicio cualificado de conservación de firmas electrónicas cualificadas y un servicio cualificado de conservación de sellos electrónicos cualificados prestados en un Estado miembro serán reconocidos, respectivamente, como servicio cualificado de conservación de firmas electrónicas cualificadas y servicio cualificado de conservación de sellos electrónicos cualificados en todos los demás Estados miembros.

6. Un sello cualificado de tiempo electrónico proporcionado en un Estado miembro será reconocido como sello cualificado de tiempo electrónico en todos los demás Estados miembros.

7. Un certificado cualificado de autenticación de sitio web expedido en un Estado miembro será reconocido como certificado cualificado de autenticación de sitio web en cualquier otro Estado miembro.

8. Un servicio cualificado de entrega electrónica certificada proporcionado en un Estado miembro será reconocido como servicio cualificado de entrega electrónica certificada en todos los demás Estados miembros.

9. Una declaración electrónica cualificada de atributos expedida en un Estado miembro será reconocida como declaración electrónica cualificada de atributos en todos los demás Estados miembros.

10. Un servicio cualificado de archivo electrónico prestado en un Estado miembro será reconocido como servicio cualificado de archivo electrónico en todos los demás Estados miembros.

▼M1

11. Un libro mayor electrónico cualificado proporcionado en un Estado miembro será reconocido como libro mayor electrónico cualificado en todos los demás Estados miembros.

▼B

SECCIÓN 4

Firma electrónica

Artículo 25

Efectos jurídicos de las firmas electrónicas

1. No se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a una firma electrónica por el mero hecho de ser una firma electrónica o porque no cumpla los requisitos de la firma electrónica cualificada.

2. Una firma electrónica cualificada tendrá un efecto jurídico equivalente al de una firma manuscrita.

▼M1

_____

▼B

Artículo 26

Requisitos para firmas electrónicas avanzadas

►M1 1. ◄ Una firma electrónica avanzada cumplirá los requisitos siguientes:

a) estar vinculada al firmante de manera única;

b) permitir la identificación del firmante;

c) haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo, y

d) estar vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable.

▼M1

2. A más tardar el 21 de mayo de 2026, la Comisión evaluará sobre si es necesario adoptar actos de ejecución para establecer una lista de normas de referencia y, en su caso, establecer especificaciones y procedimientos para firmas electrónicas avanzadas. Sobre la base de dicha evaluación, la Comisión puede adoptar tales actos de ejecución. Se presumirá el cumplimiento de los requisitos aplicables a las firmas electrónicas avanzadas cuando la firma electrónica avanzada sea conforme a dichos procedimientos, especificaciones y normas. Los actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

▼B

Artículo 27

Firmas electrónicas en servicios públicos

1. Si un Estado miembro requiere una firma electrónica avanzada con el fin de utilizar un servicio en línea ofrecido por un organismo del sector público, o en nombre del mismo, dicho Estado miembro

▼B

reconocerá las firmas electrónicas avanzadas, las firmas electrónicas avanzadas basadas en un certificado cualificado de firma electrónica y las firmas electrónicas cualificadas por lo menos en los formatos o con los métodos definidos en los actos de ejecución contemplados en el apartado 5.

2. Si un Estado miembro requiere una firma electrónica avanzada basada en un certificado cualificado con el fin de utilizar un servicio en línea ofrecido por un organismo del sector público, o en nombre del mismo, dicho Estado miembro reconocerá las firmas electrónicas avanzadas basadas en un certificado cualificado y las firmas electrónicas cualificadas por lo menos en los formatos o con los métodos definidos en los actos de ejecución contemplados en el apartado 5.

3. Los Estados miembros no exigirán para la utilización transfronteriza de un servicio en línea ofrecido por un organismo del sector público una firma electrónica cuyo nivel de garantía de la seguridad sea superior al de una firma electrónica cualificada.

▼M1

_____

▼B

5. A más tardar el 18 de septiembre de 2015, y teniendo en cuenta las prácticas, normas y actos jurídicos de la Unión existentes, la Comisión, mediante actos de ejecución, definirá los formatos de referencia de las firmas electrónicas avanzadas o métodos de referencia cuando se utilicen formatos alternativos. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

Artículo 28

Certificados cualificados de firma electrónica

1. Los certificados cualificados de firma electrónica cumplirán los requisitos establecidos en el anexo I.

2. Los certificados cualificados de firma electrónica no estarán sometidos a ningún requisito obligatorio que exceda de los requisitos establecidos en el anexo I.

3. Los certificados cualificados de firmas electrónicas podrán incluir atributos específicos adicionales no obligatorios. Esos atributos no afectarán a la interoperabilidad y el reconocimiento de las firmas electrónicas cualificadas.

4. Si un certificado cualificado de firma electrónica ha sido revocado después de su activación inicial, perderá su validez desde el momento de su revocación y no podrá en ninguna circunstancia recuperar su estado.

5. Según las condiciones que siguen, los Estados miembros podrán fijar normas nacionales sobre la suspensión temporal de certificados cualificados de firma electrónica:

a) Si un certificado cualificado de firma electrónica ha sido suspendido temporalmente, ese certificado perderá su validez durante el período de suspensión.

b) El período de suspensión se indicará claramente en la base de datos de certificados y el estado de suspensión será visible, durante el período de suspensión, a partir del servicio que proporcione la información sobre el estado del certificado.

▼M1

6. A más tardar el 21 de mayo de 2025, la Comisión establecerá, mediante actos de ejecución, una lista de normas de referencia y, en su caso, establecerá las especificaciones y los procedimientos para los certificados cualificados de firma electrónica. Se presumirá el cumplimiento de los requisitos establecidos en el anexo I cuando el certificado cualificado de firma electrónica sea conforme a dichos procedimientos, especificaciones y normas. Los actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

▼B

Artículo 29

Requisitos de los dispositivos cualificados de creación de firmas electrónicas

1. Los dispositivos cualificados de creación de firmas electrónicas cumplirán los requisitos establecidos en el anexo II.

▼M1

1 *bis*. La creación o la gestión de datos de creación de firma electrónica o la duplicación de estos datos de creación de firma con fines de copia de seguridad se llevará a cabo únicamente en nombre del firmante, a solicitud de este, y por un prestador cualificado de servicios de confianza que preste un servicio de confianza cualificado para la gestión de un dispositivo cualificado de creación de firma electrónica a distancia.

▼B

2. La Comisión podrá, mediante actos de ejecución, establecer números de referencia de normas relativas a los dispositivos cualificados de creación de firmas electrónicas. Se presumirá el cumplimiento de los requisitos establecidos en el anexo II cuando un dispositivo cualificado de creación de firmas electrónicas se ajuste a dichas normas. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

▼M1

Artículo 29 bis

Requisitos aplicables a un servicio cualificado para la gestión de dispositivos cualificados de creación de firma electrónica a distancia

1. La gestión de dispositivos cualificados de creación de firma electrónica a distancia como servicio cualificado se llevará a cabo únicamente por un prestador cualificado de servicios de confianza que:

a) cree o gestione datos de creación de firmas electrónicas en nombre del signatario;

b) no obstante lo dispuesto en el punto 1, letra d), del anexo II, duplique los datos de creación de firmas electrónicas exclusivamente con fines de copia de seguridad, siempre y cuando se cumplan los requisitos siguientes:

   i) la seguridad de los conjuntos de datos duplicados debe ser del mismo nivel que el previsto para los conjuntos de datos originales,

   ii) el número de conjuntos de datos duplicados no debe superar el mínimo necesario para garantizar la continuidad del servicio;

▼M1

c) cumpla todos los requisitos definidos en el informe de certificación del dispositivo cualificado específico de creación de firmas electrónicas a distancia expedido en virtud del artículo 30.

2. A más tardar el 21 de mayo de 2025, la Comisión establecerá, mediante actos de ejecución, una lista de normas de referencia y, en su caso, las especificaciones y los procedimientos a los efectos del apartado 1 del presente artículo. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

▼B

Artículo 30

Certificación de los dispositivos cualificados de creación de firmas electrónicas

1. La conformidad de los dispositivos cualificados de creación de firmas electrónicas con los requisitos que figuran en el anexo II será certificada por los organismos públicos o privados adecuados designados por los Estados miembros.

2. Los Estados miembros notificarán a la Comisión los nombres y direcciones de los organismos públicos o privados a que se refiere el apartado 1. La Comisión pondrá la información a disposición de los Estados miembros.

3. La certificación contemplada en el apartado 1 se basará en los elementos siguientes:

a) un proceso de evaluación de la seguridad llevado a cabo de conformidad con las normas para la evaluación de la seguridad de los productos de tecnología de la información incluidos en la lista que se establecerá de conformidad con el párrafo segundo, o

b) un proceso distinto del proceso contemplado en la letra a), con tal de que ese proceso haga uso de niveles de seguridad equivalentes y que los organismos públicos o privados a los que se refiere el apartado 1 notifiquen ese proceso a la Comisión. Podrá recurrirse a ese proceso únicamente a falta de las normas a que se refiere la letra a) o cuando esté en curso el proceso de evaluación de la seguridad a que se refiere la letra a).

La Comisión establecerá, por medio de actos de ejecución, la lista de las normas para la evaluación de la seguridad de los productos de tecnología de la información a que se refiere la letra a). Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

▼M1

3 *bis*. La certificación a que se refiere el apartado 1 tendrá una validez máxima de cinco años, siempre que se lleve a cabo una evaluación de las vulnerabilidades cada dos años. Cuando se detecten vulnerabilidades y no se subsanen, se cancelará la certificación.

▼B

4. La Comisión estará facultada para adoptar actos delegados, de conformidad con el artículo 47, en lo que respecta al establecimiento de criterios específicos que deben satisfacer los organismos designados a que se refiere el apartado 1 del presente artículo.

▼B

Artículo 31

Publicación de una lista de dispositivos cualificados de creación de firmas electrónicas certificados

1. Los Estados miembros comunicarán a la Comisión, sin retrasos indebidos y no más tarde de un mes después de que haya concluido la certificación, información sobre los dispositivos cualificados de creación de firmas electrónicas que hayan sido certificados por los organismos a que se refiere el artículo 30, apartado 1. También notificarán a la Comisión, sin retrasos indebidos y no más tarde de un mes después de que haya expirado la certificación, información sobre los dispositivos de creación de firmas electrónicas que hayan dejado de estar certificados.

2. Sobre la base de la información recibida, la Comisión establecerá, publicará y mantendrá una lista de dispositivos cualificados de creación de firmas electrónicas certificados.

▼M1

3. A más tardar el 21 de mayo de 2025, la Comisión establecerá, por medio de actos de ejecución, los formatos y procedimientos aplicables a efectos de lo dispuesto en el apartado 1 del presente artículo. Los actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

▼B

Artículo 32

Requisitos de la validación de las firmas electrónicas cualificadas

1. El proceso de validación de una firma electrónica cualificada confirmará la validez de una firma electrónica cualificada siempre que:

a) el certificado que respalda la firma fuera, en el momento de la firma, un certificado cualificado de firma electrónica que se ajusta al anexo I;

b) el certificado cualificado fuera emitido por un prestador de servicios de confianza y fuera válido en el momento de la firma;

c) los datos de validación de la firma corresponden a los datos proporcionados a la parte usuaria;

d) el conjunto único de datos que representa al firmante en el certificado se facilite correctamente a la parte usuaria;

e) en caso de que se utilice un seudónimo, la utilización del mismo se indique claramente a la parte usuaria en el momento de la firma;

f) la firma electrónica se haya creado mediante un dispositivo cualificado de creación de firmas electrónicas;

g) la integridad de los datos firmados no se haya visto comprometida;

h) se hayan cumplido los requisitos previstos en el artículo 26, en el momento de la firma.

▼M1

Se presumirá el cumplimiento de los requisitos establecidos en el párrafo primero del presente apartado cuando la validación de firmas electrónicas cualificadas sea conforme a las normas, las especificaciones y los procedimientos a que se refiere el apartado 3.

▼B

2. El sistema utilizado para validar la firma electrónica cualificada ofrecerá a la parte usuaria el resultado correcto del proceso de validación y le permitirá detectar cualquier problema que afecte a la seguridad.

▼M1

3. A más tardar el 21 de mayo de 2025, la Comisión establecerá, mediante actos de ejecución, una lista de normas de referencia y, en su caso, establecerá las especificaciones y los procedimientos para la validación de firmas electrónicas cualificadas. Los actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

Artículo 32 bis

Requisitos aplicables a la validación de las firmas electrónicas avanzadas basadas en certificados cualificados

1. El proceso de validación de una firma electrónica avanzada basada en un certificado cualificado confirmará la validez de dicha firma siempre que:

a) el certificado que respalda la firma fuera, en el momento de la firma, un certificado cualificado de firma electrónica que se ajusta al anexo I;

b) el certificado cualificado fuera expedido por un prestador cualificado de servicios de confianza y fuera válido en el momento de la firma;

c) los datos de validación de la firma correspondan a los datos proporcionados a la parte usuaria;

d) el conjunto único de datos que representa al firmante en el certificado se facilite correctamente a la parte usuaria;

e) en caso de que se utilice un seudónimo, la utilización de este se indique claramente a la parte usuaria en el momento de la firma;

f) la integridad de los datos firmados no se haya visto comprometida;

g) se hayan cumplido los requisitos previstos en el artículo 26 en el momento de la firma.

2. El sistema utilizado para validar la firma electrónica avanzada basada en un certificado cualificado ofrecerá a la parte usuaria el resultado correcto del proceso de validación y le permitirá detectar cualquier problema que afecte a la seguridad.

3. A más tardar el 21 de mayo de 2025, la Comisión establecerá, mediante actos de ejecución, una lista de normas de referencia y, en su caso, establecerá las especificaciones y los procedimientos para la validación de firmas electrónicas avanzadas basadas en certificados cualificados. Se presumirá el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo cuando la validación de firmas electrónicas avanzadas basadas en certificados cualificados sea conforme a dichos procedimientos, especificaciones y normas. Los actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

▼B

Artículo 33

Servicio de validación cualificado de firmas electrónicas cualificadas

1. Solo podrá prestar un servicio de validación cualificado de firmas electrónicas cualificadas el prestador cualificado de servicios de confianza que:

a) realice la validación de conformidad con el artículo 32, apartado 1, y

b) permita que las partes usuarias reciban el resultado del proceso de validación de una manera automatizada que sea fiable, eficiente e incluya la firma electrónica avanzada o el sello electrónico avanzado del prestador cualificado de servicio de validación.

▼M1

2. A más tardar el 21 de mayo de 2025, la Comisión establecerá, mediante actos de ejecución, una lista de normas de referencia y, en su caso, establecerá las especificaciones y los procedimientos aplicables al servicio de validación cualificado a que se refiere el apartado 1 del presente artículo. Se presumirá el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo cuando el servicio de validación cualificado para firmas electrónicas cualificadas sea conforme a dichos procedimientos, especificaciones y normas. Los actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

▼B

Artículo 34

Servicio cualificado de conservación de firmas electrónicas cualificadas

1. Solo podrá prestar un servicio cualificado de conservación de firmas electrónicas cualificadas el prestador cualificado de servicios de confianza que utilice procedimientos y tecnologías capaces de ampliar la fiabilidad de los datos de la firma electrónica cualificada más allá del período de validez tecnológico.

▼M1

1 *bis*. Se presumirá el cumplimiento de los requisitos establecidos en el apartado 1 cuando los mecanismos del servicio cualificado de conservación de firmas electrónicas cualificadas sean conformes a los procedimientos, las especificaciones y las normas a que se refiere el apartado 2.

2. A más tardar el 21 de mayo de 2025, la Comisión establecerá, mediante actos de ejecución, una lista de normas de referencia y, en su caso, establecerá las especificaciones y los procedimientos para los mecanismos del servicio cualificado de conservación de firmas electrónicas cualificadas. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 48, apartado 2.

▼B

SECCIÓN 5

Sellos electrónicos

Artículo 35

Efectos jurídicos del sello electrónico

1. No se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a un sello electrónico por el mero hecho de estar en formato electrónico o de no cumplir los requisitos del sello electrónico cualificado.

2. Un sello electrónico cualificado disfrutará de la presunción de integridad de los datos y de la corrección del origen de los datos a los que el sello electrónico cualificado esté vinculado.

▼M1

_____

▼B

Artículo 36

Requisitos para los sellos electrónicos avanzados

►M1 1. ◄ Un sello electrónico avanzado cumplirá los requisitos siguientes:

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

b) permitir la identificación del creador del sello;

▼C1

c) haber sido creado utilizando datos de creación del sello electrónico que el creador del sello puede utilizar para la creación de un sello electrónico, con un alto nivel de confianza, bajo su control, y

▼B

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

▼M1

2. A más tardar el 21 de mayo de 2026, la Comisión realizará una evaluación sobre si es necesario adoptar actos de ejecución para establecer una lista de normas de referencia y, en su caso, establecer especificaciones y procedimientos para sellos electrónicos avanzados. Sobre la base de dicha evaluación, la Comisión puede adoptar dichos actos de ejecución. Se presumirá el cumplimiento de los requisitos aplicables a los sellos electrónicos avanzados cuando el sello electrónico avanzado sea conforme a dichos procedimientos, especificaciones y normas. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

▼B

Artículo 37

Sellos electrónicos en servicios públicos

1. Si un Estado miembro requiere un sello electrónico avanzado con el fin de utilizar un servicio en línea ofrecido por un organismo del sector público, o en nombre del mismo, dicho Estado miembro reconocerá los sellos electrónicos avanzados, los sellos electrónicos avanzados basados en un certificado reconocido de sellos electrónicos y los sellos electrónicos cualificados por lo menos en los formatos o con los métodos definidos en los actos de ejecución contemplados en el apartado 5.

▼B

2. Si un Estado miembro requiere un sello electrónico avanzado basado en un certificado cualificado con el fin de utilizar un servicio en línea ofrecido por un organismo del sector público, o en nombre del mismo, dicho Estado miembro reconocerá los sellos electrónicos avanzados basados en un certificado cualificado y los sellos electrónicos cualificados por lo menos en los formatos o con los métodos definidos en los actos de ejecución contemplados en el apartado 5.

3. Los Estados miembros no exigirán, para el uso transfronterizo en un servicio en línea ofrecido por un organismo del sector público, un sello electrónico cuyo nivel de seguridad sea superior al de un sello electrónico cualificado.

▼M1

_____

▼B

5. A más tardar el 18 de septiembre de 2015, y teniendo en cuenta las prácticas existentes, las normas y actos jurídicos de la Unión, la Comisión adoptará actos de ejecución que definan los formatos de referencia de los sellos electrónicos avanzados o métodos de referencia cuando se utilicen formatos alternativos. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

Artículo 38

Certificados cualificados de sello electrónico

1. Los certificados cualificados de sello electrónico cumplirán los requisitos establecidos en el anexo III.

2. Los certificados cualificados de sello electrónico no estarán sometidos a ningún requisito obligatorio que exceda de los requisitos establecidos en el anexo III.

3. Los certificados cualificados de sello electrónico podrán incluir atributos específicos adicionales no obligatorios. Esos atributos no afectarán a la interoperabilidad y reconocimiento de los sellos electrónicos cualificados.

4. Si un certificado cualificado de sello electrónico ha sido revocado después de su activación inicial, perderá su validez desde el momento de su revocación y no podrá en ninguna circunstancia recuperar su estado.

5. Según las condiciones expuestas a continuación, los Estados miembros podrán fijar normas nacionales sobre la suspensión temporal de certificados cualificados de sello electrónico:

a) Si un certificado cualificado de sello electrónico ha sido suspendido temporalmente, ese certificado perderá su validez durante el período de suspensión.

b) El período de suspensión se indicará claramente en la base de datos de certificados y el estado de suspensión será visible, durante el período de suspensión, a partir del servicio que proporcione la información sobre el estado del certificado.

▼M1

6. A más tardar el 21 de mayo de 2025, la Comisión establecerá, mediante actos de ejecución, una lista de normas de referencia y, en su caso, establecerá las especificaciones y los procedimientos para los certificados cualificados de sello electrónico. Se presumirá el cumplimiento de los requisitos establecidos en el anexo III cuando el certificado cualificado de sello electrónico sea conforme a dichos procedimientos, especificaciones y normas. Los actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

▼B

Artículo 39

Dispositivos cualificados de creación de sello electrónico

1. El artículo 29 se aplicará *mutatis mutandis* a los requisitos de los dispositivos cualificados de creación de sello electrónico.

2. El artículo 30 se aplicará *mutatis mutandis* a la certificación de los dispositivos cualificados de creación de sello electrónico.

3. El artículo 31 se aplicará *mutatis mutandis* a la publicación de una lista de dispositivos cualificados de creación de sello electrónico certificados.

▼M1

Artículo 39 bis

Requisitos aplicables a un servicio cualificado para la gestión de dispositivos cualificados de creación de sello electrónico a distancia

El artículo 29 *bis* se aplicará *mutatis mutandis* a los servicios cualificados para la gestión de dispositivos cualificados de creación de sello electrónico a distancia.

▼B

Artículo 40

Validación y conservación de sellos electrónicos cualificados

Los artículos 32, 33 y 34 se aplicarán *mutatis mutandis* a la validación y conservación de los sellos electrónicos cualificados.

▼M1

Artículo 40 bis

Requisitos aplicables a la validación de los sellos electrónicos avanzados basados en certificados cualificados

El artículo 32 *bis* se aplicará *mutatis mutandi*s a la validación de los sellos electrónicos avanzados basados en certificados cualificados.

▼B

SECCIÓN 6

Sello de tiempo electrónico

Artículo 41

Efecto jurídico de los sellos de tiempo electrónicos

1. No se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a un sello de tiempo electrónico por el mero hecho de estar en formato electrónico o de no cumplir los requisitos de sello cualificado de tiempo electrónico.

2. Los sellos cualificados de tiempo electrónicos disfrutarán de una presunción de exactitud de la fecha y hora que indican y de la integridad de los datos a los que la fecha y hora estén vinculadas.

▼M1

———————

▼B

Artículo 42

Requisitos de los sellos cualificados de tiempo electrónicos

1. Un sello cualificado de tiempo electrónico cumplirá los requisitos siguientes:

a) vincular la fecha y hora con los datos de forma que se elimine razonablemente la posibilidad de modificar los datos sin que se detecte;

b) basarse en una fuente de información temporal vinculada al Tiempo Universal Coordinado, y

►C2 c) haber sido firmado mediante el uso de una firma electrónica avanzada o sellado con un sello ◄ electrónico avanzado del prestador cualificado de servicios de confianza o por cualquier método equivalente.

▼M1

1 *bis*. Se presumirá el cumplimiento de los requisitos establecidos en el apartado 1 cuando la vinculación de la fecha y hora con los datos y exactitud de la fuente de información temporal sea conforme a las normas, las especificaciones y procedimientos a que se refiere el apartado 2.

2. A más tardar el 21 de mayo de 2025, la Comisión establecerá, mediante actos de ejecución, una lista de normas de referencia y, en su caso, las especificaciones y los procedimientos para la vinculación de la fecha y hora con los datos y para el establecimiento de la exactitud de las fuentes de información temporal. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

▼B

SECCIÓN 7

Servicio de entrega electrónica certificada

Artículo 43

Efecto jurídico de un servicio de entrega electrónica certificada

1. A los datos enviados y recibidos mediante un servicio de entrega electrónica certificada no se les denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales por el mero hecho de que estén en formato electrónico o no cumplan los requisitos de servicio cualificado de entrega electrónica certificada.

2. Los datos enviados y recibidos mediante un servicio cualificado de entrega electrónica certificada disfrutarán de la presunción de la integridad de los datos, el envío de dichos datos por el remitente identificado, la recepción por el destinatario identificado y la exactitud de la fecha y hora de envío y recepción de los datos que indica el servicio cualificado de entrega electrónica certificada.

Artículo 44

Requisitos de los servicios cualificados de entrega electrónica certificada

1. Los servicios cualificados de entrega electrónica certificada cumplirán los requisitos siguientes:

▼B

a) ser prestados por uno o más prestadores cualificados de servicios de confianza;

b) asegurar con un alto nivel de fiabilidad la identificación del remitente;

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

d) estar protegidos el envío y recepción de datos por una firma electrónica avanzada o un sello electrónico avanzado de un prestador cualificado de servicios de confianza de tal forma que se impida la posibilidad de que se modifiquen los datos sin que se detecte;

e) indicar claramente al emisor y al destinatario de los datos cualquier modificación de los datos necesarios a efectos del envío o recepción de los datos;

f) indicar mediante un sello cualificado de tiempo electrónico la fecha y hora de envío, recepción y eventual modificación de los datos.

En caso de que los datos se transfieran entre dos o más prestadores cualificados de servicios de confianza, se aplicarán los requisitos establecidos en las letras a) a f) a todos los prestadores cualificados de servicios de confianza.

▼M1

1 *bis*. Se presumirá el cumplimiento de los requisitos establecidos en el apartado 1 cuando el proceso de envío y recepción de datos sea conforme a las normas, especificaciones y procedimientos a que se refiere el apartado 2.

2. A más tardar el 21 de mayo de 2025, la Comisión establecerá, mediante actos de ejecución, una lista de normas de referencia y, en su caso, las especificaciones y los procedimientos para los procesos de envío y recepción de datos. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

2 *bis*. Los prestadores de servicios cualificados de entrega electrónica certificada podrán acordar la interoperabilidad entre los servicios cualificados de entrega electrónica certificada que presten. Dicho marco de interoperabilidad cumplirá los requisitos establecidos en el apartado 1 y dicho cumplimiento será confirmado por un organismo de evaluación de la conformidad.

2 *ter*. La Comisión podrá establecer, mediante actos de ejecución, una lista de normas de referencia y, en su caso, las especificaciones y los procedimientos aplicables al marco de interoperabilidad a que se refiere el apartado 2 *bis* del presente artículo. Las especificaciones técnicas y el contenido de las normas serán rentables y proporcionados. Los actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

▼B

SECCIÓN 8

Autenticación de sitios web

▼M1

Artículo 45

Requisitos aplicables a los certificados cualificados de autenticación de sitios web

1. Los certificados cualificados de autenticación de sitios web cumplirán los requisitos establecidos en el anexo IV. La evaluación del cumplimiento de dichos requisitos se llevará a cabo de conformidad con las normas, especificaciones y procedimientos a que se refiere el apartado 2 del presente artículo.

1 *bis*. Los proveedores de navegadores web reconocerán los certificados cualificados de autenticación de sitios web expedidos de conformidad con el apartado 1 del presente artículo. Los proveedores de navegadores web garantizarán que los datos de identificación de la persona declarados en el certificado y los atributos declarados adicionales se muestren al usuario de un modo fácil de consultar. Los proveedores de navegadores web garantizarán la compatibilidad e interoperabilidad con los certificados cualificados de autenticación de sitios web a que se refiere el apartado 1 del presente artículo, con la excepción de las microempresas y pequeñas empresas según se definen en el artículo 2 del anexo de la Recomendación 2003/361/CE durante sus primeros cinco años de actividad como prestadores de servicios de navegación web.

1 *ter*. Los certificados cualificados de autenticación de sitios web no estarán sometidos a ningún requisito obligatorio que no sean los requisitos establecidos en el apartado 1.

2. A más tardar el 21 de mayo de 2025, la Comisión establecerá, mediante actos de ejecución, una lista de normas de referencia y, en su caso, las especificaciones y los procedimientos aplicables a los certificados cualificados de autenticación de sitios web a que se refiere el apartado 1 del presente artículo. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

Artículo 45 bis

Medidas cautelares en materia de ciberseguridad

1. Los proveedores de navegadores web no adoptarán ninguna medida contraria a sus obligaciones establecidas en el artículo 45, en particular los requisitos de reconocer los certificados cualificados de autenticación de sitios web y de mostrar los datos de identificación de la persona proporcionados de un modo que sea fácil de consultar.

2. No obstante lo dispuesto en el apartado 1 y solo en caso de preocupaciones justificadas relacionadas con violaciones de la seguridad o la pérdida de integridad de un certificado o conjunto de certificados identificados, los proveedores de navegadores web podrán adoptar medidas cautelares en relación con dicho certificado o conjunto de certificados.

3. Cuando se adopten medidas, los proveedores de navegadores web notificarán, en virtud del apartado 2, sus preocupaciones por escrito, sin demora indebida, junto con una descripción de las medidas adoptadas para mitigarlas, a la Comisión, al organismo de supervisión competente, a la entidad a la que se haya expedido el certificado y al prestador

▼M1

cualificado de servicios de confianza que haya expedido dicho certificado o conjunto de certificados. Tras la recepción de dicha notificación, el organismo de supervisión competente expedirá un acuse de recibo al proveedor del navegador web en cuestión.

4. El organismo de supervisión competente investigará las cuestiones planteadas en la notificación, de conformidad con el artículo 46 *ter*, apartado 4, letra k). Cuando el resultado de la investigación no implique la retirada de la cualificación del certificado, el organismo de supervisión informará de ello al proveedor del navegador web y solicitará que ese proveedor ponga fin a las medidas cautelares a que se refiere el apartado 2 del presente artículo.

SECCIÓN 9

declaración electrónica de atributos

Artículo 45 ter

Efectos jurídicos de la declaración electrónica de atributos

1. No se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a una declaración electrónica de atributos por el mero hecho de estar en formato electrónico o de no cumplir los requisitos aplicables a las declaraciones electrónicas cualificadas de atributos.

2. Las declaraciones electrónicas cualificadas de atributos y las declaraciones de atributos expedidas por, o en nombre de, un organismo del sector público responsable de una fuente auténtica tendrán los mismos efectos jurídicos que las declaraciones lícitamente expedidas en papel.

3. Una declaración de atributos expedida por, o en nombre de, un organismo del sector público responsable de una fuente auténtica en un Estado miembro será reconocida en todos los Estados miembros como declaración de atributos expedida por, o en nombre de, un organismo del sector público responsable de una fuente auténtica.

Artículo 45 quater

Declaración electrónica de atributos en servicios públicos

Cuando el Derecho nacional exija una identificación electrónica en la que se utilice un medio de identificación electrónica y una autenticación para acceder a un servicio en línea prestado por un organismo del sector público, los datos de identificación de la persona contenidos en la declaración electrónica de atributos no sustituirán a la identificación electrónica en la que se utilice un medio de identificación electrónica y una autenticación para la identificación electrónica a menos que el Estado miembro lo autorice expresamente. En tal caso, también se aceptarán las declaraciones electrónicas cualificadas de atributos procedentes de otros Estados miembros.

Artículo 45 quinquies

Requisitos aplicables a la declaración electrónica cualificada de atributos

1. La declaración electrónica cualificada de atributos cumplirá los requisitos establecidos en el anexo V.

▼M1

2. La evaluación del cumplimiento de los requisitos establecidos en el anexo V se llevará a cabo de conformidad con las normas, especificaciones y procedimientos a que se refiere el apartado 5 del presente artículo.

3. Las declaraciones electrónicas cualificadas de atributos no estarán sometidas a ningún requisito obligatorio además de los requisitos establecidos en el anexo V.

4. Si una declaración electrónica cualificada de atributos ha sido revocada después de su emisión inicial, perderá su validez desde el momento de su revocación y no podrá en ninguna circunstancia recuperar su estado.

5. A más tardar el 21 de noviembre de 2024, la Comisión establecerá, mediante actos de ejecución, una lista de normas de referencia y, en su caso, las especificaciones y los procedimientos para las declaraciones electrónicas cualificadas de atributos. Dichos actos de ejecución serán coherentes con los actos de ejecución a que se refiere el artículo 5 *bis*, apartado 23, sobre la implantación de la cartera europea de identidad digital. Se adoptarán con arreglo al procedimiento de examen tal como prevé el artículo 48, apartado 2.

Artículo 45 sexies

Cotejo de atributos con fuentes auténticas

1. En un plazo de veinticuatro meses a partir de la fecha de entrada en vigor de los actos de ejecución a que se refieren el artículo 5 *bis*, apartado 23, y el artículo 5 *quater*, apartado 6, los Estados miembros garantizarán que, al menos para los atributos que se enumeran en el anexo VI, cuando tales atributos se basen en fuentes auténticas pertenecientes al sector público, se adopten medidas para permitir que los prestadores cualificados de servicios de confianza de declaraciones electrónicas de atributos verifiquen dichos atributos por medios electrónicos, a petición del usuario, de conformidad con el Derecho de la Unión o nacional.

2. A más tardar el 21 de noviembre de 2024, la Comisión, teniendo en cuenta las normas internacionales aplicables, mediante actos de ejecución, establecerá una lista de normas de referencia y, en su caso, las especificaciones y los procedimientos en lo que respecta al catálogo de atributos, así como a los sistemas de declaración de atributos y a los procedimientos de verificación de declaraciones electrónicas cualificadas de atributos a los efectos del apartado 1 del presente artículo. Dichos actos de ejecución serán coherentes con el acto de ejecución a que se refiere el artículo 5 *bis*, apartado 23, sobre la implantación de la cartera europea de identidad digital. Se adoptarán con arreglo al procedimiento de examen tal como prevé el artículo 48, apartado 2.

Artículo 45 septies

Requisitos aplicables a la declaración electrónica de atributos expedida por un organismo del sector público responsable de una fuente auténtica, o en nombre de este

1. Las declaraciones electrónicas de atributos expedidas por un organismo del sector público responsable de una fuente auténtica, o en su nombre cumplirán los requisitos siguientes:

a) los establecidos en el anexo VII;

▼M1

b) el certificado cualificado que respalde la firma electrónica cualificada o el sello electrónico cualificado del organismo del sector público a que se refiere el artículo 3, punto 46, identificado como el emisor a que se refiere el anexo VII, letra b), contendrá un conjunto específico de atributos certificados en un formato adecuado para el tratamiento automático que:

i) indicará que el organismo emisor está establecido de conformidad con el Derecho de la Unión o nacional, bien como responsable de la fuente auténtica con arreglo a la cual se expide la declaración electrónica de atributos, bien como el organismo designado para actuar en su nombre,

ii) proporcionará un conjunto de datos que representen inequívocamente la fuente auténtica a que se refiere el inciso i), y

iii) determinará el Derecho de la Unión o nacional a que se refiere el inciso i).

2. El Estado miembro en el que estén establecidos los organismos del sector público a que se refiere el artículo 3, punto 46, velará por que los organismos del sector público que expidan declaraciones electrónicas de atributos cumplan un nivel de fiabilidad equivalente al de los prestadores cualificados de servicios de confianza de conformidad con el artículo 24.

3. Los Estados miembros notificarán a la Comisión los organismos del sector público a que se refiere el artículo 3, punto 46. Dicha notificación incluirá un informe de evaluación de la conformidad expedido por un organismo de evaluación de la conformidad que confirme que se cumplen los requisitos establecidos en los apartados 1, 2 y 6 del presente artículo. La Comisión pondrá a disposición del público, a través de un canal seguro, la información de los organismos del sector público a que se refiere el artículo 3, punto 46, en una forma firmada o sellada electrónicamente adecuada para el tratamiento automático.

4. Si una declaración electrónica de atributos expedida por un organismo del sector público responsable de una fuente auténtica, o en nombre de este ha sido revocada después de su emisión inicial, perderá su validez desde el momento de su revocación y su estado será irreversible.

5. Se considerará que una declaración electrónica de atributos expedida por un organismo del sector público responsable de una fuente auténtica, o en nombre de este cumple los requisitos establecidos en el apartado 1 del presente artículo cuando sea conforme a las normas, especificaciones y procedimientos a que se refiere el apartado 6.

6. A más tardar el 21 de noviembre de 2024, la Comisión establecerá, mediante actos de ejecución, una lista de normas de referencia y, en su caso, las especificaciones y los procedimientos para la declaración electrónica de atributos expedida por un organismo del sector público responsable de una fuente auténtica o en nombre de este. Dichos actos de ejecución serán coherentes con los actos de ejecución a que se refiere el artículo 5 *bis*, apartado 23, sobre la implantación de la cartera europea de identidad digital. Se adoptarán con arreglo al procedimiento de examen tal como prevé el artículo 48, apartado 2.

▼M1

7. A más tardar el 21 de noviembre de 2024, la Comisión establecerá, mediante actos de ejecución, una lista de normas de referencia y, en su caso, las especificaciones y los procedimientos para el apartado 3 del presente artículo. Dichos actos de ejecución serán coherentes con los actos de ejecución a que se refiere el artículo 5 *bis*, apartado 23, sobre la implantación de la cartera europea de identidad digital. Se adoptarán con arreglo al procedimiento de examen tal como prevé el artículo 48, apartado 2.

8. Los organismos del sector público a que se refiere el artículo 3, punto 46, que expidan declaraciones electrónicas de atributos facilitarán una interfaz con las carteras europeas de identidad digital que se proporcionen de conformidad con el artículo 5 *bis*.

Artículo 45 octies

Emisión de declaraciones electrónicas de atributos a las carteras europeas de identidad digital

1. Los prestadores de declaraciones electrónicas de atributos brindarán a los usuarios de carteras europeas de identidad digital la posibilidad de solicitar, obtener, almacenar y gestionar la declaración electrónica de atributos independientemente del Estado miembro en el que se proporcione la cartera europea de identidad digital.

2. Los prestadores de declaraciones electrónicas cualificadas de atributos facilitarán una interfaz con las carteras europeas de identidad digital que se proporcionen con arreglo al artículo 5 *bis*.

Artículo 45 nonies

Normas adicionales para la prestación de servicios de declaración electrónica de atributos

1. Los prestadores de servicios cualificados y no cualificados de declaración electrónica de atributos se abstendrán de combinar datos personales relacionados con la prestación de dichos servicios con datos personales obtenidos a través de otros servicios que ofrezcan ellos o sus socios comerciales.

2. Se establecerá una separación lógica entre los datos personales relacionados con la prestación de servicios de declaración electrónica de atributos y otros datos que obren en poder del prestador de declaraciones electrónicas de atributos.

3. Los prestadores de servicios de declaraciones electrónicas cualificadas de atributos llevarán a cabo la prestación de dichos servicios de confianza cualificados de manera funcionalmente separada de otros servicios que presten.

SECCIÓN 10

servicios de archivo electrónico

Artículo 45 decies

Efecto jurídico de los servicios de archivo electrónico

1. No se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a los datos electrónicos ni a los documentos electrónicos conservados mediante un servicio de archivo electrónico por

▼M1

el mero hecho de que estén en formato electrónico o no estén conservados mediante un servicio cualificado de archivo electrónico.

2. Los datos electrónicos y documentos electrónicos conservados mediante un servicio cualificado de archivo electrónico gozarán de la presunción de su integridad y origen durante el período de conservación por el prestador cualificado de servicios de confianza.

Artículo 45 undecies

Requisitos aplicables a los servicios cualificados de archivo electrónico

1. Los servicios cualificados de archivo electrónico cumplirán los requisitos siguientes:

a) ser prestados por prestadores cualificados de servicios de confianza;

b) utilizar procedimientos y tecnologías capaces de asegurar la durabilidad y legibilidad de los datos y documentos electrónicos más allá del período de validez tecnológica y, al menos, durante el período de conservación legal o contractual, manteniendo al mismo tiempo su integridad y la exactitud de su origen;

c) garantizar que dichos datos y documentos electrónicos se conserven de tal manera que queden protegidos contra su pérdida o alteración, excepto en el caso de los cambios relativos a su soporte o formato electrónico;

d) permitir que las partes usuarias autorizadas reciban de forma automatizada un informe que confirme que los datos o documentos electrónicos recuperados de un archivo electrónico cualificado gozan de la presunción de integridad desde el inicio del período de conservación hasta el momento de su recuperación.

El informe a que se refiere el párrafo primero, letra d), se proporcionará de manera fiable y eficiente e incluirá la firma electrónica cualificada o el sello electrónico cualificado del prestador del servicio cualificado de archivo electrónico.

2. A más tardar el 21 de mayo de 2025, la Comisión establecerá, mediante actos de ejecución, una lista de normas de referencia y, en su caso, las especificaciones y los procedimientos para los servicios cualificados de archivo electrónico. Se presumirá el cumplimiento de los requisitos aplicables a los servicios cualificados de archivo electrónico cuando un servicio cualificado de archivo electrónico sea conforme a dichas normas, especificaciones y procedimientos. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

SECCIÓN 11

libros mayores electrónicos

Artículo 45 duodecies

Efectos jurídicos de los libros mayores electrónicos

1. No se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a un libro mayor electrónico por el mero hecho de estar en formato electrónico o de no cumplir los requisitos aplicables a los libros mayores electrónicos cualificados.

▼M1

2. Los registros de datos contenidos en un libro mayor electrónico cualificado gozarán de la presunción de unicidad y exactitud de su orden cronológico secuencial y de su integridad.

Artículo 45 terdecies

Requisitos aplicables a los libros mayores electrónicos cualificados

1. Un libro mayor electrónico cualificado cumplirá los requisitos siguientes:

a) estar creado y gestionado por uno o más prestadores cualificados de servicios de confianza;

b) establecer el origen de los registros de datos en el libro mayor;

c) garantizar la unicidad del orden cronológico secuencial de los registros de datos en el libro mayor;

d) grabar datos de modo que sea posible detectar de forma inmediata cualquier modificación posterior de estos, garantizando su integridad a lo largo del tiempo.

2. Se presumirá el cumplimiento de los requisitos establecidos en el apartado 1 cuando un libro mayor electrónico sea conforme a las normas, especificaciones y procedimientos a que se refiere el apartado 3.

3. A más tardar el 21 de mayo de 2025, la Comisión establecerá, mediante actos de ejecución, una lista de normas de referencia y, en su caso, las especificaciones y los procedimientos para los requisitos a que se refiere el apartado 1 del presente artículo. Los actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

▼B

CAPÍTULO IV

DOCUMENTOS ELECTRÓNICOS

Artículo 46

Efectos jurídicos de los documentos electrónicos

No se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a un documento electrónico por el mero hecho de estar en formato electrónico.

▼M1

CAPÍTULO IV *bis*

MARCO DE GOBERNANZA

Artículo 46 bis

Supervisión del marco de la cartera europea de identidad digital

1. Los Estados miembros designarán uno o más organismos de supervisión establecidos en su territorio.

Los organismos de supervisión designados en virtud del párrafo primero disfrutarán de las competencias necesarias y los recursos adecuados para el ejercicio de sus funciones de forma eficaz, eficiente e independiente.

▼**M1**

2. Los Estados miembros notificarán a la Comisión los nombres y direcciones de los organismos de supervisión designados en virtud del apartado 1, así como cualquier modificación posterior de los mismos. La Comisión publicará una lista de los organismos de supervisión notificados.

3. Las funciones de los organismos de supervisión designados en virtud del apartado 1 serán las siguientes:

a) supervisar a los proveedores de carteras europeas de identidad digital establecidos en el Estado miembro que lo designa y garantizar, mediante actividades de supervisión previas y posteriores, que dichos proveedores y las carteras europeas de identidad digital que proporcionan cumplen los requisitos establecidos en el presente Reglamento;

b) adoptar medidas, en caso necesario, en relación con los proveedores de carteras europeas de identidad digital establecidos en el territorio del Estado miembro que lo designa, mediante actividades de supervisión posteriores, cuando se les haya informado de que los proveedores o las carteras europeas de identidad digital que proporcionan infringen el presente Reglamento.

4. Las tareas de los organismos de supervisión designados s en virtud del apartado 1 incluirán, en concreto, las siguientes:

a) cooperar con otros organismos de supervisión y prestarles asistencia de conformidad con los artículos 46 *quater* y 46 *sexies*;

b) solicitar la información necesaria para controlar el cumplimiento del presente Reglamento;

c) informar a las autoridades competentes pertinentes designadas o establecidas en virtud del artículo 8, apartado 1, de la Directiva (UE) 2022/2555 de los Estados miembros de que se trate de cualquier violación significativa de la seguridad o la pérdida de integridad de la que tengan conocimiento en el desempeño de sus funciones y, en caso de violación significativa de la seguridad o la pérdida de integridad que afecte a otros Estados miembros, informar al punto de contacto único designado con arreglo al artículo 8, apartado 3, de la Directiva (UE) 2022/2555 del Estado miembro de que se trate y a los puntos de contacto únicos designados de conformidad con el artículo 46 *quater*, apartado 1, del presente Reglamento en los demás Estados miembros de que se trate, e informar al público o exigir a los proveedores de carteras europeas de identidad digital que lo hagan en caso de que el organismo de supervisión determine que la divulgación de la violación de la seguridad o la pérdida de integridad reviste interés público;

d) emprender inspecciones *in situ* y actividades de supervisión externa;

e) requerir que los proveedores de carteras europeas de identidad digital corrijan cualquier incumplimiento de los requisitos establecidos en el presente Reglamento;

f) suspender o cancelar el registro y la inclusión de las partes usuarias en el mecanismo a que se refiere el artículo 5 *ter*, apartado 7, en caso de uso ilegal o fraudulento de la cartera europea de identidad digital;

g) cooperar con las autoridades de control competentes establecidas en virtud del artículo 51 del Reglamento (UE) 2016/679, en particular, informándolas sin dilación indebida en caso de posible vulneración de las normas de protección de datos personales, así como sobre violaciones de la seguridad que parezcan constituir violaciones de la seguridad de los datos personales;

▼M1

5. Cuando el organismo de supervisión designado en virtud del apartado 1 exija al proveedor de una cartera europea de identidad digital que subsane cualquier incumplimiento de los requisitos establecidos en el presente Reglamento de conformidad con el apartado 4, letra e), y dicho proveedor no actúe en consecuencia y, si procede, dentro del plazo fijado por dicho organismo de supervisión, el organismo de supervisión designado en virtud del apartado 1, teniendo en cuenta, en particular, el alcance, la duración y las consecuencias de dicho incumplimiento, podrá ordenar al proveedor que suspenda o cese la provisión de la cartera europea de identidad digital. El organismo de supervisión informará a los organismos de supervisión de otros Estados miembros, a la Comisión, a las partes usuarias y a los usuarios de la cartera europea de identidad digital, sin demora indebida, de la decisión de exigir la suspensión o el cese de la provisión de la cartera europea de identidad digital.

6. A más tardar el 31 de marzo de cada año, cada organismo de supervisión designado en virtud del apartado 1 presentará a la Comisión un informe sobre las principales actividades que haya llevado a cabo en el año natural anterior. La Comisión pondrá dichos informes anuales a disposición del Parlamento Europeo y del Consejo.

7. A más tardar el 21 de mayo de 2025, la Comisión establecerá, mediante actos de ejecución, los formatos y procedimientos para el informe a que se refiere el apartado 6 del presente artículo. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 48, apartado 2.

Artículo 46 ter

Supervisión de los servicios de confianza

1. Los Estados miembros designarán un organismo de supervisión establecido en su territorio o designarán, previo acuerdo mutuo con otro Estado miembro, un organismo de supervisión establecido en ese otro Estado miembro. Dicho organismo de supervisión será responsable de las funciones de supervisión en el Estado miembro que efectúa la designación en lo que respecta a los servicios de confianza.

Los organismos de supervisión designados en virtud del párrafo primero disfrutarán de las competencias necesarias y los recursos adecuados para el ejercicio de sus funciones.

2. Los Estados miembros notificarán a la Comisión los nombres y direcciones de sus organismos de supervisión, designados en virtud del apartado 1, así como cualquier modificación posterior a este respecto. La Comisión publicará una lista de los organismos de supervisión notificados.

3. La función de los organismos de supervisión designados en virtud del apartado 1 será la siguiente:

a) supervisar a los prestadores cualificados de servicios de confianza establecidos en el territorio del Estado miembro que lo designa y garantizar, mediante actividades de supervisión previas y posteriores, que dichos prestadores cualificados de servicios de confianza, y los servicios de confianza cualificados prestados por ellos, cumplen los requisitos establecidos en el presente Reglamento;

b) adoptar medidas, en caso necesario, en relación con los prestadores no cualificados de servicios de confianza establecidos en el territorio del Estado miembro que lo designa, mediante actividades de supervisión posteriores, cuando se le informe de que dichos prestadores no cualificados de servicios de confianza, o los servicios de confianza prestados por ellos incumplen presuntamente los requisitos establecidos en el presente Reglamento.

▼M1

4. Las funciones del organismo de supervisión designado en virtud del apartado 1 incluirán, en particular, las siguientes:

a) informar a las autoridades competentes pertinentes de los Estados miembros de que trate designadas o establecidas en virtud del artículo 8, apartado 1, de la Directiva (UE) 2022/2555 de cualquier violación significativa de la seguridad o pérdida de integridad de las que tenga conocimiento en el desempeño de sus funciones y, en caso de una violación significativa de la seguridad o pérdida de integridad que afecte a otros Estados miembros, informar al punto de contacto único del Estado miembro de que se trate designado o establecido en virtud del artículo 8, apartado 3, de la Directiva (UE) 2022/2555 y a los puntos de contacto únicos de los demás Estados miembros de que se trate designados en virtud del artículo 46 *quater*, apartado 1, del presente Reglamento, e informar al público —o exigir al prestador de servicios de confianza que lo haga— en caso de que el organismo de supervisión considere que la divulgación de la violación de la seguridad o pérdida de integridad revistiera interés público;

b) cooperar con otros organismos de supervisión y prestarles asistencia de conformidad con los artículos 46 *quater* y 46 *sexies*;

c) analizar los informes de evaluación de la conformidad a que se refieren el artículo 20, apartado 1, y el artículo 21, apartado 1;

d) informar a la Comisión de sus actividades principales de conformidad con el apartado 6 del presente artículo;

e) realizar auditorías o solicitar a un organismo de evaluación de la conformidad que realice una evaluación de la conformidad de prestadores cualificados de servicios de confianza, de conformidad con el artículo 20, apartado 2;

f) cooperar con las autoridades de control competentes establecidas en virtud del artículo 51 del Reglamento (UE) 2016/679, en particular, informándolas, sin dilación indebida, en caso de posible vulneración de las normas de protección de datos personales, así como sobre violaciones de la seguridad que parezcan constituir violaciones de la seguridad de los datos personales;

g) conceder la cualificación a los prestadores de servicios de confianza y a los servicios de confianza que prestan, y retirar dicha cualificación, de conformidad con los artículos 20 y 21;

h) comunicar al organismo responsable de la lista de confianza a que se refiere el artículo 22, apartado 3, de su decisión de conceder o retirar la cualificación, salvo si dicho organismo es también el organismo de supervisión designado en virtud del apartado 1 del presente artículo;

i) verificar la existencia y la correcta aplicación de las disposiciones relativas a los planes de cese cuando los prestadores cualificados de servicios de confianza cesen sus actividades, con inclusión de la forma en que se hace accesible la información, de conformidad con el artículo 24, apartado 2, letra h);

j) requerir que los prestadores de servicios de confianza corrijan cualquier incumplimiento de los requisitos establecidos en el presente Reglamento;

▼M1

k) investigar las denuncias de los proveedores de navegadores web en virtud del artículo 45 *bis* y tomar medidas en caso necesario.

5. Los Estados miembros podrán disponer que el organismo de supervisión designado en virtud del apartado 1 establezca, mantenga y actualice una infraestructura de confianza de conformidad con el Derecho nacional.

6. A más tardar el 31 de marzo de cada año, cada organismo de supervisión designado en virtud del apartado 1 presentará a la Comisión un informe sobre las principales actividades que haya llevado a cabo en el año natural anterior. La Comisión pondrá dichos informes anuales a disposición del Parlamento Europeo y del Consejo.

7. A más tardar el 21 de mayo de 2025, la Comisión adoptará directrices sobre el ejercicio, por los organismos de supervisión designado en virtud del apartado 1 del presente artículo, de las funciones a que se refiere el apartado 4 del presente artículo y, mediante actos de ejecución, definirá los formatos y procedimientos del informe previsto en el apartado 6 del presente artículo. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 48, apartado 2.

Artículo 46 quater

Puntos de contacto únicos

1. Cada Estado miembro designará un punto de contacto único para los servicios de confianza, las carteras europeas de identidad digital y los sistemas de identificación electrónica notificados.

2. Cada punto de contacto único ejercerá una función de enlace para facilitar la cooperación transfronteriza entre los organismos de supervisión de los prestadores de servicios de confianza y entre los organismos de supervisión de los proveedores de carteras europeas de identidad digital y, cuando proceda, con la Comisión y la Agencia de la Unión Europea para la Ciberseguridad (ENISA) y con otras autoridades competentes de su Estado miembro.

3. Cada Estado miembro hará públicos y, sin demora indebida, notificará a la Comisión los nombres y direcciones del punto de contacto único designado en virtud del apartado 1, así como cualquier modificación posterior a este respecto.

4. La Comisión publicará una lista de los puntos de contacto únicos notificados en virtud del apartado 3.

Artículo 46 quinquies

Asistencia mutua

1. A fin de facilitar la supervisión y el cumplimiento de las obligaciones establecidas en virtud del presente Reglamento, los organismos de supervisión designados en virtud del artículo 46 *bis*, apartado 1, y del artículo 46 *ter*, apartado 1, podrán solicitar —también a través del Grupo de Cooperación establecido de conformidad con el artículo 46 *sexies*, apartado 1— asistencia mutua de organismos de supervisión de otro Estado miembro en el que el prestador de la cartera europea de identidad digital o el prestador de servicios de confianza esté establecido, o en el que se encuentren sus redes y sistemas de información o se presten sus servicios.

2. La asistencia mutua implicará, como mínimo, lo siguiente:

▼M1

a) el organismo de supervisión que aplique medidas de supervisión y ejecución en un Estado miembro informará y consultará al organismo de supervisión del otro Estado miembro afectado;

b) un organismo de supervisión podrá solicitar al organismo de supervisión de otro Estado miembro afectado que adopte medidas de supervisión o ejecución, entre las que se podrá contar, por ejemplo, cursar solicitudes de inspección en relación con los informes de evaluación de la conformidad contemplados en los artículos 20 y 21 en lo referente a la prestación de servicios de confianza;

c) cuando proceda, los organismos de supervisión podrán llevar a cabo investigaciones conjuntas con los organismos de supervisión de otros Estados miembros.

Los acuerdos y procedimientos para las acciones conjuntas con arreglo al párrafo primero serán aprobados y establecidos por los Estados miembros de que se trate de conformidad con su Derecho nacional.

3. El organismo de supervisión al que se haya dirigido una solicitud de asistencia podrá denegar dicha solicitud por alguno de los motivos siguientes:

a) la asistencia solicitada no guarda proporción con las actividades de supervisión del organismo de supervisión realizadas de conformidad con los artículos 46 *bis* y 46 *ter*;

b) el organismo de supervisión no es competente para prestar la asistencia solicitada;

c) la prestación de la asistencia solicitada sería incompatible con el presente Reglamento.

4. A más tardar el 21 de mayo de 2025, y posteriormente cada dos años, el Grupo de Cooperación establecido en virtud del artículo 46 *sexies*, apartado 1, formulará orientaciones sobre los aspectos organizativos y los procedimientos para la asistencia mutua a que se refieren los apartados 1 y 2 del presente artículo.

Artículo 46 sexies

El Grupo de Cooperación sobre la Identidad Digital Europea

1. Con el fin de apoyar y facilitar la cooperación transfronteriza de los Estados miembros y el intercambio de información sobre los servicios de confianza, las carteras europeas de identidad digital y los sistemas de identificación electrónica notificados, la Comisión creará el Grupo de Cooperación sobre la Identidad Digital Europea.

2. El Grupo de Cooperación estará formado por representantes nombrados por los Estados miembros y la Comisión. El Grupo de Cooperación estará presidido por la Comisión. La Comisión asumirá la secretaría del Grupo de Cooperación.

3. Podrá invitarse a representantes de las partes interesadas pertinentes a asistir a las reuniones del Grupo de Cooperación y a participar en sus trabajos en calidad de observadores *ad hoc*.

4. Se invitará a la ENISA a participar en calidad de observadora en los trabajos del Grupo de Cooperación cuando este intercambie puntos de vista, mejores prácticas e información sobre aspectos pertinentes en materia de ciberseguridad, como la notificación de violaciones de la seguridad, y cuando se trate del uso de certificados o las normas sobre ciberseguridad.

5. El Grupo de Cooperación desempeñará las siguientes funciones:

▼M1

a) intercambiar recomendaciones y cooperar con la Comisión en las iniciativas políticas emergentes en el ámbito de las carteras de identidad digital, los medios de identificación electrónica y los servicios de confianza;

b) asesorar a la Comisión, según proceda, en la preparación temprana de los proyectos de actos delegados y de ejecución que deban adoptarse en virtud del presente Reglamento;

c) con el fin de apoyar a los organismos de supervisión en la aplicación de las disposiciones del presente Reglamento:

i) intercambiar las mejores prácticas e información sobre la aplicación de las disposiciones del presente Reglamento,

ii) evaluar los avances pertinentes en el ámbito de los sectores de la cartera de identidad digital, la identificación electrónica y los servicios de confianza,

iii) organizar reuniones conjuntas con las partes interesadas pertinentes de toda la Unión para tratar las actividades realizadas por el Grupo de Cooperación y recabar apreciaciones sobre los desafíos políticos emergentes,

iv) con el apoyo de la ENISA, intercambiar opiniones, mejores prácticas e información sobre los aspectos de ciberseguridad pertinentes relativos a las carteras europeas de identidad digital, los sistemas de identificación electrónica y los servicios de confianza,

v) intercambiar mejores prácticas en relación con el desarrollo y la ejecución de políticas sobre la notificación de violaciones de la seguridad y las medidas comunes a que se refieren los artículos 5 *sexies* y 10,

vi) organizar reuniones conjuntas con el Grupo de Cooperación SRI establecido en virtud del artículo 14, apartado 1, de la Directiva (UE) 2022/2555 para intercambiar la información pertinente referente a ciberamenazas, incidencias, vulnerabilidades, iniciativas de sensibilización, formación, ejercicios y destrezas, desarrollo de capacidades, capacidad relativa a las normas y especificaciones técnicas y las propias normas y especificaciones técnicas en relación con los servicios de confianza y la identificación electrónica,

vii) debatir, a petición de un organismo de supervisión, las solicitudes concretas de asistencia mutua a que se refiere el artículo 46 *quinquies*,

viii) facilitar el intercambio de información entre los organismos de supervisión, orientando sobre los aspectos organizativos y los procedimientos de la asistencia mutua a que se refiere el artículo 46 *quinquies*;

d) organizar revisiones *inter pares* de los sistemas de identificación electrónica que vayan a notificarse con arreglo al presente Reglamento.

6. Los Estados miembros garantizarán una cooperación efectiva y eficiente de sus representantes designados en el Grupo de cooperación.

▼M1

7. A más tardar el 21 de mayo de 2025, la Comisión establecerá, mediante actos de ejecución, los mecanismos de procedimiento necesarios para facilitar la cooperación entre los Estados miembros a que se refiere el apartado 5, letra d), del presente artículo. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 48, apartado 2.

▼B

CAPÍTULO V

DELEGACIÓN DE PODERES Y DISPOSICIONES DE EJECUCIÓN

Artículo 47

Ejercicio de la delegación

1. Se faculta a la Comisión para adoptar actos delegados en las condiciones establecidas en el presente artículo.

▼M1

2. Los poderes para adoptar actos delegados mencionados en el artículo 5 *quater*, apartado 7, el artículo 24, apartado 4 *ter*, y el artículo 30, apartado 4, se otorgan a la Comisión por un período de tiempo indefinido a partir del 17 de septiembre de 2014.

3. La delegación de poderes mencionada en el artículo 5 *quater*, apartado 7, el artículo 24, apartado 4 *ter*, y el artículo 30, apartado 4, podrá ser revocada en cualquier momento por el Parlamento Europeo o por el Consejo. La decisión de revocación pondrá término a la delegación de los poderes que en ella se especifiquen. La decisión surtirá efecto el día siguiente al de su publicación en el *Diario Oficial de la Unión Europea* o en una fecha posterior indicada en ella. No afectará a la validez de los actos delegados que ya estén en vigor.

▼B

4. En cuanto la Comisión adopte un acto delegado, lo notificará simultáneamente al Parlamento Europeo y al Consejo.

▼M1

5. Los actos delegados adoptados en virtud del artículo 5 *quater*, apartado 7, el artículo 24, apartado 4 *ter*, y el artículo 30, apartado 4, entrarán en vigor únicamente si, en un plazo de dos meses a partir de su notificación al Parlamento Europeo y al Consejo, ninguna de estas instituciones formula objeciones o si, antes del vencimiento de dicho plazo, ambas informan a la Comisión de que no las formularán. El plazo se prorrogará dos meses a iniciativa del Parlamento Europeo o del Consejo.

▼B

Artículo 48

Procedimiento de comité

1. La Comisión estará asistida por un comité. El comité será conforme a lo dispuesto en el Reglamento (UE) nº 182/2011.

2. En los casos en que se haga referencia al presente apartado, será de aplicación el artículo 5 del Reglamento (UE) nº 182/2011.

▼B

CAPÍTULO VI

DISPOSICIONES FINALES

▼M1

Artículo 48 bis

Requisitos de información

1. Los Estados miembros garantizarán la recopilación de estadísticas relativas al funcionamiento de las carteras europeas de identidad digital y los servicios de confianza cualificados prestados en su territorio.

2. Las estadísticas recopiladas de conformidad con el apartado 1 incluirán los siguientes elementos:

a) el número de personas físicas y jurídicas poseedoras de una cartera europea de identidad digital válida;

b) el tipo y cantidad de servicios que aceptan el uso de la cartera europea de identidad digital;

c) la cantidad de reclamaciones de usuarios e incidencias de protección de los consumidores o de protección de datos relacionadas con las partes usuarias y los servicios de confianza cualificados;

d) un informe resumido que incluya datos sobre las incidencias que impidan utilizar la cartera europea de identidad digital;

e) un resumen de las incidencias de seguridad importantes, de las violaciones de la seguridad de los datos y de los usuarios de carteras europeas de identidad digital o de servicios de confianza cualificados que hayan resultado afectados.

3. Las estadísticas a que se refiere el apartado 2 se harán públicas en un formato abierto, de uso común y legible por máquina.

4. Cada año, a más tardar el 31 de marzo, los Estados miembros presentarán a la Comisión un informe sobre las estadísticas recopiladas de conformidad con el apartado 2.

Artículo 49

Revisión

1. La Comisión revisará la aplicación del presente Reglamento y, a más tardar el 21 de mayo de 2026, informará al Parlamento Europeo y al Consejo. En dicho informe, la Comisión evaluará, en particular, si es apropiado modificar el ámbito de aplicación del presente Reglamento o sus disposiciones específicas, incluidas, en concreto, las disposiciones que figuran en el artículo 5 *quater*, apartado 5, teniendo en cuenta la experiencia adquirida en la aplicación del presente Reglamento, así como la evolución tecnológica, del mercado y jurídica. Si fuera necesario, dicho informe irá acompañado de una propuesta de modificación del presente Reglamento.

2. El informe a que se refiere el apartado 1 incluirá una evaluación de la disponibilidad, seguridad y facilidad de uso de los medios de identificación electrónica notificados y las carteras europeas de identidad digital que entran dentro del ámbito de aplicación del presente

▼M1

Reglamento y evaluarán si debe requerirse a todos los prestadores de servicios privados en línea que se apoyan en servicios de identificación electrónica de terceros con fines de autenticación de los usuarios que acepten el uso de los medios de identificación electrónicos notificados y la cartera europea de identidad digital.

3. A más tardar el 21 de mayo de 2030, la Comisión presentará un informe al Parlamento Europeo y al Consejo sobre la marcha hacia el logro de los objetivos del presente Reglamento.

▼B

Artículo 50

Derogación

1. Queda derogada la Directiva 1999/93/CE con efectos a partir del 1 de julio de 2016.

2. Las referencias a la Directiva derogada se entenderán hechas al presente Reglamento.

▼M1

Artículo 51

Disposiciones transitorias

1. Los dispositivos de creación de firma segura cuya conformidad se haya determinado con arreglo al artículo 3, apartado 4, de la Directiva 1999/93/CE continuarán considerándose dispositivos cualificados de creación de firma electrónica con arreglo al presente Reglamento hasta el 21 de mayo de 2027.

2. Los certificados cualificados expedidos a personas físicas con arreglo a la Directiva 1999/93/CE seguirán considerándose certificados cualificados de firma electrónica en virtud del presente Reglamento hasta el 21 de mayo de 2026.

3. Los prestadores cualificados de servicios de confianza distintos de aquellos que presten servicios cualificados de confianza para la gestión de dispositivos cualificados de creación de firma y sello electrónicos a distancia de conformidad con los artículos 29 *bis* y 39 *bis* podrán seguir llevando a cabo la gestión de certificados cualificados de firma electrónica sin la necesidad de obtener la cualificación para la prestación de dichos servicios de gestión hasta el 21 de mayo de 2026.

4. Los prestadores cualificados de servicios de confianza a los que se haya concedido su cualificación en virtud del presente Reglamento antes del 20 de mayo de 2024 presentarán al organismo de supervisión un informe de evaluación de la conformidad que demuestre el cumplimiento del artículo 24, apartados 1, 1 *bis* y 1 *ter*, tan pronto como sea posible y, en cualquier caso, antes del 21 de mayo de 2026.

▼B

Artículo 52

Entrada en vigor

1. El presente Reglamento entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

2. El presente Reglamento será aplicable a partir del 1 de julio de 2016, a excepción de las disposiciones siguientes:

▼B

a) los artículos 8, apartado 3, 9, apartado 5, 12, apartados 2 a 9, 17, apartado 8, 19, apartado 4, 20, apartado 4, 21, apartado 4, 22, apartado 5, 23, apartado, 3, 24, apartado 5, 27, apartados 4 y 5, 28, apartado 6, 29, apartado 2, 30, apartados 3 y 4, 31, apartado 3, 32, apartado 3, 33, apartado 2, 34, apartado 2, 37, apartados 4 y 5, 38, apartado 6, 42, apartado 2, 44, apartado 2, 45, apartado 2, y los artículos 47 y 48 se aplicarán a partir del 17 de septiembre de 2014;

b) el artículo 7, el artículo 8, apartados 1 y 2, los artículos 9, 10, 11 y el artículo 12, apartado 1, se aplicarán a partir de la fecha de aplicación de los actos de ejecución previstos en los artículos 8, apartado 3, y 12, apartado 8;

c) el artículo 6 se aplicará a partir de los tres años de la fecha de aplicación de los actos de ejecución previstos en los artículos 8, apartado 3, y 12, apartado 8.

3. Cuando el sistema de identificación electrónica notificado esté incluido en la lista publicada por la Comisión con arreglo al artículo 9 antes de la fecha mencionada en la letra c) del apartado 2 del presente artículo, el reconocimiento de los medios de identificación electrónica expedidos bajo dicho sistema en virtud del artículo 6 se llevará a cabo a más tardar 12 meses después de la publicación de dicho sistema, pero no antes de la fecha mencionada en la letra c) del apartado 2 del presente artículo.

4. No obstante lo dispuesto en la letra c) del apartado 2 del presente artículo, un Estado miembro podrá decidir que los medios de identificación electrónica con arreglo al sistema de identificación electrónica notificado de conformidad con el artículo 9, apartado 1, por otro Estado miembro se reconozcan en el primer Estado miembro a partir de la fecha de aplicación de los actos de ejecución previstos en los artículos 8, apartado 3, y 12, apartado 8. Los Estados miembros de que se trate se lo comunicarán a la Comisión. La Comisión hará pública esa información.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

▼B

ANEXO I

REQUISITOS DE LOS CERTIFICADOS CUALIFICADOS DE FIRMA ELECTRÓNICA

Los certificados cualificados de firma electrónica contendrán:

a) una indicación, al menos en un formato adecuado para el procesamiento automático, de que el certificado ha sido expedido como certificado cualificado de firma electrónica;

b) un conjunto de datos que represente inequívocamente al prestador cualificado de servicios de confianza que expide los certificados cualificados, incluyendo como mínimo el Estado miembro en el que dicho prestador está establecido, y

   — para personas jurídicas: el nombre y, cuando proceda, el número de registro según consten en los registros oficiales,

   — para personas físicas, el nombre de la persona;

c) al menos el nombre del firmante o un seudónimo; si se usara un seudónimo, se indicará claramente;

d) datos de validación de la firma electrónica que correspondan a los datos de creación de la firma electrónica;

e) los datos relativos al inicio y final del período de validez del certificado;

f) el código de identidad del certificado, que debe ser único para el prestador cualificado de servicios de confianza;

g) la firma electrónica avanzada o el sello electrónico avanzado del prestador de servicios de confianza expedidor;

h) el lugar en que está disponible gratuitamente el certificado que respalda la firma electrónica avanzada o el sello electrónico avanzado a que se hace referencia en la letra g);

▼M1

i) la información o la localización de los servicios que pueden utilizarse para consultar el estado de validez del certificado cualificado;

▼B

j) cuando los datos de creación de firma electrónica relacionados con los datos de validación de firma electrónica se encuentren en un dispositivo cualificado de creación de firma electrónica, una indicación adecuada de esto, al menos en una forma apta para el procesamiento automático.

▼B

ANEXO II

REQUISITOS DE LOS DISPOSITIVOS CUALIFICADOS DE CREACIÓN DE FIRMA ELECTRÓNICA

1. Los dispositivos cualificados de creación de firma electrónica garantizarán como mínimo, por medios técnicos y de procedimiento adecuados, que:

   a) esté garantizada razonablemente la confidencialidad de los datos de creación de firma electrónica utilizados para la creación de firmas electrónicas;

   b) los datos de creación de firma electrónica utilizados para la creación de firma electrónica solo puedan aparecer una vez en la práctica;

   c) exista la seguridad razonable de que los datos de creación de firma electrónica utilizados para la creación de firma electrónica no pueden ser hallados por deducción y de que la firma está protegida con seguridad contra la falsificación mediante la tecnología disponible en el momento;

   d) los datos de creación de la firma electrónica utilizados para la creación de firma electrónica puedan ser protegidos por el firmante legítimo de forma fiable frente a su utilización por otros.

2. Los dispositivos cualificados de creación de firmas electrónicas no alterarán los datos que deben firmarse ni impedirán que dichos datos se muestren al firmante antes de firmar.

▼M1

_____

▼B

ANEXO III

REQUISITOS DE LOS CERTIFICADOS CUALIFICADOS DE SELLO ELECTRÓNICO

Los certificados cualificados de sello electrónico contendrán:

a) una indicación, al menos en un formato adecuado para el procesamiento automático, de que el certificado ha sido expedido como certificado cualificado de sello electrónico;

b) un conjunto de datos que represente inequívocamente al prestador cualificado de servicios de confianza que expide los certificados cualificados, incluyendo como mínimo el Estado miembro en el que dicho prestador está establecido, y

   — para personas jurídicas: el nombre y, cuando proceda, el número de registro según consten en los registros oficiales,

   — para personas físicas, el nombre de la persona;

c) al menos, el nombre del creador del sello y, cuando proceda, el número de registro, tal como se recojan en los registros oficiales;

d) los datos de validación del sello electrónico que correspondan a los datos de creación del sello electrónico;

e) los datos relativos al inicio y final del período de validez del certificado;

f) el código de identidad del certificado, que debe ser único para el prestador cualificado de servicios de confianza;

g) la firma electrónica avanzada o el sello electrónico avanzado del prestador de servicios de confianza expedidor;

h) el lugar en que está disponible gratuitamente el certificado que respalda la firma electrónica avanzada o el sello electrónico avanzado a que se hace referencia en la letra g);

▼M1

i) la información o la localización de los servicios que pueden utilizarse para consultar el estado de validez del certificado cualificado;

▼B

j) cuando los datos de creación del sello electrónico relacionados con los datos de validación del sello electrónico se encuentren en un dispositivo cualificado de creación de sellos electrónicos, una indicación adecuada de esto, al menos en una forma apta para el procesamiento automático.

▼B

ANEXO IV

REQUISITOS DE LOS CERTIFICADOS CUALIFICADOS DE AUTENTICACIÓN DE SITIOS WEB

Los certificados cualificados de autenticación de sitios web contendrán:

a) una indicación, al menos en un formato adecuado para el procesamiento automático, de que el certificado ha sido expedido como certificado cualificado de autenticación de sitio web;

b) un conjunto de datos que represente inequívocamente al prestador cualificado de servicios de confianza que expide los certificados cualificados, incluyendo como mínimo el Estado miembro en el que dicho prestador está establecido, y

— para personas jurídicas: el nombre y, cuando proceda, el número de registro según consten en los registros oficiales,

— para personas físicas, el nombre de la persona;

▼M1

c) para las personas físicas: al menos el nombre de la persona a la que se expida el certificado, o un seudónimo; y, cuando se use un seudónimo, una indicación clara en este sentido;

c *bis*) para las personas jurídicas: un conjunto único de datos que represente inequívocamente a la persona jurídica a la que se expide el certificado, con al menos el nombre de la persona jurídica a la que se expide el certificado y, en su caso, el número de registro tal como figura en los registros oficiales;

▼B

d) elementos de la dirección, incluida al menos la ciudad y el Estado, de la persona física o jurídica a quien se expida el certificado, y, cuando proceda, según figure en los registros oficiales;

e) el nombre o los nombres de dominio explotados por la persona física o jurídica a la que se expida el certificado;

f) los datos relativos al inicio y final del período de validez del certificado;

g) el código de identidad del certificado, que debe ser único para el prestador cualificado de servicios de confianza;

h) la firma electrónica avanzada o el sello electrónico avanzado del prestador de servicios de confianza expedidor;

i) el lugar en que está disponible gratuitamente el certificado que respalda la firma electrónica avanzada o el sello electrónico avanzado a que se hace referencia en la letra h);

▼M1

j) la información o la localización de los servicios de estado de validez del certificado que pueden utilizarse para consultar el estado de validez del certificado cualificado.

▼M1

ANEXO V

REQUISITOS APLICABLES A LA DECLARACIÓN ELECTRÓNICA CUALIFICADA DE ATRIBUTOS

La declaración electrónica cualificada de atributos contendrá:

a) una indicación, al menos en una forma adecuada para el tratamiento automático, de que la declaración ha sido expedida como declaración electrónica cualificada de atributos;

b) un conjunto de datos que represente inequívocamente al prestador cualificado de servicios de confianza que expide la declaración electrónica cualificada de atributos, que ha de incluir, como mínimo, el Estado miembro en el que dicho prestador está establecido, y:

   i) para personas jurídicas, el nombre y, cuando proceda, el número de registro según consten en los registros oficiales,

   ii) para personas físicas, el nombre de la persona;

c) un conjunto de datos que represente inequívocamente a la entidad a que se refieren los atributos declarados; y, cuando se use un seudónimo, una indicación clara en este sentido;

d) el atributo o atributos declarados, incluida, cuando proceda, la información necesaria para identificar el alcance de dichos atributos;

e) los datos relativos al inicio y final del período de validez de la declaración;

f) el código de identidad de la declaración, que debe ser único para el prestador cualificado de servicios de confianza y, si procede, la indicación del régimen de declaraciones al que pertenece la declaración de atributos;

g) la firma electrónica cualificada o el sello electrónico cualificado del prestador cualificado de servicios de confianza expedidor;

h) el lugar en que está disponible gratuitamente el certificado que respalda la firma electrónica cualificada o el sello electrónico cualificado a que se refiere la letra g);

i) la información o la localización de los servicios que pueden utilizarse para consultar el estado de validez de la declaración cualificada.

▼**M1**

ANEXO VI

LISTA MÍNIMA DE ATRIBUTOS

En virtud de lo dispuesto en el artículo 45 *sexies*, los Estados miembros garantizarán la adopción de medidas que permitan a los prestadores cualificados de servicios de confianza de declaraciones electrónicas de atributos verificar por medios electrónicos, a petición del usuario, la autenticidad de los atributos siguientes, cotejándolos con las fuentes auténticas pertinentes a escala nacional o a través de intermediarios designados reconocidos a escala nacional, de conformidad con el Derecho de la Unión o nacional y cuando tales atributos se basen en fuentes auténticas pertenecientes al sector público:

1. dirección,
2. edad,
3. sexo,
4. estado civil,
5. composición familiar,
6. nacionalidad o ciudadanía,
7. cualificaciones, títulos y licencias académicos,
8. cualificaciones, títulos y licencias profesionales,
9. facultades y mandatos para representar a personas físicas o jurídicas,
10. permisos y licencias públicos,
11. en el caso de las personas jurídicas, datos financieros y sociales.

▼M1

ANEXO VII

REQUISITOS APLICABLES A LA DECLARACIÓN ELECTRÓNICA DE ATRIBUTOS EXPEDIDA POR UN ORGANISMO PÚBLICO RESPONSABLE DE UNA FUENTE AUTÉNTICA O EN NOMBRE DE ESTE

Las declaraciones electrónicas de atributos expedidas por un organismo público responsable de una fuente auténtica, o en nombre de este, contendrán:

a) una indicación, al menos en una forma adecuada para el tratamiento automático, de que la declaración ha sido expedida como declaración electrónica de atributos por un organismo público responsable de una fuente auténtica, o en nombre de este;

b) un conjunto de datos que represente inequívocamente al organismo público que expide la declaración electrónica de atributos, que ha de incluir, como mínimo, el Estado miembro en el que dicho organismo público tiene su sede y su nombre y, en su caso, su número de registro tal como figura en los registros oficiales;

c) un conjunto de datos que represente inequívocamente a la entidad a que se refieren los atributos declarados; y, cuando se use un seudónimo, una indicación clara en este sentido;

d) el atributo o atributos declarados, incluida, cuando proceda, la información necesaria para identificar el alcance de dichos atributos;

e) los datos relativos al inicio y final del período de validez de la declaración;

f) el código de identidad de la declaración, que debe ser único para el organismo público expedidor y, si procede, una indicación del régimen de declaraciones al que pertenece la declaración de atributos;

g) la firma electrónica cualificada o el sello electrónico cualificado del organismo expedidor;

h) el lugar en que está disponible gratuitamente el certificado que respalda la firma electrónica cualificada o el sello electrónico cualificado a que se refiere la letra g);

i) la información o la localización de los servicios que pueden utilizarse para consultar el estado de validez de la declaración.