Consejo de la Unión Europea

Bruselas, 25 de noviembre de 2022
(OR. en)

14959/22

Expediente interinstitucional: 2021/0136(COD)

LIMITE

TELECOM 473
COMPET 919
MI 844
DATAPROTECT 321
JAI 1497
CODEC 1774

NOTA

De:	Comité de Representantes Permanentes (1.ª parte)
A:	Consejo
N.º doc. prec.:	14344/22
N.° doc. Ción.:	9471/21
Asunto:	Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento de un marco europeo para una identidad digital - Orientación general

I. INTRODUCCIÓN

1. El 3 de junio de 2021, la Comisión adoptó la propuesta de Reglamento sobre la Identidad Digital Europea (**eID europea**)[1]. Con esta iniciativa se pretende modificar el Reglamento eIDAS de 2014[2], con el que se habían sentado las bases necesarias para disfrutar de servicios y realizar transacciones en línea de manera segura a través de las fronteras de la UE.

[1] 9471/21.
[2] Reglamento (UE) n.º 910/2014.

2. Mediante esta propuesta, que se basa en el artículo 114 del TFUE, se exige a los Estados miembros que expidan una cartera europea de identidad digital, en el marco de un sistema de identidad electrónica notificado, sobre la base de normas técnicas comunes y tras una certificación obligatoria. A fin de establecer la arquitectura técnica necesaria, acelerar la aplicación del Reglamento revisado, facilitar directrices a los Estados miembros y evitar la fragmentación, la propuesta iba acompañada de una Recomendación sobre la creación de un conjunto de instrumentos de la Unión.

3. La propuesta de Reglamento pretende garantizar un acceso universal, para personas y empresas, a una identificación y una autenticación electrónicas seguras y fiables, y ello mediante una cartera digital personal almacenada en el teléfono móvil.

II. TRABAJOS EN LAS OTRAS INSTITUCIONES

1. En el Parlamento Europeo, la propuesta se remitió a la Comisión de Industria, Investigación y Energía (ITRE), y se solicitó el dictamen de tres comisiones asociadas, a saber, la Comisión de Mercado Interior y Protección del Consumidor (IMCO), la Comisión de Asuntos Jurídicos (JURI) y la Comisión de Libertades Civiles, Justicia y Asuntos de Interior (LIBE). La ponente del expediente es Romana Jerković (S&D, Croacia). La Comisión ITRE aún no ha aprobado su informe.

2. El 15 de julio de 2021, se solicitó al Comité Económico y Social Europeo que dictaminase sobre la propuesta, cosa que hizo el 20 de octubre de 2021. El Comité Europeo de las Regiones emitió por iniciativa propia un dictamen el 12 de octubre de 2021.

3. El Supervisor Europeo de Protección de Datos (SEPD) publicó a su vez observaciones formales al respecto el 28 de julio de 2021.

III. SITUACIÓN DE LOS TRABAJOS EN EL CONSEJO

1. En el Consejo, ha estudiado la propuesta el Grupo «Telecomunicaciones y Sociedad de la Información» (en lo sucesivo, «Grupo TELECOM»), que comenzó los debates durante la Presidencia portuguesa, en junio de 2021. El análisis de la propuesta prosiguió en el Grupo TELECOM durante la Presidencia eslovena, y la primera lectura finalizó satisfactoriamente el 15 de noviembre de 2021.

2. La Presidencia francesa presentó su **primera propuesta transaccional** el 15 de febrero y el 5 de abril, y **la segunda** se debatió el 23 de mayo y el 9 de junio. En relación con un debate de orientación celebrado en el Grupo TELECOM el 19 de julio de 2022, la Presidencia checa, a partir de la labor de la Presidencia francesa, identificó importantes cuestiones de alto nivel que estaban pendientes y solicitó a las delegaciones que indicaran sus preferencias, con vistas a la consiguiente reformulación de las partes pertinentes del segundo texto transaccional. La versión revisada dio como resultado una **tercera propuesta transaccional** que la Presidencia checa presentó en el Grupo TELECOM los días 5 y 8 de septiembre. Las iteraciones adicionales y los ajustes conexos propiciaron un mayor nivel de convergencia en relación con la mayoría de las cuestiones pendientes.

3. No obstante, la **cuarta propuesta transaccional**, presentada a las delegaciones en el Grupo TELECOM el 28 de septiembre, puso de relieve las persistentes divergencias entre Estados miembros en relación con una cuestión concreta de alto nivel, a saber, el nivel de seguridad seleccionado para la cartera europea de identidad digital. Algunos de los Estados miembros que ya cuentan con un sistema de identidad electrónica nacional adoptaron inicialmente un nivel de seguridad «sustancial», e invirtieron en él, mientras que la actual propuesta de identidad digital exige un nivel «alto». Conscientes del alto número de medios de identificación electrónica con nivel de seguridad «sustancial» emitidos en algunos Estados miembros, la Presidencia checa ha propuesto también un mecanismo para facilitar el registro de usuarios, contribuyendo así a la adopción de las carteras europeas de identidad digital. Esta disposición permite a los usuarios apuntarse a la cartera europea de identidad digital empleando medios existentes del sistema de identidad digital nacional a nivel «sustancial» que, junto con procedimientos remotos adicionales, cumplan los requisitos del nivel de seguridad «alto». Las especificaciones técnicas y operativas son objeto de legislación de aplicación, y se certificará su conformidad con los requisitos.

4. En la reunión del Grupo TELECOM del 25 de octubre se debatió la **quinta propuesta transaccional**. Durante la reunión del Grupo TELECOM del 8 de noviembre de 2022, la Presidencia checa presentó las leves modificaciones realizadas y preparó la **versión final del texto transaccional**, con vistas a su presentación al Coreper, tras recibir comentarios adicionales y sugerencias de redacción de las delegaciones.

5. El 18 de noviembre, el Coreper estudió la propuesta transaccional y **acordó de manera unánime presentarla al Consejo de Transporte, Telecomunicaciones y Energía (Telecomunicaciones), sin cambios, con vistas a una orientación general** en su reunión del 6 de diciembre de 2022.

IV. PRINCIPALES ELEMENTOS DE LA PROPUESTA TRANSACCIONAL

1. La cartera europea de identidad digital

Uno de los principales objetivos estratégicos de la propuesta de la Comisión relativa a una cartera de identidad digital europea (en lo sucesivo, «cartera») consiste en proporcionar a los ciudadanos y a otros residentes, con arreglo a la definición en el Derecho nacional, un medio de identidad digital europeo normalizado basado en el concepto de una cartera de identidad digital europea. Como medio de identidad electrónica expedido con arreglo a sistemas nacionales con nivel de seguridad «alto», la cartera constituiría un medio de identidad electrónica por derecho propio basado en la expedición de datos de identificación personal y de la cartera por parte de los Estados miembros.

2. Nivel de seguridad de las carteras europeas de identidad digital

Los niveles de seguridad deben caracterizar el grado de confianza de un medio de identificación electrónica para establecer la identidad de una persona, garantizando así que la persona que afirma poseer una identidad determinada es de hecho la persona a quien se ha atribuido dicha identidad. Gracias al amplio apoyo recibido en las reuniones de Grupo y en el debate del Coreper del 14 de octubre, la cartera debe expedirse dentro de un sistema de identificación electrónica de nivel de seguridad «alto». Además, se ha añadido al **artículo 6 *bis*** una disposición específica para el registro de usuarios. El objetivo de este cambio es resolver las inquietudes de aquellos Estados miembros en los que ya se ha expedido un gran número de medios de identidad electrónica nacionales con nivel de seguridad «sustancial». Esta disposición permite a los usuarios emplear su medio de identidad electrónica nacional junto con

procedimientos remotos de registro adicionales para permitir la acreditación con nivel «alto» y, en última instancia, para permitir la obtención de una cartera. En vista de que el proyecto de Reglamento de identidad electrónica se basa en esquemas de certificación de la ciberseguridad que deben proporcionar un nivel armonizado de confianza en la seguridad de las carteras europeas de identidad digital, está previsto que el almacenamiento seguro de materiales criptográficos pase también a ser un asunto sometido a certificación de ciberseguridad. Por consiguiente, la Presidencia ha propuesto un nuevo **considerando (10 *ter*)** en el que se abordan las condiciones técnicas previas para alcanzar un nivel de seguridad «alto» y permitir un proceso de seguimiento dentro de la aplicación de las carteras europeas de identidad digital.

3. Notificación de partes usuarias

3.1 Se ha cambiado la redacción del **artículo 6 *ter*** sobre la notificación de partes usuarias. Por norma general, el proceso de notificación mediante el cual la parte usuaria comunica su intención de confiar en la cartera debe ser rentable y proporcionado al riesgo, y debe asegurar que la parte usuaria proporciona a la cartera al menos la información que es necesario autenticar. Por defecto solo se necesita la información mínima, y la notificación debe permitir el recurso a procedimientos automáticos o sencillos de autonotificación.

3.2 No obstante, puede resultar necesario un régimen específico debido a requisitos sectoriales, como por ejemplo aquellos que se aplican al procesamiento de categorías especiales de datos personales. Por consiguiente, se ha introducido una disposición correspondiente con objeto de abarcar casos en los que se requiera un procedimiento de registro o autorización más estricto. Por otra parte, en aquellos casos en los que el Derecho nacional o de la Unión no establezca requisitos específicos para acceder a la información proporcionada por la cartera, los Estados miembros podrán eximir a dichas partes usuarias de la obligación de notificar su intención de recurrir a las carteras.

4. Certificación

4.1 El Reglamento debe aprovechar los esquemas de certificación pertinentes y existentes del Reglamento sobre la ciberseguridad, o de partes de ellos, así como confiar en ellos y obligar a su utilización, para certificar el cumplimiento de las carteras, o de partes de ellas, con los requisitos de ciberseguridad aplicables. Por consiguiente, el marco del Reglamento sobre la ciberseguridad se aplica plenamente, también el mecanismo de evaluación interpares entre autoridades nacionales de certificación de ciberseguridad contemplado en el Reglamento sobre la ciberseguridad. Con objeto de armonizar lo más posible el Reglamento de identidad electrónica y el Reglamento sobre la ciberseguridad, los Estados miembros designarán organismos públicos y privados acreditados para certificar la cartera, tal como se contempla en el Reglamento sobre la ciberseguridad.

4.2 Además, se anima a la Comisión a que encargue a la Agencia de la Unión Europea para la Ciberseguridad (ENISA) que emprenda el desarrollo y la adopción de un esquema de certificación en materia de ciberseguridad de la cartera específico para el Reglamento sobre la ciberseguridad. Hasta que se desarrolle dicho esquema, el esquema europeo de certificación de la ciberseguridad basado en criterios comunes (EUCC, por sus siglas en inglés) publicado al amparo del Reglamento sobre la ciberseguridad se empleará como metodología de base para la certificación de la cartera. En el caso de requisitos no relacionados con la ciberseguridad, especialmente aquellos que no abarquen otros aspectos funcionales y operativos de la cartera, se establecerá una lista de especificaciones, procedimientos y normas de referencia. Estos requisitos son objeto de certificación.

5. Período de aplicación para la prestación de la cartera

A partir de las directrices de los Estados miembros, se ha propuesto que el período de aplicación de veinticuatro meses se cuente a partir de la adopción de los actos de ejecución a que se refieren el **artículo 6 *bis*, apartado 11**, y el **artículo 6 *quater*, apartado 4**.

6. Tasas

En el **artículo 6 *bis*, apartado 6 *bis*,** y en el considerando correspondiente se ha aclarado que la emisión, utilización para autenticación y revocación de las carteras debe ser gratuita para las personas físicas. Los servicios que utilicen la cartera pueden conllevar gastos, como por ejemplo la expedición de declaraciones electrónicas de atributos de la cartera, excepto cuando las carteras se empleen con fines de autenticación.

7. Acceso a funciones de los equipos informáticos y de los programas informáticos, en particular las medidas de seguridad

La Presidencia ha propuesto la inclusión de una conexión explícita con el Reglamento (UE) 2022/1925, que asegura el acceso a funciones de los equipos informáticos (*hardware*) y de los programas informáticos (*software*) como parte de los servicios básicos de plataforma proporcionados por los guardianes de acceso. El nuevo artículo **12 *ter*** aclara que los prestadores de servicios de carteras y los emisores de medios de identificación electrónica notificados, actuando a título comercial o profesional, son usuarios profesionales de guardianes de acceso a tenor de lo dispuesto en la definición correspondiente del Reglamento de mercados digitales. Se ha añadido texto a los considerandos para exponer la implicación que tiene la interconexión con el Reglamento de mercados digitales, en concreto que los guardianes de acceso deben permitir la interoperabilidad y el acceso con fines de interoperabilidad de forma gratuita al mismo sistema operativo y a las funciones de equipos informáticos o programas informáticos disponibles o utilizadas en la prestación de sus servicios complementarios y de apoyo.

8. Alternativas para la expedición de la declaración electrónica de atributos por parte de organismos públicos.

Se ha mantenido la expedición de declaraciones electrónicas de atributos cualificadas por parte de proveedores cualificados, en particular la obligación para los Estados miembros de asegurar que los atributos se puedan contrastar con una fuente auténtica en el sector público. Además, se ha introducido la posibilidad de que el organismo del sector público responsable de la fuente auténtica o el organismo del sector público designado en nombre de un organismo del sector público responsable de una fuente auténtica puedan expedir en la cartera directamente las declaraciones electrónicas de atributos con los mismos efectos jurídicos que las declaraciones electrónicas de atributos cualificadas, siempre que se cumplan los requisitos necesarios. La propuesta se indica en los nuevos artículos **45 *bis*** y **45 *quinquies bis*** y en el **anexo VII**.

9. Correspondencia entre registros

Se ha cambiado el nombre del **artículo 11 *bis*** original por Correspondencia de registros, para reflejar así mejor el objetivo de la disposición. A partir de este debate, se ha mantenido el concepto de identificador único y persistente para carteras. La definición correspondiente aclara que el identificador puede estar formado por una combinación de varios identificadores nacionales y sectoriales, siempre que cumpla su cometido. Se establece explícitamente que la correspondencia entre registros se puede facilitar mediante las declaraciones electrónicas de atributos cualificadas. Además, se ha incorporado al **artículo 11 *bis*** una disposición de salvaguardia con arreglo a la cual los Estados miembros asegurarán la protección de datos personales y evitarán la elaboración de perfiles de usuarios. Por último, los Estados miembros, en calidad de partes usuarias, asegurarán la correspondencia entre registros.

VI. CONCLUSIÓN

1. Habida cuenta de lo anterior, se invita al Consejo a que:

   – examine el texto transaccional que figura en el anexo de la presente nota;

   – confirme una orientación general acerca de la propuesta de Reglamento sobre la identidad digital europea en la reunión del Consejo TTE (Telecomunicaciones) del 6 de diciembre de 2022.

ANEXO

Propuesta de

REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO

por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento de un Marco para una Identidad Digital Europea

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular su artículo 114,

Vista la propuesta de la Comisión Europea,

Previa transmisión del proyecto de acto legislativo a los Parlamentos nacionales,

Visto el dictamen del Comité Económico y Social Europeo[3],

De conformidad con el procedimiento legislativo ordinario,

Considerando lo siguiente:

(1) La Comunicación de la Comisión de 19 de febrero de 2020, titulada «Configurar el futuro digital de Europa»[4], anuncia una revisión del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo para mejorar su eficacia, extender sus beneficios al sector privado y promover unas identidades digitales de confianza para todos los europeos.

[3] DO C , , p. .
[4] COM/2020/67 final

(2) En sus conclusiones de 1 y 2 de octubre de 2020[5], el Consejo Europeo instó a la Comisión a que presentara una propuesta relativa al desarrollo, a escala de la UE, de un marco para la identificación electrónica pública segura, en particular de las firmas digitales interoperables, de modo que las personas puedan tener el control de su identidad y sus datos en línea y se facilite el acceso a los servicios digitales públicos, privados y transfronterizos.

(3) La Comunicación de la Comisión de 9 de marzo de 2021, titulada «Brújula Digital 2030: el enfoque de Europa para el Decenio Digital»[6] establece el objetivo de crear un marco a escala de la Unión que, a más tardar en 2030, dé lugar a un amplio despliegue de una identidad fiable y controlada por el usuario, que permita a cada usuario controlar sus propias interacciones y su presencia en línea.

(4) Un enfoque más armonizado en lo que respecta a la identificación digital debería reducir los riesgos y los costes asociados a la actual fragmentación derivada del uso de soluciones nacionales divergentes, y reforzará el mercado interior al permitir que los ciudadanos, otros residentes definidos en las leyes nacionales y las empresas se identifiquen en línea de manera cómoda y uniforme en toda la Unión. La cartera europea de identidad digital proporcionará un medio de identificación electrónica armonizado para todas las personas físicas y jurídicas de la Unión, y les permitirá autenticar y compartir datos relacionados con su identidad. Toda persona debe ser capaz de acceder de forma segura a servicios públicos y privados apoyándose en un ecosistema reforzado de servicios de confianza y en pruebas de identidad y declaraciones de atributos verificados, como un título universitario legalmente reconocido y aceptado en cualquier lugar de la Unión. El Marco para una Identidad Digital Europea aspira a lograr un cambio que permita pasar de la utilización exclusiva de soluciones de identidad digital al suministro de declaraciones electrónicas de atributos que sean válidas a escala europea. Los proveedores de declaraciones electrónicas de atributos deben beneficiarse de un conjunto de normas claras y uniformes, y las administraciones públicas deben poder confiar en los documentos electrónicos expedidos en un determinado formato.

---

5 https://www.consilium.europa.eu/es/press/press-releases/2020/10/02/european-council-conclusions-1-2-december-2020/

6 COM/2021/118 final/2

(4 *bis*) Varios Estados miembros han aplicado y emplean de forma generalizada medios de identificación electrónica que hoy en día son aceptados por prestadores de servicios en la Unión. Asimismo, se han realizado inversiones en soluciones tanto nacionales como transfronterizas basadas en el actual Reglamento eIDAS, en particular la infraestructura técnica de interoperabilidad de nodos del eIDAS. Con el fin de garantizar la complementariedad y la rápida adopción de las carteras europeas de identidad digital europeas por parte de usuarios existentes de los medios de identificación electrónica notificados, así como de minimizar las repercusiones sobre los prestadores de servicios existentes, se espera que las carteras europeas de identidad digital se beneficien de la experiencia adquirida con medios de identificación electrónicos existentes y aprovechen la infraestructura eIDAS desplegada a escala europea y nacional.

(5) Con el fin de fomentar la competitividad de las empresas europeas, los prestadores de servicios en línea deben poder contar con soluciones de identidad digital reconocidas en toda la Unión, independientemente del Estado miembro en el que se hayan proporcionado, de tal manera que se beneficien de un enfoque europeo armonizado de la confianza, la seguridad y la interoperabilidad. Tanto los usuarios como los proveedores de servicios deben poder beneficiarse de que se confiera el mismo valor jurídico a las declaraciones electrónicas de atributos en toda la Unión.

(6) El Reglamento (UE) 2016/679[7] es aplicable al tratamiento de datos personales efectuado en aplicación del presente Reglamento. En consecuencia, este Reglamento debe establecer salvaguardias específicas para evitar que los proveedores de medios de identificación electrónica y declaraciones electrónicas de atributos combinen datos personales obtenidos a través de otros servicios con los datos personales relacionados con los servicios contemplados en el ámbito de aplicación del presente Reglamento. El emisor conservará los datos personales relacionados con la provisión de carteras europeas de identidad digital en soporte lógico por separado de cualesquier otros datos mantenidos. El presente Reglamento no impide a los usuarios de las carteras europeas de identidad digital solicitar medidas técnicas adicionales que contribuyan a la protección de los datos personales, como por ejemplo la separación física de los datos personales relacionados con la prestación de carteras de cualquier otro dato en poder del emisor.

[7] 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).

(7) Es necesario definir las condiciones armonizadas para el establecimiento de un marco para las carteras europeas de identidad digital que proporcionarán los Estados miembros; dicho marco debe facultar a todos los ciudadanos y otros residentes de la Unión, según lo dispuesto en el Derecho nacional, para intercambiar datos relacionados con su identidad de manera segura, sencilla y cómoda, un proceso que estará bajo el control exclusivo del usuario. Se deberán desarrollar tecnologías que permitan lograr estos objetivos con el máximo nivel de seguridad, privacidad y comodidad de uso, garantizando asimismo una elevada facilidad de utilización. Los Estados miembros deben garantizar la igualdad de acceso a la identificación digital para todos sus ciudadanos y residentes.

(8) Con objeto de asegurar que las partes usuarias pueden recurrir a las carteras europeas de identidad digital y para proteger a los usuarios frente a la utilización ilícita de datos sensibles, las partes usuarias deben registrarse en el marco de un proceso de notificación. En la mayoría de los casos, los requisitos de notificación que se aplican a las partes usuarias deben basarse en la transmisión de una cantidad limitada de información necesaria para la autenticación de la parte usuaria en la cartera europea de identidad digital. Los requisitos también deben contemplar la posibilidad de utilizar procedimientos automáticos o sencillos de autonotificación, en particular el recurso y la utilización de registros existentes de los Estados miembros. Al mismo tiempo, en el caso de categorías de datos sensibles, es posible que existan regímenes específicos a escala nacional o de la Unión que puedan imponer requisitos de registro y autorización más estrictos a las partes usuarias para evitar la utilización ilícita de datos de identidad en tales casos. En otros casos de utilización, las partes usuarias pueden estar exentas de notificar su intención de usar la cartera digital europea, por ejemplo cuando un derecho de comprobar atributos concretos no exige o permite la autenticación de la parte usuaria por medios electrónicos. Normalmente, en estas situaciones presenciales el usuario es capaz de identificar a la parte usuaria gracias al contexto, como por ejemplo al interactuar con el personal de una agencia de alquiler de vehículos o de una farmacia. Se prevé que el proceso de notificación se rija por el Derecho sectorial nacional o de la Unión, puesto que esto permite asimilar varios casos de utilización que puedan tener diferencias en cuanto a requisitos de registro, modo de operación (en línea/fuera de línea) o en lo que respecta al requisito de autenticar los dispositivos que puedan tener interfaces con la cartera europea de identidad digital. No se debe establecer la obligación de verificar la utilización de la cartera europea de identidad digital por partes usuarias a escala de la cartera europea de identidad digital.

(9) Todas las carteras europeas de identidad digital deben permitir a los usuarios identificarse y autenticarse electrónicamente a través de las fronteras, tanto en línea como fuera de línea, para acceder a una amplia gama de servicios públicos y privados. Sin perjuicio de las prerrogativas de los Estados miembros en lo que respecta a la identificación de sus ciudadanos y residentes, las carteras también pueden dar respuesta a las necesidades institucionales de las administraciones públicas, las organizaciones internacionales y las instituciones, organismos, oficinas y agencias de la Unión. El uso fuera de línea será importante en numerosos sectores, especialmente el sanitario, en el que los servicios se prestan a menudo mediante la interacción cara a cara, y las recetas electrónicas deben poder utilizar códigos QR o tecnologías similares para verificar su autenticidad. Basándose en el nivel de seguridad «alto», las carteras europeas de identidad digital deben beneficiarse del potencial que ofrecen las soluciones inviolables, como las medidas de protección, para cumplir los requisitos de seguridad previstos en el presente Reglamento. Asimismo, las carteras europeas de identidad digital deben permitir a los usuarios crear y utilizar firmas y sellos electrónicos cualificados que se acepten en toda la UE. En aras de la simplificación y la reducción de costes en beneficio de las personas y empresas de toda la UE, en particular mediante la posibilidad de otorgar poderes de representación y mandatos electrónicos, los Estados miembros deberán expedir carteras europeas de identidad digital basándose en normas comunes para garantizar una interoperabilidad fluida y un nivel de seguridad elevado. Las autoridades competentes de los Estados miembros son las únicas que pueden proporcionar un alto grado de confianza en la determinación de la identidad de una persona y, por lo tanto, ofrecer garantías de que la persona que afirma o manifiesta poseer una determinada identidad es, de hecho, quien dice ser. Por lo tanto, es necesario que las carteras europeas de identidad digital se basen en la identidad legal de los ciudadanos, otros residentes o entidades jurídicas. La confianza en las carteras europeas de identidad digital aumentará por el hecho de que las partes emisoras tienen el deber de introducir medidas técnicas y organizativas adecuadas para asegurar un nivel de seguridad proporcional a los riesgos planteados para los derechos y libertades de las personas físicas, en consonancia con el Reglamento (UE) 2016/679. La expedición, utilización para autenticación y revocación de las carteras europeas de identidad digital será gratuita para las personas físicas. Los servicios que utilicen la cartera pueden conllevar gastos, como por ejemplo la expedición de declaraciones electrónicas de atributos de la cartera.

(9 *bis*) Resulta beneficioso facilitar la adopción y utilización de carteras europeas de identidad digital mediante su integración sin dificultades en el ecosistema de servicios públicos y privados ya vigente a escala nacional, local o regional. A tal fin, los Estados miembros pueden contemplar medidas jurídicas y organizativas que mejoren la flexibilidad para los emisores de carteras europeas de identidad digital y que hagan posibles otras funcionalidades de las carteras europeas de identidad digital aparte de las indicadas en el presente Reglamento, en particular mediante un refuerzo de la interoperabilidad con los medios de identidad electrónica nacionales existentes. Esto no debería en ningún caso ir en detrimento de la prestación de las funciones esenciales de las carteras europeas de identidad digital, tal como figuran en el presente Reglamento, o de la promoción de soluciones nacionales existentes en lugar de las carteras europeas de identidad digital. Estas funcionalidades adicionales exceden el ámbito de aplicación del presente Reglamento, y por ello no se benefician de las disposiciones sobre uso transfronterizo de carteras europeas de identidad digital que figuran en el presente Reglamento.

(10) Para lograr un nivel alto de seguridad y fiabilidad de protección de datos, el presente Reglamento debe establecer un marco armonizado en el que se establezcan las especificaciones y los requisitos comunes que deben satisfacer las carteras europeas de identidad digital. La acreditación de la conformidad de las carteras europeas de identidad digital con estos requisitos corresponderá a organismos acreditados de la evaluación de la conformidad designados por los Estados miembros. En particular, la certificación debe usar esquemas europeos de certificación de la ciberseguridad, o parte de ellos, establecidos en virtud del Reglamento (UE) 2019/881[8], en la medida en que abarquen los requisitos de ciberseguridad de aplicación a las carteras europeas de identidad digital. La utilización de esquemas europeos de certificación de la ciberseguridad debe proporcionar un nivel armonizado de confianza en la seguridad de las carteras europeas de identidad digital, independientemente del lugar de su expedición dentro de la Unión. La certificación de la ciberseguridad de las carteras europeas de identidad digital debe apoyarse en la función de las autoridades nacionales de certificación de la ciberseguridad consistente en supervisar y verificar la conformidad de los certificados emitidos por los organismos de evaluación de la conformidad dentro de su jurisdicción con los sistemas europeos de ciberseguridad pertinentes. Del mismo modo, la certificación debe emplear, según convenga, las normas y especificaciones técnicas que se indican en el Reglamento (UE) 2019/881. Dichas especificaciones se pueden emplear como documentos de tecnología avanzada, tal como se contempla en los esquemas de certificación de la ciberseguridad pertinentes con arreglo al Reglamento (UE) 2019/881. En aquellos casos en que ningún esquema europeo de certificación de ciberseguridad pertinente establecido con arreglo al Reglamento (UE) 2019/881 abarque la certificación de servicios o procesos pertinentes que contribuyan a la seguridad de la cartera, se crearán esquemas adecuados de conformidad con el título III de dicho Reglamento. Se establecerá un esquema común y armonizado para la certificación de las carteras europeas de identidad digital con el fin de evaluar su cumplimiento de las especificaciones y los requisitos comunes contemplados en el presente Reglamento, aparte de aquellos relacionados con la ciberseguridad y la protección de los datos, en particular los que abarquen aspectos funcionales y operativos. En lo que respecta a esta certificación, se establecerán mecanismos y procedimientos para fomentar el aprendizaje inter pares y la cooperación entre Estados miembros en relación con el seguimiento y la revisión de los organismos de certificación y los certificados y los informes de certificación que emiten, para así asegurar un alto nivel de confianza y transparencia. Este mecanismo de aprendizaje inter pares se entenderá sin perjuicio de lo dispuesto en el Reglamento (UE) 2016/679 y en el Reglamento (UE) 2019/881. La certificación de la cartera con arreglo al Reglamento (UE) 2016/679 es una de las herramientas voluntarias que se pueden emplear para demostrar el cumplimiento de los requisitos establecidos en el Reglamento (UE) 2016/679 en la medida en que se aplican a las carteras europeas de identidad digital y su prestación a la ciudadanía europea.

---

8 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).

(10 *bis*) El registro de ciudadanos y residentes en la cartera europea de identidad digital se debe permitir mediante la utilización de medios de identificación electrónicos expedidos a un nivel de seguridad «alto». Solo se debe recurrir a los medios de identificación electrónicos expedidos a un nivel de seguridad «sustancial» en aquellos casos en los que las especificaciones técnicas y operativas armonizadas que empleen medios de identificación electrónicos expedidos a un nivel de seguridad «sustancial» en combinación con otros medios complementarios de verificación de la identidad permitan el cumplimiento de los requisitos establecidos en el presente Reglamento en relación con el nivel de seguridad «alto». Estos medios o medidas complementarios deben ser fiables y sencillos de utilizar para los usuarios, y se pueden desarrollar teniendo en cuenta la posibilidad de emplear procedimientos remotos de registro adicionales, certificados cualificados sustentados en firmas cualificadas, declaraciones electrónicas de atributos cualificadas o una combinación de estos. Para asegurar una implantación suficiente de las carteras europeas de identidad digital, se establecerán mediante actos de ejecución especificaciones técnicas y operativas armonizadas para el registro de usuarios por medios de identificación electrónica, en particular aquellos expedidos a un nivel de seguridad «sustancial».

(10 *ter*) El objetivo del presente Reglamento consiste en proporcionar al usuario una cartera europea de identidad digital que sea completamente portátil, segura y fácil de utilizar. Como medida transitoria hasta que estén disponibles soluciones certificadas inviolables, como por ejemplo elementos seguros dentro de los dispositivos de los usuarios, las carteras europeas de identidad digital podrán emplear bien elementos seguros externos certificados para proteger el material criptográfico y otros datos sensibles, bien soluciones nacionales notificadas con un nivel de seguridad «alto» para demostrar el cumplimiento de los requisitos pertinentes del Reglamento en lo que respecta al nivel de seguridad de la cartera. La utilización de esta medida transitoria se debe limitar a aquellos casos que exijan un nivel de seguridad «alto», como el registro del usuario en la cartera y la autenticación para acceder a servicios que requieran un nivel de seguridad «alto». En aquellos casos en los que se realice la autenticación para acceder a servicios que requieran un nivel de seguridad «sustancial», las carteras europeas de identidad digital no deben exigir la utilización de dicha medida transitoria. El presente Reglamento se entiende sin perjuicio de las condiciones nacionales para la expedición y utilización de elementos seguros externos certificados en caso de que esta medida transitoria los necesite.

(11) Las carteras europeas de identidad digital deben garantizar el máximo nivel de protección y seguridad para los datos personales utilizados con fines de autenticación, con independencia de que dichos datos se almacenen de forma local o mediante soluciones en la nube, teniendo en cuenta los diferentes niveles de riesgo. El tratamiento de los datos biométricos como factor de autenticación en la autenticación reforzada de usuario es uno de los métodos de identificación que proporcionan un nivel alto de confianza, en particular cuando se combinan con otros elementos de autenticación. Dado que los datos biométricos representan una característica única de una persona, su tratamiento solo esta permitido en virtud de las excepciones del artículo 9, apartado 2, del Reglamento (UE) 2016/679 y requiere garantías adecuadas, proporcionales al riesgo que dicho tratamiento puede conllevar para los derechos y las libertades de las personas físicas.

(11 *bis*) El funcionamiento de las carteras europeas de identidad digital debe ser transparente y permitir un tratamiento verificable de los datos personales. Para lograrlo, se anima a los Estados miembros a que revelen el código fuente de los componentes de programas informáticos de las carteras europeas de identidad digital relacionados con el tratamiento de datos personales y datos de personas jurídicas. La divulgación de dicho código fuente permite a la sociedad, incluidos los usuarios y desarrolladores, comprender su funcionamiento. Asimismo, puede aumentar la confianza de los usuarios en el ecosistema de carteras y contribuir a la seguridad de las mismas, al permitir que cualquier persona denuncie vulnerabilidades y errores en el código. Esto anima a los proveedores a ofrecer y mantener un producto altamente seguro. Además, y cuando proceda, también se anima a los Estados miembros a que pongan a disposición el código fuente con una licencia de código abierto. Una licencia de código abierto permite a la sociedad, incluidos los usuarios y desarrolladores, modificar y reutilizar el código fuente.

(12) Con el objetivo de asegurar que el marco de identidad digital europea esté abierto a la innovación y al desarrollo tecnológico y ofrezca garantías ante el futuro, se debe alentar a los Estados miembros a que establezcan conjuntamente entornos de pruebas para experimentar con soluciones innovadoras en un entorno controlado y seguro, en particular para mejorar la funcionalidad, la protección de los datos personales, la seguridad y la interoperabilidad de las soluciones, así como para obtener información útil de cara a futuras actualizaciones de las referencias técnicas y los requisitos legales. Este entorno debe fomentar la inclusión de las pequeñas y medianas empresas europeas, las empresas emergentes y los innovadores e investigadores individuales.

(13) El Reglamento (UE) 2019/1157[9] aumenta la seguridad de los documentos de identidad al introducir características de seguridad reforzadas a más tardar en agosto de 2021. Los Estados miembros deben analizar la viabilidad de notificar estas características en el marco de los sistemas de identificación electrónica para ampliar la disponibilidad transfronteriza de medios de identificación electrónica.

(14) Es necesario simplificar y agilizar el proceso de notificación de sistemas de identificación electrónica para favorecer el acceso a soluciones de autenticación e identificación cómodas, seguras, innovadoras y de confianza y, cuando proceda, alentar a los proveedores de identidad privada a que ofrezcan sistemas de identificación electrónica a las autoridades de los Estados miembros con fines de notificación, como los sistemas nacionales de identificación electrónica contemplados en el Reglamento 910/2014.

(15) La racionalización de los procedimientos de notificación y revisión por pares actualmente existentes evitará la heterogeneidad de enfoques con respecto a la evaluación de los diversos sistemas de identificación electrónica notificados y facilitará la creación de confianza entre los Estados miembros. Unos mecanismos nuevos y más sencillos deberán estimular la cooperación de los Estados miembros en materia de seguridad e interoperabilidad de sus sistemas de identificación electrónica notificados.

(16) Los Estados miembros deben beneficiarse de la disponibilidad de herramientas nuevas y flexibles que garanticen el cumplimiento de los requisitos del presente Reglamento y en los actos de ejecución pertinentes. El presente Reglamento debe permitir que los Estados miembros utilicen los informes elaborados y las evaluaciones realizadas por los organismos de evaluación de la conformidad acreditados, como los esquemas de certificación que deben establecerse a escala de la Unión en virtud del Reglamento (UE) 2019/881, para respaldar sus afirmaciones sobre la conformidad de dichos esquemas o de determinadas partes de ellos con los requisitos del Reglamento sobre la interoperabilidad y la seguridad de los sistemas de identificación electrónica notificados.

[9] Reglamento (UE) 2019/1157 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, sobre el refuerzo de la seguridad de los documentos de identidad de los ciudadanos de la Unión y de los documentos de residencia expedidos a ciudadanos de la Unión y a los miembros de sus familias que ejerzan su derecho a la libre circulación (DO L 188 de 12.7.2019, p. 67).

(17 *bis*) El uso de identificadores únicos y persistentes expedidos por los Estados miembros o generados por la cartera europea de identidad digital, junto con el uso de datos de identificación personal, es esencial para garantizar que pueda verificarse la identidad del usuario, en particular en el sector público y cuando así lo exija el Derecho nacional o de la Unión. El presente Reglamento debe garantizar que la cartera europea de identidad digital puede proporcionar un mecanismo que permita la correspondencia entre registros, en particular mediante el uso de declaraciones electrónicas cualificadas de atributos, y permitir la inclusión de identificadores únicos y persistentes en el conjunto de datos de identificación de personas. Un identificador único y persistente puede consistir en datos de identificación únicos o múltiples que pueden ser sectoriales siempre que sirvan para identificar de manera unívoca al usuario en toda la Unión. La cartera europea de identidad digital también debe proporcionar un mecanismo que permita el uso de identificadores específicos de la parte usuaria en los casos en que el Derecho nacional o de la Unión exija el uso de un identificador único y persistente. En todos los casos, el mecanismo previsto para facilitar la correspondencia entre registros y el uso de identificadores únicos y persistentes debe garantizar que el usuario esté protegido contra el uso indebido de datos personales, de conformidad con el presente Reglamento y el Derecho de la Unión aplicable, en particular el Reglamento (UE) 2016/679, incluido el riesgo de elaboración de perfiles y seguimiento relacionado con el uso de la cartera europea de identidad digital.

(17 *bis bis*) Es esencial tener en cuenta las necesidades de los usuarios, impulsando así la demanda de carteras europeas de identidad digital. Deben existir casos de uso significativos y servicios en línea basados en las carteras europeas de identidad digital disponibles. En aras de la comodidad de los usuarios y con el fin de garantizar la disponibilidad transfronteriza de dichos servicios, es importante emprender acciones para facilitar un enfoque similar en el diseño, el desarrollo y la aplicación de los servicios en línea en todos los Estados miembros. Las directrices no vinculantes sobre cómo diseñar, desarrollar y aplicar servicios en línea basados en las carteras europeas de identidad digital tienen el potencial de convertirse en una herramienta útil para alcanzar este objetivo. Estas directrices deben elaborarse teniendo debidamente en cuenta el marco de interoperabilidad de la Unión. Los Estados miembros deben desempeñar un papel de liderazgo a la hora de adoptarlos.

(18) En consonancia con la Directiva (UE) 2019/882[10], las personas con discapacidad deben poder utilizar las carteras europeas de identidad digital, los servicios de confianza y los productos destinados a los usuarios finales empleados en la prestación de dichos servicios, en igualdad de condiciones que el resto de los usuarios.

(19) El presente Reglamento no debe regular los aspectos relacionados con la celebración y validez de los contratos u otras obligaciones legales cuando existan requisitos de forma establecidos por el Derecho nacional o de la Unión. Por otro lado, no debe afectar a los requisitos nacionales de formato correspondientes a los registros públicos, en particular los registros mercantiles y de la propiedad.

(20) La prestación y utilización de servicios de confianza está adquiriendo una importancia creciente para el comercio y la cooperación internacionales. Los socios internacionales de la UE están creando marcos de confianza inspirados en el Reglamento (UE) n.º 910/2014. Por consiguiente, para facilitar el reconocimiento de dichos servicios y de los proveedores que los prestan, se podrán establecer mediante legislación de aplicación las condiciones en las que los marcos de confianza de terceros países podrán considerarse equivalentes al marco de confianza para los servicios y proveedores de confianza cualificados previsto en este Reglamento, como complemento a la posibilidad del reconocimiento mutuo de los servicios y proveedores de confianza establecidos en la Unión y en terceros países de conformidad con el artículo 218 del Tratado. Al establecer las condiciones en las que los marcos de confianza de terceros países podrían considerarse equivalentes al marco de confianza para los servicios y proveedores de confianza cualificados en el presente Reglamento, también debe garantizarse el cumplimiento de las disposiciones pertinentes de la Directiva XXXX/XXXX (Directiva SRI 2) y del Reglamento (UE) 2016/679, así como el uso de listas de confianza como elementos esenciales para generar confianza.

[10] 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).

(21) Este Reglamento debe basarse en actos de la Unión que garanticen mercados disputables y equitativos en el sector digital. En particular, se basa en el Reglamento (UE) 2022/1925, que establece normas para los proveedores de servicios básicos de plataforma designados como guardianes y, entre otras cosas, prohíbe que estos últimos exijan a los usuarios profesionales que utilicen, ofrezcan o interoperen con un servicio de identificación del guardián en el contexto de los servicios ofrecidos por los usuarios profesionales que utilizan los servicios básicos de plataforma del mencionado guardián. El artículo 6, apartado 7, del Reglamento 2022/1925 obliga a los guardianes a permitir a los usuarios profesionales y proveedores de servicios complementarios el acceso y la interoperabilidad con las mismas funciones del sistema operativo, el equipo o el programa informático que están disponibles o se utilizan en la prestación de servicios complementarios por parte del guardián. De acuerdo con el artículo 2, apartado 15, del Reglamento de Mercados Digitales, los servicios de identificación constituyen un tipo de servicios complementarios. Los usuarios profesionales y los proveedores de servicios complementarios deben, por tanto, poder acceder a dichas funciones del equipo (*hardware*) o del programa informático (*software*), como las medidas de seguridad de los teléfonos inteligentes, e interoperar con ellas a través de las carteras europeas de identidad digital o de los medios de identificación electrónica notificados por los Estados miembros.

(22) Con el fin de racionalizar las obligaciones impuestas a los prestadores de servicios de confianza en materia de ciberseguridad y de posibilitar que dichos prestadores y sus respectivas autoridades competentes se beneficien del marco jurídico que se establece en la Directiva XXXX/XXXX (Directiva SRI 2), los servicios de confianza deben adoptar medidas técnicas y organizativas adecuadas en virtud de la Directiva XXXX/XXXX (Directiva SRI 2), como medidas dirigidas a corregir fallos del sistema, errores humanos, actos maliciosos o fenómenos naturales, con objeto de gestionar los riesgos para la seguridad de las redes y los sistemas de información que emplean dichos prestadores, así como con objeto de notificar incidentes y ciberamenazas importantes de conformidad con la Directiva XXXX/XXXX (Directiva SRI 2) Con respecto a la notificación de incidentes, los prestadores de servicios de confianza deberán notificar cualquier incidente que tenga un impacto significativo en la prestación de sus servicios, especialmente los causados por el robo o extravío de dispositivos, el deterioro de los cables de red o incidentes producidos en el contexto de la identificación de personas. Los requisitos en materia de gestión de riesgos de la ciberseguridad y las obligaciones de notificación que contempla la Directiva XXXXXX (Directiva SRI 2) deben considerarse complementarios a los requisitos impuestos a los prestadores de servicios de confianza en virtud del presente Reglamento. Cuando corresponda, las autoridades competentes designadas al amparo de la Directiva XXXX/XXXX (Directiva SRI 2) deberán seguir aplicando las prácticas u orientaciones nacionales establecidas en relación con el cumplimiento de los requisitos de seguridad y notificación y con la supervisión de la conformidad con dichos requisitos en virtud del Reglamento (UE) n.º 910/2014. Los requisitos que se establecen en este Reglamento no afectan a la obligación de notificar las violaciones de los datos personales con arreglo al Reglamento (UE) 2016/679.

(23) Se deberá prestar la debida atención para garantizar una cooperación eficaz entre las autoridades competentes en materia de seguridad de las redes y de la información y las responsables de la identificación electrónica, la autenticación y los servicios de confianza. En los casos en que el órgano de control previsto en este Reglamento sea distinto de las autoridades competentes designadas en virtud de la Directiva XXXX/XXXX (SRI 2), dichas autoridades cooperarán estrechamente y de manera oportuna, intercambiando entre ellas la información pertinente para garantizar una supervisión eficaz y la conformidad de los prestadores de servicios de confianza con los requisitos establecidos en este Reglamento y en la Directiva XXXX/XXXX (SRI 2). En particular, los órganos de control contemplados en este Reglamento deben estar facultados para solicitar a la autoridad competente designada en virtud de la Directiva XXXXX/XXXX (SRI 2) que proporcione la información pertinente necesaria para otorgar la condición de «cualificado» y que lleve a cabo las actuaciones de control requeridas para verificar la conformidad de los prestadores de servicios de confianza con los requisitos pertinentes de la Directiva SRI 2 o exigir a estos que subsanen cualquier incumplimiento.

(24) Es esencial proporcionar un marco jurídico para facilitar el reconocimiento transfronterizo entre los ordenamientos jurídicos nacionales existentes relacionados con servicios de entrega electrónica certificada. Dicho marco puede abrir, además, nuevas oportunidades de mercados para que los prestadores de servicios de confianza de la Unión ofrezcan nuevos servicios paneuropeos de entrega electrónica certificada. A fin de garantizar que los datos que utilizan un servicio cualificado de entrega electrónica certificada se entreguen al destinatario correcto, los servicios cualificados de entrega electrónica certificada deben garantizar con total certeza la identificación del destinatario, mientras que para identificar al remitente es suficiente un nivel alto de confianza. Los Estados miembros deben alentar a los proveedores de servicios cualificados de entrega electrónica certificada a que sus servicios sean interoperables con los servicios cualificados de entrega electrónica certificada prestados por otros prestadores cualificados de servicios de confianza a fin de transferir fácilmente los datos electrónicos registrados entre dos o más prestadores cualificados de servicios de confianza y promover prácticas justas en el mercado interior.

(25) En la mayoría de los casos, los ciudadanos y otros residentes no pueden intercambiar por medios electrónicos información relacionada con su identidad (como sus direcciones, su edad o sus cualificaciones profesionales, sus permisos de conducción y otros permisos y datos de pago), a escala transfronteriza, de forma segura y con un nivel alto de protección de los datos.

(26) Debe ser posible emitir y gestionar atributos digitales fiables, así como contribuir a reducir la carga administrativa; de ese modo se facultará a los ciudadanos y a otros residentes para utilizar estos atributos en sus transacciones públicas y privadas. Los ciudadanos y otros residentes deben poder, por ejemplo, demostrar la titularidad de un permiso de conducción válido expedido por una autoridad de un Estado miembro, que pueda ser verificada y admitida por las autoridades competentes de otro Estado miembro, así como utilizar sus credenciales de la seguridad social o los futuros documentos digitales de viaje en un contexto transfronterizo.

(27) Cualquier entidad que recopile, cree y emita atributos certificados, como diplomas, permisos o certificados de nacimiento, debe tener la posibilidad de expedir declaraciones electrónicas de atributos. Las partes usuarias deben utilizar las declaraciones electrónicas de atributos como equivalentes a las declaraciones emitidas en formato impreso. En consecuencia, no se deben denegar los efectos jurídicos de una declaración electrónica de atributos por el mero hecho de que esta haya sido emitida en formato electrónico o porque no cumpla todos los requisitos de la declaración electrónica de atributos cualificada. Con este fin, deberán establecerse requisitos generales para asegurar que una declaración electrónica de atributos cualificada tenga un efecto jurídico equivalente al de las declaraciones legalmente emitidas en formato impreso. Sin embargo, tales requisitos deberán aplicarse sin perjuicio del Derecho nacional o de la Unión que defina los requisitos adicionales específicos del sector con respecto a los efectos jurídicos subyacentes de cada formato, y, en particular, el reconocimiento transfronterizo de la declaración electrónica de atributos cualificada, cuando corresponda.

(28) Para lograr una amplia disponibilidad y facilidad de uso de las carteras europeas de identidad digital es necesario que los prestadores de servicios privados las acepten. Las partes usuarias privadas que prestan servicios en los ámbitos del transporte, la energía, la banca, los servicios financieros, la seguridad social, la salud, el agua potable, los servicios postales, la infraestructura digital, la educación o las telecomunicaciones deben aceptar el uso de las carteras europeas de identidad digital para la prestación de servicios en los casos en los que el Derecho nacional, el de la Unión o una obligación contractual requieran una autenticación reforzada de los usuarios. Para facilitar el uso y la aceptación de la cartera europea de identidad digital, deben tenerse en cuenta las normas y especificaciones industriales ampliamente aceptadas. Cuando las plataformas en línea de muy gran tamaño, según se definen en el artículo 25, apartado 1, del Reglamento [referencia al Reglamento de Servicios Digitales] exijan a los usuarios autenticarse para acceder a servicios en línea, dichas plataformas deberán tener la obligación de aceptar el uso de carteras europeas de identidad digital si así lo solicita voluntariamente el usuario. Los usuarios no deben tener ninguna obligación de utilizar la cartera para acceder a servicios privados, pero si desean hacerlo, las plataformas en línea de gran tamaño deberán aceptar la cartera europea de identidad digital con ese fin, respetando en todo momento el principio de minimización de datos. Dada la importancia de las plataformas en línea de muy gran tamaño y debido a su alcance, en particular por lo que respecta al número de receptores del servicio y de transacciones económicas, esto es necesario para incrementar la protección de los usuarios frente al fraude y garantizar un nivel alto de protección de datos. Es preciso desarrollar códigos de conducta de autorregulación a escala de la Unión («códigos de conducta») para contribuir a una amplia disponibilidad y facilidad de uso de los medios de identificación electrónica (en particular, de las carteras europeas de identidad digital) contemplados en el ámbito de aplicación de este Reglamento. Estos códigos de conducta deben facilitar una aceptación amplia de los medios de identificación electrónica, incluidas las carteras europeas de identidad digital, por parte de los prestadores de servicios que no se ajusten a la definición de plataformas de muy gran tamaño y que se apoyen en servicios de identificación electrónica de terceros para autenticar a sus usuarios. Los códigos de conducta deberán elaborarse dentro de los doce meses siguientes a la adopción de este Reglamento. La Comisión deberá evaluar la eficacia de estas disposiciones relativas a la disponibilidad y facilidad de uso de las carteras europeas de identidad digital para los usuarios al cabo de veinticuatro meses de su implantación.

(29) La divulgación selectiva es un concepto que faculta al propietario de los datos para revelar solo determinadas partes de un conjunto de datos más amplio, a fin de que la entidad receptora obtenga únicamente la información necesaria; por ejemplo, un usuario revela a una parte usuaria solo los datos necesarios para la prestación de un servicio solicitado por el usuario. La cartera europea de identidad digital debe permitir técnicamente la divulgación selectiva de atributos a las partes usuarias. Estos atributos divulgados selectivamente, incluso cuando originalmente formen partes de diferentes declaraciones electrónicas múltiples, se podrán combinar posteriormente y presentar a las partes usuarias. Esta función debe convertirse en una característica básica del diseño de la cartera, reforzando así la comodidad y la protección de los datos personales, en especial la minimización.

(30) Los atributos proporcionados por los prestadores cualificados de servicios de confianza como parte de la declaración cualificada de atributos deberán cotejarse con las fuentes auténticas, ya sea directamente por el prestador cualificado de servicios de confianza o a través de intermediarios designados reconocidos a escala nacional, de conformidad con el Derecho nacional o de la Unión, a efectos de proteger el intercambio de los atributos declarados entre los prestadores de servicios de identidad o de declaración de atributos y las partes usuarias. Los Estados miembros deben establecer mecanismos adecuados a nivel nacional para garantizar que los prestadores cualificados de servicios de confianza que emitan declaraciones electrónicas de atributos cualificadas puedan, sobre la base del consentimiento de la persona a la que se expide la declaración, verificar la autenticidad de los atributos que dependen de fuentes auténticas. Los mecanismos adecuados podrán incluir el uso de intermediarios específicos o soluciones técnicas de conformidad con el Derecho nacional que permitan el acceso a fuentes auténticas. Garantizar la disponibilidad de un mecanismo que permita la verificación de atributos frente a fuentes auténticas debe facilitar la conformidad de los prestadores cualificados de servicios de confianza de declaraciones electrónicas de atributos cualificadas con las obligaciones que les impone el presente Reglamento. El anexo VI contiene una lista de categorías de atributos para las cuales los Estados miembros deben velar por que se adopten medidas para que los proveedores cualificados de declaraciones electrónicas de atributos puedan verificar por medios electrónicos, a petición del usuario, su autenticidad con respecto a la fuente auténtica pertinente. Los Estados miembros deben acordar atributos específicos que correspondan a estas categorías.

(31) La identificación electrónica segura y la provisión de declaraciones de atributos deben ofrecer una flexibilidad y soluciones adicionales para el sector de los servicios financieros, con objeto de posibilitar la identificación de los clientes y el intercambio de los atributos específicos que sea necesario cumplir, como los requisitos de debida diligencia con los clientes en virtud del Reglamento relativo a la lucha contra el blanqueo de capitales, [añádase la referencia una vez adoptada la propuesta], los requisitos de idoneidad que emanan de la legislación sobre la protección de los inversores, o para facilitar el cumplimiento de los requisitos de autenticación reforzada de los clientes para la identificación en línea a efectos de la conexión a las cuentas o la realización de transacciones en el ámbito de los servicios de pago.

(31 *bis*) A fin de garantizar la coherencia de las prácticas de certificación en toda la UE, la Comisión debe publicar directrices sobre la certificación y la renovación de los dispositivos cualificados de creación de firma electrónica y de los dispositivos cualificados de creación de sello electrónico, incluidas su validez y sus limitaciones temporales. El presente Reglamento no impide a los Estados miembros permitir que los organismos públicos o privados que hayan certificado dispositivos cualificados de creación de firma electrónica prorroguen temporalmente la validez de la certificación cuando una nueva certificación del mismo dispositivo no pueda realizarse en el plazo legalmente definido por una razón distinta de una violación o incidente de seguridad, y sin perjuicio de la práctica de certificación aplicable.

(32) Los servicios de autenticación de sitios web proporcionan a los usuarios un nivel alto de certeza de que existe una entidad auténtica y legítima que respalda la existencia del sitio web, independientemente de la plataforma utilizada para mostrarlo. Estos servicios contribuyen a crear confianza y fe en la realización de operaciones mercantiles en línea y a reducir los casos de fraude en línea. El uso de servicios de autenticación de sitios web por parte de estos últimos debe ser voluntario. No obstante, para que la autenticación de sitios web llegue a ser un medio de aumentar la confianza, proporcionar al usuario una experiencia mejor y propiciar el crecimiento en el mercado interior, el presente Reglamento debe establecer obligaciones mínimas de seguridad y responsabilidad para los prestadores de servicios de autenticación de sitios web y los servicios que prestan. Con este fin, los proveedores de navegadores web deben garantizar la compatibilidad e interoperabilidad con los certificados cualificados para la autenticación de sitios web previstos en el Reglamento (UE) n.º 910/2014. Deben reconocer los certificados cualificados de autenticación de sitios web y permitir la visualización de los datos de identidad certificados al usuario final en el entorno del navegador con arreglo a las especificaciones establecidas de conformidad con el presente Reglamento. El reconocimiento de un certificado cualificado de autenticación de sitios web como certificado cualificado expedido por un prestador cualificado de servicios de confianza debe garantizar que los datos de identidad incluidos en el certificado puedan autenticarse y verificarse de conformidad con el presente Reglamento. Esto no debe afectar a la posibilidad de que los proveedores de navegadores web subsanen las principales irregularidades relacionadas con la violación de la seguridad y la pérdida de integridad de los certificados individuales, contribuyendo así a la seguridad en línea de los usuarios finales. Para mejorar la protección de los ciudadanos y promover su uso, las autoridades públicas de los Estados miembros deben estudiar la posibilidad de incorporar en sus sitios web certificados cualificados para la autenticación de sitios web.

(33) Muchos Estados miembros han introducido requisitos nacionales para la prestación de servicios de archivo digital seguros y fiables con el objetivo de posibilitar la conservación de datos electrónicos y de los servicios de confianza asociados a estos durante largos períodos. Para garantizar la seguridad jurídica, la confianza y la armonización en todos los Estados miembros, debe establecerse un marco jurídico para los servicios cualificados de archivo electrónico, inspirado en el marco de los demás servicios de confianza establecidos en el presente Reglamento. Este marco debe ofrecer a los prestadores de servicios de confianza y a los usuarios un conjunto de herramientas eficiente que incluya requisitos funcionales para el servicio de archivo electrónico, así como efectos jurídicos claros cuando se utilice un servicio cualificado de archivo electrónico. Estas disposiciones deben aplicarse a los documentos de origen electrónico, así como a los documentos en papel escaneados y digitalizados. Cuando sea necesario, estas disposiciones deben permitir la reproducción de los datos electrónicos conservados en diferentes soportes o formatos con el fin de ampliar su durabilidad y legibilidad más allá del período de validez tecnológica, minimizando al mismo tiempo la pérdida y la alteración en la mayor medida posible. Cuando los datos electrónicos presentados al servicio de archivo digital contengan una o varias firmas electrónicas cualificadas o sellos electrónicos cualificados, el servicio debe utilizar procedimientos y tecnologías capaces de ampliar su fiabilidad durante el período de conservación de dichos datos, posiblemente basándose en el uso de otros servicios de confianza electrónicos cualificados establecidos por el presente Reglamento. Para crear pruebas de conservación cuando se utilicen firmas electrónicas, sellos electrónicos o sellos de tiempo electrónicos, deben utilizarse servicios de confianza electrónicos cualificados. En la medida en que los servicios de archivo electrónico no estén armonizados por el presente Reglamento, los Estados miembros podrán mantener o introducir disposiciones nacionales, de conformidad con el Derecho de la Unión, relativas a dichos servicios, tales como disposiciones específicas que permitan algunas excepciones para los servicios integrados en una organización y estrictamente utilizados para los «archivos internos» de dicha organización. El presente Reglamento no debe distinguir entre documentos de origen electrónico y documentos físicos que han sido digitalizados.

(33 *bis*) Los archivos nacionales y las instituciones de memoria, en su calidad de organizaciones dedicadas a la conservación del patrimonio documental en interés público, suelen tener sus actividades estipuladas por la legislación nacional y no necesariamente prestan servicios de confianza en el sentido del presente Reglamento. En la medida en que estas instituciones no presten tales servicios, el presente Reglamento se entiende sin perjuicio de su funcionamiento.

(34) Los libros mayores electrónicos son una secuencia de registros electrónicos de datos que garantizan su integridad y la exactitud de su orden cronológico. La finalidad de los libros mayores electrónicos es establecer una secuencia cronológica de registros de datos para evitar que los activos digitales se copien y vendan a varios destinatarios. Los libros mayores electrónicos pueden utilizarse, por ejemplo, para los registros digitales de propiedad en el comercio mundial, la financiación de la cadena de suministro, la digitalización de los derechos de propiedad intelectual o de mercancías como la electricidad. Junto con otras tecnologías, pueden contribuir a encontrar soluciones para unos servicios públicos más eficientes y con capacidad transformadora, como el voto electrónico, la cooperación transfronteriza de las autoridades aduaneras o de las instituciones académicas o el registro de la propiedad de bienes inmuebles en registros descentralizados de la propiedad inmobiliaria. Los libros mayores electrónicos cualificados crean una presunción legal para el orden cronológico secuencial único y exacto y la integridad de los registros de datos del libro mayor. Los atributos específicos de los libros mayores electrónicos, es decir, el orden cronológico secuencial de los registros de datos, distinguen los libros mayores electrónicos de otros servicios de confianza, como los sellos de tiempo electrónicos y los servicios de entrega electrónica certificada. En concreto, ni el sellado de tiempo de los documentos digitales ni su transferencia mediante servicios de entrega electrónica certificada podrían impedir suficientemente, sin otras medidas técnicas u organizativas, copiar y vender más de una vez el mismo activo digital a diferentes partes. El proceso de creación y actualización de un libro mayor electrónico depende del tipo de libro mayor utilizado (centralizado o distribuido).

(35) Para evitar la fragmentación del mercado interior, se debe establecer un marco jurídico a escala europea que permita el reconocimiento transfronterizo de servicios de confianza para la grabación de datos en libros mayores electrónicos cualificados. Los proveedores de servicios de confianza para los libros mayores electrónicos deben tener la obligación de comprobar el registro secuencial de los datos en el libro mayor. El presente Reglamento se entiende sin perjuicio de las obligaciones jurídicas que los usuarios de libros mayores electrónicos puedan tener que cumplir en virtud del Derecho nacional y de la Unión. Por ejemplo, los casos de uso que conlleven el tratamiento de datos personales deben cumplir el Reglamento (UE) 2016/679. Los casos de uso que impliquen criptoactivos deben ser compatibles con todas las normas financieras aplicables, incluidas, por ejemplo, la Directiva relativa a los mercados de instrumentos financieros[11], la Directiva sobre servicios de pago[12] y la Directiva sobre el dinero electrónico[13], así como con la posible futura legislación sobre los mercados de criptoactivos y con las normas contra el blanqueo de capitales que podrían incluirse en el Reglamento sobre transferencias de fondos[14], y podría exigir a los prestadores de servicios de criptoactivos que verifiquen la identidad de los usuarios de los libros mayores electrónicos a fin de cumplir las normas internacionales contra el blanqueo de capitales.

---

11 Directiva 2014/65/UE del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, relativa a los mercados de instrumentos financieros y por la que se modifica la Directiva 2002/92/CE (DO L 173 de 12.6.2014, p. 349).

12 Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) n.º 1093/2010 y se deroga la Directiva 2007/64/CE (DO L 337 de 23.12.2015, p. 35).

13 Directiva 2009/110/CE del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009, sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como sobre la supervisión prudencial de dichas entidades, por la que se modifican las Directivas 2005/60/CE y 2006/48/CE y se deroga la Directiva 2000/46/CE (DO L 267 de 10.10.2009, p. 7).

14 Véase la propuesta de 20.7.2021 de la Comisión de refundición del Reglamento (UE) 2015/847 del Parlamento Europeo y del Consejo, de 20 de mayo de 2015, relativo a la información que acompaña a las transferencias de fondos (COM/2021/422 final).

(36) Al objeto de evitar la fragmentación y los obstáculos derivados de unas normas y unas restricciones técnicas divergentes, y de garantizar un proceso coordinado para impedir poner en peligro la aplicación del futuro Marco para una Identidad Digital Europea, se necesita un proceso de cooperación estrecha y estructurada entre la Comisión, los Estados miembros y el sector privado. Para lograr este objetivo, los Estados miembros deberán cooperar dentro del marco establecido en la Recomendación XXX/XXXX de la Comisión [sobre un conjunto de herramientas para adoptar un enfoque coordinado de cara a un Marco para una Identidad Digital Europea][15] con el fin de identificar un conjunto de herramientas para el Marco para una Identidad Digital Europea. El conjunto de herramientas debe incluir una arquitectura técnica y un marco de referencia detallados, un conjunto de normas y referencias técnicas comunes y un conjunto de directrices y descripciones de prácticas idóneas que aborden, como mínimo, todos los aspectos de las funciones y la interoperabilidad de las carteras europeas de identidad digital (incluidas las firmas electrónicas) y del servicio de confianza cualificado para la declaración de atributos, según lo dispuesto en el presente Reglamento. En este contexto, los Estados miembros deberán alcanzar asimismo un acuerdo sobre los elementos comunes del modelo de negocio y la estructura de las tasas de las carteras europeas de identidad digital para facilitar su adopción, en particular por parte de las pequeñas y medianas empresas en un contexto transfronterizo. El contenido del conjunto de herramientas debe reflejar y evolucionar de forma paralela a los resultados del debate y del proceso de adopción del Marco para una Identidad Digital Europea.

(36 *bis*) Los Estados miembros deben establecer normas sobre las sanciones aplicables a las infracciones, como las prácticas directas o indirectas que den lugar a confusión entre servicios de confianza no cualificados y cualificados o al uso abusivo de la marca de confianza «UE» por parte de prestadores cualificados de servicios de confianza. La marca de confianza de la UE no debe utilizarse en condiciones que, directa o indirectamente, lleven a la creencia de que los servicios de confianza no cualificados ofrecidos por este prestador están cualificados.

[15] [Insértese la referencia una vez adoptada].

(36 *ter*) El presente Reglamento debe garantizar un nivel armonizado de calidad, fiabilidad y seguridad de los servicios de confianza cualificados, independientemente del lugar en el que se lleven a cabo las operaciones. Por lo tanto, un prestador cualificado de servicios de confianza debe estar autorizado a externalizar sus operaciones relacionadas con la prestación de un servicio de confianza cualificado fuera de la Unión, siempre que ofrezca las garantías de que las actividades de supervisión y las auditorías puedan ejecutarse como si estas operaciones se llevaran a cabo en la Unión. Cuando no pueda garantizarse plenamente el cumplimiento del Reglamento, los organismos de supervisión deben poder adoptar medidas proporcionadas y justificadas, incluida la retirada de la cualificación del servicio de confianza prestado.

(36 *quater*) Para ofrecer seguridad jurídica sobre la validez de las firmas electrónicas avanzadas basadas en certificados cualificados, es esencial detallar los componentes de una firma electrónica avanzada basada en certificados cualificados, que debe evaluar la parte usuaria que efectúa la validación.

(36 *quinquies)*) Los prestadores de servicios de confianza deben utilizar algoritmos criptográficos que reflejen las mejores prácticas actuales y las implementaciones fiables de estos algoritmos a fin de garantizar la seguridad y fiabilidad de sus servicios de confianza.

(36 *sexies*) El presente Reglamento debe establecer la obligación de que los prestadores cualificados de servicios de confianza comprueben la identidad de una persona física o jurídica a la que se expida el certificado cualificado conforme a diversos métodos armonizados en toda la UE. Dichos métodos pueden incluir el uso de medios de identificación electrónica que cumplan los requisitos del nivel de seguridad «sustancial» en combinación con procedimientos a distancia armonizados adicionales que garanticen la identificación de la persona con un alto nivel de confianza.

(36*septies*) Los emisores de carteras europeas de identidad digital y los emisores de medios de identificación electrónica notificados que actúen a título comercial o profesional utilizando servicios básicos de plataforma ofrecidos por guardianes de acceso con el fin de ofrecer bienes y servicios a los usuarios finales o en el curso de dicho suministro deben considerarse usuarios profesionales de conformidad con el artículo 2, apartado 21, del Reglamento (UE) 2022/1925. Por lo tanto, debe obligarse a los guardianes de acceso a garantizar, de forma gratuita, la interoperabilidad efectiva con las mismas funciones del sistema operativo, del equipo o del programa informático a las que puede acceder o que utiliza el guardián de acceso cuando presta sus propios servicios o suministra su propio equipo informático complementarios y de apoyo, así como el acceso a dichas funciones a efectos de interoperabilidad. Esto debe permitir a los emisores de carteras europeas de identidad digital europea y a los emisores de medios de identificación electrónica notificados interconectarse a través de interfaces o soluciones similares a las características respectivas de manera tan eficaz como los propios servicios o equipos informáticos del guardián de acceso.

(36 *octies*) Para mantener el presente Reglamento en consonancia con la evolución actual y seguir las prácticas en el mercado interior, los actos delegados y de ejecución adoptados por la Comisión deben revisarse y, en caso necesario, actualizarse periódicamente. La evaluación de la necesidad de estas actualizaciones debe tener en cuenta las nuevas tecnologías, prácticas, normas o especificaciones técnicas surgidas en el mercado interior.

(37) Se ha consultado al Supervisor Europeo de Protección de Datos, de conformidad con el artículo 42, apartado 1, del Reglamento (UE) 2018/1525 del Parlamento Europeo y del Consejo[16].

(38) Procede, por lo tanto, modificar el Reglamento (UE) n.º 910/2014 en consecuencia.

---

16 Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE (DO L 295 de 21.11.2018, p. 39).

HAN ADOPTADO EL PRESENTE REGLAMENTO:

Artículo 1

El Reglamento (UE) n.º 910/2014 se modifica como sigue:

1) El artículo 1 se sustituye por el texto siguiente:

«El presente Reglamento tiene por objeto garantizar el correcto funcionamiento del mercado interior y proporcionar un nivel de seguridad adecuado de los medios de identificación electrónica y los servicios de confianza. A tales efectos, el presente Reglamento:

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

a *ter*) establece las condiciones en las cuales los Estados miembros 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 de certificados para la autenticación de sitios web, la validación electrónica de las firmas electrónicas, los sellos electrónicos y sus certificados, la validación electrónica de los certificados de autenticación de sitios web, la conservación electrónica de las firmas electrónicas, los sellos electrónicos y sus certificados, el archivado electrónico, la declaración electrónica de atributos, la gestión de dispositivos cualificados remotos de creación de firmas y sellos electrónicos y los libros mayores electrónicos;».

2) El artículo 2 se modifica como sigue:

a) el apartado 1 se sustituye por el texto siguiente:

«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) el apartado 3 se sustituye por el texto siguiente:

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

3) El artículo 3 se modifica como sigue:

X) el punto 1 se sustituye por el texto siguiente:

«1) "identificación electrónica", el proceso de utilizar los datos de identificación de una persona en forma electrónica que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona física o jurídica;»;

a) el punto 2 se sustituye por el texto siguiente:

«2) "medios de identificación electrónica", una unidad material y/o inmaterial, como las carteras europeas de identidad digital, que contiene los datos de identificación de una persona y que se utiliza para la autenticación en servicios en línea o, cuando proceda, en servicios fuera de línea;

a *bis*) el punto 3 se sustituye por el texto siguiente:

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

b) el punto 4 se sustituye por el texto siguiente:

«4) "sistema de identificación electrónica", un 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 personas físicas o jurídicas;»;

b *bis*) el punto 5 se sustituye por el texto siguiente:

«5) "autenticación", un proceso electrónico que permite confirmar la identificación electrónica de una persona física o jurídica, o el origen y la integridad de datos en forma electrónica;»;

b *ter*) se añade el punto 5 *bis* siguiente:

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

c) el punto 14 se sustituye por el texto siguiente:

«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;»;

d) el punto 16 se sustituye por el texto siguiente:

«16) “servicio de confianza”, el servicio electrónico prestado habitualmente a cambio de una remuneración, consistente en:

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

a *bis*) la validación de certificados de firma electrónica, de certificados de sellos electrónicos, de certificados de autenticación de sitios web o de certificados para la prestación de otros servicios de confianza;

b) la creación de firmas electrónicas o de sellos electrónicos;

c) la validación de firmas electrónicas o de sellos electrónicos;

d) la conservación de firmas electrónicas, de sellos electrónicos, de certificados de firma electrónica o de certificados de sellos electrónicos;

e) la gestión de dispositivos cualificados remotos de creación de firmas electrónicas o de dispositivos cualificados remotos de creación de sellos electrónicos;

f) la expedición de declaraciones electrónicas de atributos;

f *bis*) la validación de declaraciones electrónicas de atributos;

g) la creación de sellos de tiempo electrónicos;

g *bis*) la validación de sellos de tiempo electrónicos;

g *ter*) la prestación de servicios de entrega electrónica certificada;

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

h) el archivado electrónico de datos electrónicos; o

i) la actividad de registro de datos electrónicos en un libro mayor electrónico.»;

d *bis*) el punto 18 se sustituye por el texto siguiente:

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

e) el punto 21 se sustituye por el texto siguiente:

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

f) se insertan los puntos 23 *bis* y 23 *ter* siguientes:

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

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

g) el punto 29 se sustituye por el texto siguiente:

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

h) el punto 41 se sustituye por el texto siguiente:

«41) «validación»: el proceso consistente en verificar y confirmar que los datos en forma electrónica son válidos con arreglo a los requisitos del presente Reglamento»;

i) se añaden los siguientes puntos 42 a 55:

«42) "cartera europea de identidad digital", un medio de identificación electrónica que permite al usuario almacenar y recuperar datos de identidad, como los datos de identificación de una persona y las declaraciones electrónicas de atributos vinculados a su identidad, con el fin de proporcionarlos a las partes usuarias a petición de estas y de utilizarlos con fines de autenticación, en línea y, cuando proceda, fuera de línea, para un servicio de conformidad con lo dispuesto en el artículo 6 *bis*; y que permite firmar por medio de firmas electrónicas cualificadas y sellar por medio de sellos electrónicos cualificados;

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

44) “declaración electrónica de atributos”, una declaración en formato electrónico que permite la autenticación de atributos;

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

45 *bis*) “declaración electrónica de atributos expedida por un organismo del sector público responsable de una fuente auténtica o en su nombre”, una declaración electrónica de atributos expedida por un organismo del sector público responsable de una fuente auténtica o por un organismo del sector público 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 *quinquies bis* y con arreglo a los requisitos establecidos en el anexo VII;

46) “fuente auténtica”, un 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 y se considera una fuente principal de dicha información, o que está reconocido como auténtico en virtud del Derecho nacional o de la Unión, que incluye las prácticas administrativas;

47) “archivado electrónico”, un servicio que garantiza la recepción, el almacenamiento, la recuperación y la eliminación de datos electrónicos para garantizar su durabilidad y legibilidad, así como para preservar su integridad, confidencialidad y prueba de origen durante todo el período de conservación;

48) “servicio cualificado de archivado electrónico”, un servicio que cumple los requisitos establecidos en el artículo 45 *octies bis*;

49) “marca de confianza de la UE para la cartera de identidad digital”, una indicación sencilla, reconocible y clara de que una cartera europea de identidad digital se ha proporcionado de conformidad con el presente Reglamento;

50) “autenticación reforzada de usuario”, la 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;

53) “libro mayor electrónico”, secuencia de registros electrónicos de datos que garantiza la integridad y la exactitud del orden cronológico de estos;

53 *bis*) “libro mayor electrónico cualificado”, un libro mayor electrónico que cumple los requisitos establecidos en el artículo 45 *decies*;

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

55) “correspondencia entre registros”, proceso en el que los datos de identificación o los medios de identificación de una persona, la declaración electrónica cualificada de atributos o las declaraciones de atributos expedidas por un organismo del sector público responsable de una fuente auténtica o en su nombre coinciden con una cuenta existente perteneciente a la misma persona o están vinculados a dicha cuenta;

(55 *bis*)"identificador único y persistente", identificador que puede consistir en datos de identificación únicos o múltiples de carácter nacional o sectorial, está asociado a un único usuario en un sistema determinado y persiste en el tiempo;

(55 *ter*) "registro de datos", datos electrónicos registrados con metadatos (o atributos) relacionados que respaldan el tratamiento de los datos;

55 *quater*) "uso de carteras europeas de identidad digital fuera de línea", interacción entre un usuario y una parte usuaria en una ubicación física, en la que la cartera no está obligada a acceder a sistemas remotos a través de redes de comunicaciones electrónicas a efectos de la interacción.».

«*Artículo 5*

Seudónimos en transacciones electrónicas

Sin perjuicio de los efectos jurídicos que el Derecho nacional contemple para los seudónimos, no se prohibirá su utilización en las transacciones electrónicas.».

5) En el capítulo II se inserta el título siguiente antes del artículo 6 *bis*:

«SECCIÓN I

Carteras europeas de identidad digital».

7) Se insertan los artículos 6 *bis*, 6 *ter*, 6 *quater* y 6 *quinquies* siguientes:

«*Artículo 6* 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, cada Estado miembro velará por que se proporcione una cartera europea de identidad digital dentro de los veinticuatro meses siguientes a la entrada en vigor de los actos de ejecución a que se refieren el apartado 11 y el artículo 6 *quater*, apartado 4.

2. Las carteras europeas de identidad digital serán proporcionadas:

   a) por un Estado miembro;

   b) en virtud de un mandato de un Estado miembro; o

   c) por entidades independientes de un Estado miembro, pero reconocidas por un Estado miembro.

3. Las carteras europeas de identidad digital son medios de identificación electrónica que permitirán al usuario, de forma transparente y rastreable por este:

   a) solicitar, seleccionar, combinar, almacenar, eliminar y presentar de forma segura una declaración electrónica de atributos y datos de identificación de una persona a las partes usuarias, incluida la autenticación en línea y, cuando proceda, fuera de línea, con el fin de utilizar servicios públicos y privados, velando al mismo tiempo por que sea posible divulgar los datos selectivamente;

   b) firmar por medio de firmas electrónicas cualificadas y sellar por medio de sellos electrónicos cualificados.

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

a) proporcionarán un conjunto común de interfaces:

1) para la expedición de datos de identificación de una persona, declaraciones electrónicas cualificadas y no cualificadas de atributos o certificados cualificados y no cualificados a la cartera europea de identidad digital;

2) para que las partes usuarias soliciten datos de identificación de una persona y declaraciones electrónicas de atributos;

3) para presentar a las partes usuarias datos de identificación de una persona o la declaración electrónica de atributos en línea y, cuando proceda, también fuera de línea;

4) para que el usuario permita la interacción con la cartera europea de identidad digital y muestre una "marca de confianza de la UE para la cartera de identidad digital";

b) no facilitarán información alguna a los prestadores de servicios de confianza de declaraciones electrónicas de atributos sobre el uso de estos atributos después de su expedición;

b *bis*) garantizarán que la identidad de las partes usuarias pueda validarse mediante la aplicación de mecanismos de autenticación de conformidad con el artículo 6 *ter*;

c) cumplirán los requisitos establecidos en el artículo 8 con respecto al nivel de seguridad "alto" aplicable *mutatis mutandis* a la gestión y el uso de los datos de identificación de la persona a través de la cartera, incluida la identificación y autenticación electrónicas;

e) garantizarán que los datos de identificación de la persona a que se refiere el artículo 12, apartado 4, letra d), correspondan de forma única y persistente a la persona física o jurídica, o a la persona jurídica que represente a la persona física o jurídica, asociada con la cartera.

4 *bis*. Los Estados miembros establecerán procedimientos que permitan al usuario notificar la posible pérdida o uso indebido de su cartera y solicitar su revocación.

5. Los Estados miembros proporcionarán mecanismos de validación para las carteras europeas de identidad digital:

a) para garantizar que se pueda verificar su autenticidad y validez;

d) para permitir al usuario autenticar a las partes usuarias de conformidad con el artículo 6 *ter*;

6. Las carteras europeas de identidad digital se expedirán en el marco de un sistema de identificación electrónica notificado con nivel de seguridad "alto".

6 *bis*. La expedición, la utilización para autenticación y la revocación de las carteras europeas de identidad digital serán gratuitas para las personas físicas.

6 *ter*. Sin perjuicio de lo dispuesto en el artículo 6 *quinquies ter*, los Estados miembros podrán prever, 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.

7. Los usuarios tendrán pleno control sobre el uso de su cartera europea de identidad digital y sobre los datos que consten en ella. El emisor de la cartera europea de identidad digital no recopilará información sobre el uso de la cartera que no sea necesaria para la prestación de los servicios de esta, ni combinará datos de identificación personal 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 emisor o a través de servicios de terceros que no sean necesarios para la prestación de los servicios de la cartera, a menos que el usuario lo haya solicitado expresamente. Los datos personales relativos a la provisión de carteras europeas de identidad digital se conservarán en soporte lógico por separado de otros datos que obren en poder del emisor de las carteras. Si la cartera europea de identidad digital ha sido proporcionada por agentes privados de conformidad con lo dispuesto en el apartado 2, letras b) y c), se aplicarán *mutatis mutandis* las disposiciones del artículo 45 *septies*, apartado 4.

7 *bis*. Los Estados miembros notificarán a la Comisión, sin dilación indebida, información sobre:

a) el organismo responsable de establecer y mantener la lista de partes usuarias notificadas que utilizan las carteras europeas de identidad digital de conformidad con el artículo 6 *ter*, apartado 2;

b) los organismos responsables de la provisión de carteras europeas de identidad digital de conformidad con el artículo 6 *bis*, apartado 1;

c) los organismos responsables de garantizar que los datos de identificación de la persona estén asociados a la cartera de conformidad con el artículo 6 *bis*, apartado 4, letra e):

La notificación también proporcionará información sobre el mecanismo que permite validar los datos de identificación de la persona a que se refiere el artículo 12, apartado 4, y la identidad de las partes usuarias.

La Comisión pondrá a disposición del público, 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.

8. El artículo 11 se aplicará *mutatis mutandis* a la cartera de identidad digital europea.

9. El artículo 24, apartado 2, letras b), e), g) y h), se aplicará *mutatis mutandis* al emisor de carteras europeas de identidad digital.

10. Se garantizará la accesibilidad de la cartera europea de identidad digital para las personas con discapacidad, conforme a los requisitos de accesibilidad previstos en la Directiva (UE) 2019/882.

11. Dentro de los seis meses siguientes a la entrada en vigor del presente Reglamento, la Comisión establecerá especificaciones técnicas y operativas y normas de referencia para los requisitos mencionados en los apartados 3, 4, 5 y 7 *bis*, por medio de un acto de ejecución relativo a la implantación de la cartera europea de identidad digital. El acto de ejecución se adoptará con arreglo al procedimiento de examen a que se refiere el artículo 48, apartado 2.

11 *bis*. La Comisión establecerá especificaciones técnicas y operativas, así como normas de referencia, 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 «alto», bien medios de identificación electrónica conformes con el nivel «sustancial» junto con procedimientos remotos adicionales de incorporación, de modo que, en conjunto, cumplan los requisitos del nivel de seguridad «alto». El acto de ejecución se adoptará con arreglo al procedimiento de examen a que se refiere el artículo 48, apartado 2.

Artículo 6 ter

Partes usuarias de las carteras europeas de identidad digital

1. Cuando las partes usuarias que presten servicios públicos o privados tengan previsto utilizar carteras europeas de identidad digital proporcionadas de conformidad con el presente Reglamento, lo notificarán al Estado miembro en el que estén establecidas las partes usuarias.

1 *bis*. El procedimiento de notificación será rentable y proporcional al riesgo y garantizará que las partes usuarias faciliten al menos la información necesaria para autenticarse en las carteras europeas de identidad digital. Esto debe incluir, como mínimo, el Estado miembro en el que estén establecidas y el nombre de la parte usuaria y, cuando proceda, su número de registro según conste en los registros oficiales.

1 *ter*. El requisito de notificación se entenderá sin perjuicio de otros requisitos de notificación y registro de conformidad con el Derecho nacional o de la Unión, como los aplicables a las categorías especiales de datos personales, que tal vez exijan requisitos de autorización adicionales.

1 *quater*. Los Estados miembros podrán eximir a las partes usuarias del requisito de notificación cuando el Derecho nacional o de la Unión no prevea requisitos específicos de notificación o registro para acceder a la información facilitada a través de la cartera europea de identidad digital. Es posible que las partes usuarias exentas no tengan que autenticarse en la cartera europea de identidad digital.

1 *quinquies*. Las partes usuarias notificadas de conformidad con el presente artículo informarán sin demora al Estado miembro de cualquier cambio posterior en la información facilitada inicialmente.

2. Las partes usuarias garantizarán la aplicación de los mecanismos de autenticación a que se refiere el artículo 6 *bis*, apartado 4, letra b *bis*).

3. Las partes usuarias serán responsables de llevar a cabo el procedimiento de autenticación de personas y de validación de la declaración electrónica de atributos que se origina en las carteras europeas de identidad digital y se obtiene a través de la interfaz común prevista en el artículo 6 *bis*, apartado 4, letra a), y apartado 2.

4. Dentro de los seis meses siguientes a la entrada en vigor del presente Reglamento, la Comisión establecerá especificaciones técnicas y operativas para los requisitos mencionados en los apartados 1, 1 *bis* y 1 *quinquies*, por medio de un acto de ejecución relativo a la implantación de las carteras europeas de identidad digital, tal como prevé el artículo 6 *bis*, apartado 11. El acto de ejecución se adoptará con arreglo al procedimiento de examen a que se refiere el artículo 48, apartado 2.

Artículo 6 quater

Certificación de las carteras europeas de identidad digital

1. La conformidad de las carteras europeas de identidad digital con los requisitos establecidos en el artículo 6 *bis*, apartado 3, 4 y 5, con el requisito de separación lógica establecido en el artículo 6 *bis*, apartado 7, y, cuando proceda, con los requisitos establecidos en el artículo 6 *bis*, apartado 11 *bis*, será certificada por organismos de evaluación de la conformidad acreditados de conformidad con el artículo 60 del Reglamento sobre la Ciberseguridad y con los sistemas, especificaciones, normas y procedimientos previstos en el apartado 4, letras a), a *bis*) y a *bis bis*), y designados por los Estados miembros. La certificación no excederá de cinco años y estará supeditada a una evaluación periódica bienal de las vulnerabilidades. Cuando se detecten vulnerabilidades y no se subsanen en un plazo de tres meses, se cancelará la certificación.

2. Por lo que se refiere al cumplimiento de los requisitos de protección de datos establecidos en el artículo 6 *bis*, apartado 7, la certificación prevista en el apartado 1 podrá complementarse con una certificación con arreglo al artículo 42 del Reglamento (UE) 2016/679.

3. La conformidad de las carteras europeas de identidad digital, o de partes de ellas, con los requisitos pertinentes de ciberseguridad establecidos en el artículo 6 *bis*, apartado 3, 4, 5, 7 y, cuando proceda, 11 *bis*, será certificada por los organismos de evaluación de la conformidad a que se refiere el apartado 1, con arreglo a los esquemas de certificación de la ciberseguridad pertinentes previstos en el Reglamento (UE) 2019/881, tal como se hace referencia a ellos en los apartados 4, letra a) y letra a *bis*).

3 *bis*. Las carteras europeas de identidad digital certificadas no estarán sujetas a los requisitos mencionados en los artículos 7 y 9.

4. Dentro de los seis meses siguientes a la entrada en vigor del presente Reglamento, la Comisión establecerá, por medio de actos de ejecución:

a) una lista de los esquemas de certificación de la ciberseguridad con arreglo al Reglamento (UE) 2019/881, exigidos para la certificación de las carteras europeas de identidad digital a que se refiere el apartado 3;

a *bis*) las especificaciones, los procedimientos y las normas de referencia para su utilización en el marco de los esquemas de certificación de la ciberseguridad pertinentes enumerados de conformidad con la letra a);

a *bis bis*) una lista de especificaciones, procedimientos y normas de referencia que prevean requisitos de certificación comunes no incluidos en los esquemas de certificación de la ciberseguridad contemplados en el Reglamento (UE) 2019/881 a efectos de la certificación prevista en el apartado 1, con el fin de demostrar que la cartera europea de identidad digital cumple los requisitos establecidos en el apartado 1;

b) especificaciones técnicas, de procedimiento, organizativas y operativas para la designación de los organismos de evaluación de la conformidad a que se refiere el apartado 1 y, en lo que respecta a los requisitos de certificación establecidos con arreglo a la letra a *bis bis*), para el seguimiento y la revisión de los esquemas de certificación y los métodos de evaluación conexos que utilizan estos organismos, así como de los certificados e informes de certificación que expiden.

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

6. Los actos de ejecución a que se refiere el apartado 4 se adoptarán de conformidad con el procedimiento de examen contemplado en el artículo 48, apartado 2.

Artículo 6 quinquies

Publicación de una lista de carteras europeas de identidad digital certificadas

1. Los Estados miembros informarán a la Comisión, sin dilación indebida, de las carteras europeas de identidad digital que se hayan proporcionado de conformidad con el artículo 6 *bis* y que hayan sido certificadas por los organismos a que se refiere el artículo 6 *quater*, apartado 1. Asimismo, informarán a la Comisión sin dilación indebida cuando la certificación sea cancelada.

2. A tenor de la información recibida, la Comisión establecerá, publicará y actualizará una lista legible por máquina de carteras europeas de identidad digital certificadas.

3. Dentro de los seis meses siguientes a la entrada en vigor del presente Reglamento, la Comisión definirá los formatos y procedimientos aplicables a efectos de los apartados 1 y 2, por medio de un acto de ejecución relativo a la implantación de las carteras europeas de identidad digital, tal como prevé el artículo 6 *bis*, apartado 11. El acto de ejecución se adoptará con arreglo al procedimiento de examen a que se refiere el artículo 48, apartado 2.

Artículo 6 quinquies bis

Violación de la seguridad de las carteras europeas de identidad digital

1. Cuando se produzca una violación o vulneración parcial que afecte a carteras europeas de identidad digital proporcionadas en virtud del artículo 6 *bis* o de los mecanismos de validación a que se refiere el artículo 6 *bis*, apartado 5, letras a), d) o e), de un modo que afecte a su fiabilidad o a la de otras carteras europeas de identidad digital, el emisor de las carteras afectadas suspenderá, sin dilación indebida, la emisión y el uso de dichas carteras. El Estado miembro donde se proporcionaron las carteras afectadas informará al resto de los Estados miembros y a la Comisión sin dilación indebida. El emisor de las carteras o el Estado miembro de que se trate informará de ello a las partes usuarias y a los usuarios.

2. Cuando se haya subsanado la violación o la vulneración a que se refiere el apartado 1, el emisor de la cartera europea de identidad digital restablecerá la emisión y el uso de esta. El Estado miembro donde se proporcionaron las carteras afectadas informará al resto de los Estados miembros y a la Comisión sin dilación indebida. El emisor de las carteras afectadas o el Estado miembro de que se trate informará de ello a las partes usuarias y a los usuarios sin dilación indebida.

3. Si la violación o vulneración a que se refiere el apartado 1 no se subsana en un plazo de tres meses desde la suspensión, el Estado miembro afectado retirará la cartera europea de identidad digital en cuestión e informará de ello a los demás Estados miembros y a la Comisión. Cuando la gravedad de la violación lo justifique, la cartera europea de identidad digital afectada será retirada sin dilación indebida.

4. La Comisión publicará en el *Diario Oficial de la Unión Europea* las modificaciones correspondientes de la lista a que se refiere el artículo 6 quinquies, sin dilación indebida.

5. En un plazo máximo de seis meses desde la entrada en vigor del presente Reglamento, la Comisión especificará además las medidas a que se refieren los apartados 1, 2 y 3 por medio de un acto de ejecución relativo a la implantación de las carteras europeas de identidad digital, tal como prevé el artículo 6 *bis*, apartado 11. El acto de ejecución se adoptará con arreglo al procedimiento de examen a que se refiere el artículo 48, apartado 2.

Artículo 6 quinquies bis

Uso transfronterizo de carteras europeas de identidad digital

1. Cuando los Estados miembros exijan una identificación electrónica utilizando un medio de identificación electrónica y una autenticación para acceder a un servicio en línea prestado por un organismo del sector público, también aceptarán las carteras europeas de identidad digital proporcionadas con arreglo al presente Reglamento para la autenticación del usuario.

2. Cuando el Derecho nacional o de la Unión exija a las partes usuarias privadas prestadoras de servicios, con la excepción de las microempresas y pequeñas empresas según se definen en la Recomendación 2003/361/CE de la Comisión, que utilicen métodos reforzados para la autenticación de los usuarios, o cuando se requiera dicha autenticación reforzada 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, las partes usuarias privadas también aceptarán, a más tardar doce meses tras la fecha de entrega de las carteras europeas de identidad digital de conformidad con el artículo 6 *bis*, apartado 1, y estrictamente a petición voluntaria del usuario, el uso de las carteras europeas de identidad digital proporcionadas con arreglo al presente Reglamento y respetando los datos mínimos necesarios para el servicio en línea específico para el que se solicita la autenticación del usuario.

3. Cuando las plataformas en línea de muy gran tamaño, según se definen en el artículo 25, apartado 1, del Reglamento [referencia a la Ley de Servicios Digitales] exijan a los usuarios autenticarse para acceder a servicios en línea, también aceptarán el uso de carteras europeas de identidad digital proporcionadas con arreglo al presente Reglamento para la autenticación del usuario, estrictamente a petición voluntaria del usuario y respetando los datos mínimos necesarios para el servicio en línea específico para el que se solicita la autenticación.

4. En colaboración con los Estados miembros, la Comisión fomentará y facilitará el desarrollo de códigos de conducta para contribuir a una amplia disponibilidad y facilidad de uso de las carteras europeas de identidad digital contempladas en el ámbito de aplicación del presente Reglamento. Los códigos de conducta facilitarán la aceptación de los medios de identificación electrónica, incluidas las carteras europeas de identidad digital contempladas en el ámbito de aplicación del presente Reglamento, en particular por parte de prestadores de servicios que se basen en servicios de identificación electrónica de terceros para autenticar a los usuarios. La Comisión facilitará el desarrollo de dichos códigos de conducta en estrecha cooperación con todas las partes interesadas y alentará a los prestadores de servicios a ultimar el desarrollo de códigos de conducta en un plazo máximo de doce meses a contar desde la adopción del presente Reglamento, así como a implantarlos efectivamente dentro de los dieciocho meses siguientes a la adopción del Reglamento.

5. Dentro de los veinticuatro meses siguientes a la implantación de las carteras europeas de identidad digital, la Comisión evaluará si, con base en datos que muestren la demanda, disponibilidad y facilidad de uso de la cartera europea de identidad digital, los prestadores adicionales de servicios en línea privados tienen la obligación de aceptar el uso de la cartera europea de identidad digital estrictamente a petición voluntaria del usuario. Los criterios de evaluación incluirán la dimensión de la base de usuarios, la presencia transfronteriza de prestadores de servicios, el desarrollo tecnológico, la evolución de los patrones de uso y la demanda de los usuarios.

8) Antes del artículo 7 se inserta el título siguiente:

«SECCIÓN II

SISTEMAS DE IDENTIFICACIÓN ELECTRÓNICA».

9) La frase introductoria del artículo 7 se sustituye por el texto siguiente:

«De conformidad con el artículo 9, apartado 1, los Estados miembros que aún no lo hayan hecho notificarán, en un plazo de veinticuatro meses a partir de la entrada en vigor de los actos de ejecución a que se refieren el artículo 6 *bis*, apartado 11, y el artículo 6 *quater*, apartado 4, al menos un sistema de identificación electrónica que incluya al menos un medio de identificación del nivel de seguridad "alto". Un sistema de identificación electrónica podrá ser objeto de notificación con arreglo al artículo 9, apartado 1, si se cumple la totalidad de las condiciones siguientes:».

10) En el artículo 9, los apartados 2 y 3 se sustituyen por el texto siguiente:

«2. La Comisión publicará en el Diario Oficial de la Unión Europea la lista de los sistemas de identificación electrónica notificados de conformidad con el apartado 1 del presente artículo y la información básica al respecto.

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

12) Se inserta el artículo 11 bis siguiente:

«*Artículo 11* bis

Correspondencia entre registros

1. Cuando se utilicen medios de identificación electrónica notificados o carteras europeas de identidad digital para la autenticación, los Estados miembros, cuando actúen como partes usuarias, garantizarán la correspondencia entre registros.

2. A efectos de proporcionar carteras europeas de identidad digital, los Estados miembros incluirán en el conjunto mínimo de datos de identificación personal a que se refiere el artículo 12, apartado 4, letra d), al menos un identificador único y persistente conforme con el Derecho de la Unión y nacional para identificar al usuario, a petición de este, en los casos en que la ley exija identificar al usuario.

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

2 *bis bis*. Los Estados miembros podrán disponer, de conformidad con el Derecho nacional, que el usuario de la cartera europea de identidad digital pueda solicitar que un identificador único y persistente incluido en el conjunto mínimo de datos de identificación personal y asociado a la cartera de conformidad con el artículo 6 *bis*, apartado 4, letra e), sea sustituido por otro identificador único y persistente emitido por el Estado miembro.

3. En un plazo máximo de seis meses desde la entrada en vigor del presente Reglamento, la Comisión especificará además las medidas a que se refiere el apartado 1 por medio de un acto de ejecución. El acto de ejecución se adoptará con arreglo al procedimiento de examen a que se refiere el artículo 48, apartado 2.

3 *bis*. En un plazo máximo de seis meses desde la entrada en vigor del presente Reglamento, la Comisión especificará las medidas a que se refieren los apartados 2 y 2 *bis bis* por medio de un acto de ejecución. El acto de ejecución se adoptará con arreglo al procedimiento de examen a que se refiere el artículo 48, apartado 2.

13) El artículo 12 se modifica como sigue:

Cooperación e interoperabilidad

a) en el apartado 3, se suprime la letra d);

b) en el apartado 4, la letra d) se sustituye por el texto siguiente:

«d) una referencia a un conjunto mínimo de datos de identificación personal necesarios para representar de manera única y persistente a una persona física, jurídica o a una persona física que representa a una persona física o jurídica;»;

b *bis*) en el apartado 5 se inserta la letra c) siguiente:

«c) un enfoque similar con respecto a los servicios en línea que aceptan el uso de carteras europeas de identidad digital proporcionadas de conformidad con el presente Reglamento;»;

c) en el apartado 6, la letra a) se sustituye por el texto siguiente:

«a) un intercambio de información, experiencia y prácticas idóneas sobre sistemas de identificación electrónica, en particular sobre los requisitos técnicos relacionados con la interoperabilidad, la correspondencia entre registros y los niveles de seguridad;».

c *bis*) en el apartado 6, se inserta la letra e) siguiente:

«e) el intercambio de información, experiencia y buenas prácticas y la publicación de directrices sobre cómo pueden diseñarse, desarrollarse y aplicarse los servicios en línea con el fin de basarse en las carteras europeas digitales».

14) se insertan los artículos 12 *bis* y 12 *ter* siguientes:

«*Artículo 12* bis

Certificación de los sistemas de identificación electrónica

1. La conformidad de los sistemas de identificación electrónica que deban notificarse con los requisitos establecidos en el presente Reglamento se certificará para demostrar la conformidad de dichos sistemas (o partes de ellos) con los requisitos establecidos en el artículo 8, apartado 2, en relación con los niveles de seguridad de los sistemas de identificación electrónica en virtud de un esquema de certificación de la ciberseguridad pertinente con arreglo al Reglamento (UE) 2019/881, o partes del mismo, en la medida en que el certificado de ciberseguridad o partes del mismo cubran los requisitos establecidos en el artículo 8, apartado 2, en relación con los niveles de seguridad de los sistemas de identificación electrónica. La certificación no excederá de cinco años, supeditada a una evaluación periódica bienal de las vulnerabilidades. Cuando se identifiquen vulnerabilidades y no se subsanen en un plazo de tres meses, se cancelará la certificación.

   La certificación será realizada por organismos de evaluación de la conformidad acreditados, públicos o privados, designados por los Estados miembros y de conformidad con el Reglamento (CE) n.º 765/2008.

2. La revisión por pares de los sistemas de identificación electrónica a que se refiere el artículo 12, apartado 6, letra c), no se aplicará a los sistemas de identificación electrónica (o parte de ellos) certificados de conformidad con el apartado 1.

2 *bis*. No obstante lo dispuesto en el apartado 2 del presente artículo, los Estados miembros podrán solicitar a un Estado miembro que efectúe la notificación información adicional sobre los sistemas de identificación electrónica o parte de ellos certificados de conformidad con el apartado 2 del presente artículo.

3. 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 dicha información a disposición de los Estados miembros.».

«Artículo 12 *ter*

Acceso a las funciones de los equipos y programas informáticos

Los emisores de carteras europeas de identidad digital y los emisores de medios de identificación electrónica notificados que actúen a título comercial o profesional utilizando servicios básicos de plataforma según se define en el artículo 2, apartado 2, del Reglamento (UE) 2022/1925 con el fin de ofrecer servicios de cartera europea de identidad digital y medios de identificación electrónica a usuarios finales o en el curso de dicho suministro deben considerarse usuarios profesionales de conformidad con el artículo 2, apartado 21, del Reglamento (UE) 2022/1925.

17) En el artículo 13, el apartado 1 se sustituye por el texto siguiente:

«1. No obstante lo dispuesto en el apartado 2 del presente artículo, 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.

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 intención ni negligencia por su parte.

18) El artículo 14 se sustituye por el texto siguiente:

«*Artículo 14*

Aspectos internacionales

1. Los servicios de confianza prestados por los 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 la organización internacional son reconocidos en virtud de una decisión de ejecución o un acuerdo celebrado entre la Unión y el tercer país o la organización internacional de conformidad con el artículo 218 del Tratado.

2. Las decisiones de ejecución y los acuerdos a que se refiere el apartado 1 garantizarán que los prestadores de servicios de confianza de terceros países u 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 de servicios de confianza reconocidos.

   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 son reconocidos como legalmente equivalentes a los servicios de confianza prestados por prestadores de servicios en terceros países u organizaciones internacionales con los que se celebran acuerdos.

3. La decisiones de ejecución a que se refiere el apartado 1 se adoptarán de conformidad con el procedimiento de examen contemplado en el artículo 48, apartado 2.

19) El artículo 15 se sustituye por el texto siguiente:

«*Artículo 15*

Accesibilidad para las personas con discapacidad

La prestación de servicios de confianza y los productos destinados a los usuarios finales utilizados en el marco de la prestación de dichos servicios deberán ser accesibles para las personas con discapacidad, de conformidad con los requisitos de accesibilidad establecidos en la Directiva (UE) 2019/882 sobre los requisitos de accesibilidad de los productos y servicios.».

20) El artículo 17 se modifica como sigue:

a) el apartado 4 se modifica como sigue:

1) en el apartado 4, la letra c) se sustituye por el texto siguiente:

«c) informar a las autoridades nacionales competentes de los Estados miembros afectados, designadas en virtud de la Directiva (UE) XXXX/XXXX [SRI 2], de cualquier violación significativa de la seguridad o pérdida de integridad de la que tengan conocimiento en el desempeño de sus tareas. Cuando la violación significativa de la seguridad o la pérdida de integridad afecte a otros Estados miembros, el organismo de control informará al punto de contacto único del Estado miembro en cuestión designado con arreglo a la Directiva (UE) XXXX/XXXX (SRI 2) y a los organismos de supervisión designados con arreglo al artículo 17 del presente Reglamento en los demás Estados miembros afectados. 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;»;

2) la letra f) se sustituye por el texto siguiente:

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

b) el apartado 6 se sustituye por el texto siguiente:

«6. A más tardar el 31 de marzo de cada año, cada organismo de control presentará a la Comisión un informe sobre las principales actividades que haya llevado a cabo durante el año natural anterior.»;

c) el apartado 8 se sustituye por el texto siguiente:

«8. En un plazo máximo de doce meses a contar desde la entrada en vigor del presente Reglamento, la Comisión adoptará directrices sobre el ejercicio por parte de los órganos de supervisión de las funciones a que se refiere el apartado 4 y, por medio de actos de ejecución adoptados de conformidad con el procedimiento de examen contemplado en el artículo 48, apartado 2, definirá los formatos y procedimientos del informe mencionado en el apartado 6.»;

21) El artículo 18 se modifica como sigue:

a) el título del artículo 18 se sustituye por el texto siguiente:

«Asistencia mutua y cooperación»;

b) el apartado 1 se sustituye por el texto siguiente:

«1. los organismos de control cooperarán con vistas a intercambiar prácticas idóneas e información acerca de la prestación de servicios de confianza.»;

c) se añaden los apartados 4 y 5 siguientes:

«4. Los organismos de control y las autoridades nacionales competentes en virtud de la Directiva (UE) XXXX/XXXX del Parlamento Europeo y del Consejo [SRI 2] cooperarán y se prestarán mutuamente asistencia para asegurar que los prestadores de servicios de confianza cumplan los requisitos establecidos en el presente Reglamento y en la Directiva (UE) XXXX/XXXX [SRI 2]. Los organismos de control solicitarán a las autoridades nacionales competentes en virtud de la Directiva (UE) XXXX/XXXX [SRI 2] que lleven a cabo actuaciones de control para verificar la conformidad de los prestadores de servicios de confianza con los requisitos establecidos en la Directiva (UE) XXXX/XXXX [SRI 2], exigir a los prestadores de servicios de confianza que subsanen cualquier falta de conformidad con dichos requisitos, proporcionar en los plazos previstos los resultados de cualquier actividad de control vinculada a los prestadores de servicios de confianza e informar a los órganos de control acerca de los incidentes pertinentes importantes notificados con arreglo a lo dispuesto en la Directiva (UE) XXXX/XXXX [SRI 2].

5. Dentro de los doce meses siguientes a la entrada en vigor del presente Reglamento, la Comisión establecerá, por medio de actos de ejecución, los mecanismos de procedimiento necesarios para facilitar la cooperación entre las autoridades de control 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.»;

21 *bis*) Se inserta el artículo 19 *bis* siguiente:

«Requisitos para 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. Sin perjuicio de lo dispuesto en el artículo 18 de la Directiva (UE) XXXX/XXX [SRI 2], tales medidas incluirán, como mínimo, las siguientes:

i) medidas relacionadas con los procedimientos de registro en un servicio e incorporación a este;

ii) medidas relacionadas con controles administrativos o de procedimiento;

iii) medidas relacionadas con la gestión e implantación de servicios.

b) notificarán al organismo de control, a las personas afectadas identificables, al público si es de interés público y, cuando proceda, a otros organismos pertinentes cualquier infracción o interrupción en la prestación del servicio o en la aplicación de las medidas a que se refiere la letra a), incisos i), ii) y 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 haber tenido conocimiento de ello.

2. Dentro de los doce meses siguientes a la entrada en vigor del presente Reglamento, la Comisión especificará, mediante actos de ejecución, las características técnicas de las medidas a que se refiere el apartado 1 *bis*. Los actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

22) El artículo 20 se modifica como sigue:

a) el apartado 1 se sustituye por el texto siguiente:

«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 18 de la Directiva (UE) XXXX/XXXX [SRI 2]. 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.»;

a *bis*) se inserta el apartado siguiente:

1 *bis*. Los Estados miembros podrán disponer que los prestadores cualificados de servicios de confianza informen con antelación al organismo de supervisión de las auditorías previstas y permitan, previa solicitud, la participación del organismo de supervisión en calidad de observador.

b) en el apartado 2, la última frase se sustituye por el texto siguiente:

«En caso de posible infracción de las normas sobre protección de datos personales, el organismo de control informará, sin dilación indebida, a las autoridades de control competentes en virtud del Reglamento (UE) 2016/679 de los resultados de sus auditorías.»;

c) los apartados 3 y 4 se sustituyen por el texto siguiente:

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

Si el prestador no subsanase el incumplimiento dentro del plazo fijado por el organismo de control, si procede, este, teniendo en cuenta en particular el alcance, la duración y las consecuencias del incumplimiento, podrá retirar la cualificación a dicho prestador o al servicio en cuestión que este presta.

3 *bis*. Cuando las autoridades nacionales competentes informen al organismo de control, en virtud de la Directiva (UE) XXXX/XXXX [SRI 2], de que el prestador cualificado de servicios de confianza incumple alguno de los requisitos establecidos en el artículo 18 de la Directiva (UE) XXXX/XXXX [NIS2], el organismo de control, teniendo en cuenta, en particular, el alcance, la duración y las consecuencias de dicho incumplimiento, podrá retirar la cualificación a dicho prestador o al servicio en cuestión que este presta.

3 *ter*. Cuando las autoridades de control informen al organismo de control, en virtud del Reglamento (UE) 2016/679, de que el prestador cualificado de servicios de confianza incumple alguno de los requisitos establecidos en el Reglamento (UE) 2016/679, el organismo de control, teniendo en cuenta, en particular, el alcance, la duración y las consecuencias de dicho incumplimiento, podrá retirar la cualificación a dicho prestador o al servicio en cuestión que este presta.

3 *quater*. El organismo de control 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 control informará al órgano a que se refiere el artículo 22, apartado 3, a efectos de la actualización de las listas de confianza a las que se refiere el artículo 22, apartado 1, y las autoridades nacionales competentes a que se refiere la Directiva (UE) XXXX/XXXX [SRI 2].

4. Dentro de los doce meses siguientes a la entrada en vigor del presente Reglamento, la Comisión establecerá, por medio de actos de ejecución, las especificaciones técnicas y los números de referencia de lo siguiente:

a) la acreditación de los organismos de evaluación de la conformidad y para 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 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.»;

23) El artículo 21 se modifica como sigue:

«1. Cuando los prestadores de servicios de confianza tengan intención de iniciar la prestación de un servicio de confianza cualificado, presentarán al organismo de control una notificación de 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 18 de la Directiva (UE) XXXX/XXXX [SRI 2].»;

a) el apartado 2 se sustituye por el texto siguiente:

«2. El organismo de control 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 establecidos para los prestadores cualificados de servicios de confianza y para los servicios de confianza cualificados que estos prestan.

Con el fin de verificar que el proveedor de servicios de confianza cumple los requisitos establecidos en el artículo 18 de la Directiva XXXX [SRI 2], el organismo de control solicitará a las autoridades competentes a que se refiere la citada Directiva que lleven a cabo actuaciones de control en ese sentido y que proporcionen información sobre los resultados de dichas actuaciones sin dilación indebida, a más tardar dos meses después de la recepción de dicha solicitud por parte de las autoridades competentes a que se refiere la Directiva XXXX [SRI 2]. Si la verificación no ha concluido en el plazo de dos meses a partir de la notificación, las autoridades competentes a que se refiere la Directiva XXXX [SRI 2] informarán al organismo de control especificando los motivos de la dilación y el plazo previsto para concluir la verificación.

Si el organismo de control 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 control 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 a que se refiere 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, el organismo de control informará al prestador de servicios de confianza especificando los motivos de la dilación y el plazo previsto para concluir la verificación.»;

b) el apartado 4 se sustituye por el texto siguiente:

«4. Dentro de los doce meses siguientes a la entrada en vigor del presente Reglamento, la Comisión definirá, 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. Los actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.».

25) El artículo 24 se modifica como sigue:

a) el apartado 1 se sustituye por el texto siguiente:

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

La información a que se refiere el párrafo primero será verificada por el prestador cualificado de servicios de confianza, bien directamente, bien por medio de un tercero, de cualquiera de las formas siguientes:

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 declaraciones electrónicas cualificadas de atributos o de un certificado de una firma electrónica cualificada o de un sello electrónico cualificado expedido de conformidad con la letra a), c) o d);

c) utilizando cualesquier 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 procedimientos adecuados y de conformidad con el Derecho nacional.»;

b) se inserta el apartado 1 *bis* siguiente:

«1 *bis*. Dentro de los doce meses siguientes a la entrada en vigor del presente Reglamento, la Comisión establecerá, mediante actos de ejecución, las especificaciones técnicas, las normas y los procedimientos mínimos con respecto a la verificación de la identidad y los atributos de conformidad con lo dispuesto en el apartado 1, letra c). Los actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.»;

c) el apartado 2 se modifica como sigue:

0) la letra a) se modifica como sigue:

«a) informarán al organismo de control de cualquier cambio en la prestación de servicios de confianza cualificados al menos un mes antes de llevarlo a cabo, y de su intención de cesar tales actividades con una antelación de al menos tres meses. El organismo de control podrá solicitar información adicional o el resultado de una evaluación de la conformidad antes de conceder la autorización para aplicar los cambios previstos en los servicios de confianza cualificados. Si la verificación no ha concluido en el plazo de tres meses, el organismo de supervisión informará al prestador de servicios de confianza especificando los motivos de la demora y el plazo previsto para concluir la verificación;».

1) las letras d) y e) se sustituyen por el texto siguiente:

«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 sustentan, en particular utilizando algoritmos criptográficos, longitud de la clave y funciones resumen adecuados en los sistemas, productos y procesos que sustentan;».

2) se insertan las letras f *bis*) y f *ter*) siguientes:

«f *bis*) 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. No obstante lo dispuesto en el artículo 18 de la Directiva (UE) XXXX/XXX [SRI 2], tales medidas incluirán, como mínimo, las siguientes:

i) medidas relacionadas con los procedimientos de registro en un servicio e incorporación a este;

ii) medidas relacionadas con controles administrativos o de procedimiento;

iii) medidas relacionadas con la gestión e implantación de servicios;

f *ter*) notificarán al organismo de control, a las personas afectadas identificables, a otros organismos competentes pertinentes cuando proceda y, a solicitud del organismo de control, al público si es de interés público, cualquier infracción 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) y 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;».

3) las letras g) y h) se sustituyen por el texto siguiente:

«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;».

4) se suprime la letra j);

d) se inserta el apartado 4 *bis* siguiente:

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

e) el apartado 5 se sustituye por el texto siguiente:

«5. Dentro de los doce meses siguientes a la entrada en vigor del presente Reglamento, la Comisión establecerá, mediante actos de ejecución, las especificaciones técnicas, los procedimientos y los números de referencia de las normas respecto de los requisitos a que se refiere el apartado 2. Se presumirá el cumplimiento de los requisitos establecidos en el presente artículo cuando se cumplan dichos procedimientos, especificaciones técnicas y normas. Los actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.»;

f) se añade el apartado 6 siguiente:

«6. La Comisión estará facultada para adoptar actos de ejecución en los que se especifiquen las características técnicas de las medidas a que se refiere el apartado 2, letra f *bis*).».

25 *bis*) El artículo 26 se modifica como sigue:

«2. Dentro de los doce meses siguientes a la entrada en vigor del presente Reglamento, la Comisión establecerá, mediante actos de ejecución, las especificaciones técnicas y los números de referencia de las normas relativas a firmas electrónicas avanzadas. Se presumirá el cumplimiento de los requisitos relativos a las firmas electrónicas avanzadas cuando una firma electrónica avanzada se ajuste a dichas especificaciones y normas. Los actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.».

25 *ter*) El artículo 27 se modifica como sigue:

Se suprime el apartado 4.

26) En el artículo 28, el apartado 6 se sustituye por el texto siguiente:

«6. Dentro de los doce meses siguientes a la entrada en vigor del presente Reglamento, la Comisión establecerá, mediante actos de ejecución, las especificaciones técnicas y los números de referencia de las normas para los certificados cualificados de firma electrónica. Se presumirá el cumplimiento de los requisitos establecidos en el anexo I cuando un certificado cualificado de firma electrónica se ajuste a dichas especificaciones y normas. Los actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.».

27) En el artículo 29 se añade el siguiente apartado 1 *bis*:

«1 *bis*. La creación, la gestión de datos de creación de firma electrónica en nombre del signatario o la duplicación de estos datos de creación de firma con fines de copia de seguridad son funciones reservadas en exclusiva a un prestador cualificado de servicios de confianza que preste un servicio de confianza cualificado para la gestión de un dispositivo cualificado remoto de creación de firma electrónica.».

28) Se inserta el artículo 29 *bis* siguiente:

«*Artículo 29* bis

Requisitos que debe cumplir un servicio cualificado para la gestión de dispositivos cualificados remotos de creación de firma electrónica

1. La gestión de dispositivos cualificados remotos de creación de firma electrónica como servicio cualificado es una función reservada en exclusiva a 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, pueda duplicar 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 es del mismo nivel que el previsto para los conjuntos de datos originales;

      ii. el número de conjuntos de datos duplicados no supera el mínimo necesario para garantizar la continuidad del servicio;

   c) cumple todos los requisitos definidos en el informe de certificación del dispositivo cualificado remoto específico de creación de firmas emitido en virtud del artículo 30.

2. Dentro de los doce meses siguientes a la entrada en vigor del presente Reglamento, la Comisión establecerá, mediante actos de ejecución, las especificaciones técnicas y los números de referencia de las normas a efectos de lo dispuesto en el apartado 1.».

29) En el artículo 30, se inserta el apartado 3 *bis* siguiente:

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

30) En el artículo 31, el apartado 3 se sustituye por el texto siguiente:

«3. Dentro de los doce meses siguientes a la entrada en vigor del presente Reglamento, la Comisión definirá, mediante actos de ejecución, los formatos y procedimientos aplicables a efectos del apartado 1. Los actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.».

31) El artículo 32 se modifica como sigue:

a) en el apartado 1 se añade el párrafo siguiente:

«Se presumirá el cumplimiento de los requisitos establecidos en el párrafo primero cuando la validación de firmas electrónicas cualificadas se ajuste a las especificaciones y las normas a que se refiere el apartado 3.»;

b) el apartado 3 se sustituye por el texto siguiente:

«3. En un plazo máximo de doce meses a contar desde la entrada en vigor del presente Reglamento, la Comisión dispondrá, mediante actos de ejecución, las especificaciones y los números de referencia de las normas relativas a la validación de las firmas electrónicas cualificadas. Los actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.».

31 *bis*) Se inserta el artículo 32 *bis* siguiente:

«Requisitos de 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 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 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. Se presumirá el cumplimiento de los requisitos establecidos en el párrafo primero cuando la validación de firmas electrónicas avanzadas basadas en certificados cualificados se ajuste a las especificaciones y las normas a que se refiere el apartado 3.

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. En un plazo máximo de doce meses a contar desde la entrada en vigor del presente Reglamento, la Comisión dispondrá, mediante actos de ejecución, las especificaciones y los números de referencia de las normas relativas a la validación de firmas electrónicas avanzadas basadas en certificados cualificados. Los actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.».

31 *ter*) El artículo 33 se modifica como sigue:

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

«2. Dentro de los doce meses siguientes a la entrada en vigor del presente Reglamento, la Comisión establecerá, mediante actos de ejecución, las especificaciones técnicas y los números de referencia de las normas relativas al servicio de validación cualificado a que se refiere el apartado 1. Se presumirá el cumplimiento de los requisitos establecidos en el apartado 1 cuando la validación del servicio de firma electrónica cualificada se ajuste a dichas especificaciones y normas. Los actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.».

32) El artículo 34 se sustituye por el texto siguiente:

«*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.

2. Se presumirá el cumplimiento de los requisitos establecidos en el apartado 1 cuando los mecanismos del servicio cualificado de conservación de firmas electrónicas cualificadas se ajusten a las especificaciones y las normas a que se refiere el apartado 3.

3. En un plazo máximo de doce meses a contar desde la entrada en vigor del presente Reglamento, la Comisión establecerá, mediante actos de ejecución, las especificaciones técnicas y los números de referencia de las normas relativas al servicio cualificado de conservación de firmas electrónicas cualificadas. Los actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.».

32 *bis*) En el artículo 36, se añade el apartado 2 siguiente:

2. «Dentro de los doce meses siguientes a la entrada en vigor del presente Reglamento, la Comisión establecerá, mediante actos de ejecución, las especificaciones técnicas y los números de referencia de las normas relativas a los sellos electrónicos avanzados.

Se presumirá el cumplimiento de los requisitos relativos a los sellos electrónicos avanzados cuando un sello electrónico avanzado se ajuste a dichas especificaciones y normas. Los actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.».

33) El artículo 37 se modifica como sigue:

Se suprime el apartado 4.

34) El artículo 38 se modifica como sigue:

a) el apartado 1 se sustituye por el texto siguiente:

«1. Los certificados cualificados de sello electrónico cumplirán los requisitos establecidos en el anexo III. Se presumirá el cumplimiento de los requisitos establecidos en el anexo III cuando un certificado cualificado de sello electrónico se ajuste a las especificaciones y las normas a que se refiere el apartado 6.»;

b) el apartado 6 se sustituye por el texto siguiente:

«6. En un plazo máximo de doce meses a contar desde la entrada en vigor del presente Reglamento, la Comisión establecerá, por medio de actos de ejecución, las especificaciones técnicas y los números de referencia de las normas para los certificados cualificados de sello electrónico. Los actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.».

35) Se inserta el artículo 39 *bis* siguiente:

«*Artículo 39* bis

Requisitos que debe cumplir un servicio cualificado para la gestión de dispositivos cualificados remotos de creación de sello electrónico

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

35 *bis*) Se inserta el artículo 40 *bis* siguiente:

«*Artículo 40* bis

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

(1) El artículo 32 *bis* se aplicará *mutatis mutandis* a la validación de los sellos electrónicos avanzados basados en certificados cualificados.».

36) El artículo 42 se modifica como sigue:

a) se añade el apartado 1 *bis* siguiente:

«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 la fuente de información temporal exacta se ajuste a las especificaciones y las normas a que se refiere el apartado 2.»;

b) el apartado 2 se sustituye por el texto siguiente:

«2. En un plazo máximo de doce meses a contar desde la entrada en vigor del presente Reglamento, la Comisión establecerá, mediante actos de ejecución, las especificaciones técnicas y los números de referencia de las normas relativas a la vinculación de la fecha y hora con los datos y a fuentes de información temporal exacta. Los actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.».

36 *bis*) En el artículo 43, se añade el apartado 3 siguiente:

2 *bis*. Un servicio cualificado de entrega electrónica certificada en un Estado miembro será reconocido como servicio cualificado de entrega electrónica certificada en cualquier otro Estado miembro.».

37) El artículo 44 se modifica como sigue:

a) se inserta el apartado 1 *bis* siguiente:

«1 *bis*. Se presumirá el cumplimiento de los requisitos establecidos en el apartado 1 cuando el proceso de envío y recepción de datos se ajuste a las especificaciones y las normas a que se refiere el apartado 2.»;

b) el apartado 2 se sustituye por el texto siguiente:

«2. En un plazo máximo de doce meses a contar desde la entrada en vigor del presente Reglamento, la Comisión establecerá, por medio de actos de ejecución, las especificaciones técnicas y los números de referencia de las normas para los procesos de envío y recepción de datos. Los actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.»;

c) se insertan los apartados 3 y 4 siguientes:

«3. 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. La conformidad será confirmada por un organismo de evaluación de la conformidad.

4. La Comisión podrá establecer, mediante un acto de ejecución, las especificaciones técnicas y los números de referencia de las normas para facilitar la transferencia de datos entre dos o más prestadores de servicios de confianza. 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.».

38) El artículo 45 se sustituye por el texto siguiente:

«*Artículo 45*

Requisitos de 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 los requisitos establecidos en el anexo IV se llevará a cabo de conformidad con las especificaciones y las normas a que se refiere el apartado 4.

2. Los navegadores web reconocerán los certificados cualificados de autenticación de sitios web a que se refiere el apartado 1. Con este fin, los navegadores web garantizarán que los datos de identificación proporcionados mediante cualquiera de los métodos se muestren al usuario de un modo fácil de entender. Los navegadores web garantizarán la compatibilidad e interoperabilidad con los certificados cualificados de autenticación de sitios web a que se refiere el apartado 1, con la excepción de las empresas consideradas microempresas y pequeñas empresas de conformidad con la Recomendación 2003/361/CE de la Comisión en sus primeros cinco años de actividad como prestadores de servicios de navegación web.

4. Dentro de los doce meses siguientes a la entrada en vigor del presente Reglamento, la Comisión dispondrá, por medio de actos de ejecución, las especificaciones y los números de referencia de las normas para los certificados cualificados de autenticación de sitios web a que se refieren los apartados 1 y 2. Los actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.».

39) Tras el artículo 45, se insertan las secciones 9, 10 y 11 siguientes:

«SECCIÓN 9

DECLARACIÓN ELECTRÓNICA DE ATRIBUTOS

Artículo 45 bis

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 de las declaraciones electrónicas cualificadas de atributos.

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

3. Una declaración electrónica cualificada de atributos emitida en un Estado miembro será reconocida como declaración electrónica cualificada de atributos en cualquier otro Estado miembro.

4. Una declaración de atributos emitida por —o en nombre de— un organismo del sector público responsable de una fuente auténtica será reconocida como declaración de atributos emitida por —o en nombre de— un organismo del sector público responsable de una fuente auténtica en todos los Estados miembros.

Artículo 45 ter

Declaración electrónica de atributos en servicios públicos

Cuando el Derecho nacional exija una identificación electrónica utilizando un medio de identificación electrónica y una autenticación para acceder a un servicio en línea prestado por un organismo público, los datos de identificación personal contenidos en la declaración electrónica de atributos no sustituirán a la identificación electrónica utilizando 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 quater

Requisitos que debe cumplir la declaración electrónica cualificada de atributos

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

1 *bis*. La evaluación del cumplimiento de los requisitos establecidos en el anexo V se llevará a cabo de conformidad con las especificaciones y las normas a que se refiere el apartado 4.

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

3. 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.

4. Dentro de los seis meses siguientes a la entrada en vigor del presente Reglamento, la Comisión establecerá las especificaciones técnicas y los números de referencia de las normas para las declaraciones electrónicas cualificadas de atributos por medio de un acto de ejecución sobre la implantación de las carteras europeas de identidad digital, tal como prevé el artículo 6 *bis*, apartado 11.

Artículo 45 quinquies

Cotejo de atributos con fuentes auténticas

1. En un plazo de veinticuatro meses a partir de la entrada en vigor de los actos de ejecución a que se refieren el artículo 6 *bis*, apartado 11, y el artículo 6 *quater*, apartado 4, 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 proveedores cualificados de declaraciones electrónicas de atributos verifiquen dichos atributos por medios electrónicos, a petición del usuario y de conformidad con el Derecho nacional o de la Unión.

2. Dentro de los seis meses siguientes a la entrada en vigor del presente Reglamento, la Comisión, teniendo en cuenta las normas internacionales aplicables, establecerá las especificaciones técnicas, normas y procedimientos mínimos en referencia al catálogo de atributos y sistemas para la declaración de atributos y los procedimientos de verificación de declaraciones electrónicas cualificadas de atributos, por medio de un acto de ejecución relativo a la implantación de las carteras europeas de identidad digital, tal como prevé el artículo 6 *bis*, apartado 11.

Artículo 45 quinquies bis

Requisitos que debe cumplir la declaración electrónica de atributos emitida por —o en nombre de— un organismo del sector público responsable de una fuente auténtica

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

a) los requisitos establecidos en el anexo VII;

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 45 *bis*, 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:

i) que indicará que el organismo emisor está establecido de conformidad con el Derecho nacional o de la Unión, 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) que proporcionará un conjunto de datos que representen inequívocamente la fuente auténtica a que se refiere la letra i); y

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

2. El Estado miembro en el que estén establecidos los organismos del sector público a que se refiere el artículo 3, punto 45 *bis*, velará por que los organismos del sector público que emitan 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.

2 *bis*. Los Estados miembros notificarán a la Comisión los organismos del sector público a que se refiere el artículo 3, punto 45 *bis*. Esta 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 organismos del sector público a que se refiere el artículo 3, punto 45 *bis*, en una forma firmada o sellada electrónicamente apropiada para el tratamiento automático.

3. Si una declaración electrónica de atributos emitida por —o en nombre de— un organismo del sector público responsable de una fuente auténtica ha sido revocada después de su emisión inicial, perderá su validez desde el momento de su revocación. La revocación de una declaración electrónica es irreversible.

4. Se considerará que una declaración electrónica de atributos emitida por —o en nombre de— un organismo del sector público responsable de una fuente auténtica cumple los requisitos establecidos en el apartado 1 del presente artículo cuando se ajuste a las normas a que se refiere el apartado 5.

5. Dentro de los seis meses siguientes a la entrada en vigor del presente Reglamento, la Comisión establecerá las especificaciones técnicas y los números de referencia de las normas para las declaraciones electrónicas de atributos emitidas por —o en nombre de— un organismo del sector público responsable de una fuente auténtica, por medio de un acto de ejecución sobre la implantación de las carteras europeas de identidad digital, tal como prevé el artículo 6 *bis*, apartado 11.

5 *bis*. Dentro de los seis meses siguientes a la entrada en vigor del presente Reglamento, la Comisión definirá los formatos, los procedimientos, las especificaciones y las normas a efectos del apartado 2 *bis*, por medio de un acto de ejecución relativo a la implantación de las carteras europeas de identidad digital, tal como prevé el artículo 6 *bis*, apartado 11.

6. Los organismos del sector público a que se refiere el artículo 3, punto 45 *bis,* que expidan declaraciones electrónicas de atributos proporcionarán una interfaz con las carteras europeas de identidad digital proporcionadas con arreglo al artículo 6 *bis*.

Artículo 45 sexies

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

Los proveedores de declaraciones electrónicas cualificadas de atributos proporcionarán una interfaz con las carteras europeas de identidad digital proporcionadas con arreglo al artículo 6 *bis*.

Artículo 45 septies

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. Los datos personales relacionados con la prestación de servicios de declaración electrónica de atributos se conservarán en soporte lógico por separado de otros datos que mantenga el proveedor de declaraciones electrónicas de atributos.

4. Los prestadores de servicios cualificados de declaraciones electrónicas de atributos aplicarán una separación funcional para prestar dichos servicios.

SECCIÓN 10

SERVICIOS DE ARCHIVO ELECTRÓNICO

Artículo 45 octies

Efecto jurídico de un servicio de archivo electrónico

1. No se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a los datos electrónicos almacenados mediante un servicio de archivo electrónico por el mero hecho de que estén en formato electrónico o no estén almacenados mediante un servicio cualificado de archivo electrónico.

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

3. Un servicio cualificado de archivo electrónico en un Estado miembro será reconocido como servicio cualificado de archivo electrónico en cualquier otro Estado miembro.

Artículo 45 octies bis

Requisitos de 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 ampliar la durabilidad y legibilidad de los datos electrónicos más allá del período de validez tecnológico y, al menos, durante el período de conservación legal o contractual, manteniendo al mismo tiempo su integridad y su origen;

c) garantizar que los datos 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 un dato electrónico recuperado de un archivo electrónico cualificado goza de la presunción de integridad desde el inicio del período de conservación hasta el momento de su recuperación. Dicho informe se proporcionará de una manera que sea fiable y eficiente e incluya la firma electrónica avanzada o el sello electrónico avanzado del prestador del servicio cualificado de archivo electrónico.

2. Dentro de los doce meses siguientes a la entrada en vigor del presente Reglamento, la Comisión establecerá, mediante actos de ejecución, las especificaciones técnicas y los números de referencia de las normas para los servicios cualificados de archivo electrónico. Se presumirá el cumplimiento de los requisitos relativos a los servicios cualificados de archivo electrónico cuando un servicio cualificado de archivo electrónico se ajuste a dichas especificaciones y normas. Los 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 nonies

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 de los libros mayores electrónicos cualificados.

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 la presunción de integridad.

3. Un libro mayor electrónico cualificado en un Estado miembro será reconocido como libro mayor electrónico cualificado en cualquier otro Estado miembro.

Artículo 45 decies

Requisitos de los libros mayores electrónicos cualificados

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

   a) estar creado 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 se ajuste a las especificaciones y las normas a que se refiere el apartado 3.

3. La Comisión podrá establecer, por medio de actos de ejecución, las especificaciones técnicas y los números de referencia de normas para la creación y funcionamiento de un libro mayor electrónico cualificado. Los actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.».

40) Se inserta el artículo 48 *bis* siguiente:

«*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 una vez que estén disponibles 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 de identidad digital europea válida;

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

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

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.».

41) El artículo 49 se sustituye por el texto siguiente:

«*Artículo 49*

Revisión

1. La Comisión revisará la aplicación del presente Reglamento e informará al Parlamento Europeo y al Consejo en un plazo máximo de treinta y seis meses desde su entrada en vigor. La Comisión evaluará en particular el ámbito de aplicación de los artículos 6 y 6 *quinquies ter* y si es apropiado modificar el ámbito de aplicación del presente Reglamento o sus disposiciones específicas, teniendo en cuenta la experiencia adquirida en la aplicación del presente Reglamento, así como la evolución de las demandas de los clientes, tecnológica, del mercado y jurídica. Si fuera necesario, el informe irá acompañado de una propuesta de modificación del presente Reglamento.

2. El informe de evaluación incluirá una evaluación de la disponibilidad y facilidad de uso de las carteras europeas de identidad digital contempladas en el ámbito de aplicación del presente Reglamento, y evaluará si 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 tendrán la obligación de aceptar el uso de las carteras europeas de identidad digital.

3. Asimismo, la Comisión presentará un informe al Parlamento Europeo y al Consejo cada cuatro años tras el informe mencionado en el párrafo primero sobre la marcha hacia el logro de los objetivos del presente Reglamento.».

42) El artículo 51 se sustituye por el texto siguiente:

«*Artículo 51*

Medidas transitorias

1. Los dispositivos de creación de firmas seguras 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 firmas electrónicas en virtud del presente Reglamento durante un período de treinta y seis meses tras la entrada en vigor del presente Reglamento.

2. Los certificados cualificados expedidos a personas físicas en virtud de la Directiva 1999/93/CE seguirán considerándose certificados cualificados de firma electrónica en virtud del presente Reglamento durante un período de veinticuatro meses tras la entrada en vigor del presente Reglamento.

2 *bis*. Durante veinticuatro meses tras la entrada en vigor del presente Reglamento, seguirá considerándose que no es necesaria la obtención de la cualificación para la prestación de servicios de gestión de los dispositivos cualificados remotos de creación de firma y sello electrónicos por parte de prestadores cualificados de servicios de confianza distintos de los prestadores cualificados de servicios de confianza que prestan servicios cualificados de confianza para la gestión de dispositivos cualificados remotos de creación de firma y sello electrónicos de conformidad con los artículos 29 *bis* y 39 *bis*.

2 *ter* Los proveedores cualificados de servicios de confianza a los que se haya concedido su cualificación en virtud del presente Reglamento antes del [fecha de entrada en vigor del Reglamento modificativo] utilizando métodos de verificación de la identidad para la expedición de certificados cualificados con arreglo al artículo 24, apartado 1, presentarán al organismo de control un informe de evaluación de la conformidad que demuestre el cumplimiento del artículo 24, apartado 1, tan pronto como sea posible, y a más tardar treinta meses después de la entrada en vigor del Reglamento modificativo. Hasta la presentación de dicho informe de evaluación de la conformidad y la finalización de su evaluación por parte del organismo de control, el prestador cualificado de servicios de confianza podrá seguir recurriendo a los métodos de verificación de la identidad establecidos en el artículo 24, apartado 1, del Reglamento (UE) n.º 910/2014.».

43) El anexo I se modifica de conformidad con el anexo I del presente Reglamento.

44) El anexo II se sustituye por el texto que figura en el anexo II del presente Reglamento.

45) El anexo III queda modificado con arreglo a lo dispuesto en el anexo III del presente Reglamento.

46) El anexo IV se modifica de conformidad con el anexo IV del presente Reglamento.

47) Se añade un nuevo anexo V, tal como figura en el anexo V del presente Reglamento.

48) Se añade un nuevo anexo VI al presente Reglamento.

Artículo 52

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

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

Hecho en Bruselas, el

Por el Parlamento Europeo	Por el Consejo
La Presidenta / El Presidente	La Presidenta / El Presidente

ANEXO I

En el anexo I, el punto i) se sustituye por el texto siguiente:

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

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 firmas electrónicas 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 firmas electrónicas no pueden ser hallados por deducción y de que la firma electrónica 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 firmas electrónicas puedan ser protegidos con seguridad por el firmante legítimo contra 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.

ANEXO III

En el anexo III, el punto i) se sustituye por el texto siguiente:

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

ANEXO IV

En el anexo IV, el punto j) se sustituye por el texto siguiente:

«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.».

ANEXO V

REQUISITOS DE LA DECLARACIÓN ELECTRÓNICA DE ATRIBUTOS CUALIFICADA

La declaración electrónica de atributos cualificada contendrá:

(e) una indicación, al menos en un formato adecuado para el tratamiento automático, de que la declaración ha sido expedida como declaración electrónica de atributos cualificada;

(f) un conjunto de datos que represente inequívocamente al prestador cualificado de servicios de confianza que expide la declaración electrónica de atributos cualificada, 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;

(g) un conjunto de datos que represente inequívocamente a la entidad a que se refieren los atributos declarados; si se usara un seudónimo, se indicará claramente;

(h) el atributo o atributos declarados, incluyendo, cuando proceda, la información necesaria para identificar el alcance de dichos atributos;

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

(j) 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;

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

(l) el lugar en que está disponible gratuitamente el certificado que respalda la firma electrónica cualificada o el sello electrónico cualificado a que se hace referencia en la letra g);

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

ANEXO VI

LISTA MÍNIMA DE ATRIBUTOS

Además de lo dispuesto en el artículo 45 quinquies, los Estados miembros garantizarán la adopción de medidas que permitan a los prestadores cualificados 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 nacional o de la Unión y en los casos en que 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. permisos y licencias públicos,
10. datos financieros y sociales.

ANEXO VII

REQUISITOS PARA DECLARACIONES ELECTRÓNICAS DE ATRIBUTOS EXPEDIDAS POR O EN NOMBRE DE UN ORGANISMO PÚBLICO RESPONSABLE DE UNA FUENTE AUTÉNTICA

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

a) una indicación, como mínimo en un formato adecuado para el procesamiento automático, de que la declaración ha sido expedida como una declaración electrónica de atributos por o en nombre de un organismo público responsable de una fuente auténtica;
b) un conjunto de datos que represente inequívocamente al organismo público que expide la declaración electrónica de atributos, en particular, 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; si se usara un seudónimo, se indicará claramente;
d) el atributo o atributos declarados, incluyendo, 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, la 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 hace referencia en la letra g);
i) la información o la localización de los servicios que pueden utilizarse para consultar el estado de validez de la declaración.

_____