BASE DE DATOS DE Norma CEF.-
Referencia: NCL013368

REGLAMENTO (UE) 2024/1183, DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 11 de abril, por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital.

(DOUE L, de 30 de abril de 2024)

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,
Visto el dictamen del Comité de las Regiones,
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», 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.

(2) En sus Conclusiones de 1 y 2 de octubre de 2020, 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 los ciudadanos 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) El Programa Estratégico de la Década Digital para 2030, establecido por la Decisión (UE) 2022/2481 del Parlamento Europeo y del Consejo, fija los objetivos y las metas digitales de un marco de la Unión que, de aquí a 2030, deben dar lugar a la implantación generalizada de una identidad digital fiable, voluntaria y controlada por el usuario, reconocida en toda la Unión y que permita a todos los usuarios controlar sus datos en las interacciones en línea.

(4) La Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital, proclamada por el Parlamento Europeo, el Consejo y la Comisión (en lo sucesivo, «Declaración»), subraya el derecho de todas las personas a acceder a tecnologías, productos y servicios digitales que sean seguros y protejan la privacidad desde el diseño. Esto incluye velar por que se ofrezca a todas las personas que viven en la Unión una identidad digital accesible, segura y fiable que permita acceder a una amplia gama de servicios en línea y fuera de línea, protegida contra los riesgos de ciberseguridad y los ciberdelitos, por ejemplo, la violación de la seguridad de los datos y la usurpación o la manipulación de identidad. En la Declaración también se afirma que toda persona tiene derecho a la protección de sus datos personales. Este derecho incluye el control de cómo se utilizan esos datos y con quién se comparten.

(5) Los ciudadanos de la Unión y los residentes en la Unión deben tener derecho a poseer una identidad digital que se mantenga bajo su control exclusivo y les permita ejercer sus derechos en el entorno digital y participar en la economía digital. Para alcanzar este objetivo, debe establecerse un marco europeo de identidad digital que permita a los ciudadanos de la Unión y los residentes en la Unión acceder a servicios públicos y privados en línea y fuera de línea en toda la Unión.

(6) Un marco de identidad digital armonizado debe contribuir a la creación de una Unión más integrada digitalmente al reducir los obstáculos digitales entre los Estados miembros y capacitar a los ciudadanos de la Unión y los residentes en la Unión para que disfruten de los beneficios de la digitalización, aumentando al mismo tiempo la transparencia y la protección de sus derechos.

(7) Un enfoque más armonizado en lo que respecta a la identificación electrónica debe reducir los riesgos y los costes asociados a la actual fragmentación derivada del uso de soluciones nacionales divergentes o, en algunos Estados miembros, a la ausencia de tales soluciones de identificación electrónica. Este enfoque debe reforzar el mercado interior al permitir que los ciudadanos de la Unión, los residentes en la Unión tal como se definen en el

Derecho nacional y las empresas se identifiquen y proporcionen una autenticación de su identidad en línea y fuera de línea de manera segura, fiable, fácil de usar, cómoda, accesible y armonizada en toda la Unión. La cartera europea de identidad digital debe proporcionar a las personas físicas y jurídicas de la Unión un medio de identificación electrónica armonizado que permita autenticar y compartir datos relacionados con su identidad. Toda persona debe poder 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 electrónicas de atributos verificadas, como cualificaciones académicas, por ejemplo, títulos universitarios u otros títulos profesionales o académicos. El marco europeo de identidad digital tiene por finalidad lograr un cambio que permita pasar de la utilización exclusiva de soluciones nacionales de identidad digital a la provisión de declaraciones electrónicas de atributos que sean válidas y estén legalmente reconocidas en toda la Unión. Los prestadores 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.

(8) Varios Estados miembros han aplicado y emplean medios de identificación electrónica que son aceptados por prestadores de servicios en la Unión. Asimismo, se han realizado inversiones en soluciones tanto nacionales como transfronterizas atendiendo al Reglamento (UE) n.º 910/2014, incluida la interoperabilidad de los sistemas de identificación electrónica notificados con arreglo a dicho Reglamento. Con el fin de garantizar la complementariedad y la rápida adopción de las carteras europeas de identidad digital por los usuarios existentes de los medios de identificación electrónica notificados, así como de reducir al mínimo las repercusiones sobre los prestadores de servicios existentes, se espera que las carteras europeas de identidad digital se beneficien de la experiencia adquirida con los medios de identificación electrónica existentes y de la infraestructura de los sistemas de identificación electrónica notificados implantada a escala nacional y de la Unión.

(9) El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo y, en su caso, la Directiva 2002/58/CE del Parlamento Europeo y del Consejo se aplican a todas las actividades de tratamiento de datos personales en virtud del Reglamento (UE) n.º 910/2014. Las soluciones que forman parte del marco de interoperabilidad previsto en el presente Reglamento también cumplen dichas normas. El Derecho de la Unión en materia de protección de datos establece principios, como los de minimización de datos y limitación de finalidad, y obligaciones, como la protección de datos desde el diseño y por defecto.

(10) Con el fin de fomentar la competitividad de las empresas de la Unión, los prestadores de servicios tanto en línea como fuera de línea deben poder contar con soluciones de identidad digital reconocidas en toda la Unión, independientemente del Estado miembro en el que se proporcionen, de tal manera que se beneficien de un enfoque armonizado de la Unión en lo que respecta a la confianza, la seguridad y la interoperabilidad. Tanto los usuarios como los prestadores de servicios deben poder beneficiarse de que se confiera el mismo valor jurídico a las declaraciones electrónicas de atributos en toda la Unión. El objetivo de un marco armonizado para una identidad digital es crear valor económico al facilitar el acceso a bienes y servicios y reducir considerablemente los costes de explotación asociados a los procedimientos de identificación y autenticación electrónicas, por ejemplo, durante la incorporación de nuevos clientes, así como las posibilidades de que se cometan ciberdelitos, como la usurpación de identidad, el robo de datos y el fraude en línea, y, así, propiciar una mayor eficiencia y una transformación digital segura de las pymes de la Unión.

(11) Las carteras europeas de identidad digital deben facilitar la aplicación del principio de «solo una vez» y, de esta manera, reducir la carga administrativa que recae sobre los ciudadanos de la Unión y los residentes en la Unión, así como sobre las empresas de toda la Unión, y apoyar su movilidad transfronteriza, además de fomentar el desarrollo de servicios de administración electrónica interoperables en toda la Unión.

(12) El Reglamento (UE) 2016/679, el Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo y la Directiva 2002/58/CE son aplicables al tratamiento de datos personales efectuado en aplicación del presente Reglamento. En consecuencia, el presente Reglamento debe establecer salvaguardas específicas para evitar que los proveedores de medios de identificación electrónica y declaraciones electrónicas de atributos combinen los datos personales obtenidos al prestar otros servicios con los datos personales tratados para prestar los servicios contemplados en el ámbito de aplicación del presente Reglamento. Se debe establecer una separación lógica entre los datos personales relacionados con la provisión de carteras europeas de identidad digital y cualesquier otros datos que obren en poder del proveedor de la cartera. El presente Reglamento no debe impedir a los proveedores de las carteras europeas de identidad digital aplicar medidas técnicas adicionales que contribuyan a la protección de los datos personales, como por ejemplo la separación física entre los datos personales relacionados con la provisión de carteras europeas de identidad digital y cualesquier otros datos en poder del proveedor. Sin perjuicio de lo dispuesto en el Reglamento (UE) 2016/679, el presente Reglamento especifica la aplicación de los principios de limitación de finalidad, minimización de datos y protección de datos desde el diseño y por defecto.

(13) La función de panel común debe integrarse en el diseño de las carteras europeas de identidad digital, a fin de garantizar un mayor grado de transparencia, privacidad y control por parte de los usuarios de sus datos personales. Dicha función debe ofrecer una interfaz fácil y de uso sencillo con una visión general de todas las partes usuarias con las que el usuario comparte datos, incluidos los atributos, y el tipo de datos compartidos con cada parte usuaria. Debe permitir al usuario efectuar un seguimiento de todas las transacciones ejecutadas a través de la cartera europea de identidad digital con al menos los siguientes datos: la hora y la fecha de la transacción, la identificación de la contraparte, los datos personales solicitados y los datos compartidos. Tal información debe almacenarse aun cuando la transacción no se haya concluido. No debe ser posible repudiar la autenticidad de la información contenida en el historial de transacciones. Tal función debe estar activada por defecto. Debe permitir al usuario solicitar fácilmente a una parte usuaria que suprima inmediatamente datos personales en virtud del artículo 17 del Reglamento (UE) 2016/679 y denunciar fácilmente a una parte usuaria ante la autoridad nacional competente de protección de datos cuando se reciba una solicitud presuntamente ilícita o sospechosa de datos personales directamente a través de la cartera europea de identidad digital.

(14) Los Estados miembros deben integrar en la cartera europea de identidad digital distintas tecnologías de protección de la privacidad, como la prueba de conocimiento cero. Estos métodos criptográficos deben permitir que una parte usuaria valide si una declaración dada basada en los datos de identificación y la declaración de atributos de la persona es verdadera sin revelar ningún dato en que se base dicha declaración, preservando así la privacidad del usuario.

(15) El presente Reglamento define las condiciones armonizadas de cara al establecimiento de un marco para las carteras europeas de identidad digital que deben proporcionar los Estados miembros. Todos los ciudadanos de la Unión, y los residentes en la Unión tal como se definen en el Derecho nacional, deben estar facultados para solicitar, seleccionar, combinar, almacenar, eliminar, compartir y presentar datos relacionados con su identidad y solicitar la supresión de sus datos personales de una manera sencilla y cómoda que esté bajo el control exclusivo del usuario y permita al mismo tiempo la divulgación selectiva de datos personales. El presente Reglamento refleja los valores europeos comunes y respeta los derechos fundamentales, las garantías jurídicas y la responsabilidad y, para así proteger las sociedades democráticas, los ciudadanos de la Unión y los residentes en la Unión. Deben desarrollarse tecnologías que permitan lograr estos objetivos y que aspiren al máximo nivel de seguridad, privacidad, comodidad de uso y accesibilidad, garantizando asimismo una elevada facilidad de utilización y una interoperabilidad fluida. Los Estados miembros deben garantizar la igualdad de acceso a la identificación electrónica para todos sus ciudadanos y residentes. Los Estados miembros no deben limitar, directa o indirectamente, el acceso a los servicios públicos o privados a personas físicas o jurídicas que no opten por utilizar carteras europeas de identidad digital y deben facilitar otras soluciones adecuadas.

(16) Los Estados miembros deben aprovechar las posibilidades que ofrece el presente Reglamento para proporcionar, bajo su responsabilidad, carteras europeas de identidad digital, para su uso, a las personas físicas y jurídicas que residan en su territorio. A fin de ofrecer flexibilidad a los Estados miembros y aprovechar las tecnologías más avanzadas, el presente Reglamento debe permitir el suministro de carteras europeas de identidad digital directamente por un Estado miembro, en virtud de un mandato de un Estado miembro, o independientemente de un Estado miembro, pero con el reconocimiento de dicho Estado miembro.

(17) A efectos del registro, las partes usuarias deben facilitar la información necesaria para permitir su identificación y autenticación electrónicas en las carteras europeas de identidad digital. Al declarar el uso que pretenden hacer de la cartera europea de identidad digital, las partes usuarias deben facilitar información sobre los datos que solicitarán, en su caso, para prestar sus servicios, así como el motivo de la solicitud. El registro de las partes usuarias facilita las verificaciones por parte de los Estados miembros por lo que respecta a la legalidad de las actividades de las partes usuarias de conformidad con el Derecho de la Unión. La obligación de registro prevista en el presente Reglamento debe entenderse sin perjuicio de las obligaciones establecidas en el Derecho de la Unión o nacional, como la información que debe facilitarse a los interesados en virtud del Reglamento (UE) 2016/679. Las partes usuarias deben cumplir las garantías ofrecidas por los artículos 35 y 36 de dicho Reglamento, en particular realizando evaluaciones de impacto relativas a la protección de datos y consultando a las autoridades competentes en materia de protección de datos antes del tratamiento de datos en los casos en que las evaluaciones de impacto relativas a la protección de datos indiquen que el tratamiento daría lugar a un riesgo elevado. Dichas garantías deben apoyar el tratamiento lícito de datos personales por las partes usuarias, en particular por lo que respecta a las categorías especiales de datos personales, como los datos relativos a la salud. El registro de las partes usuarias tiene por objeto aumentar la transparencia y la confianza en el uso de las carteras europeas de identidad digital. El registro debe tener un coste razonable y proporcionado a los riesgos conexos, a fin de garantizar la aceptación por parte de los prestadores de servicios. En este contexto, el registro debe ofrecer la posibilidad de utilizar

procedimientos automáticos, en particular de que los Estados miembros recurran a registros existentes y los utilicen, y no debe conllevar un proceso de autorización previa. El proceso de registro debe permitir diversos casos de uso que pueden presentar diferencias en cuanto al modo de operación, ya sea en línea o fuera de línea, o en lo que respecta al requisito de autenticar los dispositivos con el objetivo de interactuar con la cartera europea de identidad digital. El registro debe aplicarse exclusivamente a las partes usuarias que presten servicios mediante una interacción digital.

(18) A fin de que se confíe en las carteras europeas de identidad digital y de que estas carteras se adopten ampliamente, es muy importante proteger a los ciudadanos de la Unión y los residentes en la Unión frente al uso no autorizado o fraudulento de las carteras europeas de identidad digital. Debe ofrecerse a los usuarios una protección eficaz contra este uso indebido. En particular, cuando una autoridad judicial nacional establezca, en el contexto de otro procedimiento, hechos que constituyan la base de un uso fraudulento o ilegal de una cartera europea de identidad digital, los organismos de supervisión responsables de los emisores de carteras europeas de identidad digital deben adoptar, tras la notificación, las medidas necesarias para garantizar la retirada o la suspensión del registro de la parte usuaria y de la inclusión de las partes usuarias en el mecanismo de autenticación hasta que la autoridad notificante confirme que las irregularidades detectadas se han subsanado.

(19) Todas las carteras europeas de identidad digital deben permitir a los usuarios identificarse y autenticarse electrónicamente de forma transfronteriza, tanto en línea como en modo 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 europeas de identidad digital también pueden dar respuesta a las necesidades institucionales de las administraciones públicas, las organizaciones internacionales y las instituciones, órganos y organismos de la Unión. La autenticación en modo fuera de línea será importante en numerosos sectores, especialmente el sanitario, en el que los servicios se prestan a menudo mediante una interacción presencial, y las recetas electrónicas deben poder utilizar códigos QR o tecnologías similares para verificar su autenticidad. Basándose en el nivel de seguridad alto por lo que respecta a los sistemas de identificación electrónica, las carteras europeas de identidad digital deben beneficiarse del potencial que ofrecen las soluciones inalterables, 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 Unión. Una vez incorporadas a una cartera europea de identidad digital, las personas físicas deben poder utilizarla para firmar con firmas electrónicas cualificadas, por defecto y de forma gratuita, sin tener que seguir ningún otro procedimiento administrativo. Los usuarios deben poder firmar o sellar declaraciones personales o atributos autodeclarados. En aras de la simplificación y la reducción de costes en beneficio de las personas y empresas de toda la Unión, en particular mediante la posibilidad de otorgar poderes de representación y mandatos electrónicos, los Estados miembros deben proporcionar carteras europeas de identidad digital que utilicen normas y especificaciones técnicas comunes para garantizar una interoperabilidad fluida y elevar adecuadamente el nivel de seguridad informática, reforzar la solidez frente a los ciberataques y, de este modo, reducir considerablemente los riesgos que entraña la digitalización en curso para los ciudadanos de la Unión, los residentes en la Unión y las empresas. Las autoridades competentes de los Estados miembros son las únicas que pueden proporcionar un nivel de confianza alto 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, para la provisión de carteras europeas de identidad digital, es necesario basarse en la identidad legal de los ciudadanos de la Unión, los residentes en la Unión o las personas jurídicas. La utilización de la identidad legal no debe impedir que los usuarios de carteras europeas de identidad digital accedan a servicios mediante un seudónimo cuando no exista una obligación jurídica de utilizar la identidad legal para la autenticación. La confianza en las carteras europeas de identidad digital aumentaría si se impusiera a las partes emisoras y gestoras el deber de introducir medidas técnicas y organizativas adecuadas para garantizar el nivel de seguridad más elevado que sea proporcional a los riesgos planteados para los derechos y libertades de las personas físicas, de conformidad con el Reglamento (UE) 2016/679.

(20) El uso de una firma electrónica cualificada debe ser gratuito para todas las personas físicas con fines no profesionales. Los Estados miembros deben tener la posibilidad de establecer medidas para impedir el uso gratuito de firmas electrónicas cualificadas con fines profesionales por parte de personas físicas, garantizando al mismo tiempo que tales medidas sean proporcionadas a los riesgos detectados y estén justificadas.

(21) Resulta beneficioso facilitar la implantación y la 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 fin de alcanzar este objetivo, los Estados miembros deben tener la posibilidad de establecer medidas jurídicas y organizativas que mejoren la flexibilidad para los proveedores de carteras europeas de identidad digital y que hagan posibles otras funcionalidades de las carteras europeas de identidad digital aparte

de las establecidas en el presente Reglamento, en particular mediante un refuerzo de la interoperabilidad con los medios nacionales de identificación electrónica existentes. Tales funcionalidades adicionales no deben en ningún caso ir en detrimento de la prestación de las funciones esenciales de las carteras europeas de identidad digital establecidas en el presente Reglamento, ni promover soluciones nacionales existentes en lugar de las carteras europeas de identidad digital. Tales funcionalidades adicionales exceden el ámbito de aplicación del presente Reglamento, y por ello no se benefician de las disposiciones sobre el uso transfronterizo de las carteras europeas de identidad digital que figuran en el presente Reglamento.

(22) Las carteras europeas de identidad digital deben incluir una funcionalidad para generar seudónimos elegidos y gestionados por el usuario con fines de autenticación a la hora de acceder a servicios en línea.

(23) Para lograr un nivel de seguridad y fiabilidad alto, el presente Reglamento establece los requisitos 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 evaluación de la conformidad designados por los Estados miembros.

(24) A fin de evitar enfoques divergentes y armonizar la aplicación de los requisitos establecidos en el presente Reglamento, la Comisión debe, a fin de certificar las carteras europeas de identidad digital, adoptar actos de ejecución para establecer una lista de normas de referencia y, en su caso, las especificaciones y los procedimientos con el fin de establecer especificaciones técnicas detalladas para dichos requisitos. En la medida en que la certificación de la conformidad de las carteras europeas de identidad digital con los requisitos de ciberseguridad pertinentes no está cubierta por los esquemas de certificación de la ciberseguridad existentes a que se refiere el presente Reglamento, y en lo que respecta a los requisitos no relacionados con la ciberseguridad pertinentes para las carteras europeas de identidad digital, los Estados miembros deben establecer esquemas nacionales de certificación con arreglo a los requisitos armonizados establecidos en el presente Reglamento y adoptados en virtud de este. Los Estados miembros deben transmitir sus proyectos de esquemas nacionales de certificación al Grupo de Cooperación sobre la Identidad Digital Europea, que debe estar facultado para emitir dictámenes y recomendaciones.

(25) La certificación de la conformidad con los requisitos de ciberseguridad establecidos en el presente Reglamento debe basarse, cuando estén disponibles, en los esquemas europeos de certificación de la ciberseguridad pertinentes establecidos en virtud del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, que establece un marco europeo voluntario de certificación de la ciberseguridad para los productos, procesos y servicios de TIC.

(26) Con el fin de evaluar y mitigar continuamente los riesgos relacionados con la seguridad, las carteras europeas de identidad digital certificadas deben ser objeto de evaluaciones periódicas de las vulnerabilidades encaminadas a detectar cualquier vulnerabilidad en los componentes relacionados con los productos, procesos y servicios certificados de la cartera europea de identidad digital.

(27) Al proteger a los usuarios y a las empresas de los riesgos de ciberseguridad, los requisitos esenciales de ciberseguridad establecidos en el presente Reglamento también contribuyen a mejorar la protección de los datos personales y la privacidad de las personas. Deben tenerse en cuenta las sinergias tanto en materia de normalización como de certificación en los aspectos relativos a la ciberseguridad a través de la cooperación entre la Comisión, las organizaciones europeas de normalización, la Agencia de la Unión Europea para la Ciberseguridad (ENISA), el Comité Europeo de Protección de Datos creado por el Reglamento (UE) 2016/679 y las autoridades nacionales de supervisión de la protección de datos.

(28) Debe facilitarse la incorporación de los ciudadanos de la Unión y los residentes en la Unión a la cartera europea de identidad digital mediante la utilización de medios de identificación electrónica expedidos a un nivel de seguridad alto. Solo se debe recurrir a los medios de identificación electrónica expedidos a un nivel de seguridad sustancial cuando las especificaciones y procedimientos técnicos armonizados que empleen medios de identificación electrónica expedidos a un nivel de seguridad sustancial en combinación con 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. Tales medios complementarios deben ser fiables y fáciles de utilizar, y se pueden desarrollar teniendo en cuenta la posibilidad de emplear procedimientos de incorporación a distancia, certificados cualificados sustentados en firmas electrónicas cualificadas, declaraciones electrónicas cualificadas de atributos o una combinación de estos. Para garantizar una implantación suficiente de las carteras europeas de identidad digital, deben establecerse, mediante actos de ejecución, especificaciones y procedimientos técnicos

armonizados para la incorporación de los usuarios por medios de identificación electrónica, en particular aquellos expedidos a un nivel de seguridad sustancial.

(29) 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 inalterables -por ejemplo, medidas de protección dentro de los dispositivos de los usuarios-, las carteras europeas de identidad digital deben poder emplear bien medidas de protección externas certificadas para proteger el material criptográfico y otros datos sensibles, bien medios de identificación electrónica notificados con un nivel de seguridad alto para demostrar el cumplimiento de los requisitos pertinentes del presente Reglamento en lo que respecta al nivel de seguridad de la cartera europea de identidad digital. El presente Reglamento se entiende sin perjuicio de las condiciones nacionales por lo que respecta a la expedición y utilización de una medida de protección externa certificada en caso de que esta medida transitoria las necesite.

(30) Las carteras europeas de identidad digital deben garantizar el máximo nivel de protección de datos y de seguridad a efectos de identificación y autenticación electrónicas para facilitar el acceso a los servicios públicos y privados, con independencia de que dichos datos se almacenen de forma local o mediante soluciones en la nube, teniendo debidamente en cuenta los diferentes niveles de riesgo.

(31) Las carteras europeas de identidad digital deben ser seguras desde el diseño y deben aplicar características de seguridad avanzadas para proteger contra la usurpación de identidad, el robo de datos, la denegación de servicio y cualquier otra ciberamenaza. Dichas medidas de seguridad deben incluir métodos de cifrado y almacenamiento de última generación que solo sean accesibles al usuario y descifrables por este, y basados en una comunicación cifrada de extremo a extremo con otras carteras europeas de identidad digital y las partes usuarias. Además, las carteras europeas de identidad digital deben requerir la confirmación segura, explícita y activa del usuario para las operaciones realizadas a través de dichas carteras.

(32) El uso gratuito de las carteras europeas de identidad digital no debe dar lugar a que el tratamiento de datos exceda lo necesario para la prestación de servicios de carteras europeas de identidad digital. El presente Reglamento no debe permitir el tratamiento de datos personales almacenados o que se deriven del uso de la cartera europea de identidad digital por el proveedor de esta con fines distintos a la prestación de servicios de cartera europea de identidad digital. Para garantizar la privacidad, los proveedores de carteras europeas de identidad digital deben garantizar la falta de observabilidad no recopilando datos y no pudiendo ver la información de las transacciones de los usuarios de la cartera europea de identidad digital. Dicha falta de observabilidad significa que los proveedores no pueden ver los detalles de las transacciones realizadas por el usuario. No obstante, en casos específicos, sobre la base del consentimiento explícito previo del usuario para cada uno de dichos casos específicos, y de plena conformidad con el Reglamento (UE) 2016/679, se puede conceder acceso a los proveedores de carteras europeas de identidad digital a la información necesaria para la prestación de un servicio concreto relacionado con las carteras europeas de identidad digital.

(33) La transparencia de las carteras europeas de identidad digital y la responsabilidad de sus proveedores son elementos clave para fomentar la confianza social y activar la aceptación del marco. Por tanto, el funcionamiento de las carteras europeas de identidad digital debe ser transparente y, en concreto, permitir un tratamiento verificable de los datos personales. Para lograrlo, los Estados miembros deben revelar el código fuente de los componentes de programas informáticos de las aplicaciones de usuario de las carteras europeas de identidad digital, incluidos los relacionados con el tratamiento de los datos personales y los datos de personas jurídicas. La publicación de este código fuente con una licencia de código abierto debe permitir a la sociedad, incluidos los usuarios y desarrolladores, comprender su funcionamiento y auditar y revisar el código. Esto aumentará la confianza de los usuarios en el ecosistema y contribuirá a la seguridad de las carteras europeas de identidad digital, al permitir que cualquier persona denuncie vulnerabilidades y errores en el código. En general, esto debe ser un incentivo para que los proveedores ofrezcan y mantengan un producto con un nivel de seguridad elevado. Sin embargo, en determinados casos, por razones debidamente justificadas, en especial con fines de seguridad pública, los Estados miembros pueden limitar la divulgación del código fuente de las librerías usadas, el canal de comunicación u otros elementos que no estén alojados en el dispositivo del usuario.

(34) El uso de las carteras europeas de identidad digital, así como la interrupción de su uso, debe ser un derecho y una opción exclusivos de los usuarios. Los Estados miembros deben desarrollar procedimientos sencillos y seguros para que los usuarios soliciten la revocación inmediata de la validez de las carteras europeas de identidad digital, también en el caso de pérdida o robo. En caso de fallecimiento del usuario o de cese de la actividad de una persona jurídica, debe establecerse un mecanismo que permita a la autoridad responsable de liquidar la sucesión

de la persona física o los bienes de la persona jurídica solicitar la revocación inmediata de las carteras europeas de identidad digital.

(35) Con el fin de promover la adopción de las carteras europeas de identidad digital y un uso más extendido de las identidades digitales, los Estados miembros no solo deben promover los beneficios de los servicios pertinentes, sino también, en cooperación con el sector privado, los investigadores y el mundo académico, desarrollar programas de formación destinados a reforzar las capacidades digitales de sus ciudadanos y residentes, en particular en lo relativo a los grupos vulnerables, como las personas con discapacidad y las personas de edad avanzada. Los Estados miembros deben sensibilizar acerca de las ventajas y los riesgos de las carteras europeas de identidad digital mediante campañas de comunicación.

(36) Con el objetivo de garantizar que el marco europeo de identidad digital esté abierto a la innovación y al desarrollo tecnológico y ofrezca garantías ante el futuro, se alienta a los Estados miembros, conjuntamente, a que establezcan 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 pymes, las empresas emergentes y los innovadores e investigadores individuales, así como de las partes interesadas industriales pertinentes. Dichas iniciativas deben apoyar y reforzar el cumplimiento normativo y la solidez técnica de las carteras europeas de identidad digital que se proporcionará a los ciudadanos de la Unión y los residentes en la Unión, evitando así el desarrollo de soluciones que no cumplan el Derecho de la Unión en materia de protección de datos o que estén abiertas a vulnerabilidades de seguridad.

(37) El Reglamento (UE) 2019/1157 del Parlamento Europeo y del Consejo refuerza la seguridad de los documentos de identidad con la introducción de características de seguridad reforzadas a más tardar en agosto de 2021. Los Estados miembros deben analizar la viabilidad de notificar estos documentos en el marco de los sistemas de identificación electrónica para ampliar la disponibilidad transfronteriza de medios de identificación electrónica.

(38) Es necesario simplificar y agilizar el proceso de notificación de los 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 identidades privados 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 (UE) n.º 910/2014.

(39) La racionalización de los procedimientos de notificación y revisión inter pares vigentes evitará la heterogeneidad de enfoques con respecto a la evaluación de los diversos sistemas de identificación electrónica notificados y facilitará la instauración de confianza entre los Estados miembros. Los mecanismos nuevos y más sencillos están destinados a estimular la cooperación de los Estados miembros en materia de seguridad e interoperabilidad de sus sistemas de identificación electrónica notificados.

(40) Los Estados miembros deben beneficiarse de la disponibilidad de herramientas nuevas y flexibles que garanticen el cumplimiento de los requisitos del presente Reglamento y de los actos de ejecución pertinentes adoptados en virtud de este. 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, según lo previsto en el contexto de 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 el Reglamento (UE) n.º 910/2014.

(41) Los prestadores de servicios públicos utilizan los datos de identificación de la persona proporcionados por los medios de identificación electrónica en virtud del Reglamento (UE) n.º 910/2014 para determinar que la identidad electrónica de los usuarios procedentes de otros Estados miembros se corresponde con los datos de identificación de la persona facilitados a dichos usuarios en el Estado miembro que lleva a cabo el proceso transfronterizo de correspondencia de la identidad. No obstante, en muchos casos, a pesar del uso del conjunto mínimo de datos facilitado por los sistemas de identificación electrónica notificados, para garantizar una correspondencia precisa de la identidad cuando los Estados miembros actúan como partes usuarias se necesita información adicional sobre el usuario y que se lleven a cabo procedimientos específicos complementarios de identificación única a escala nacional. Para mejorar la facilidad de uso de los medios de identificación electrónica, prestar un mejor servicio público en línea y aumentar la seguridad jurídica respecto a la identidad electrónica de los usuarios, el Reglamento (UE) n.º 910/2014 debe establecer que los Estados miembros adopten medidas específicas

en línea para garantizar la correspondencia inequívoca de la identidad cuando los usuarios pretenden acceder a servicios públicos transfronterizos en línea.

(42) Al desarrollar las carteras europeas de identidad digital es esencial tener en cuenta las necesidades de los usuarios. Deben existir casos de uso significativos y servicios en línea que utilicen 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 que utilicen las carteras europeas de identidad digital tienen el potencial de convertirse en una herramienta útil para alcanzar ese objetivo. Dichas directrices deben elaborarse teniendo en cuenta el marco de interoperabilidad de la Unión. Los Estados miembros deben desempeñar un papel de liderazgo a la hora de adoptarlas.

(43) En consonancia con la Directiva (UE) 2019/882 del Parlamento Europeo y del Consejo, 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.

(44) A fin de garantizar el cumplimiento efectivo del presente Reglamento, se debe establecer un mínimo para el máximo de las multas administrativas para los prestadores de servicios de confianza, tanto los cualificados como los no cualificados. Los Estados miembros deben establecer sanciones efectivas, proporcionales y disuasorias. Al determinar las sanciones, se deben tener debidamente en cuenta el tamaño de las entidades afectadas, sus modelos de negocio y la gravedad de las infracciones.

(45) 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 etiqueta de confianza de la UE por parte de prestadores no cualificados de servicios de confianza. La etiqueta de confianza de la UE no debe utilizarse en condiciones que, directa o indirectamente, lleven a la percepción de que los servicios de confianza no cualificados ofrecidos por esos prestadores están cualificados.

(46) 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 índole formal establecidos por el Derecho de la Unión o nacional. Por otro lado, no debe afectar a los requisitos nacionales de índole formal correspondientes a los registros públicos, en particular los registros mercantiles y de la propiedad.

(47) La prestación y utilización de servicios de confianza y las ventajas que conllevan en términos de comodidad y seguridad jurídica en el contexto de las transacciones transfronterizas, en especial cuando se utilizan servicios de confianza cualificados, está adquiriendo una importancia creciente para el comercio y la cooperación internacionales. Los socios internacionales de la Unión están creando marcos de confianza inspirados en el Reglamento (UE) n.º 910/2014. Para facilitar el reconocimiento de servicios de confianza cualificados y de sus prestadores, la Comisión podrá adoptar actos de ejecución en los que se establezcan las condiciones en las que los marcos de confianza de terceros países podrían considerarse equivalentes al marco de confianza para servicios de confianza cualificados y sus prestadores previsto en el presente Reglamento. Dicho enfoque debe complementar la posibilidad del reconocimiento mutuo de los servicios de confianza y sus prestadores establecidos en la Unión y en terceros países de conformidad con el artículo 218 del Tratado de Funcionamiento de la Unión Europea (TFUE). Al establecer las condiciones en las que los marcos de confianza de terceros países podrían considerarse equivalentes al marco de confianza previsto con arreglo al Reglamento (UE) n.º 910/2014 para los servicios de confianza cualificados y sus prestadores, debe garantizarse el cumplimiento de las disposiciones pertinentes de la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo y del Reglamento (UE) 2016/679, así como el uso de listas de confianza por ser elementos esenciales para generar confianza.

(48) El presente Reglamento debe fomentar la elección entre carteras europeas de identidad digital y la posibilidad de cambiarlas cuando el Estado miembro haya refrendado más de una solución de carteras europeas de identidad digital en su territorio. Con el fin de evitar efectos de bloqueo en tales situaciones, cuando sea técnicamente posible, los proveedores de carteras europeas de identidad digital deben garantizar la portabilidad efectiva de los datos a petición de los usuarios de las carteras europeas de identidad digital, y no se les debe permitir que utilicen barreras contractuales, económicas o técnicas para impedir o desalentar el cambio efectivo entre diferentes carteras europeas de identidad digital.

(49) Para garantizar el correcto funcionamiento de las carteras europeas de identidad digital, los proveedores de estas necesitan una interoperabilidad efectiva y condiciones justas, razonables y no discriminatorias para que las carteras europeas de identidad digital accedan a las características y de equipo y programa informático específicas de los dispositivos móviles. Dichos componentes pueden incluir, en particular, antenas de comunicación de campo próximo y medidas de protección, como tarjetas de circuito integrado universal, medidas de protección integradas, tarjetas microSD y Bluetooth de baja energía. El acceso a estos componentes podría estar bajo el control de los operadores de redes móviles y los fabricantes de equipos. Por tanto, cuando se necesiten para ofrecer los servicios de las carteras europeas de identidad digital, los fabricantes de los equipos originales de dispositivos móviles o los prestadores de servicios de comunicación electrónica no deben rechazar el acceso a dichos componentes. Asimismo, las empresas designadas como guardianes de acceso para los prestadores de servicios básicos en la lista publicada por la Comisión en virtud del Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo deben seguir sujetas a las disposiciones específicas de dicho Reglamento, sobre la base de su artículo 6, apartado 7.

(50) A fin de racionalizar las obligaciones impuestas a los prestadores de servicios de confianza en materia de ciberseguridad y de permitir a dichos prestadores y sus respectivas autoridades competentes beneficiarse del marco jurídico que se establece en la Directiva (UE) 2022/2555, los servicios de confianza deben adoptar medidas técnicas y organizativas adecuadas en virtud de dicha Directiva -como las dirigidas a corregir fallos del sistema, errores humanos, actos malintencionados o fenómenos naturales-, con objeto de gestionar los riesgos para la seguridad de las redes y los sistemas de información que emplean dichos prestadores en la prestación de sus servicios, y de notificar incidentes y ciberamenazas importantes de conformidad con dicha Directiva. Con respecto a la notificación de incidentes, los prestadores de servicios de confianza deben notificar cualquier incidente que tenga un efecto considerable 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 que ocurran 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 (UE) 2022/2555 deben considerarse complementarios a los requisitos impuestos a los prestadores de servicios de confianza con arreglo al presente Reglamento. Cuando corresponda, las autoridades competentes designadas en virtud de la Directiva (UE) 2022/2555 deben seguir aplicando las prácticas u orientaciones nacionales establecidas en relación con la aplicación de los requisitos de seguridad y notificación y con la supervisión del cumplimiento de dichos requisitos en virtud del Reglamento (UE) n.º 910/2014. El presente Reglamento no afecta a la obligación de notificar las violaciones de la seguridad de los datos personales en virtud del Reglamento (UE) 2016/679.

(51) Se debe prestar la debida atención para garantizar una cooperación eficaz entre los organismos de supervisión designados en virtud del artículo 46 ter del Reglamento (UE) n.º 910/2014 y las autoridades competentes designadas o establecidas en virtud del artículo 8, apartado 1, de la Directiva (UE) 2022/2555. Cuando dicho organismo de supervisión sea distinto de dicha autoridad competente, deben cooperar estrechamente y de manera oportuna, intercambiando la información pertinente a fin de garantizar que se realiza una supervisión eficaz y que los prestadores de servicios de confianza cumplen los requisitos establecidos en el Reglamento (UE) n.º 910/2014 y en la Directiva (UE) 2022/2555. En particular, los organismos de supervisión designados en virtud del Reglamento (UE) n.º 910/2014 deben estar facultados para solicitar a la autoridad competente designada o establecida en virtud de la Directiva (UE) 2022/2555 que proporcione la información pertinente necesaria para otorgar la cualificación y que emprenda las acciones de supervisión requeridas para verificar que los prestadores de servicios de confianza cumplen los requisitos pertinentes de la Directiva (UE) 2022/2555 o exigir a estos que subsanen cualquier incumplimiento.

(52) 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 mercado que permitan a los prestadores de servicios de confianza de la Unión ofrecer nuevos servicios de entrega electrónica certificada en toda la Unión. 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 en lo que respecta a la identificación del remitente es suficiente un nivel de confianza alto. Los Estados miembros deben animar a los prestadores 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.

(53) En la mayoría de los casos, los ciudadanos de la Unión y los residentes en la Unión no pueden intercambiar información digital relacionada con su identidad, como su dirección, su edad, sus cualificaciones profesionales, su permiso de conducción y otros permisos y datos de pago, a escala transfronteriza, de forma segura y con un nivel de protección de datos alto.

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

(55) Todo prestador de servicios que emita atributos declarados en formato electrónico -como diplomas, permisos, certificados de nacimiento o poderes y mandatos para representar a personas físicas o jurídicas o actuar en su nombre- debe considerarse un prestador de servicios de confianza de declaraciones electrónicas de atributos. 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 cualificada de atributos. Deben establecerse requisitos generales para asegurar que una declaración electrónica cualificada de atributos tenga un efecto jurídico equivalente al de las declaraciones legalmente emitidas en papel. Sin embargo, tales requisitos deben aplicarse sin perjuicio de que el Derecho de la Unión o nacional defina requisitos de índole formal adicionales específicos del sector con efectos jurídicos subyacentes, y, en particular, el reconocimiento transfronterizo de la declaración electrónica cualificada de atributos, cuando corresponda.

(56) La amplia disponibilidad y facilidad de uso de las carteras europeas de identidad digital debe fomentar su aceptación y confianza tanto por los particulares como por los prestadores de servicios privados. Por consiguiente, las partes usuarias privadas que prestan servicios, por ejemplo, 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, las telecomunicaciones o la educación deben aceptar el uso de las carteras europeas de identidad digital para la prestación de servicios en los casos en los que el Derecho de la Unión, nacional o una obligación contractual requieran una autenticación reforzada de usuario para la identificación en línea. Toda solicitud formulada por una parte usuaria de información del usuario de una cartera europea de identificación digital debe ser necesaria y proporcionada al uso previsto en un caso determinado, debe seguir el principio de minimización de datos y debe garantizar la transparencia en lo que respecta a los datos que se comparten y sus fines. Para facilitar el uso y la aceptación de las carteras europeas de identidad digital, en su implantación deben tenerse en cuenta las normas y especificaciones industriales ampliamente aceptadas.

(57) Cuando las plataformas en línea de muy gran tamaño, en el sentido del artículo 33, apartado 1, del Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo exijan a los usuarios que están autenticados a fin de acceder a servicios en línea, debe requerirse a dichas plataformas que acepten el uso de carteras europeas de identidad digital si así lo solicita voluntariamente el usuario. Los usuarios no deben tener ninguna obligación de utilizar una cartera europea de identidad digital para acceder a servicios privados y su acceso a los servicios no debe verse restringido ni obstaculizado por no utilizar una cartera europea de identidad digital. No obstante, si los usuarios así lo desean, las plataformas en línea de muy gran tamaño deben aceptarlas a tal fin, respetando en todo momento el principio de minimización de datos y el derecho de los usuarios a utilizar seudónimos libremente elegidos. La obligación de aceptar carteras europeas de identidad digital es necesaria para incrementar la protección de los usuarios frente al fraude y garantizar un nivel de protección de datos alto, 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.

(58) Deben desarrollarse códigos de conducta a escala de la Unión para contribuir a una amplia disponibilidad y facilidad de uso de los medios de identificación electrónica (como las carteras europeas de identidad digital) contemplados en el ámbito de aplicación del presente Reglamento. Los 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 recurran a servicios de identificación electrónica de terceros para autenticar a sus usuarios.

(59) 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 que sea necesaria 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. Debe ser técnicamente posible para el usuario divulgar esos atributos de manera selectiva, incluso a partir de varias declaraciones electrónicas distintas y combinarlos y presentarlos sin incidencias a las partes usuarias. Esta característica debe convertirse en una característica básica del diseño de las carteras europeas de identidad digital, reforzando así la comodidad y la protección de los datos personales, en especial la minimización de datos.

(60) A menos que haya normas específicas del Derecho de la Unión o nacional que exijan que los usuarios se identifiquen, no debe prohibirse el acceso a los servicios utilizando un seudónimo.

(61) Los atributos proporcionados por los prestadores cualificados de servicios de confianza como parte de la declaración cualificada de atributos deben ser cotejados con 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 de la Unión o nacional, a efectos de proteger el intercambio de atributos declarados entre los prestadores de servicios de identificación o de servicios de declaración de atributos y las partes usuarias. Los Estados miembros deben establecer mecanismos adecuados a escala nacional para garantizar que los prestadores cualificados de servicios de confianza que emitan declaraciones electrónicas cualificadas de atributos 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. Debe ser posible que los mecanismos adecuados incluyan el recurso a intermediarios específicos o a soluciones técnicas de acuerdo con el Derecho nacional que permitan el acceso a fuentes auténticas. Garantizar la disponibilidad de un mecanismo que permita el cotejo de atributos con fuentes auténticas tiene por objeto facilitar que los prestadores cualificados de servicios de confianza de declaraciones electrónicas cualificadas de atributos cumplan las obligaciones que les impone el Reglamento (UE) n.º 910/2014. Un nuevo anexo de dicho Reglamento debe contener una lista de categorías de atributos respecto de los cuales los Estados miembros deben velar por que se adopten medidas para que los prestadores cualificados de declaraciones electrónicas de atributos puedan cotejar su autenticidad con la fuente auténtica pertinente por medios electrónicos, a petición del usuario.

(62) La identificación electrónica segura y la provisión de declaraciones de atributos deben ofrecer 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 necesarios para cumplir, entre otros, los requisitos de debida diligencia con los clientes en virtud de un futuro Reglamento por el que se establezca la autoridad de lucha contra el blanqueo de capitales, [añádase la referencia una vez adoptada la propuesta], los requisitos de idoneidad que emanan del Derecho sobre la protección de los inversores, o para facilitar el cumplimiento de los requisitos de autenticación reforzada del cliente 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.

(63) No se han de impugnar los efectos jurídicos de una firma electrónica por el mero hecho de que se haya emitido en formato electrónico o porque no cumpla todos los requisitos de la firma electrónica cualificada. Sin embargo, corresponde al Derecho nacional determinar el efecto jurídico de la firma electrónica excepto los requisitos establecidos en el presente Reglamento conforme a los que el efecto jurídico de una firma electrónica se considera equivalente al de una firma manuscrita. Al determinar los efectos jurídicos de las firmas electrónicas, los Estados miembros deben tener en cuenta el principio de proporcionalidad entre el valor jurídico de un documento que debe firmarse y el nivel de seguridad y coste que exige una firma electrónica. Para aumentar la accesibilidad y el uso de las firmas electrónicas, se anima a los Estados miembros a considerar el uso de firmas electrónicas avanzadas en las transacciones diarias, para las que proporcionan un nivel suficiente de seguridad y confianza.

(64) A fin de garantizar la coherencia de las prácticas de certificación en toda la Unión, la Comisión debe emitir directrices sobre la certificación y la renovación de la certificación 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 que los organismos públicos o privados que hayan certificado dispositivos cualificados de creación de firma electrónica recertifiquen temporalmente dicho producto durante un corto período de certificación, sobre la base del resultado del proceso de certificación anterior, cuando dicha recertificación no pueda realizarse dentro del plazo legalmente establecido por un motivo distinto de una infracción o incidente de seguridad, sin perjuicio de la obligación de llevar a cabo una evaluación de la vulnerabilidad y de la práctica de certificación aplicable.

(65) La expedición de certificados de autenticación de sitios web tiene la finalidad de proporcionar a los usuarios una certeza, con un nivel de confianza alto, sobre la identidad de la entidad que respalda la existencia del sitio web, independientemente de la plataforma utilizada para mostrar dicha identidad. Estos certificados deben contribuir a crear confianza en la realización de operaciones mercantiles en línea, dado que los usuarios confiarían

en un sitio web que haya sido autenticado. El uso tales certificados por parte de los sitios web debe ser voluntario. Para que la autenticación de sitios web llegue a ser un medio a través del cual aumentar la confianza, proporcionar al usuario una experiencia mejor y fomentar el crecimiento en el mercado interior, el presente Reglamento establece un marco de confianza que incluye obligaciones mínimas de seguridad y responsabilidad para los proveedores de certificados cualificados de autenticación de sitios web y los requisitos para la expedición de dichos certificados. Las listas de confianza nacionales deben confirmar la cualificación de los servicios de autenticación de sitios web y de sus prestadores cualificados de servicios de confianza, incluido su pleno cumplimiento de los requisitos del presente Reglamento en lo que respecta a la expedición de certificados cualificados de autenticación de sitios web. El reconocimiento de certificados cualificados de autenticación de sitios web conlleva que los proveedores de navegadores web no deben denegar la autenticidad de los certificados cualificados de autenticación de sitios web a efectos de declarar el vínculo entre el nombre de dominio del sitio web y la persona física o jurídica a la que se expide el certificado o confirmar la identidad de dicha persona. Los proveedores de navegadores web deben mostrar los datos de identificación de la persona certificados y los demás atributos declarados al usuario final de manera fácil de usar en el entorno del navegador, mediante los medios técnicos de su elección. Con este fin, los proveedores de navegadores web deben garantizar la compatibilidad e interoperabilidad con los certificados cualificados para la autenticación de sitios web expedidos en pleno cumplimiento del presente Reglamento. La obligación de reconocimiento e interoperabilidad y apoyo de los certificados cualificados para la autenticación de sitios web no afecta a la libertad de los proveedores de navegadores web para garantizar la seguridad de la web, la autenticación de dominios y el cifrado del tráfico en la web de la manera y mediante la tecnología que consideren más adecuada. Con el fin de contribuir a la seguridad en línea de los usuarios finales, los proveedores de navegadores web deben poder -en circunstancias excepcionales- adoptar medidas cautelares necesarias y proporcionadas en respuesta a preocupaciones justificadas en relación con violaciones de la seguridad o pérdida de integridad de un certificado o conjunto de certificados identificados. Cuando adopten tales medidas cautelares, los proveedores de navegadores web deben notificar, sin demora indebida, a la Comisión, al organismo nacional de supervisión, a la entidad a la que se haya expedido el certificado y al prestador cualificado de servicios de confianza que haya emitido dicho certificado o conjunto de certificados, cualquier preocupación relacionada con una violación de la seguridad o pérdida de integridad de ese tipo, así como las medidas adoptadas en relación con el único certificado o conjunto de certificados. Dichas medidas deben entenderse sin perjuicio de la obligación de los proveedores de navegadores web de reconocer los certificados cualificados de autenticación de sitios web de conformidad con las listas de confianza nacionales. Para mejorar la protección de los ciudadanos de la Unión y los residentes en la Unión y promover el uso de certificados cualificados para la autenticación de sitios web, las autoridades públicas de los Estados miembros deben estudiar la posibilidad de incorporar dichos certificados en sus sitios web. Las medidas previstas en el presente Reglamento destinadas a aumentar la coherencia entre los enfoques y prácticas divergentes de los Estados miembros en relación con los procedimientos de supervisión tienen por objeto contribuir a mejorar la confianza en la seguridad, la calidad y la disponibilidad de los certificados cualificados para la autenticación de sitios web.

(66) Muchos Estados miembros han introducido requisitos nacionales aplicables a la prestación de servicios que proporcionen un archivo electrónico seguro y fiable con el objetivo de posibilitar la conservación a largo plazo de datos documentos electrónicos y de los servicios de confianza asociados a estos. A fin de 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. El marco jurídico para los servicios cualificados de archivo electrónico debe ofrecer a los prestadores de servicios de confianza y a los usuarios un conjunto de herramientas eficiente que incluya requisitos funcionales aplicables al servicio de archivo electrónico, así como efectos jurídicos claros cuando se utilice un servicio cualificado de archivo electrónico. Dichas disposiciones deben aplicarse a los datos y documentos electrónicos creados en forma digital, así como a los documentos en papel escaneados y digitalizados. Cuando sea necesario, dichas disposiciones deben permitir la reproducción de los datos y documentos electrónicos conservados en diferentes soportes o formatos con el fin de ampliar su durabilidad y legibilidad después del período de validez tecnológica, evitando al mismo tiempo la pérdida y la alteración en la medida de lo posible. Cuando los datos y documentos electrónicos presentados al servicio de archivo electrónico 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 cualificados establecidos por el presente Reglamento. Con el fin de crear pruebas de conservación cuando se utilicen firmas electrónicas, sellos electrónicos o sellos de tiempo electrónicos, deben utilizarse servicios de confianza cualificados. En la medida en que los servicios de archivo electrónico no están armonizados por el presente Reglamento, los Estados miembros deben poder mantener o introducir disposiciones nacionales, de conformidad con el Derecho de la Unión, relativas a dichos servicios, tales como disposiciones específicas para los servicios integrados en una organización y únicamente utilizados para los archivos internos de

dicha organización. El presente Reglamento no debe distinguir entre datos y documentos electrónicos creados en forma digital y documentos físicos que han sido digitalizados.

(67) Las actividades de los archivos nacionales y las instituciones de la memoria, en su calidad de organizaciones dedicadas a la conservación del patrimonio documental en interés público, suelen estar reguladas por el Derecho nacional y no prestan necesariamente servicios de confianza en el sentido del presente Reglamento. En la medida en que dichas instituciones no presten tales servicios de confianza, el presente Reglamento se entiende sin perjuicio de su funcionamiento.

(68) Los libros mayores electrónicos son una secuencia de registros electrónicos de datos que deben garantizar su integridad y la exactitud de su orden cronológico. Los libros mayores electrónicos deben establecer una secuencia cronológica de registros de datos. Junto con otras tecnologías, deben 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 y la inscripción de la propiedad de bienes inmuebles en registros descentralizados de la propiedad inmobiliaria. Los libros mayores electrónicos cualificados deben establecer una presunción legal sobre el orden cronológico secuencial único y exacto y la integridad de los registros de datos del libro mayor. Habida cuenta de sus particularidades, como el orden cronológico secuencial de los registros de datos, los libros mayores electrónicos deben distinguirse de otros servicios de confianza, como los sellos de tiempo electrónicos y los servicios de entrega electrónica certificada. Para garantizar la seguridad jurídica y promover la innovación, debe establecerse un marco jurídico a escala de la Unión que prevea el reconocimiento transfronterizo de servicios de confianza para el registro de los datos en libros mayores electrónicos. Esto debe impedir suficientemente 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; en particular, si es centralizado o distribuido. El presente Reglamento debe garantizar la neutralidad tecnológica; es decir, no favorecer ni discriminar a ninguna tecnología utilizada para implantar el nuevo servicio de confianza para libros mayores electrónicos. Además, la Comisión debe tener en cuenta los indicadores de sostenibilidad con respecto a cualquier repercusión negativa sobre el clima u otras repercusiones negativas relacionadas con el medio ambiente y utilizar métodos adecuados, a la hora de preparar los actos de ejecución que especifiquen los requisitos aplicables a los libros mayores electrónicos cualificados.

(69) El papel de los prestadores de servicios de confianza de los libros mayores electrónicos debe ser comprobar la actividad de registro secuencial de los datos en el libro mayor. El presente Reglamento se entiende sin perjuicio de las obligaciones jurídicas que tengan los usuarios de libros mayores electrónicos con arreglo al Derecho de la Unión o nacional. Por ejemplo, los casos de uso que conlleven el tratamiento de datos personales deben cumplir el Reglamento (UE) 2016/679 y los casos de uso que se relacionen con los servicios financieros deben cumplir con el Derecho pertinente de la Unión en materia de servicios financieros.

(70) Al objeto de evitar la fragmentación del mercado interior y los obstáculos en este, derivados de unas normas y unas restricciones técnicas divergentes, y de garantizar un proceso coordinado para impedir que se vea afectada la aplicación del futuro marco europeo de identidad digital, se necesita un proceso de cooperación estrecha y estructurada entre la Comisión, los Estados miembros, la sociedad civil, el mundo académico y el sector privado. Para lograr ese objetivo, los Estados miembros y la Comisión deben cooperar dentro del marco establecido en la Recomendación (UE) 2021/946 de la Comisión para determinar un conjunto de instrumentos común de la Unión para el marco para una identidad digital europea. En este contexto, los Estados miembros deben ponerse de acuerdo sobre una arquitectura técnica y un marco de referencia detallados, un conjunto de normas y referencias técnicas comunes -incluidas las normas reconocidas existentes- y un conjunto de directrices y descripciones de las mejores prácticas que aborden, como mínimo, todas las funcionalidades y la interoperabilidad de las carteras europeas de identidad digital (incluidas las firmas electrónicas) y de los prestadores cualificados de servicios de confianza para la declaración electrónica de atributos, según lo dispuesto en el presente Reglamento. En este contexto, los Estados miembros deben 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 los resultados del debate y del proceso de adopción del marco europeo de identidad digital, y evolucionar de forma paralela a dichos resultados.

(71) El presente Reglamento establece 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 en un tercer país, siempre que ese tercer país ofrezca garantías adecuadas de que las actividades de supervisión y las auditorías puedan ejecutarse como si estas se

llevaran a cabo en la Unión. Cuando no pueda garantizarse plenamente el cumplimiento del presente Reglamento, los organismos de supervisión deben poder adoptar medidas proporcionadas y justificadas, incluida la retirada de la cualificación del servicio de confianza prestado.

(72) Para ofrecer seguridad jurídica en lo que respecta a la validez de las firmas electrónicas avanzadas basadas en certificados cualificados, es esencial que se especifique la evaluación por la parte usuaria que lleva a cabo la validación de dicha firma electrónica avanzada basada en certificados cualificados.

(73) Los prestadores de servicios de confianza deben utilizar métodos criptográficos que reflejen las mejores prácticas actuales y la ejecución fiable de los algoritmos a fin de garantizar la seguridad y fiabilidad de sus servicios de confianza.

(74) El presente Reglamento establece la obligación de que los prestadores cualificados de servicios de confianza verifiquen la identidad de una persona física o jurídica a la que se expida el certificado cualificado o la declaración electrónica cualificada de atributos conforme a diversos métodos armonizados en toda la Unión. Para garantizar que los certificados cualificados y las declaraciones electrónicas cualificadas de atributos se expidan a la persona a la que pertenecen y que atestigüen el conjunto de datos correcto y único que representa la identidad de dicha persona, los prestadores cualificados de servicios de confianza que expidan certificados cualificados o declaraciones electrónicas cualificadas de atributos deben, en el momento de la expedición de dichos certificados y declaraciones, garantizar con total certeza la identificación de dicha persona. Asimismo, además de la verificación obligatoria de la identidad de la persona, si procede para la expedición de los certificados cualificados y al expedir una declaración electrónica cualificada de atributos, los prestadores cualificados de servicios de confianza deben garantizar con total certeza la corrección y la exactitud de los atributos declarados de la persona a la que se expide el certificado cualificado o la declaración electrónica cualificada de atributos. Esas obligaciones de resultado y total certeza a la hora de verificar los datos declarados deben respaldarse a través de medios adecuados, en particular utilizando uno de los métodos concretos previstos en el presente Reglamento o, cuando sea necesario, una combinación de estos. Debe ser posible combinar dichos métodos a fin de proporcionar una base adecuada para la verificación de la identidad de la persona a la que se expide el certificado cualificado o una declaración electrónica cualificada de atributos. Dicha combinación debe poder incluir el recurso a medios de identificación electrónica que cumplan los requisitos del nivel de seguridad sustancial en combinación con otros medios de verificación de la identidad. Dicha identificación electrónica permitiría el cumplimiento de los requisitos armonizados establecidos en el presente Reglamento en lo que respecta al nivel de seguridad alto como parte de procedimientos a distancia armonizados adicionales que garanticen la identificación con un nivel de confianza alto. Dichos métodos deben incluir la posibilidad de que el prestador cualificado de servicios de confianza que expida una declaración electrónica cualificada de atributos coteje los atributos que deben declararse por medios electrónicos a petición del usuario, de conformidad con el Derecho de la Unión o nacional, también con fuentes auténticas.

(75) Para mantener el presente Reglamento en consonancia con la evolución mundial y seguir las mejores 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 dichas actualizaciones debe tener en cuenta las nuevas tecnologías, prácticas, normas o especificaciones técnicas.

(76) Dado que los objetivos del presente Reglamento -a saber, el desarrollo del marco europeo de identidad digital a escala de la UE y de un marco de servicios de confianza- no pueden ser alcanzados de manera suficiente por los Estados miembros, sino que, debido a sus dimensiones y efectos, pueden lograrse mejor a escala de la Unión, esta puede adoptar medidas, de acuerdo con el principio de subsidiariedad establecido en el artículo 5 del Tratado de la Unión Europea. De conformidad con el principio de proporcionalidad establecido en el mismo artículo, el presente Reglamento no excede de lo necesario para alcanzar dichos objetivos.

(77) Se ha consultado al Supervisor Europeo de Protección de Datos de conformidad con el artículo 42, apartado 1, del Reglamento (UE) 2018/1725.

(78) Por lo tanto, procede modificar el Reglamento (UE) n.º 910/2014 en consecuencia.

HAN ADOPTADO EL PRESENTE REGLAMENTO:

Artículo 1. *Modificaciones al Reglamento (UE) n.º 910/2014.*

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

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

«Artículo 1. *Objeto.*

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

a) establece las condiciones en las cuales los Estados miembros reconocerán los medios de identificación electrónica de las personas físicas y jurídicas pertenecientes a un sistema de identificación electrónica notificado de otro Estado miembro y en las que proporcionarán y reconocerán las carteras europeas de identidad digital;
b) establece normas para los servicios de confianza, en particular para las transacciones electrónicas;
c) establece un marco jurídico para las firmas electrónicas, los sellos electrónicos, los sellos de tiempo electrónicos, los documentos electrónicos, los servicios de entrega electrónica certificada, los servicios certificados para la autenticación de sitios web, el archivo electrónico, la declaración electrónica de atributos, los dispositivos de creación de firmas electrónicas y de sellos electrónicos, y los libros mayores electrónicos.»

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 de la Unión o nacional relacionado con la celebración y validez de los contratos, otras obligaciones jurídicas o de procedimiento de índole formal o requisitos sectoriales de índole formal.

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

3) El artículo 3 se modifica como sigue:

a) los puntos 1 a 5 se sustituyen por el texto siguiente:

«1) “identificación electrónica”, proceso consistente en utilizar los datos de identificación de la persona en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a otra persona física o a una persona jurídica;
2) “medios de identificación electrónica”, unidad material yo inmaterial que contiene los datos de identificación de la persona y que se utiliza para la autenticación en servicios en línea o, cuando proceda, en servicios fuera de línea;
3) “datos de identificación de la persona”, conjunto de datos que se emite de conformidad con el Derecho de la Unión o nacional y permite establecer la identidad de una persona física o jurídica, o de una persona física que representa a otra persona física o a una persona jurídica;
4) “sistema de identificación electrónica”, régimen para la identificación electrónica en virtud del cual se expiden medios de identificación electrónica a personas físicas o jurídicas o a personas físicas que representan a otras personas físicas o personas jurídicas;
5) “autenticación”, proceso electrónico que permite la confirmación de la identificación electrónica de una persona física o jurídica, o la confirmación del origen y la integridad de datos en formato electrónico;»;

b) se inserta el punto siguiente:

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

c) el punto 6 se sustituye por el texto siguiente:

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

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

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

a) la expedición de certificados de firma electrónica, certificados de sello electrónico, certificados de autenticación de sitios web o certificados para la prestación de otros servicios de confianza;
b) la validación de certificados de firma electrónica, certificados de sello electrónico, certificados de autenticación de sitios web o certificados para la prestación de otros servicios de confianza;
c) la creación de firmas electrónicas o sellos electrónicos;
d) la validación de firmas electrónicas o sellos electrónicos;
e) la conservación de firmas electrónicas, sellos electrónicos, certificados de firma electrónica o certificados de sello electrónico;
f) la gestión de dispositivos de creación de firma electrónica a distancia o dispositivos de creación de sello electrónico a distancia;
g) la expedición de declaraciones electrónicas de atributos;
h) la validación de declaraciones electrónicas de atributos;
i) la creación de sellos de tiempo electrónicos;
j) la validación de sellos de tiempo electrónicos;
k) la prestación de servicios de entrega electrónica certificada;
l) la validación de los datos transmitidos a través de servicios de entrega electrónica certificada y las pruebas correspondientes;
m) el archivo electrónico de datos y documentos electrónicos;
n) la actividad de registro de datos electrónicos en un libro mayor electrónico.»;

e) el punto 18 se sustituye por el texto siguiente:

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

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

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

g) se insertan los puntos siguientes:

«23 bis) “dispositivo cualificado de creación de firma electrónica a distancia”, dispositivo cualificado de creación de firmas electrónicas que está gestionado por un prestador cualificado de servicios de confianza, de conformidad con el artículo 29 bis, en nombre de un firmante;
23 ter) “dispositivo cualificado de creación de sello electrónico a distancia”, dispositivo cualificado de creación de sellos electrónicos que está gestionado por un prestador cualificado de servicios de confianza, de conformidad con el artículo 39 bis, en nombre de un creador de sellos;»;

h) el punto 38 se sustituyen por el texto siguiente:

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

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

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

j) se añaden los puntos siguientes:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4) El artículo 5 se sustituye por el texto siguiente:

«Artículo 5. *Seudónimos en transacciones electrónicas.*

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

5) En el capítulo II, se inserta la sección siguiente:

«SECCIÓN 1 CARTERA EUROPEA DE IDENTIDAD DIGITAL

Artículo 5 bis. *Carteras europeas de identidad digital.*

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

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

a) directamente por un Estado miembro;
b) con arreglo a un mandato de un Estado miembro;
c) de manera independiente de un Estado miembro, pero con el reconocimiento de dicho Estado miembro.

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

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

a) solicitar, obtener, seleccionar, combinar, almacenar, eliminar, compartir y presentar de forma segura, bajo el control exclusivo del usuario, datos de identificación de la persona y, cuando proceda, en combinación con declaraciones electrónicas de atributos, autenticarse ante partes usuarias en línea y, en su caso, en modo fuera de línea, con el fin de acceder a servicios públicos y privados, velando al mismo tiempo por que sea posible divulgar los datos selectivamente;
b) generar seudónimos y almacenarlos cifrados y localmente en la cartera europea de identidad digital;
c) autenticar de forma segura la cartera europea de identidad digital de otra persona, así como recibir y compartir datos de identificación de la persona y declaraciones electrónicas de atributos de manera segura entre las dos carteras europeas de identidad digital;
d) acceder a un registro de todas las transacciones realizadas a través de la cartera europea de identidad digital mediante un panel común que permita al usuario:

i) ver una lista actualizada de las partes usuarias con las que ha establecido una conexión y, en su caso, todos los datos intercambiados,
ii) solicitar fácilmente a una parte usuaria que suprima los datos personales en virtud del artículo 17 del Reglamento (UE) 2016/679,
iii) notificar fácilmente una parte usuaria a la autoridad nacional de protección de datos en los casos en los que se reciba una solicitud de datos presuntamente ilícita o sospechosa;

e) firmar por medio de firmas electrónicas cualificadas o sellar por medio de sellos electrónicos cualificados;
f) descargar, en la medida en que sea técnicamente viable, los datos, la declaración electrónica de atributos y las configuraciones del usuario;
g) ejercer los derechos del usuario a la portabilidad de los datos.

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

a) admitirán protocolos e interfaces comunes:

i) para expedir datos de identificación de la persona, declaraciones electrónicas cualificadas y no cualificadas de atributos o certificados cualificados y no cualificados para la cartera europea de identidad digital,
ii) para que las partes usuarias soliciten y validen datos de identificación de la persona y declaraciones electrónicas de atributos,
iii) para compartir con las partes usuarias, y presentarles, datos de identificación de la persona, una declaración electrónica de atributos o datos conexos divulgados selectivamente, en línea y, cuando proceda, en modo fuera de línea,

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

a) a petición expresa del usuario;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Artículo 5 ter. *Partes usuarias de las carteras europeas de identidad digital.*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Artículo 5 quater. *Certificación de las carteras europeas de identidad digital.*

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

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

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

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

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

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

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

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

Artículo 5 quinquies. *Publicación de una lista de carteras europeas de identidad digital certificadas.*

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

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

a) el certificado y el informe de evaluación de la certificación de la cartera europea de identidad digital certificada;
b) una descripción del sistema de identificación electrónica en virtud del cual se proporciona la cartera europea de identidad digital;
c) el régimen de supervisión aplicable y la información sobre el régimen de responsabilidades respecto de la parte que proporciona la cartera europea de identidad digital;
d) la autoridad o autoridades responsables del sistema de identificación electrónica;
e) disposiciones relativas a la suspensión o revocación del sistema de identificación electrónica de la autenticación o de las partes afectadas.

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

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

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

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

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

Artículo 5 sexies. *Violación de la seguridad de las carteras europeas de identidad digital.*

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

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

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

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

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

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

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

Artículo 5 septies. *Uso transfronterizo de las carteras europeas de identidad digital.*

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

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

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

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

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

6) Antes del artículo 6 se inserta el título siguiente:

«SECCIÓN 2 SISTEMAS DE IDENTIFICACIÓN ELECTRÓNICA»

7) En el artículo 7, la letra g) se sustituye por el texto siguiente:

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

8) En el artículo 8, apartado 3, el párrafo primero se sustituye por el texto siguiente:

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

9) 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*, sin dilación indebida, la lista de los sistemas de identificación electrónica notificados de conformidad con el apartado 1 junto con información básica sobre dichos sistemas.

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

10) El título del artículo 10 se sustituye por el texto siguiente:

«*Violación de la seguridad de los sistemas de identificación electrónica.*»

11) Se inserta el artículo siguiente:

«Artículo 11 bis. *Correspondencia transfronteriza de la identidad.*

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

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

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

12) El artículo 12 se modifica como sigue:

a) El título se sustituye por el texto siguiente:

«*Interoperabilidad.*»;

b) el apartado 3 se modifica como sigue:

i) la letra c) se sustituye por el texto siguiente:

«c) facilitarla aplicación de la privacidad y la seguridad desde el diseño.»,

ii) se suprime la letra d);

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

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

d) los apartados 5 y 6 se sustituyen por el texto siguiente:

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

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

e) se suprime el apartado 7;
f) el apartado 8 se sustituye por el texto siguiente:

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

13) En el capítulo II se insertan los artículos siguientes:

«Artículo 12 bis. *Certificación de los sistemas de identificación electrónica.*

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

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

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

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

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

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

Artículo 12 ter. *Acceso a características de equipo y programa informático.*

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

14) 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 y sin perjuicio del Reglamento (UE) 2016/679, los prestadores de servicios de confianza serán responsables de los perjuicios causados de forma intencional o por negligencia a cualquier persona física o jurídica debido al incumplimiento de las obligaciones establecidas en el presente Reglamento. Toda persona física o jurídica que haya sufrido perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento por parte de un prestador de servicios de confianza tendrá derecho a solicitar una indemnización de conformidad con el Derecho de la Unión y nacional.

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

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

15) Los artículos 14, 15 y 16 se sustituyen por el texto siguiente:

«Artículo 14. *Aspectos internacionales.*

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

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

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

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

Artículo 15. *Accesibilidad para las personas con discapacidad y necesidades especiales.*

La provisión de medios de identificación electrónica, así como la prestación de servicios de confianza y los productos destinados a los usuarios finales empleados en la prestación de dichos servicios, deberán estar disponibles en un lenguaje claro y comprensible, de conformidad con la Convención de las Naciones Unidas sobre

los Derechos de las Personas con Discapacidad y con los requisitos de accesibilidad de la Directiva (UE) 2019/882, beneficiando así también a las personas que experimentan limitaciones funcionales, como las personas de edad avanzada y las personas con un acceso limitado a las tecnologías digitales.

Artículo 16. *Sanciones.*

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

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

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

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

16) En el capítulo III, sección 2, el título se sustituye por el texto siguiente:

«SERVICIOS DE CONFIANZA NO CUALIFICADOS»

17) Se suprimen los artículos 17 y 18.
18) En el capítulo III, sección 2, se inserta el artículo siguiente:

«Artículo 19 bis. *Requisitos aplicables a los prestadores no cualificados de servicios de confianza.*

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

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

i) procedimientos de registro para un servicio de confianza e incorporación a este,
ii) controles administrativos o de procedimiento necesarios para prestar servicios de confianza,
iii) gestión e implantación de servicios de confianza;

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

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

19) 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 21 de la Directiva (UE) 2022/2555. Los prestadores cualificados de servicios de confianza enviarán el informe de evaluación de la conformidad correspondiente al organismo de supervisión en el plazo de tres días hábiles tras su recepción.»;

b) Se insertan los apartados siguientes:

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

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

c) los apartados 2, 3 y 4 se sustituyen por el texto siguiente:

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

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

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

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

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

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

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

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

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

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

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

20) El artículo 21 se modifica como sigue:

a) los apartados 1 y 2 se sustituyen por el texto siguiente:

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

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

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

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

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

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

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

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

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

a) a través de la cartera europea de identidad digital o de un medio de identificación electrónica notificado que satisfaga los requisitos establecidos en el artículo 8 con respecto al nivel de seguridad alto;
b) por medio de un certificado de una firma electrónica cualificada o de un sello electrónico cualificado expedido de conformidad con la letra a), c) o d);
c) utilizando otros métodos de identificación que garanticen la identificación de la persona con un nivel alto de confianza, cuya conformidad será confirmada por un organismo de evaluación de la conformidad;
d) a través de la presencia física de la persona física o de un representante autorizado de la persona jurídica, mediante pruebas y procedimientos adecuados, de conformidad con el Derecho nacional.

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

a) a través de la cartera europea de identidad digital o de un medio de identificación electrónica notificado que satisfaga los requisitos establecidos en el artículo 8 con respecto al nivel de seguridad alto;
b) por medio de un certificado de una firma electrónica cualificada o de un sello electrónico cualificado expedido de conformidad con el apartado 1 bis, letra a), c) o d);
c) por medio de una declaración electrónica cualificada de atributos;
d) utilizando otros métodos que garanticen la verificación de los atributos con un nivel alto de confianza, cuya conformidad será confirmada por un organismo de evaluación de la conformidad;
e) mediante la presencia física de la persona física o de un representante autorizado de la persona jurídica, mediante pruebas y procedimientos adecuados, de conformidad con el Derecho nacional.»;

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

b) el apartado 2 se modifica como sigue:

i) la letra a) se sustituye por el texto siguiente:

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

ii) 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 sustenten, en particular utilizando técnicas criptográficas adecuadas;»,

iii) se insertan los puntos siguientes:

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

i) procedimientos de registro en un servicio e incorporación a este,
ii) controles administrativos o de procedimiento,
iii) gestión e implantación de servicios;

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

iv) las letras g), h) e i) 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;

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

v) se suprime la letra j),

vi) se añade el párrafo siguiente:

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

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

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

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

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

22) En el capítulo III, sección 3, se añade el artículo siguiente:

«Artículo 24 bis. *Reconocimiento de servicios de confianza cualificados.*

1. Las firmas electrónicas cualificadas basadas en un certificado cualificado expedido en un Estado miembro y los sellos electrónicos cualificados basados en un certificado cualificado expedido en un Estado miembro serán reconocidos, respectivamente, como firmas electrónicas cualificadas y sellos electrónicos cualificados en todos los demás Estados miembros.

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

3. Un certificado cualificado de firma electrónica, un certificado cualificado de sello electrónico, un servicio de confianza cualificado para la gestión de dispositivos cualificados de creación de firma electrónica a distancia y un servicio de confianza cualificado para la gestión de dispositivos cualificados de creación de sello electrónico a

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

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

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

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

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

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

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

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

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

23) En el artículo 25, se suprime el apartado 3.
24) El artículo 26 se modifica como sigue:

a) el párrafo primero pasa a ser apartado 1;
b) se añade el apartado siguiente:

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

25) En el artículo 27, se suprime el apartado 4.
26) En el artículo 28, el apartado 6 se sustituye por el texto siguiente:

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

27) En el artículo 29, se inserta el apartado siguiente:

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

28) Se inserta el artículo siguiente:

«Artículo 29 bis. *Requisitos aplicables a un servicio cualificado para la gestión de dispositivos cualificados de creación de firma electrónica a distancia.*

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

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

i) la seguridad de los conjuntos de datos duplicados debe ser del mismo nivel que el previsto para los conjuntos de datos originales,
ii) el número de conjuntos de datos duplicados no debe superar el mínimo necesario para garantizar la continuidad del servicio;

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

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

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

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

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

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

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 del presente apartado cuando la validación de firmas electrónicas cualificadas sea conforme a las normas, las especificaciones y los procedimientos a que se refiere el apartado 3.»;

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

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

32) Se inserta el artículo siguiente:

«Artículo 32 bis. *Requisitos aplicables a la validación de las firmas electrónicas avanzadas basadas en certificados cualificados.*

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

a) el certificado que respalda la firma fuera, en el momento de la firma, un certificado cualificado de firma electrónica que se ajusta al anexo I;
b) el certificado cualificado fuera expedido por un prestador cualificado de servicios de confianza y fuera válido en el momento de la firma;
c) los datos de validación de la firma correspondan a los datos proporcionados a la parte usuaria;
d) el conjunto único de datos que representa al firmante en el certificado se facilite correctamente a la parte usuaria;
e) en caso de que se utilice un seudónimo, la utilización de este se indique claramente a la parte usuaria en el momento de la firma;
f) la integridad de los datos firmados no se haya visto comprometida;
g) se hayan cumplido los requisitos previstos en el artículo 26 en el momento de la firma.

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

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

33) En el artículo 33, el apartado 2 se sustituye por el texto siguiente:

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

34) El artículo 34 se modifica como sigue:

a) se inserta el apartado siguiente:

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

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

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

35) En el artículo 35, se suprime el apartado 3.
36) El artículo 36 se modifica como sigue:

a) el párrafo primero pasa a ser apartado 1;
b) se añade el apartado siguiente:

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

37) En el artículo 37, se suprime el apartado 4.
38) En el artículo 38, el apartado 6 se sustituye por el texto siguiente:

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

39) Se inserta el artículo siguiente:

«Artículo 39 bis. *Requisitos aplicables a un servicio cualificado para la gestión de dispositivos cualificados de creación de sello electrónico a distancia.*

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

40) En el capítulo III, sección 5 se inserta el artículo siguiente:

«Artículo 40 bis. *Requisitos aplicables a la validación de los sellos electrónicos avanzados basados en certificados cualificados.*

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

41) En el artículo 41, se suprime el apartado 3.
42) El artículo 42 se modifica como sigue:

a) se inserta el apartado 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 exactitud de la fuente de información temporal sea conforme a las normas, las especificaciones y procedimientos a que se refiere el apartado 2.»;

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

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

43) El artículo 44 se modifica como sigue:

a) se inserta el apartado siguiente:

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

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

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

c) se insertan los apartados siguientes:

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

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

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

«Artículo 45. *Requisitos aplicables a los certificados cualificados de autenticación de sitios web.*

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

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

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

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

45) Se inserta al artículo siguiente:

«Artículo 45 bis. *Medidas cautelares en materia de ciberseguridad.*

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

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

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

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

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

46) En el capítulo III se insertan las secciones siguientes:

«SECCIÓN 9 DECLARACIÓN ELECTRÓNICA DE ATRIBUTOS

Artículo 45 ter. *Efectos jurídicos de la declaración electrónica de atributos.*

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

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

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

Artículo 45 quater. *Declaración electrónica de atributos en servicios públicos.*

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

Artículo 45 quinquies. *Requisitos aplicables a la declaración electrónica cualificada de atributos.*

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

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

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

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

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

Artículo 45 sexies. *Cotejo de atributos con fuentes auténticas.*

1. En un plazo de veinticuatro meses a partir de la fecha de entrada en vigor de los actos de ejecución a que se refieren el artículo 5 bis, apartado 23, y el artículo 5 quater, apartado 6, los Estados miembros garantizarán que, al menos para los atributos que se enumeran en el anexo VI, cuando tales atributos se basen en fuentes auténticas

pertenecientes al sector público, se adopten medidas para permitir que los prestadores cualificados de servicios de confianza de declaraciones electrónicas de atributos verifiquen dichos atributos por medios electrónicos, a petición del usuario, de conformidad con el Derecho de la Unión o nacional.

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

Artículo 45 septies. *Requisitos aplicables a la declaración electrónica de atributos expedida por un organismo del sector público responsable de una fuente auténtica, o en nombre de este.*

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

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

i) indicará que el organismo emisor está establecido de conformidad con el Derecho de la Unión o nacional, bien como responsable de la fuente auténtica con arreglo a la cual se expide la declaración electrónica de atributos, bien como el organismo designado para actuar en su nombre,
ii) proporcionará un conjunto de datos que representen inequívocamente la fuente auténtica a que se refiere el inciso i), y
iii) determinará el Derecho de la Unión o nacional a que se refiere el inciso i).

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

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

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

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

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

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

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

Artículo 45 octies. *Emisión de declaraciones electrónicas de atributos a las carteras europeas de identidad digital.*

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

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

Artículo 45 nonies. *Normas adicionales para la prestación de servicios de declaración electrónica de atributos.*

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

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

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

SECCIÓN 10 SERVICIOS DE ARCHIVO ELECTRÓNICO

Artículo 45 decies. *Efecto jurídico de los servicios de archivo electrónico.*

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

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

Artículo 45 undecies. Requisitos aplicables a los servicios cualificados de archivo electrónico.

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

a) ser prestados por prestadores cualificados de servicios de confianza;
b) utilizar procedimientos y tecnologías capaces de asegurar la durabilidad y legibilidad de los datos y documentos electrónicos más allá del período de validez tecnológica y, al menos, durante el período de conservación legal o contractual, manteniendo al mismo tiempo su integridad y la exactitud de su origen;
c) garantizar que dichos datos y documentos electrónicos se conserven de tal manera que queden protegidos contra su pérdida o alteración, excepto en el caso de los cambios relativos a su soporte o formato electrónico;

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

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

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

SECCIÓN 11 LIBROS MAYORES ELECTRÓNICOS

Artículo 45 duodecies. *Efectos jurídicos de los libros mayores electrónicos.*

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

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

Artículo 45 terdecies. *Requisitos aplicables a los libros mayores electrónicos cualificados.*

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

a) estar creado y gestionado por uno o más prestadores cualificados de servicios de confianza;
b) establecer el origen de los registros de datos en el libro mayor;
c) garantizar la unicidad del orden cronológico secuencial de los registros de datos en el libro mayor;
d) grabar datos de modo que sea posible detectar de forma inmediata cualquier modificación posterior de estos, garantizando su integridad a lo largo del tiempo.

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

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

47) Se inserta el capítulo siguiente:

«CAPÍTULO IV bis

Marco de gobernanza

Artículo 46 bis. *Supervisión del marco de la cartera europea de identidad digital.*

1. Los Estados miembros designarán uno o más organismos de supervisión establecidos en su territorio.
Los organismos de supervisión designados en virtud del párrafo primero disfrutarán de las competencias necesarias y los recursos adecuados para el ejercicio de sus funciones de forma eficaz, eficiente e independiente.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Artículo 46 ter. *Supervisión de los servicios de confianza.*

1. Los Estados miembros designarán un organismo de supervisión establecido en su territorio o designarán, previo acuerdo mutuo con otro Estado miembro, un organismo de supervisión establecido en ese otro Estado

miembro. Dicho organismo de supervisión será responsable de las funciones de supervisión en el Estado miembro que efectúa la designación en lo que respecta a los servicios de confianza.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Artículo 46 quater. *Puntos de contacto únicos.*

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

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

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

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

Artículo 46 quinquies. *Asistencia mutua.*

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

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

a) el organismo de supervisión que aplique medidas de supervisión y ejecución en un Estado miembro informará y consultará al organismo de supervisión del otro Estado miembro afectado;
b) un organismo de supervisión podrá solicitar al organismo de supervisión de otro Estado miembro afectado que adopte medidas de supervisión o ejecución, entre las que se podrá contar, por ejemplo, cursar solicitudes de inspección en relación con los informes de evaluación de la conformidad contemplados en los artículos 20 y 21 en lo referente a la prestación de servicios de confianza;
c) cuando proceda, los organismos de supervisión podrán llevar a cabo investigaciones conjuntas con los organismos de supervisión de otros Estados miembros.

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

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

a) la asistencia solicitada no guarda proporción con las actividades de supervisión del organismo de supervisión realizadas de conformidad con los artículos 46 bis y 46 ter;
b) el organismo de supervisión no es competente para prestar la asistencia solicitada;
c) la prestación de la asistencia solicitada sería incompatible con el presente Reglamento.

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

Artículo 46 sexies. *El Grupo de Cooperación sobre la Identidad Digital Europea.*

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

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

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

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

5. El Grupo de Cooperación desempeñará las siguientes funciones:

a) intercambiar recomendaciones y cooperar con la Comisión en las iniciativas políticas emergentes en el ámbito de las carteras de identidad digital, los medios de identificación electrónica y los servicios de confianza;
b) asesorar a la Comisión, según proceda, en la preparación temprana de los proyectos de actos delegados y de ejecución que deban adoptarse en virtud del presente Reglamento;
c) con el fin de apoyar a los organismos de supervisión en la aplicación de las disposiciones del presente Reglamento:

i) intercambiar las mejores prácticas e información sobre la aplicación de las disposiciones del presente Reglamento,
ii) evaluar los avances pertinentes en el ámbito de los sectores de la cartera de identidad digital, la identificación electrónica y los servicios de confianza,
iii) organizar reuniones conjuntas con las partes interesadas pertinentes de toda la Unión para tratar las actividades realizadas por el Grupo de Cooperación y recabar apreciaciones sobre los desafíos políticos emergentes,
iv) con el apoyo de la ENISA, intercambiar opiniones, mejores prácticas e información sobre los aspectos de ciberseguridad pertinentes relativos a las carteras europeas de identidad digital, los sistemas de identificación electrónica y los servicios de confianza,
v) intercambiar mejores prácticas en relación con el desarrollo y la ejecución de políticas sobre la notificación de violaciones de la seguridad y las medidas comunes a que se refieren los artículos 5 sexies y 10,
vi) organizar reuniones conjuntas con el Grupo de Cooperación SRI establecido en virtud del artículo 14, apartado 1, de la Directiva (UE) 2022/2555 para intercambiar la información pertinente referente a ciberamenazas, incidencias, vulnerabilidades, iniciativas de sensibilización, formación, ejercicios y destrezas, desarrollo de capacidades, capacidad relativa a las normas y especificaciones técnicas y las propias normas y especificaciones técnicas en relación con los servicios de confianza y la identificación electrónica,
vii) debatir, a petición de un organismo de supervisión, las solicitudes concretas de asistencia mutua a que se refiere el artículo 46 quinquies,
viii) facilitar el intercambio de información entre los organismos de supervisión, orientando sobre los aspectos organizativos y los procedimientos de la asistencia mutua a que se refiere el artículo 46 quinquies;

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

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

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

48) El artículo 47 se modifica como sigue:

a) los apartados 2 y 3 se sustituyen por el texto siguiente:

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

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

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

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

49) En el capítulo VI se inserta el artículo 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 y los servicios de confianza cualificados prestados en su territorio.

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

a) el número de personas físicas y jurídicas poseedoras de una cartera europea de identidad digital válida;
b) el tipo y cantidad de servicios que aceptan el uso de la cartera europea de identidad digital;
c) la cantidad de reclamaciones de usuarios e incidencias de protección de los consumidores o de protección de datos relacionadas con las partes usuarias y los servicios de confianza cualificados;
d) un informe resumido que incluya datos sobre las incidencias que impidan utilizar la cartera europea de identidad digital;
e) un resumen de las incidencias de seguridad importantes, de las violaciones de la seguridad de los datos y de los usuarios de carteras europeas de identidad digital o de servicios de confianza cualificados que hayan resultado afectados.

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

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

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

«Artículo 49. *Revisión.*

1. La Comisión revisará la aplicación del presente Reglamento y, a más tardar el 21 de mayo de 2026, informará al Parlamento Europeo y al Consejo. En dicho informe, la Comisión evaluará, en particular, si es apropiado modificar el ámbito de aplicación del presente Reglamento o sus disposiciones específicas, incluidas, en concreto, las disposiciones que figuran en el artículo 5 quater, apartado 5, teniendo en cuenta la experiencia adquirida en la

aplicación del presente Reglamento, así como la evolución tecnológica, del mercado y jurídica. Si fuera necesario, dicho informe irá acompañado de una propuesta de modificación del presente Reglamento.

2. El informe a que se refiere el apartado 1 incluirá una evaluación de la disponibilidad, seguridad y facilidad de uso de los medios de identificación electrónica notificados y las carteras europeas de identidad digital que entran dentro del ámbito de aplicación del presente Reglamento y evaluarán si debe requerirse a todos los prestadores de servicios privados en línea que se apoyan en servicios de identificación electrónica de terceros con fines de autenticación de los usuarios que acepten el uso de los medios de identificación electrónicos notificados y la cartera europea de identidad digital.

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

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

«Artículo 51. *Disposiciones transitorias.*

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

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

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

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

52) Los anexos I a IV se modifican, respectivamente, de conformidad con lo dispuesto en los anexos I a IV del presente Reglamento.

53) Se añaden los nuevos anexos V, VI y VII, tal como figuran en los anexos V, VI y VII del presente Reglamento.

Artículo 2. *Entrada en vigor.*

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 11 de abril de 2024.

Por el Parlamento Europeo	*Por el Consejo*
La Presidenta	*La Presidenta*
R. METSOLA	H. LAHBIB

ANEXO I

En el anexo I del Reglamento (UE) n.º 910/2014, la letra 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

En el anexo II del Reglamento (UE) n.º 910/2014, se suprimen los puntos 3 y 4.

ANEXO III

En el anexo III del Reglamento (UE) n.º 910/2014, la letra 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

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

1) La letra c) se sustituye por el texto siguiente:

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

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

2) La letra 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

«ANEXO V

REQUISITOS APLICABLES A LA DECLARACIÓN ELECTRÓNICA CUALIFICADA DE ATRIBUTOS

La declaración electrónica cualificada de atributos contendrá:

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

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

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

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

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

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

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

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

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

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

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

ANEXO VI

«ANEXO VI

LISTA MÍNIMA DE ATRIBUTOS

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

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

ANEXO VII

«ANEXO VII

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

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

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

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

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

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

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

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

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

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

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