Consejo de la Unión Europea

Bruselas, 3 de junio de 2021
(OR. en)

9471/21

Expediente interinstitucional: 2021/0136 (COD)

TELECOM 242
COMPET 457
MI 432
DATAPROTECT 156
JAI 670
IA 108
CODEC 826

PROPUESTA

De:	Por la secretaria general de la Comisión Europea, D.ª Martine DEPREZ, directora
Fecha de recepción:	3 de junio de 2021
A:	D. Jeppe TRANHOLM-MIKKELSEN, secretario general del Consejo de la Unión Europea
N.° doc. Ción.:	COM(2021) 281 final
Asunto:	Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento de un Marco para una Identidad Digital Europea

Adjunto se remite a las Delegaciones el documento – COM(2021) 281 final.

Adj.: COM(2021) 281 final

COMISIÓN
EUROPEA

Bruselas, 3.6.2021
COM(2021) 281 final

2021/0136 (COD)

Propuesta de

REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO

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

{SEC(2021) 228 final} - {SWD(2021) 124 final} - {SWD(2021) 125 final}

EXPOSICIÓN DE MOTIVOS

1. CONTEXTO DE LA PROPUESTA

• Razones y objetivos de la propuesta

La presente exposición de motivos acompaña a la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (Reglamento eIDAS)[1]. El objetivo del instrumento jurídico es proporcionar, para la utilización transfronteriza:

– acceso a soluciones de identidad electrónica altamente seguras y fiables,

– la garantía de que los servicios públicos y privados puedan apoyarse en soluciones de identidad digital fiables y seguras,

– la garantía de que las personas físicas y jurídicas puedan utilizar soluciones de identidad digital,

– la seguridad de que dichas soluciones presenten un conjunto de atributos y permitan el intercambio selectivo de datos de identidad, y de que dichos datos se limiten a las necesidades del servicio específico solicitado,

– la garantía de la aceptación de los servicios de confianza en la Unión Europea (UE) y de la igualdad de condiciones para su prestación.

En la actualidad, está emergiendo en el mercado un nuevo entorno cuyo enfoque ha pasado de estar centrado en la provisión y utilización de identidades digitales rígidas a la provisión de determinados atributos concretos relacionados con dichas identidades, así como en la confianza en esos atributos. Existe un aumento de la demanda de soluciones de identidad electrónica capaces de ofrecer estas prestaciones y de brindar una mayor eficiencia y un nivel alto de confianza en toda la UE, tanto en el sector privado como en el público. Esta demanda surge por la necesidad de identificar y autenticar a los usuarios con un nivel de seguridad elevado.

La evaluación del Reglamento eIDAS[2] puso de manifiesto que el Reglamento actual no consigue dar respuesta a estas nuevas demandas del mercado, lo que se debe, fundamentalmente, a sus limitaciones (inherentes al sector público), a las escasas posibilidades que tienen los prestadores privados en línea para conectarse al sistema (y la complejidad que presenta dicha conexión para ellos), a la disponibilidad insuficiente de soluciones de identidad electrónica en todos los Estados miembros y a la falta de flexibilidad del sistema para admitir diversos tipos de casos de uso. Además, las soluciones de identidad que no entran dentro del ámbito de aplicación del Reglamento eIDAS, como las que ofrecen los proveedores de medios sociales y las entidades financieras, plantean cuestiones relacionadas con la privacidad y la protección de datos. Tales soluciones no pueden responder eficazmente a las nuevas demandas del mercado y carecen del alcance transfronterizo requerido para abordar necesidades sectoriales específicas, situaciones en las que la identificación resulta delicada y requiere un grado alto de certeza.

---

1 DO L 257/73 de 28.8.2014.

2 [Añadir referencia una vez adoptada].

Desde la entrada en vigor de la sección del Reglamento relativa a la identidad electrónica en septiembre de 2018, tan solo catorce Estados miembros han notificado al menos un sistema de identidad electrónica. Como resultado de ello, solamente un 59 % de los residentes en la UE tienen acceso a sistemas transfronterizos de identidad electrónica fiables y seguros. Solo hay siete sistemas completamente móviles que responden a las expectativas actuales de los usuarios. Puesto que no todos los nodos técnicos establecidos para garantizar la conexión con el marco de interoperabilidad contemplado en el Reglamento eIDAS se encuentran plenamente operativos, el acceso transfronterizo es limitado; asimismo, los servicios públicos accesibles a escala nacional a los que también se puede acceder a través de la red eIDAS son muy escasos.

Si se ofreciera un Marco para una Identidad Digital Europea basado en la revisión del actual, al menos un 80 % de los ciudadanos deberían poder utilizar una solución de identidad digital para acceder a servicios públicos esenciales de aquí a 2030. Además, la seguridad y el control que ofrece el Marco para una Identidad Digital Europea debe proporcionar a los ciudadanos y residentes confianza plena en que dicho marco ofrecerá a todas las personas los medios necesarios para controlar quién puede acceder a su gemelo digital y a qué datos tiene acceso exactamente. Esto requerirá asimismo un nivel alto de seguridad en todos los aspectos de la provisión de la identidad digital, incluida la expedición de una cartera de identidad digital europea, y la infraestructura necesaria para la recopilación, el almacenamiento y la divulgación de datos de identidad digital.

Por otro lado, el marco actual previsto en el Reglamento eIDAS no cubre la provisión de atributos electrónicos, como certificados médicos o cualificaciones profesionales, lo que dificulta garantizar el reconocimiento legal de tales credenciales en formato electrónico a escala europea. Además, el Reglamento eIDAS no permite que los usuarios limiten el intercambio de datos personales al estrictamente necesario para la prestación de un servicio.

Pese a que la evaluación del Reglamento eIDAS muestra que el marco para la prestación de servicios de confianza ha obtenido resultados bastante satisfactorios, al proporcionar un nivel alto de confianza y garantizar la adopción y utilización de la mayoría de los servicios de confianza, es preciso continuar trabajando para lograr su armonización y aceptación plenas. Los ciudadanos, por su parte, deben poder confiar en los certificados cualificados de autenticación de sitios web y beneficiarse de la información segura y fiable que proporcionan sobre quién está detrás de un determinado sitio web, lo que reduciría el fraude.

Además, para responder a la dinámica de los mercados y a la evolución tecnológica, la presente propuesta amplía la lista actualmente vigente de servicios de confianza incluida en el Reglamento eIDAS, a saber, la prestación de servicios de archivo electrónico, los libros mayores electrónicos y la gestión de dispositivos remotos de firma electrónica y creación de sellos.

Esta propuesta ofrece también un enfoque armonizado con respecto a la seguridad, tanto para los ciudadanos que utilicen una identidad digital europea con fines de representación en línea como para los proveedores de servicios en línea, que podrán confiar plenamente en las soluciones de identidad digital y aceptarlas con independencia de dónde se hayan expedido. La propuesta implica un cambio para los emisores de soluciones de identidad digital europea, al proporcionar una arquitectura técnica, un marco de referencia y normas comunes que se desarrollarán en colaboración con los Estados miembros. Es necesario adoptar un enfoque armonizado con el fin de evitar que el desarrollo de nuevas soluciones de identidad digital en los Estados miembros provoque una mayor fragmentación debido al uso de soluciones

nacionales divergentes. Además, dicho enfoque fortalecerá el mercado interior, ya que permitirá que los ciudadanos, las empresas y otros residentes se identifiquen en línea de manera segura, cómoda y uniforme en toda la UE para acceder tanto a servicios públicos como privados. Los usuarios podrán utilizar un ecosistema reforzado de identidad digital y servicios de confianza, reconocido y aceptado en toda la Unión.

Para evitar la fragmentación y los obstáculos derivados de la existencia de normas divergentes, la Comisión adoptará una Recomendación al mismo tiempo que la presente propuesta. Dicha Recomendación definirá un proceso dirigido a respaldar un enfoque común que permita a los Estados miembros y a otras partes interesadas pertinentes de los sectores público y privado, en estrecha coordinación con la Comisión, trabajar en pos del desarrollo de un conjunto de herramientas que eviten planteamientos divergentes e impidan que se ponga en peligro la futura implantación del Marco para una Identidad Digital Europea.

- **Coherencia con las disposiciones existentes en la misma política sectorial**

La presente propuesta se basa en el Reglamento eIDAS actualmente en vigor, en el papel de los Estados miembros como proveedores de identidades legales y en el marco para la prestación de servicios electrónicos de confianza en la Unión Europea. La propuesta es complementaria y plenamente coherente con otros instrumentos políticos a escala de la UE cuyo objetivo es trasladar los beneficios del mercado interior al mundo digital, en particular mediante la ampliación de las posibilidades de acceso de los ciudadanos a servicios transfronterizos. En este sentido, la propuesta aplica el mandato político conferido por el Consejo Europeo[3] y la presidenta de la Comisión Europea[4] de proporcionar un marco para las identidades electrónicas públicas a escala de la UE que garantice que cualquier ciudadano o residente tenga acceso a una identidad electrónica europea segura; dicho marco debe poder utilizarse en toda la Unión con fines de identificación y autenticación para acceder a servicios en los sectores públicos y privados, y permitir a los ciudadanos controlar qué datos se comunican y el modo en que se usan.

- **Coherencia con otras políticas de la Unión**

La propuesta es coherente con las prioridades de transformación digital definidas en la estrategia «Configurar el futuro digital de Europa»[5] y respaldará el logro de los objetivos indicados en la Comunicación sobre el Decenio Digital[6]. Cualquier operación de tratamiento de datos personales en virtud de este Reglamento deberá llevarse a cabo en pleno cumplimiento del Reglamento General de Protección de Datos (en adelante, RGPD)[7]. Además, este Reglamento introduce una serie de salvaguardias específicas en materia de protección de datos.

---

3 https://www.consilium.europa.eu/media/45932/021020-euco-final-conclusions-es.pdf.

4 Discurso sobre el estado de la Unión, 16 de septiembre de 2020; véase https://ec.europa.eu/commission/presscorner/detail/es/SPEECH_20_1655.

5 Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, «Configurar el futuro digital de Europa».

6 Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, «Brújula Digital 2030: el enfoque de Europa para el Decenio Digital».

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

Con objeto de garantizar un nivel alto de seguridad, la propuesta también es coherente con las políticas de la Unión relativas a la ciberseguridad[8]. La propuesta se ha diseñado para reducir la fragmentación en la aplicación de los requisitos generales en materia de ciberseguridad a los prestadores de servicios de confianza regulados por el Reglamento eIDAS.

Asimismo, esta propuesta es coherente con otras políticas sectoriales basadas en la utilización de identidades electrónicas, declaraciones electrónicas de atributos y otros servicios de confianza. Entre ellas, figuran el Reglamento relativo a una pasarela digital única[9], los requisitos que se deben cumplir en el sector financiero en relación con la lucha contra el blanqueo de capitales y la financiación del terrorismo, las iniciativas destinadas a compartir las credenciales de la seguridad social o a crear un permiso de conducción o documentos de viaje digitales en el futuro, así como otras iniciativas diseñadas para reducir la carga administrativa que soportan los ciudadanos y las empresas que deseen aprovechar por completo las posibilidades que brinda la transformación digital de los procedimientos, tanto en el sector público como en el privado. La cartera permitirá además utilizar firmas electrónicas cualificadas que pueden facilitar la participación política[10].

2. BASE JURÍDICA, SUBSIDIARIEDAD Y PROPORCIONALIDAD

• Base jurídica

El propósito de la iniciativa es apoyar la transformación de la Unión en pos de la creación de un mercado único digital. Con la creciente digitalización de los servicios públicos y privados transfronterizos que dependen del uso de soluciones de identidad digital, existe el riesgo de que, dentro del marco jurídico vigente, los ciudadanos continúen enfrentándose a obstáculos y no consigan utilizar plenamente y sin incidencias los servicios en línea en toda la UE ni proteger su privacidad. También existe el riesgo de que las deficiencias del marco jurídico vigente que regula los servicios de confianza incrementen la fragmentación y reduzcan la confianza si su aplicación se deja únicamente en manos de los Estados miembros. En consecuencia, se identifica como base jurídica de la presente iniciativa el artículo 114 del Tratado de Funcionamiento de la Unión Europea (TFUE).

• Subsidiariedad (en el caso de competencia no exclusiva)

Los ciudadanos y las empresas deben poder beneficiarse de la disponibilidad de soluciones de identidad digital altamente seguras y fiables que se puedan utilizar en toda la UE, así como de la portabilidad de declaraciones electrónicas de atributos vinculados a la identidad. Los avances tecnológicos recientes, el mercado y la demanda de los usuarios exigen disponer de soluciones transfronterizas de fácil manejo que permitan acceder a servicios en línea en toda la Unión, algo que el Reglamento eIDAS no puede ofrecer con su redacción actual.

Los usuarios se han ido habituando cada vez más a soluciones disponibles a escala mundial, por ejemplo cuando aceptan utilizar las soluciones de inicio de sesión único que proporcionan las grandes plataformas de medios sociales para acceder a servicios en línea. Los Estados miembros no pueden hacer frente por sí solos a los desafíos que esto plantea en términos de poder de mercado de los grandes proveedores, que exige interoperabilidad e identidades digitales fiables a escala de la UE. Además, a menudo las declaraciones electrónicas de atributos emitidas y aceptadas en un Estado miembro, como los certificados sanitarios electrónicos, no gozan de

[8] https://ec.europa.eu/commission/presscorner/detail/es/IP_20_2391.

[9] Reglamento (UE) 2018/1724 del Parlamento Europeo y del Consejo, de 2 de octubre de 2018, relativo a la creación de una pasarela digital única de acceso a información, procedimientos y servicios de asistencia y resolución de problemas (DO L 295 de 21.11.2018, p. 1).

[10] Plan de Acción para la Democracia Europea, COM/2020/790 final.

validez ni reconocimiento legal en otros Estados miembros. Esto genera el riesgo de que los Estados miembros sigan desarrollando soluciones nacionales fragmentadas que no puedan utilizarse a escala transfronteriza.

En lo que respecta a la prestación de servicios de confianza, pese a estar ampliamente regulados y a que su funcionamiento se ajusta al marco jurídico en vigor, las prácticas nacionales también crean un riesgo de aumento de la fragmentación.

En definitiva, la intervención a escala de la UE es la más adecuada para proporcionar a ciudadanos y empresas los medios necesarios para identificar e intercambiar atributos y credenciales de identidad personal a escala transfronteriza utilizando soluciones de identidad digital altamente seguras y fiables, en cumplimiento de las normas de protección de datos de la UE. Esto requiere soluciones de identidad digital fiables y seguras y un marco regulador que las vincule con los atributos y credenciales a escala de la Unión. Únicamente a través de una intervención a escala de la UE es posible establecer unas condiciones armonizadas que garanticen el control de los usuarios y su acceso a servicios digitales transfronterizos en línea, así como crear un marco de interoperabilidad que permita a los servicios en línea confiar en la utilización de soluciones de identidad digital seguras, con independencia del lugar de la UE en el que se hayan expedido o de dónde resida un ciudadano. Como se refleja en gran medida en la evaluación del Reglamento eIDAS, no es probable que una intervención a escala nacional ofrezca el mismo nivel de eficiencia y eficacia.

- **Proporcionalidad**

La iniciativa es proporcionada a los objetivos perseguidos; ofrece un instrumento adecuado para establecer la estructura de interoperabilidad necesaria para la creación de un ecosistema de identidad digital a escala de la UE basado en identidades legales expedidas por los Estados miembros y en la provisión de atributos de identidad digital cualificados y no cualificados. Supone una contribución clara al objetivo de mejorar el mercado único digital a través de un marco jurídico más armonizado. Las carteras europeas armonizadas de identidad digital que deben expedir los Estados miembros en virtud de las normas técnicas comunes proporcionan también un enfoque común de la Unión que beneficia a los usuarios y a las partes que dependen de la disponibilidad de soluciones de identidad electrónica transfronterizas seguras. La iniciativa aborda las limitaciones de la infraestructura de interoperabilidad de la identificación electrónica actualmente existente, basada en el reconocimiento mutuo de los diversos sistemas nacionales de identificación electrónica. Teniendo en consideración los objetivos fijados, esta iniciativa se considera suficientemente proporcionada y es probable que sus costes sean proporcionales a sus beneficios potenciales. El Reglamento propuesto generará costes financieros y administrativos que deberán ser asumidos por los Estados miembros como emisores de las carteras de identidad digital europea, así como por los prestadores de servicios de confianza y en línea. Sin embargo, es probable que estos costes se vean compensados con creces por los importantes beneficios potenciales para los ciudadanos y los usuarios directamente derivados de un aumento del reconocimiento y la aceptación transfronterizos de los servicios de identidad y atributos electrónicos.

Los costes que conlleva la creación y armonización del nuevo sistema con las nuevas normas para los prestadores de servicios de confianza y los prestadores de servicios en línea son ineludibles si se pretende alcanzar el objetivo de la aptitud para el uso y la accesibilidad. La iniciativa pretende aprovechar y apoyarse en la inversión ya realizada por los Estados miembros en sus sistemas de identidad nacionales. Por otro lado, los costes adicionales que entraña la propuesta están diseñados para apoyar la armonización y se justifican por la expectativa de que, a largo plazo, reducirán la carga administrativa y los costes de conformidad. Los costes vinculados a la aceptación de los atributos de autenticación de la identidad digital en sectores regulados pueden considerarse asimismo necesarios y

proporcionados, en la medida en que respaldan el objetivo general y ofrecen a dichos sectores los medios necesarios para cumplir sus obligaciones legales en lo referente a la identificación legal de los usuarios.

- **Elección del instrumento**

La elección de un Reglamento como instrumento jurídico está justificada por la necesidad de garantizar unas condiciones uniformes en el mercado interior para la aplicación de la identidad digital europea por medio de un marco armonizado destinado a crear una interoperabilidad fluida y a prestar a los ciudadanos y las empresas europeos servicios públicos y privados con identidades digitales altamente seguras y fiables en toda la Unión.

3. RESULTADOS DE LAS EVALUACIONES *EX POST*, DE LAS CONSULTAS CON LAS PARTES INTERESADAS Y DE LAS EVALUACIONES DE IMPACTO

- **Evaluaciones *ex post* / controles de la adecuación de la legislación existente**

Como parte del proceso de revisión previsto en el artículo 49 del Reglamento eIDAS, se llevó a cabo una evaluación del funcionamiento de dicho Reglamento. La conclusión principal de la evaluación con respecto a la identidad electrónica es que el Reglamento eIDAS no ha desarrollado todo su potencial. Solo se ha notificado una cantidad limitada de identidades electrónicas, lo que reduce la cobertura de los sistemas de identidad electrónica notificados a aproximadamente un 59 % de la población de la UE. Además, la aceptación de las identidades electrónicas notificadas es limitada, tanto a escala de los Estados miembros como entre los prestadores de servicios. Por otra parte, parece que solamente unos pocos de los servicios accesibles a través de la identidad electrónica nacional están conectados a la infraestructura eIDAS nacional. La evaluación constató también que el ámbito de aplicación actual del Reglamento eIDAS y su enfoque, centrado en los sistemas de identidad electrónica notificados por los Estados miembros de la UE y en permitir el acceso a servicios públicos en línea, resulta excesivamente limitado e inadecuado. La inmensa mayoría de las necesidades de autenticación remota y de identidad electrónica sigue concentrándose en el sector privado, en particular en ámbitos como la banca, las telecomunicaciones y los operadores de plataformas, a los que la ley exige verificar la identidad de sus clientes. El valor añadido del Reglamento eIDAS con respecto a la identidad electrónica es limitado, debido a su nivel bajo de cobertura, adopción y utilización.

Los problemas identificados en esta propuesta están relacionados con las carencias del marco eIDAS actual y con cambios contextuales fundamentales que afectan a los mercados, así como con transformaciones tecnológicas y sociales que generan nuevas necesidades entre los usuarios y en los mercados.

- **Consultas con las partes interesadas**

Se inició una consulta pública el 24 de julio de 2020, que concluyó el 2 de octubre de 2020. La Comisión recibió en total 318 contribuciones. Además, también recibió 106 respuestas a una encuesta dirigida a las partes interesadas. Asimismo, se recogieron opiniones de los Estados miembros en diversas reuniones y encuestas bilaterales y multilaterales organizadas desde principios de 2020. Estas incluyeron, en particular, una encuesta a representantes de los Estados miembros en la Red de Cooperación eIDAS en julio y agosto de 2020, así como diversos talleres dedicados a este tema. La Comisión realizó asimismo entrevistas en profundidad a representantes de la industria y mantuvo reuniones bilaterales con partes interesadas del mundo de los negocios pertenecientes a diversos sectores (como el comercio

electrónico, la sanidad y los servicios financieros, pero también operadores de telecomunicaciones, fabricantes de equipos, etc.).

La gran mayoría de los participantes en la consulta pública acogieron con agrado la creación de una identidad digital única y universalmente aceptada, basada en las identidades legales expedidas por los Estados miembros. Los Estados miembros respaldan en gran medida la necesidad de reforzar el Reglamento eIDAS actualmente en vigor para ofrecer a los ciudadanos la posibilidad de acceder a servicios públicos y privados, y reconocen que es preciso establecer un servicio de confianza que permita la expedición y el uso transfronterizo de declaraciones electrónicas de atributos. En general, los Estados miembros hicieron hincapié en la necesidad de crear un Marco para una Identidad Digital Europea basado en la experiencia y la fortaleza de las soluciones nacionales, así como de tratar de encontrar sinergias y de aprovechar las inversiones realizadas. Numerosas partes interesadas hicieron referencia al hecho de que la pandemia de COVID-19 ha demostrado el valor de una identificación remota segura para el acceso de cualquier persona a servicios públicos y privados. En lo relativo a los servicios de confianza, la mayoría de los agentes está de acuerdo en que el marco actual ha sido un éxito, si bien fue necesario adoptar una serie de medidas adicionales para armonizar determinadas prácticas relacionadas con la identificación remota y la supervisión nacional. Las partes interesadas con una base de clientes principalmente nacional expresaron más dudas acerca del valor añadido de un Marco para una Identidad Digital Europea.

Tanto el sector público como el privado tienen una percepción cada vez mayor de que las carteras de identidad digital constituyen el instrumento más adecuado, ya que permite a los usuarios elegir cuándo y con qué proveedor de servicios privados compartir atributos diversos, dependiendo del caso de uso y del nivel de seguridad requerido para llevar a cabo la transacción de que se trate. Se consideró que las identidades digitales basadas en carteras digitales almacenadas de forma segura en dispositivos móviles representan un activo fundamental que puede ofrecer una solución con perspectivas de futuro. Tanto el mercado privado (por ejemplo, Apple, Google o Thales) como los gobiernos están avanzando ya en esta dirección.

- **Obtención y uso de asesoramiento especializado**

La propuesta se basa en la información recopilada en el marco de la consulta con las partes interesadas para la elaboración de los informes de evaluación y de evaluación de impacto del Reglamento eIDAS, con vistas al cumplimiento de las obligaciones de revisión previstas en el artículo 49 del Reglamento eIDAS. Se han organizado numerosas reuniones con representantes y expertos de los Estados miembros.

- **Evaluación de impacto**

Se realizó una evaluación de impacto de la presente propuesta. El 19 de marzo de 2021, el Comité de Control Reglamentario emitió un dictamen negativo con algunos comentarios. Tras la presentación de una versión revisada de la evaluación de impacto, el citado Comité emitió un dictamen positivo el 5 de mayo de 2021.

La Comisión examina diferentes opciones de política para lograr el objetivo general de la presente iniciativa, que es garantizar el buen funcionamiento del mercado interior, en particular en lo que respecta al suministro y uso de soluciones de identidad electrónica altamente seguras y fiables.

La evaluación de impacto examina la situación de referencia, las opciones de política y los efectos de las tres opciones consideradas. Cada una de estas opciones implica una decisión política en función del nivel de ambición. La primera opción presenta un nivel de ambición bajo y un conjunto de medidas dirigidas, fundamentalmente, a reforzar la eficacia y la eficiencia del Reglamento eIDAS actualmente en vigor. Al imponer un requisito de notificación obligatoria de las identidades electrónicas nacionales y racionalizar los instrumentos existentes disponibles para lograr el reconocimiento mutuo, la primera opción se basa en satisfacer las necesidades de los ciudadanos apoyándose en la disponibilidad de diversos sistemas nacionales de identidad electrónica que aspiran a ser interoperables.

La segunda opción presenta un nivel de ambición intermedio y su principal objetivo es ampliar las posibilidades de intercambio seguro de datos vinculados a la identidad, complementar las identidades electrónicas gubernamentales y apoyar el cambio actual hacia unos servicios de identidad basados en atributos. El propósito de esta opción sería dar respuesta a las demandas de los usuarios y crear un nuevo servicio de confianza cualificado para la provisión de declaraciones electrónicas de atributos vinculadas a fuentes de confianza que se puedan utilizar en operaciones transfronterizas. Esto ampliaría el ámbito de aplicación del Reglamento eIDAS actual y apoyaría la máxima cantidad posible de casos de uso, basándose en la necesidad de verificar los atributos de identidad vinculados a una persona con un nivel alto de seguridad.

La tercera opción —la preferida— presenta el mayor nivel de ambición de las tres; su objetivo es regular la provisión de una cartera personal de identidad digital con un nivel alto de seguridad, expedida por los Estados miembros. Se consideró que la opción preferida respondería de la manera más eficaz a los objetivos de la presente iniciativa. Con el fin de abordar plenamente los objetivos de la política, la opción preferida se apoya en la mayoría de las medidas evaluadas en el marco de la primera opción (utilización de las identidades legales acreditadas por los Estados miembros y aprovechamiento de la disponibilidad de medios de identidad electrónica reconocidos mutuamente) y de la segunda (declaraciones electrónicas de atributos legalmente reconocidas a escala transfronteriza).

Con respecto al marco general de los servicios de confianza, al nivel de ambición exige un conjunto de medidas que no requieren un enfoque paso a paso para alcanzar los objetivos de la política.

El nuevo servicio de confianza cualificado para la gestión de la firma electrónica remota y de dispositivos de creación de sellos aportaría un grado considerable de seguridad, uniformidad, seguridad jurídica y capacidad de elección para los consumidores; estos beneficios estarían asociados tanto a la certificación de los dispositivos cualificados de creación de firmas como a los requisitos que deberían cumplir los prestadores cualificados de servicios de confianza que gestionan dichos dispositivos. Las nuevas disposiciones reforzarían el marco regulador y de supervisión aplicable con carácter general a la prestación de servicios de confianza.

En el anexo 3 de la evaluación de impacto que respalda la presente iniciativa, se explican detalladamente los efectos de las opciones de política en las diferentes categorías de partes interesadas. La evaluación es cuantitativa y cualitativa. El estudio de evaluación de impacto indica que los costes mínimos cuantificables se pueden estimar en más de 3 200 millones EUR, dado que no es posible cuantificar algunas de las partidas de costes. Por otro lado, se ha calculado que los beneficios cuantificables totales se situarían entre 3 900 y 9 600 millones EUR. En cuanto a los efectos económicos generales, se espera que la opción preferida ejerza un impacto positivo en la innovación, el comercio internacional y la

competitividad, contribuya al crecimiento económico y genere inversiones adicionales en soluciones de identidad digital. Por ejemplo, se prevé que una inversión adicional de 500 millones EUR derivada de los cambios legislativos introducidos en el marco de la opción 3 se traduzca en un beneficio de 1 268 millones EUR al cabo de 10 años (con un nivel de adopción del 67 %).

Además, se espera que la opción preferida tenga un efecto positivo en el empleo, al generar entre 5 000 y 27 000 puestos de trabajo adicionales en los 5 años siguientes a su implantación. Esto se explica por la inversión adicional y la reducción de los costes para las empresas que se apoyan en la utilización de soluciones de identidad electrónica.

La tercera opción es la que ofrece también un impacto más favorable al medio ambiente, ya que se espera que implique el mayor aumento de la adopción y facilidad de uso de la identidad electrónica, lo que reduciría las emisiones relacionadas con la prestación de servicios públicos.

Los libros mayores electrónicos proporcionan a los usuarios una prueba y una pista de auditoría inmutable para la secuenciación de las operaciones y los registros de datos, lo que salvaguarda la integridad de estos. A pesar de que este servicio de confianza no formaba parte de la evaluación de impacto, se apoya en servicios de confianza existentes, puesto que combina los sellos de tiempo de los datos y su secuenciación con la certeza acerca del originador de los datos, lo cual es similar a la firma electrónica. Este servicio de confianza es necesario para evitar la fragmentación del mercado interior, al definir un marco único a escala europea que permite el reconocimiento transfronterizo de servicios de confianza que respaldan el funcionamiento de libros mayores electrónicos cualificados. A su vez, la integridad de los datos es muy importante para la puesta en común de datos procedentes de fuentes descentralizadas, para las soluciones de identidad autosoberana, para atribuir la propiedad a activos digitales, registrar el cumplimiento de criterios de sostenibilidad por parte de los procesos empresariales y para diversos casos de uso en los mercados de capitales.

- **Adecuación y simplificación normativa**

La propuesta establece una serie de medidas que se aplicarán a las autoridades públicas, los ciudadanos y los prestadores de servicios en línea. Reducirá el coste administrativo y de conformidad de las administraciones públicas, así como los gastos de explotación y los relacionados con la seguridad para los prestadores de servicios en línea. Los ciudadanos se beneficiarán del ahorro derivado de la reducción de la carga administrativa, de la posibilidad de apoyarse plenamente en medios digitales para identificarse y de la facilidad para intercambiar de forma segura atributos de identidad digital con idéntico valor jurídico en sus actividades transfronterizas. Los proveedores de identidad electrónica, por su parte, también se beneficiarán del ahorro de costes de conformidad.

- **Derechos fundamentales**

Puesto que los datos personales entran dentro del ámbito de aplicación de determinadas disposiciones del Reglamento, las medidas están diseñadas para cumplir plenamente la legislación en materia de protección de datos. Por ejemplo, la propuesta mejora las opciones para el intercambio de datos y para posibilitar la divulgación discrecional. Utilizando la cartera de identidad digital europea, el usuario podrá controlar la cantidad de datos que proporciona a las partes usuarias de estos y ser informado de los atributos requeridos para la prestación de un servicio específico. Los prestadores de servicios informarán a los Estados miembros de su intención de utilizar una cartera de identidad digital europea, que permitirá a

los Estados miembros controlar que los prestadores de servicios únicamente soliciten conjuntos de datos confidenciales, como los relacionados con la salud, de conformidad con la legislación nacional.

4. REPERCUSIONES PRESUPUESTARIAS

Para lograr de forma óptima los objetivos de esta iniciativa, es necesario financiar una serie de acciones tanto a nivel de la Comisión, donde se prevé la redistribución de sesenta trabajadores equivalentes a jornada completa (EJC) en el período 2022-2027, como a escala de los Estados miembros, mediante su participación activa en los grupos y comités de expertos relacionados con el trabajo de la iniciativa y compuestos por representantes de los Estados miembros. La dotación financiera total necesaria para la puesta en práctica de la propuesta en el período 2022-2027 ascenderá como máximo a 30 825 000 EUR; dicha cantidad incluye 8 825 000 EUR en concepto de costes administrativos y un máximo de 22 millones EUR en concepto de gastos de funcionamiento, que se sufragarán con cargo al programa Europa Digital (pendiente de acuerdo). La financiación contribuirá a cubrir los costes relacionados con el mantenimiento, desarrollo, alojamiento, funcionamiento y asistencia a los bloques componentes de los servicios de identidad electrónica y de confianza. También puede contribuir a financiar subvenciones para conectar servicios al ecosistema de carteras de identidad digital europea, así como el desarrollo de normas y especificaciones técnicas. Por último, la financiación apoyará también la realización de encuestas anuales y estudios sobre la eficiencia y eficacia del Reglamento en la consecución de sus objetivos. El «estado financiero» que acompaña a esta iniciativa ofrece una descripción detallada de los costes que conlleva.

5. OTROS ELEMENTOS

- **Planes de ejecución y modalidades de seguimiento, evaluación e información**

El seguimiento y la evaluación de los efectos se llevarán a cabo de conformidad con las Directrices para la mejora de la legislación durante la aplicación y ejecución del Reglamento propuesto. El mecanismo de seguimiento constituye una parte importante de la propuesta, sobre todo en vista de las deficiencias del marco de notificación actualmente existente que puso de manifiesto el estudio de evaluación. Además de los requisitos de notificación introducidos en el Reglamento propuesto, cuyo objetivo es garantizar unos datos y análisis de mayor calidad, el marco de seguimiento supervisará los aspectos siguientes: 1) el grado de ejecución de los cambios necesarios, en consonancia con las medidas adoptadas; 2) si se han aplicado los cambios necesarios en los sistemas nacionales pertinentes; 3) si se han adoptado los cambios necesarios en las obligaciones de conformidad de las entidades reguladas. La Comisión Europea (1, 2 y 3) y las autoridades nacionales competentes (2 y 3) serán responsables de la recopilación de datos con base en una serie de indicadores previamente definidos.

Con respecto a la aplicación del instrumento propuesto, la Comisión Europea y las autoridades nacionales competentes evaluarán, a través de encuestas anuales: 1) la disponibilidad de acceso a medios de identidad electrónica para todos los ciudadanos de la UE; 2) el aumento del reconocimiento y la aceptación transfronterizos de los sistemas de identidad electrónica; 3) las medidas adoptadas para estimular la adopción por parte del sector privado y el desarrollo de nuevos servicios de identidad digital.

La Comisión Europea, utilizando encuestas anuales, recabará información contextual sobre: 1) el tamaño del mercado de identidades digitales; 2) el gasto en el marco de la adjudicación

de contratos públicos vinculado a la identidad digital; 3) la proporción de empresas que prestan sus servicios en línea; 4) la proporción de transacciones en línea que requieren una identificación reforzada del cliente; 5) la proporción de ciudadanos de la UE que utilizan servicios en línea públicos y privados.

- **Explicación detallada de las disposiciones específicas de la propuesta**

El proyecto de Reglamento, en su artículo 6 *bis*, exige a los Estados miembros que expidan una cartera de identidad digital europea, en el contexto de un sistema de identidad electrónica notificado con arreglo a las normas técnicas comunes, tras una evaluación obligatoria de la conformidad y una certificación voluntaria dentro del marco europeo de certificación de la ciberseguridad, según se establece en el Reglamento sobre la Ciberseguridad. El proyecto de Reglamento incluye disposiciones destinadas a garantizar que las personas físicas y jurídicas tengan la posibilidad de solicitar y obtener, almacenar, combinar y utilizar de forma segura datos de identificación personal y declaraciones electrónicas de atributos para autenticarse en línea y fuera de línea, así como a permitir el acceso a bienes y a servicios públicos y privados en línea bajo el control del usuario. Esta certificación es acorde con lo dispuesto en el RGPD, en el sentido de que las operaciones de tratamiento de datos personales relacionadas con la cartera de identidad digital europea solo pueden certificarse con arreglo a los artículos 42 y 43 del RGPD.

En su artículo 6 *ter*, la propuesta establece un conjunto de disposiciones específicas relativas a los requisitos aplicables a las partes usuarias para la prevención del fraude y para garantizar la autenticación de los datos de identificación personal y las declaraciones electrónicas de atributos procedentes de la cartera de identidad digital europea.

En aras de aumentar la disponibilidad de medios de identificación electrónica para su uso transfronterizo, así como de mejorar la eficiencia del proceso de reconocimiento mutuo de los sistemas de identificación electrónica notificados, el artículo 7 establece para los Estados miembros la obligación de notificar al menos un sistema de identificación electrónica. Además, el artículo 11 *bis* introduce nuevas disposiciones destinadas a facilitar la identificación única, con objeto de garantizar la identificación única y persistente de las personas físicas. Esto afecta a aquellos casos en los que la identificación constituye un requisito legal, como sucede en el ámbito sanitario, en el financiero (para el cumplimiento de las obligaciones en materia de lucha contra el blanqueo de capitales) o en el judicial. Con este fin se exigirá a los Estados miembros que incluyan un identificador único y persistente en el conjunto mínimo de datos de identificación personal. La posibilidad de que los Estados miembros se basen en la certificación para garantizar la conformidad con el Reglamento y, de ese modo, sustituir el proceso de revisión por pares mejora la eficiencia del reconocimiento mutuo.

En la sección 3 se presentan nuevas disposiciones relativas a la utilización transfronteriza de la cartera de identidad digital europea para garantizar que los usuarios puedan apoyarse en el uso de estas carteras para acceder a los servicios en línea prestados por organismos del sector público y proveedores del sector privado que requieran una autenticación reforzada de los usuarios.

En el capítulo III, dedicado a los servicios de confianza, se ha modificado el artículo 14 referente a los aspectos internacionales para permitir que la Comisión adopte decisiones de ejecución por las que se acredite la equivalencia de los requisitos aplicados a los servicios de confianza establecidos en terceros países y de los servicios que prestan, además del uso de los acuerdos de reconocimiento mutuo con arreglo al artículo 218 del TFUE.

Por lo que respecta a la disposición general aplicable a los servicios de confianza, y de manera especial a los prestadores cualificados de servicios de confianza, se han modificado los artículos 17, 18, 20, 21 y 24 con objeto de armonizarlos con las normas aplicables a la seguridad de las redes y de la información en la UE. En cuanto a los métodos que deben utilizar los prestadores cualificados de servicios de confianza para verificar la identidad de las personas físicas o jurídicas a las que se expidan los certificados cualificados, las disposiciones sobre el uso de medios de identificación remotos se han armonizado y aclarado para garantizar que se apliquen las mismas normas en toda la UE.

El capítulo III incorpora un nuevo artículo 29 *bis* en el que se definen los requisitos que debe satisfacer un servicio cualificado de gestión de dispositivos de creación de firmas electrónicas remotas. El nuevo servicio de confianza cualificado estará directamente vinculado a las medidas referidas y basado en ellas, y se incluirá en la evaluación de impacto, en particular las medidas relativas a la armonización del proceso de certificación de firmas electrónicas remotas y otras medidas que requieran la armonización de las prácticas de supervisión de los Estados miembros.

Para garantizar que los usuarios puedan identificar quién está detrás de un determinado sitio web, se ha modificado el artículo 45 a fin de exigir a los proveedores de navegadores web que faciliten la utilización de certificados cualificados con fines de autenticación de sitios web.

El capítulo III presenta tres secciones nuevas.

La nueva sección 9 introduce un conjunto de disposiciones sobre los efectos jurídicos de las declaraciones electrónicas de atributos, su uso en determinados sectores y los requisitos para la obtención de declaraciones cualificadas de atributos. Para garantizar un nivel alto de confianza, el artículo 45 *quinquies* incorpora una disposición relativa al cotejo de atributos con fuentes auténticas. Con objeto de asegurar que los usuarios de la cartera de identificación digital europea puedan beneficiarse de la disponibilidad de declaraciones electrónicas de atributos y que dichas declaraciones se incorporen a la cartera de identificación digital europea, se introduce un requisito a tal efecto en el artículo 45 *sexies*. Por su parte, el artículo 45 *septies* contiene normas adicionales para la prestación de servicios de declaración electrónica de atributos, especialmente en lo que concierne a la protección de datos personales.

La nueva sección 10 permite la prestación de servicios cualificados de archivo electrónico a escala de la UE. El artículo 45 *octies*, referente a los servicios cualificados de archivo electrónico, complementa los artículos 34 y 40 relativos a los servicios cualificados de conservación de firmas electrónicas cualificadas y sellos electrónicos cualificados.

La nueva sección 11 establece un marco para los servicios de confianza en lo que respecta a la creación y el mantenimiento de libros mayores electrónicos y libros mayores electrónicos cualificados. Un libro mayor electrónico combina los sellos de tiempo de los datos y su secuenciación con la certeza sobre el originador de los datos, de manera similar a las firmas electrónicas, con la ventaja adicional de que permite una gestión más descentralizada que resulta muy adecuada para la cooperación entre múltiples partes. Esto es importante para diversos casos de uso que pueden apoyarse en la utilización de libros mayores electrónicos.

Los libros mayores electrónicos pueden ayudar a las empresas a ahorrar costes al mejorar la eficiencia y la seguridad de la coordinación entre las distintas partes, además de facilitar la supervisión de las autoridades reguladoras. En ausencia de una normativa europea, existe el riesgo de que los legisladores nacionales establezcan normas nacionales divergentes. Para evitar la fragmentación, es necesario definir un marco único a escala europea, que permitirá el reconocimiento transfronterizo de servicios de confianza que respalden el funcionamiento de

los libros mayores electrónicos. Esta norma paneuropea para los operadores de nodos se aplicará sin perjuicio del Derecho derivado de la UE. Cuando se utilicen libros mayores electrónicos para apoyar la emisión o la compraventa de bonos, o para criptoactivos, los casos de uso deberán ser compatibles con todas las normas financieras aplicables, por ejemplo la Directiva relativa a los mercados de instrumentos financieros[11], la Directiva sobre servicios de pago[12] y el futuro Reglamento relativo a los mercados de criptoactivos[13]. Cuando los casos de uso afecten a datos de carácter personal, los prestadores de servicios deberán cumplir el RGPD.

En 2017, los sectores bancario y financiero concentraban el 75 % de los casos de uso de los libros mayores electrónicos. Hoy en día dichos casos de uso presentan una diversidad creciente: el 17 % corresponde a la comunicación y los medios de información, el 15 % a la producción industrial y los recursos naturales, el 10 % al sector público, el 8 % al sector de los seguros, el 5 % al comercio al por menor, el 6 % al transporte y el 5 % a los servicios esenciales[14].

Por último, el capítulo VI incluye un nuevo artículo 48 *ter* para garantizar la recopilación de estadísticas sobre el uso de la cartera de identidad digital europea con fines de seguimiento de la eficacia del Reglamento modificado.

---

11 Directiva 2014/65/UE del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, relativa a los mercados de instrumentos financieros y por la que se modifican la Directiva 2002/92/CE y la Directiva 2011/61/UE, Texto pertinente a efectos del EEE *(DO L 173 de 12.6.2014, p. 349)*.

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

13 Propuesta de Reglamento del Parlamento Europeo y del Consejo, relativo a los mercados de criptoactivos y por el que se modifica la Directiva 2019/1937/UE (COM/2020/593 final).

14 Gartner, *Blockchain Evolution*, 2020.

2021/0136 (COD)

Propuesta de

REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO

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

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

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

Vista la propuesta de la Comisión Europea,

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

Visto el dictamen del Comité Económico y Social Europeo[15],

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»[16], 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[17], el Consejo Europeo instó a la Comisión a que presentara una propuesta relativa al desarrollo, a escala de la UE, de un marco para la identificación electrónica pública segura, en particular de las firmas digitales interoperables, de modo que las personas puedan tener el control de su identidad y sus datos en línea y se facilite el acceso a los servicios digitales públicos, privados y transfronterizos.

(3) La Comisión de la Comunicación de 9 de marzo de 2021, titulada «Brújula Digital 2030: el enfoque de Europa para el Decenio Digital»[18] establece el objetivo de crear un marco a escala de la Unión que, a más tardar en 2030, conduzca a un amplio despliegue de una identidad fiable y controlada por el usuario, que permita a cada usuario controlar sus propias interacciones y su presencia en línea.

(4) Un enfoque más armonizado en lo que respecta a la identificación digital debería reducir los riesgos y los costes asociados a la actual fragmentación derivada del uso de soluciones nacionales divergentes, y reforzará el mercado interior al permitir que los ciudadanos, otros residentes definidos en las leyes nacionales y las empresas se identifiquen en línea de manera cómoda y uniforme en toda la Unión. Toda persona debe ser capaz de acceder de forma segura a servicios públicos y privados apoyándose

---

15 DO C [] de […], p. […].

16 COM/2020/67 final.

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

18 COM/2021/118 final/2.

en un ecosistema reforzado de servicios de confianza y en pruebas de identidad y declaraciones de atributos verificados, como un título universitario legalmente reconocido y aceptado en cualquier lugar de la Unión. El Marco para una Identidad Digital Europea aspira a lograr un cambio que permita pasar de la utilización exclusiva de soluciones de identidad digital al suministro de declaraciones electrónicas de atributos que sean válidas a escala europea. Los proveedores de declaraciones electrónicas de atributos deben beneficiarse de un conjunto de normas claras y uniformes, y las administraciones públicas deben poder confiar en los documentos electrónicos expedidos en un determinado formato.

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

(6) El Reglamento (UE) 2016/679[19] es aplicable al tratamiento de datos personales efectuado en aplicación del presente Reglamento. En consecuencia, este Reglamento debe establecer salvaguardias específicas para evitar que los proveedores de medios de identificación electrónica y declaraciones electrónicas de atributos combinen datos personales obtenidos a través de otros servicios con los datos personales relacionados con los servicios contemplados en el ámbito de aplicación del presente Reglamento.

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

(8) Con el fin de garantizar la conformidad con el Derecho de la Unión (y la conformidad del Derecho nacional con el de la Unión), los proveedores de servicios deberán comunicar a los Estados miembros su intención de utilizar las carteras de identidad digital europea. Esto permitirá a los Estados miembros proteger a los usuarios frente al fraude y evitar la utilización ilícita de datos de identidad y declaraciones electrónicas de atributos, así como asegurar que las partes usuarias puedan verificar si el tratamiento de los datos confidenciales, como los sanitarios, se ajusta a lo dispuesto en el Derecho nacional o de la Unión.

(9) Todas las carteras de identidad digital europea deben permitir a los usuarios identificarse y autenticarse electrónicamente a través de las fronteras, tanto en línea como fuera de línea, para acceder a una amplia gama de servicios públicos y privados. Sin perjuicio de las prerrogativas de los Estados miembros en lo que respecta a la

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

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

(10) Para lograr un nivel alto de seguridad y fiabilidad, este Reglamento establece los requisitos que deben satisfacer las carteras de identidad digital europea. La acreditación de la conformidad de las citadas carteras con estos requisitos corresponderá a organismos acreditados del sector público o privado designados por los Estados miembros. El hecho de apoyarse en un régimen de certificación basado en la disponibilidad de normas comúnmente acordadas debe asegurar un nivel alto de confianza e interoperabilidad. La certificación debe basarse, en particular, en los esquemas europeos de certificación de la ciberseguridad establecidos en virtud del Reglamento (UE) 2019/881[20]. Tal certificación se efectuará sin perjuicio de la certificación referente al tratamiento de los datos personales en virtud del Reglamento (CE) 2016/679.

(11) Las carteras de identidad digital europea deben garantizar el máximo nivel de seguridad para los datos personales utilizados con fines de autenticación, con independencia de si dichos datos se almacenan de forma local o utilizando soluciones en la nube, teniendo en cuenta los diferentes niveles de riesgo. La utilización de la biometría para la autenticación es uno de los métodos de identificación que proporcionan un nivel alto de confianza, en particular cuando se combinan con otros elementos de autenticación. Dado que la biometría representa una característica única

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

de una persona, su uso requiere medidas organizativas y de seguridad proporcionales al riesgo que dicho tratamiento puede conllevar para los derechos y las libertades de las personas físicas y conformes al Reglamento 2016/679.

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

(13) El Reglamento (UE) 2019/1157[21] aumenta la seguridad de los documentos de identidad con la introducción características de seguridad reforzadas a más tardar en agosto de 2021. Los Estados miembros deben analizar la viabilidad de notificar estas características en el marco de los sistemas de identificación electrónica para ampliar la disponibilidad transfronteriza de medios de identificación electrónica.

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

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

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

---

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

(17) Los proveedores de servicios utilizan los datos de identidad proporcionados por el conjunto de datos de identificación personales disponibles a través de los sistemas de identificación electrónica en virtud del Reglamento (UE) n.º 910/2014 para determinar la identidad legal de los usuarios procedentes de otro Estado miembro. Sin embargo, a pesar del uso del conjunto de datos eIDAS, en muchos casos se necesita información adicional sobre el usuario y procedimientos específicos de identificación única a escala nacional para garantizar una determinación correcta de la identidad. Para mejorar la facilidad de uso de los medios de identificación electrónica, este Reglamento debe exigir a los Estados miembros la adopción de medidas concretas para asegurar una correcta determinación de la identidad en el proceso de identificación electrónica. Con ese mismo propósito, este Reglamento debe ampliar asimismo el conjunto de datos mínimo obligatorio y obligar a utilizar un identificador electrónico único y persistente, conforme con el Derecho de la Unión, en aquellos casos en que sea necesario para establecer de manera única y persistente la identidad legal de la persona usuaria a petición de esta.

(18) En consonancia con la Directiva (UE) 2019/882[22], las personas con discapacidad deben poder utilizar las carteras de identidad digital europea, los servicios de confianza y los productos destinados a los usuarios finales empleados en la prestación de dichos servicios, en igualdad de condiciones que el resto de los usuarios.

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

(20) La prestación y utilización de servicios de confianza está adquiriendo una importancia creciente para el comercio y la cooperación internacionales. Los socios internacionales de la UE están creando marcos de confianza inspirados en el Reglamento (UE) n.º 910/2014. Por consiguiente, para facilitar el reconocimiento de dichos servicios y de los proveedores que los prestan, se podrán establecer en la legislación de aplicación las condiciones en las que los marcos de confianza de terceros países podrán considerarse equivalentes al marco de confianza para los servicios y proveedores de confianza cualificados previsto en este Reglamento, como complemento a la posibilidad del reconocimiento mutuo de los servicios y proveedores de confianza establecida en la Unión y en terceros países de conformidad con el artículo 218 del Tratado.

(21) Este Reglamento debe basarse en actos de la Unión que garanticen mercados disputables y equitativos en el sector digital. En particular, se basa en el Reglamento XXX/XXXX (Ley de Mercados Digitales), que introduce normas para los proveedores de servicios básicos de plataforma designados como guardianes y, entre otras cosas, prohíbe que estos últimos exijan a los usuarios profesionales que utilicen, ofrezcan o interoperen con un servicio de identificación del guardián en el contexto de los servicios que ofrecen los usuarios profesionales que utilizan los servicios básicos de plataforma del mencionado guardián. El artículo 6, apartado 1, letra f), del Reglamento XXX/XXXX (Ley de Mercados Digitales) obliga a los guardianes a permitir a los usuarios profesionales y proveedores de servicios complementarios el

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

acceso y la interoperabilidad con las mismas funciones del sistema operativo, el hardware o el software disponibles o utilizadas en la prestación de servicios complementarios por parte del guardián. De acuerdo con el artículo 2, apartado 15, de la Ley de Mercados Digitales, los servicios de identificación constituyen un tipo de servicios complementarios. Los usuarios profesionales y los proveedores de servicios complementarios deben, por tanto, poder acceder a dichas funciones del hardware o del software, como las medidas de seguridad de los teléfonos inteligentes, e interoperar con ellas a través de las carteras de identidad digital europea o de los medios de identificación electrónica notificados por los Estados miembros.

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

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

(24) Es esencial proporcionar un marco jurídico para facilitar el reconocimiento transfronterizo entre los ordenamientos jurídicos nacionales existentes relacionados con servicios de entrega electrónica certificada. Dicho marco puede abrir, además, nuevas oportunidades de mercado para los prestadores de servicios de confianza de la Unión de ofrecer nuevos servicios paneuropeos de entrega electrónica certificada y garantizar que la identificación de los destinatarios se efectúe con un nivel de confianza mayor que la identificación del remitente.

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

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

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

(28) Para lograr una amplia disponibilidad y facilidad de uso de las carteras de identidad digital europea es necesario que los prestadores de servicios privados las acepten. Las partes usuarias privadas que prestan servicios en los ámbitos del transporte, la energía, los servicios bancarios y financieros, la seguridad social, la salud, el agua potable, los servicios postales, la infraestructura digital, la educación o las telecomunicaciones deben aceptar el uso de las carteras de identidad digital europea para la prestación de servicios en los casos en los que la legislación nacional, el Derecho de la Unión o una obligación contractual requieran una autenticación reforzada de los usuarios. Cuando las plataformas en línea de muy gran tamaño, según se definen en el artículo 25, apartado 1, del Reglamento [referencia a la Ley de Servicios Digitales] exijan a los usuarios autenticarse para acceder a servicios en línea, dichas plataformas deberán tener la obligación de aceptar el uso de carteras de identidad digital europea si así lo solicita voluntariamente el usuario. Los usuarios no deben tener ninguna obligación de utilizar la cartera para acceder a servicios privados, pero si desean hacerlo, las

plataformas en línea de gran tamaño deberán aceptar la cartera de identidad digital europea con ese fin, respetando en todo momento el principio de minimización de datos. Dada la importancia de las plataformas en línea de muy gran tamaño y debido a su alcance, en particular en términos de número de receptores del servicio y transacciones económicas, esto es necesario para incrementar la protección de los usuarios frente al fraude y garantizar un nivel alto de protección de datos. Es preciso desarrollar códigos de conducta de autorregulación a escala de la Unión («códigos de conducta») para contribuir a una amplia disponibilidad y facilidad de uso de los medios de identificación electrónica (en particular, de las carteras de identidad digital europea) contemplados en el ámbito de aplicación de este Reglamento. Estos códigos de conducta deben facilitar una aceptación amplia de los medios de identificación electrónica, incluidas las carteras de identidad digital europea, por parte de los prestadores de servicios que no se ajusten a la definición de plataformas de muy gran tamaño y que se apoyen en servicios de identificación electrónica de terceros para autenticar a sus usuarios. Los códigos de conducta deberán elaborarse dentro de los doce meses siguientes a la adopción de este Reglamento. La Comisión deberá evaluar la eficacia de estas disposiciones relativas a la disponibilidad y facilidad de uso de las carteras de identidad digital europea para los usuarios al cabo de dieciocho meses de su implantación, y revisar dichas disposiciones para garantizar su aceptación por medio de actos delegados en vista de la evaluación realizada.

(29) La cartera de identidad digital europea debe permitir técnicamente la divulgación selectiva de atributos a las partes usuarias. Esta función debe convertirse en una característica básica del diseño de la cartera, reforzando así la comodidad y la protección de los datos personales, en especial la minimización del tratamiento de estos datos.

(30) Los atributos proporcionados por los prestadores cualificados de servicios de confianza como parte de la declaración cualificada de atributos deberán cotejarse con las fuentes auténticas, ya sea directamente por el prestador cualificado de servicios de confianza o a través de intermediarios designados reconocidos a escala nacional, de conformidad con el Derecho nacional o de la Unión, a efectos de proteger el intercambio de los atributos declarados entre los prestadores de servicios de identidad o de declaración de atributos y las partes usuarias.

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

(32) Los servicios de autenticación de sitios web proporcionan a los usuarios la garantía de que existe una entidad auténtica y legítima que respalda la existencia del sitio web. Estos servicios contribuyen a crear confianza y fe en la realización de operaciones mercantiles en línea, dado que los usuarios se fiarán de un sitio web que haya sido autenticado. El uso de servicios de autenticación de sitios web por parte de estos últimos es voluntario. No obstante, para que la autenticación de sitios web se convierta en un medio de aumentar la confianza, proporcionar al usuario una experiencia mejor

y propiciar el crecimiento en el mercado interior, el presente Reglamento establece obligaciones mínimas de seguridad y responsabilidad para los prestadores de servicios de autenticación de sitios web y los servicios que prestan. Con este fin, los navegadores web deben garantizar la compatibilidad e interoperabilidad con los certificados cualificados para la autenticación de sitios web previstos en el Reglamento (UE) n.º 910/2014. A tal efecto, deben reconocer y mostrar certificados cualificados para la autenticación de sitios web con objeto de ofrecer un nivel alto de seguridad, lo que permitiría a los propietarios de los sitios web demostrar su identidad como propietarios de un sitio web y a los usuarios identificar a los propietarios de los sitios web con un alto grado de certeza. Para promover su uso, las autoridades públicas de los Estados miembros deben estudiar la posibilidad de incorporar certificados cualificados para la autenticación de sitios web en sus sitios web.

(33) Muchos Estados miembros han introducido requisitos nacionales para la prestación de servicios de archivo digital seguros y fiables con el objetivo de posibilitar la conservación de documentos electrónicos y de los servicios de confianza asociados a estos durante largos períodos. Para garantizar la seguridad jurídica y la confianza, es esencial proporcionar un marco jurídico que facilite el reconocimiento transfronterizo de los servicios de archivo electrónico cualificados. Dicho marco podría abrir además nuevas oportunidades de mercado para los prestadores de servicios de confianza de la Unión.

(34) Los libros mayores electrónicos cualificados graban datos de un modo que garantiza la unicidad, la autenticidad y la correcta secuenciación de las entradas de datos, así como su inviolabilidad. Un libro mayor electrónico combina el efecto de los sellos de tiempo de los datos con la certeza sobre el originador de los datos, de manera similar a las firmas electrónicas, con la ventaja adicional de que posibilita modelos de gestión más descentralizados que resulta muy adecuados para la cooperación entre múltiples partes. Por ejemplo, crea una pista de auditoría fiable para verificar la procedencia de las mercancías en el comercio transfronterizo, respalda la protección de los derechos de propiedad intelectual, dota de flexibilidad a los mercados de electricidad, ofrece una base para el desarrollo de soluciones avanzadas de identidad soberana propia y apoya unos servicios públicos más eficientes y con capacidad transformadora. Para evitar la fragmentación del mercado interior, es importante definir un marco jurídico a escala europea que permita el reconocimiento transfronterizo de servicios de confianza para la grabación de datos en libros mayores electrónicos.

(35) La certificación como prestadores cualificados de servicios de confianza debe ofrecer seguridad jurídica en los casos de uso en los que se utilicen libros mayores electrónicos. Este servicio de confianza para los libros mayores electrónicos y los libros mayores electrónicos cualificados, así como la certificación como prestadores cualificados de servicios de confianza para libros mayores electrónicos, deben respetar en todo caso la obligación de que los casos de uso cumplan el Derecho de la Unión o el Derecho nacional en conformidad con el Derecho de la Unión. Los casos de uso que conlleven el tratamiento de datos personales deben cumplir el Reglamento (UE) 2016/679. Los casos de uso relacionados con criptoactivos deben ser compatibles con todas las normas financieras, por ejemplo la Directiva relativa a los

mercados de instrumentos financieros[23], la Directiva sobre servicios de pago[24] y el futuro Reglamento relativo a los mercados de criptoactivos[25].

(36) Al objeto de evitar la fragmentación y los obstáculos derivados de unas normas y unas restricciones técnicas divergentes, y de garantizar un proceso coordinado para impedir poner en peligro la aplicación del futuro Marco para una Identidad Digital Europea, se necesita un proceso de cooperación estrecha y estructurada entre la Comisión, los Estados miembros y el sector privado. Para lograr este objetivo, los Estados miembros deberán cooperar dentro del marco establecido en la Recomendación XXX/XXXX de la Comisión (sobre un conjunto de instrumentos para adoptar un enfoque coordinado de cara a un Marco para una Identidad Digital Europea)[26] con el fin de identificar un conjunto de herramientas para el Marco para una Identidad Digital Europea. El conjunto de herramientas debe incluir una arquitectura técnica y un marco de referencia detallados, un conjunto de normas y referencias técnicas comunes y un conjunto de directrices y descripciones de prácticas idóneas que aborden, como mínimo, todos los aspectos de las funciones y la interoperabilidad de las carteras de identidad digital europea (incluidas las firmas electrónicas) y del servicio de confianza cualificado para la declaración de atributos, según lo dispuesto en el presente Reglamento. En este contexto, los Estados miembros deberán alcanzar asimismo un acuerdo sobre los elementos comunes del modelo de negocio y la estructura de las tasas de las carteras de identidad digital europea para facilitar su adopción, en particular por parte de las pequeñas y medianas empresas en un contexto transfronterizo. El contenido de las herramientas debe reflejar y evolucionar de forma paralela a los resultados del debate y del proceso de adopción del Marco para una Identidad Digital Europea.

(37) Se ha consultado al Supervisor Europeo de Protección de Datos, de conformidad con el artículo 42, apartado 1, del Reglamento (UE) 2018/1525 del Parlamento Europeo y del Consejo[27].

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

HAN ADOPTADO EL PRESENTE REGLAMENTO:

Artículo 1

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

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

---

23 Directiva 2014/65/UE del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, relativa a los mercados de instrumentos financieros y por la que se modifican la Directiva 2002/92/CE y la Directiva 2011/61/UE, Texto pertinente a efectos del EEE *(DO L 173 de 12.6.2014, p. 349)*.

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

25 Propuesta de Reglamento del Parlamento Europeo y del Consejo, relativo a los mercados de criptoactivos y por el que se modifica la Directiva 2019/1937/UE (COM/2020/593 final).

26 [Insértese la referencia una vez adoptada].

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

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

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

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 y la declaración electrónica de atributos, la gestión de dispositivos remotos de creación de firmas electrónicas y sellos electrónicos, y los libros mayores electrónicos,

d) establece las condiciones para la emisión de carteras de identidad digital europea por los Estados miembros.».

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 de identidad digital europea y a los prestadores de servicios de confianza establecidos en la Unión.»;

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

«3. El presente Reglamento no afecta al Derecho nacional o de la Unión relacionado con la celebración y validez de los contratos u otras obligaciones legales o de procedimiento relativos a requisitos específicos del sector con respecto a los efectos jurídicos subyacentes de cada formato.».

3) El artículo 3 se modifica como sigue:

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

«2) "medio de identificación electrónica", una unidad material o inmaterial, incluidas las carteras de identidad digital europea o los documentos de identidad con arreglo al Reglamento 2019/1157, que contiene datos de identificación personal y se utiliza con fines de autenticación en un servicio en línea o fuera de línea;»;

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

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

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

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

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

«16) "servicio de confianza", el servicio electrónico prestado habitualmente previo pago de un determinado importe, consistente en:

a) la creación, verificación y validación de firmas electrónicas, sellos electrónicos o sellos de tiempo electrónicos, servicios de entrega electrónica certificada, declaraciones electrónicas de atributos y certificados relativos a estos servicios;

b) la creación, verificación y validación de certificados para la autenticación de sitios web;

c) la preservación de firmas, sellos o certificados electrónicos relativos a estos servicios;

d) el archivo electrónico de documentos electrónicos;

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

f) la grabación de datos electrónicos en un libro mayor electrónico.»;

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

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

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

«23 *bis* "dispositivo cualificado remoto de creación de firmas", un dispositivo cualificado de creación de firmas utilizado por un prestador cualificado de servicios de confianza para generar, gestionar o duplicar los datos de creación de firmas electrónicas en nombre de un signatario;

23 *ter* "dispositivo cualificado remoto de creación de sellos", un dispositivo cualificado de creación de sellos utilizado por un prestador cualificado de servicios de confianza para generar, gestionar o duplicar los datos de creación de firmas electrónicas en nombre de un creador de sellos;»;

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

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

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

«41) "validación", el proceso consistente en verificar y confirmar la validez de una firma electrónica, un sello electrónico, los datos de identificación de una persona o una declaración electrónica de atributos;»;

i) se añaden los siguientes puntos 42 a 55:

«42) “cartera de identidad digital europea”, un producto y servicio que permite al usuario almacenar datos de identidad, credenciales y atributos vinculados a su identidad, con el fin de proporcionarlos a las partes usuarias a petición de estas y de utilizarlos con fines de autenticación, en línea y fuera de línea, para un servicio de conformidad con lo dispuesto en el artículo 6 *bis*, así como para crear firmas y sellos electrónicos cualificados;

43) “atributo”, un rasgo, característica o cualidad de una persona física o jurídica o de una entidad, en formato electrónico;

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

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

46) “fuente auténtica”, un repositorio o sistema, mantenido bajo la responsabilidad de un organismo del sector público o de una entidad privada, que contiene atributos acerca de una persona física o jurídica y se considera la principal fuente de dicha información, o que está reconocido como auténtico en virtud del Derecho nacional;

47) “archivo electrónico”, un servicio que garantiza la recepción, el almacenamiento, la eliminación y la transmisión de datos o documentos electrónicos para asegurar su integridad y la exactitud de su origen y sus características jurídicas a lo largo del período de conservación;

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

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

50) “autenticación reforzada de usuario”, la autenticación basada en la utilización de dos o más elementos categorizados como conocimiento del usuario, posesión e inherencia, 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;

51) “cuenta de usuario”, mecanismo que permite a un usuario acceder a servicios públicos o privados de acuerdo con los términos y condiciones establecidos por el prestador de esos servicios;

52) “credencial”, prueba que demuestra las capacidades, la experiencia, un derecho o un permiso de una persona;

53) “libro mayor electrónico”, registro electrónico inviolable de datos que garantiza la autenticidad y la integridad de los datos que contiene, la exactitud de su fecha y hora y su orden cronológico;

54) “datos personales”: cualquier información que se ajuste a la definición del artículo 4, punto 1, del Reglamento (UE) 2016/679;

55) “identificación única”, proceso por el cual se establece un vínculo entre los datos o medios de identificación de una persona y una cuenta existente perteneciente a esa misma persona.»;

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

«Artículo 5

Seudónimos en transacciones electrónicas

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

5) El título del capítulo II se sustituye por el texto siguiente:

«SECCIÓN I

IDENTIFICACIÓN ELECTRÓNICA».

6) Se suprime el artículo 6.

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

«Artículo 6 *bis*

Carteras de identidad digital europea

1. A los efectos de garantizar que todas las personas físicas y jurídicas dispongan de acceso seguro, de confianza y sin incidencias a servicios públicos y privados transfronterizos en la Unión, cada Estado miembro emitirá una cartera de identidad digital europea dentro de los doce meses siguientes a la entrada en vigor del presente Reglamento.

2. Las carteras de identidad digital europea serán emitidas:

   a) por un Estado miembro,

   b) en virtud de un mandato de un Estado miembro,

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

3. Las carteras de identidad digital europea permitirán al usuario:

   a) solicitar y obtener, almacenar, seleccionar, combinar y compartir de forma segura, transparente y rastreable por el usuario, los datos de identificación de persona jurídica y la declaración electrónica de atributos que sean necesarios para autenticarse en línea y fuera de línea con el fin de acceder a servicios públicos y privados en línea;

   b) firmar por medio de firmas electrónicas cualificadas.

4. En particular, las carteras de identidad digital:

   a) proporcionarán una interfaz común:

      1) a los prestadores cualificados y no cualificados de servicios de confianza que emitan declaraciones electrónicas de atributos cualificadas y no cualificadas, u otros certificados cualificados y no cualificados, a efectos de emitir dichas declaraciones y certificados para la cartera de identidad digital europea;

2) a las partes usuarias, para solicitar y validar datos de identificación personal y declaraciones electrónicas de atributos;

3) para la presentación de datos de identificación personal, declaraciones electrónicas de atributos u otros datos a las partes usuarias, tales como credenciales, de forma local sin necesidad de que la cartera acceda a internet;

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

b) garantizarán que los prestadores de servicios de confianza de declaraciones cualificadas de atributos no puedan recibir información alguna sobre el uso de dichos atributos;

c) 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;

d) proporcionarán un mecanismo para asegurar que la parte usuaria pueda autenticar al usuario y recibir declaraciones electrónicas de atributos;

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

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

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

b) para que las partes usuarias puedan verificar la validez de las declaraciones de atributos;

c) para que las partes usuarias y los prestadores cualificados de servicios de confianza puedan verificar la autenticidad y validez de los datos de identificación de la persona a quien se ha atribuido dicha identidad.

6. Las carteras de identidad digital europeas se emitirán en el marco de un sistema de identificación electrónica notificado con nivel de seguridad "alto". La utilización de las carteras de identidad digital europea será gratuita para las personas físicas.

7. El usuario mantendrá pleno control sobre la cartera de identidad digital europea. El emisor de la cartera de identidad digital europea no recopilará información sobre el uso de la cartera que no sea necesaria para la prestación de los servicios de esta, ni combinará datos de identificación personal u otros datos personales almacenados o relacionados con el uso de la cartera de identidad digital europea con datos personales obtenidos a través de otros servicios ofrecidos por dicho emisor o a través de servicios de terceros que no sean necesarios para la prestación de los servicios de la cartera, a menos que el usuario lo haya solicitado expresamente. Los datos personales relacionados con la provisión de carteras de identidad digital europea se conservarán en soporte físico y lógico por separado de cualesquier otros datos mantenidos. Si la cartera de identidad digital europea ha sido proporcionada por agentes privados de

conformidad con lo dispuesto en el apartado 1, letras b) y c), se aplicarán *mutatis mutandis* las disposiciones del artículo 45 *septies*, apartado 4.

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

9. El artículo 24, apartado 2, letras b), e), g) y h) se aplicará *mutatis mutandis* a los Estados miembros emisores de las carteras de identidad digital europea.

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

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

Artículo 6 *ter*

Partes usuarias de las carteras de identidad digital europea

1. Cuando las partes usuarias tengan previsto utilizar carteras de identidad digital europea emitidas con arreglo al presente Reglamento, lo comunicarán al Estado miembro en el que esté establecida la parte usuaria para garantizar la conformidad con los requisitos establecidos en el Derecho de la Unión o el Derecho nacional para la prestación de servicios específicos. Cuando comuniquen su intención de utilizar las carteras de identidad digital europea, informarán también sobre el uso que pretenden hacer de ellas.

2. Los Estados miembros aplicarán un mecanismo común para la autenticación de las partes usuarias.

3. Las partes usuarias serán responsables de llevar a cabo el procedimiento de autenticación de datos de identificación personal y de declaración electrónica de los atributos creados por las carteras de identidad digital europea.

4. Dentro de los seis meses siguientes a la entrada en vigor de este Reglamento, la Comisión establecerá especificaciones técnicas y operativas para los requisitos mencionados en los apartados 1 y 2, por medio de un acto de ejecución relativo a la implantación de las carteras de identidad digital europea, tal como prevé el artículo 6 *bis*, apartado 10.

Artículo 6 *quater*

Certificación de las carteras de identidad digital europea

1. Se presumirá que las carteras de identidad digital europea que hayan sido certificadas o para las que se haya expedido una declaración de conformidad con arreglo a un esquema de ciberseguridad en virtud del Reglamento (UE) 2019/881 y cuyas referencias se hayan publicado en el *Diario Oficial de la Unión Europea* cumplen los requisitos de ciberseguridad establecidos en el artículo 6 *bis*, apartados 3, 4 y 5, en la medida en que el certificado de ciberseguridad o la declaración de conformidad, o partes de esta, prevean estos requisitos.

2. La conformidad con los requisitos establecidos en el artículo 6 *bis*, apartados 3, 4 y 5, relacionados con las operaciones de tratamiento de datos personales realizadas por el emisor de las carteras de identidad digital europea se certificarán en virtud del Reglamento (UE) 2016/679.

3. La acreditación de la conformidad de las carteras de identidad digital europea con los requisitos establecidos en el artículo 6 *bis*, apartados 3, 4 y 5, corresponderá a organismos públicos o privados acreditados designados por los Estados miembros.

4. En un plazo máximo de seis meses a contar desde la entrada en vigor del presente Reglamento, la Comisión establecerá, por medio de actos de ejecución, una lista de normas para la certificación de las carteras de identidad digital europea a que se refiere el apartado 3.

5. Los Estados miembros comunicarán a la Comisión los nombres y direcciones de los organismos públicos o privados a que se refiere el apartado 3. La Comisión pondrá dicha información a disposición de los Estados miembros.

6. La Comisión estará facultada para adoptar actos delegados, de conformidad con el artículo 47, en lo que respecta al establecimiento de criterios específicos que deben satisfacer los organismos designados a que se refiere el apartado 3.

Artículo 6 *quinquies*

Publicación de una lista de carteras de identidad digital europea certificadas

1. Los Estados miembros informarán a la Comisión, sin dilación indebida, sobre las carteras de identidad digital europea que se hayan emitido de conformidad con el artículo 6 *bis* y que hayan sido certificadas por los organismos a que se refiere el artículo 6 *quater*, apartado 3. Asimismo, informarán a la Comisión sin dilación indebida cuando la certificación sea cancelada.

2. Sobre la base de la información recibida, la Comisión establecerá, publicará y mantendrá una lista de carteras de identidad digital europea certificadas.

3. Dentro de los seis meses siguientes a la entrada en vigor del presente Reglamento, la Comisión definirá los formatos y procedimientos aplicables a efectos del apartado 1, por medio de un acto de ejecución relativo a la implantación de las carteras de identidad digital europea, tal como prevé el artículo 6 *bis*, apartado 10.».

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

«SECCIÓN II

SISTEMAS DE IDENTIFICACIÓN ELECTRÓNICA».

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

«En virtud del artículo 9, apartado 1, los Estados miembros notificarán, en un plazo máximo de doce meses a contar desde la entrada en vigor del presente Reglamento, al menos un sistema de identificación electrónica que incluya como mínimo un medio de identificación:».

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

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

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

11) Se inserta el artículo 10 *bis* siguiente:

«Artículo 10 *bis*

Violación de la seguridad de las carteras de identidad digital europea

1. Cuando se produzca una violación o vulneración parcial que afecte a carteras de identidad digital europea emitidas en virtud del artículo 6 *bis* y de los mecanismos de validación a que se refiere el artículo 6 *bis*, letras a), b) y c), de un modo que afecte a su fiabilidad o a la de otras carteras de identidad digital europea, el Estado miembro emisor suspenderá sin dilación indebida la emisión de dichas carteras y revocará su validez, e informará de ello al resto de los Estados miembros y a la Comisión.

2. Cuando se haya subsanado la violación o la vulneración a que se refiere el apartado 1, el Estado miembro emisor restablecerá la emisión y el uso de la cartera de identidad digital europea e informará sin dilación indebida a los demás Estados miembros y a la Comisión.

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

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

5. En un plazo máximo de seis meses desde la entrada en vigor del presente Reglamento, la Comisión especificará además las medidas a que se refieren los apartados 1 y 3 por medio de un acto de ejecución relativo a la implantación de las carteras de identidad digital europea, tal como prevé el artículo 6 *bis*, apartado 10.».

12) Se inserta el artículo 11 *bis* siguiente:

«Artículo 11 *bis*

Identificación única

1. Cuando se utilicen medios de identificación electrónica notificados y las carteras de identidad digital europea para la autenticación, los Estados miembros garantizarán la identificación única.

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

3. En un plazo máximo de seis meses desde la entrada en vigor del presente Reglamento, la Comisión especificará además las medidas a que se refieren los

apartados 1 y 2 por medio de un acto de ejecución relativo a la implantación de las carteras de identidad digital europea, tal como prevé el artículo 6 *bis*, apartado 10.».

13) El artículo 12 se modifica como sigue:

a) en el apartado 3 se suprimen las letras c) y d);

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

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

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

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

14) Se inserta el artículo 12 *bis* siguiente:

«Artículo 12 *bis*

Certificación de los sistemas de identificación electrónica

1. La certificación de la conformidad de los sistemas de identificación electrónica notificados con los requisitos establecidos en el artículo 6 *bis*, el artículo 8 y el artículo 10 podrá correr a cargo de organismos públicos o privados acreditados designados por los Estados miembros.

2. La revisión por pares de los sistemas de identificación electrónica a que se refiere el artículo 12, apartado 6, letra c), no se aplicará a los sistemas de identificación electrónica (o parte de ellos) certificados de conformidad con el apartado 1. Los Estados miembros podrán utilizar un certificado o una declaración de conformidad de la Unión emitida con arreglo a un esquema europeo de certificación de la seguridad establecido en virtud del Reglamento (UE) 2019/881 para demostrar el cumplimiento, por parte de dichos esquemas, de los requisitos establecidos en el artículo 8, apartado 2, con respecto a los niveles de seguridad de los sistemas de identificación electrónica.

3. Los Estados miembros notificarán a la Comisión los nombres y direcciones del organismo público o privado a que se refiere el apartado 1. La Comisión pondrá dicha información a disposición de los Estados miembros.».

15) Tras el artículo 12 *bis*, se inserta el título siguiente:

«SECCIÓN III

USO TRANSFRONTERIZO DE MEDIOS DE IDENTIFICACIÓN ELECTRÓNICA».

16) Se insertan los artículos 12 *ter* y *quater* siguientes:

«Artículo 12 *ter*

Uso transfronterizo de carteras de identidad digital europea

1. Cuando los Estados miembros, en virtud de la normativa o las prácticas administrativas nacionales, exijan una identificación electrónica utilizando un medio de identificación electrónica y una autenticación para acceder a un servicio en línea prestado por un organismo del sector público, también aceptarán las carteras de identidad digital europea emitidas con arreglo al presente Reglamento.

2. Cuando el Derecho nacional o de la Unión exija a las partes usuarias privadas prestadoras de servicios que utilicen métodos reforzados para la autenticación de los usuarios, o cuando se requiera dicha autenticación reforzada en virtud de una obligación contractual, especialmente en los ámbitos del transporte, la energía, los servicios bancarios y financieros, la seguridad social, la sanidad, el agua potable, los servicios postales, la infraestructura digital, la educación o las telecomunicaciones, las partes usuarias privadas también aceptarán el uso de las carteras de identidad digital europea emitidas con arreglo al artículo 6 *bis*.

3. Cuando las plataformas en línea de muy gran tamaño, según se definen en el artículo 25, apartado 1, del Reglamento [referencia a la Ley de Servicios Digitales] exijan a los usuarios autenticarse para acceder a servicios en línea, también aceptarán el uso de carteras de identidad digital europea emitidas con arreglo al artículo 6 *bis*, estrictamente a petición voluntaria del usuario y respetando los atributos mínimos necesarios para el servicio en línea específico para el que se solicita la autenticación, como la acreditación de la edad.

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

5. Dentro de los dieciocho meses siguientes a la implantación de las carteras de identidad digital europea, la Comisión evaluará si, con base en datos que muestren la disponibilidad y facilidad de uso de la cartera de identidad digital europea, los prestadores adicionales de servicios en línea privados tienen la obligación de aceptar el uso de la cartera de identidad digital europea estrictamente a petición voluntaria del usuario. Los criterios de evaluación pueden incluir la dimensión de la base de usuarios, la presencia transfronteriza de prestadores de servicios, el desarrollo tecnológico y la evolución de los patrones de uso. Con base en dicha evaluación, la Comisión estará facultada para adoptar actos referentes a una revisión de los requisitos para el reconocimiento de la cartera de identidad digital europea contemplados en los puntos 1 a 4 de este artículo.

6. A efectos del presente artículo, las carteras de identidad digital europea no estarán sujetas a los requisitos mencionados en los artículos 7 y 9.

Artículo 12 *quater*

Reconocimiento mutuo de otros medios de identificación electrónica

1. Cuando sea necesaria una identificación electrónica utilizando un medio de identificación electrónica y una autenticación en virtud de la normativa o la práctica administrativa nacionales para acceder a un servicio en línea prestado por un organismo del sector público en un Estado miembro, se reconocerá en dicho Estado miembro, a efectos de la autenticación transfronteriza en dicho servicio en línea, el medio de identificación electrónica expedido en otro Estado miembro, siempre que:

   a) este medio de identificación electrónica haya sido expedido en virtud de un sistema de identificación electrónica incluido en la lista a la que se refiere el artículo 9;

   b) el nivel de seguridad de este medio de identificación electrónica corresponda a un nivel de seguridad igual o superior al nivel de seguridad requerido por el organismo del sector público para acceder a dicho servicio en línea en el Estado miembro en cuestión, y en todo caso ofrezca como mínimo un nivel de seguridad "sustancial";

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

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

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

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

«1. Sin perjuicio de lo dispuesto en el apartado 2 de este artículo, los proveedores de servicios de confianza serán responsables de los daños causados de forma intencionada o por negligencia a cualquier persona física o jurídica como consecuencia de un incumplimiento de las obligaciones que se establecen en este Reglamento y de las obligaciones de gestión de los riesgos para la ciberseguridad contempladas en el artículo 18 de la Directiva XXXX/XXXX [SRI 2].».

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

«Artículo 14

Aspectos internacionales

1. La Comisión podrá adoptar actos de ejecución, de conformidad con el artículo 48, apartado 2, en los que se definan las condiciones en las que los requisitos de un tercer país aplicables a los prestadores de servicios de confianza

establecidos en su territorio y a los servicios de confianza que prestan pueden considerarse equivalentes a los requisitos aplicables a los prestadores cualificados de servicios de confianza establecidos en la Unión y a los servicios de confianza cualificados que prestan.

2. Cuando la Comisión haya adoptado un acto de ejecución al amparo de lo dispuesto en el apartado 1 o haya celebrado un acuerdo internacional sobre el reconocimiento mutuo de servicios de confianza conforme al artículo 218 del Tratado, los servicios de confianza prestados por proveedores establecidos en el tercer país en cuestión se considerarán equivalentes a los servicios de confianza cualificados prestados por prestadores cualificados de servicios de confianza establecidos en la Unión.».

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

«Artículo 15

Accesibilidad para las personas con discapacidad

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

20) El artículo 17 se modifica como sigue:

a) el apartado 4 se modifica como sigue:

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

«c) informar a las autoridades nacionales competentes de los Estados miembros afectados, designadas en virtud de la Directiva (UE) XXXX/XXXX [SRI 2], de cualquier violación significativa de la seguridad o pérdida de integridad de la que tengan conocimiento en el desempeño de sus tareas; cuando la violación significativa de la seguridad o la pérdida de integridad afecte a otros Estados miembros, el organismo de control informará al punto de contacto único del Estado miembro en cuestión designado al amparo de la Directiva (UE) XXXX/XXXX (SRI 2);»;

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

«f) cooperar con las autoridades de control establecidas en virtud del Reglamento (UE) 2016/679, en particular, informándolas sin dilación indebida sobre los resultados de las auditorías de los prestadores cualificados de servicios de confianza, cuando se hayan violado las normas de protección de datos personales, así como sobre violaciones de la seguridad que constituyan violaciones de datos personales;»;

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

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

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

«8. En un plazo máximo de doce meses a contar desde la entrada en vigor de este Reglamento, la Comisión especificará, por medio de actos de ejecución, las tareas de las autoridades de control a que se refiere el apartado 4 y definirá los formatos y procedimientos del informe mencionado en el apartado 6. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.».

21) El artículo 18 se modifica como sigue:

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

«**Asistencia mutua y cooperación**»;

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

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

c) se añaden los apartados 4 y 5 siguientes:

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

5. Dentro de los doce meses siguientes a la entrada en vigor de este Reglamento, la Comisión establecerá, por medio de actos de ejecución, los mecanismos de procedimiento necesarios para facilitar la cooperación entre las autoridades de control a que se refiere el apartado 1.».

22) El artículo 20 se modifica como sigue:

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

«1. Los prestadores cualificados de servicios de confianza serán auditados al menos cada veinticuatro meses, corriendo con los gastos que ello genere, por un organismo de evaluación de la conformidad. La auditoría confirmará que los prestadores cualificados de servicios de confianza y los servicios de confianza cualificados que prestan cumplen

los requisitos establecidos en este Reglamento y en el artículo 18 de la Directiva (UE) XXXX/XXXX [SRI 2]. Los prestadores cualificados de servicios de confianza presentarán el informe de evaluación de la conformidad resultante al organismo de control en el plazo de tres días hábiles a contar desde su recepción.»;

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

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

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

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

Si el prestador no subsanase el incumplimiento dentro del plazo fijado por el organismo de control si procede, este, teniendo en cuenta en particular el alcance, la duración y las consecuencias del incumplimiento, podrá retirar la cualificación al prestador en cuestión o al servicio que preste, y requerirle para que cumpla —en un plazo establecido, si procede— los requisitos previstos en la Directiva XXXX/XXXX [SRI 2]. El organismo de control informará al órgano a que se refiere el artículo 22, apartado 3, a efectos de la actualización de las listas de confianza a las que se hace referencia en el artículo 22, apartado 1.

El organismo de control comunicará al prestador cualificado de servicios de confianza la retirada de su cualificación o de la cualificación del servicio de que se trate.

4. Dentro de los doce meses siguientes a la entrada en vigor del presente Reglamento, la Comisión establecerá, por medio de actos de ejecución, los números de referencia para las normas siguientes:

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

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

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

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

23) El artículo 21 se modifica como sigue:

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

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

Con el fin de verificar la conformidad del proveedor de servicios de confianza con los requisitos establecidos en el artículo 18 de la Directiva XXXX [SRI 2], el organismo de control solicitará a las autoridades competentes en virtud de la citada Directiva que lleven a cabo actuaciones de control en ese sentido y que proporcionen información sobre los resultados de dichas actuaciones en el plazo de tres días desde su finalización.

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

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

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

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

24) En el artículo 23 se añade el apartado 2 *bis* siguiente:

«2 *bis*. Los apartados 1 y 2 también serán de aplicación a los prestadores de servicios de confianza establecidos en terceros países y a los servicios que prestan, siempre y cuando hayan sido reconocidos en la Unión con arreglo a lo previsto en el artículo 14.».

25) El artículo 24 se modifica como sigue:

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

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

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

a) a través de un medio de identificación electrónica notificado que satisfaga los requisitos establecidos en el artículo 8 con respecto a los niveles de garantía "sustancial" o "alto";

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

c) utilizando cualesquier otros métodos de identificación que garanticen la identificación de la persona física 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, utilizando procedimientos adecuados y de conformidad con las leyes nacionales si no hay otros medios disponibles.»;

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

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

c) el apartado 2 se modifica como sigue:

1) la letra d) se sustituye 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;»;

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

« f *bis*) contarán con políticas adecuadas y adoptarán las medidas que procedan para gestionar los riesgos jurídicos, empresariales, operativos y otros riesgos directos o indirectos para la prestación del servicio de confianza cualificado. Sin perjuicio de lo dispuesto en el artículo 18 de la Directiva (UE) XXXX/XXX [SRI 2], tales medidas incluirán, como mínimo, las siguientes:

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

ii) medidas relacionadas con controles administrativos o de procedimiento;

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

f *ter*) notificarán al organismo de control y, cuando proceda, a otros organismos pertinentes cualquier infracción o interrupción asociada en la aplicación de las medidas a que se refiere la letra f *bis*), incisos i), ii) y iii), que tenga un impacto significativo en el servicio de confianza prestado o en los datos personales mantenidos en él.»;

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

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

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

4) se suprime la letra j);

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

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

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

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

f) se añade el apartado 6 siguiente:

«6. La Comisión estará facultada para adoptar actos delegados con respecto a las medidas adicionales a que se refiere el apartado 2, letra f *bis*).».

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

«6. Dentro de los doce meses siguientes a la entrada en vigor del presente Reglamento, la Comisión establecerá, por medio de actos de ejecución, los números de referencia de las normas para los certificados cualificados de firma electrónica. Se presumirá el cumplimiento de los requisitos establecidos en el anexo I cuando un certificado cualificado de firma electrónica se ajuste a

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

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

«1 *bis*. La creación, gestión y duplicación de datos de creación de firmas electrónicas en nombre del signatario son funciones reservadas en exclusiva a un prestador cualificado de servicios de confianza que preste un servicio de confianza cualificado para la gestión de un dispositivo cualificado remoto de creación de firmas electrónicas.».

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

«Artículo 29 *bis*

Requisitos que debe cumplir un servicio cualificado para la gestión de dispositivos remotos de creación de firmas electrónicas

1. La gestión de dispositivos cualificados remotos de creación de firmas electrónicas como servicio cualificado es una función reservada en exclusiva a un proveedor cualificado de servicios de confianza que:

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

   b) sin perjuicio de 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:

      la seguridad de los conjuntos de datos duplicados es del mismo nivel que para los conjuntos de datos originales;

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

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

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

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

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

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

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

31) El artículo 32 se modifica como sigue:

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

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

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

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

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

«Artículo 34

Servicio cualificado de conservación de firmas electrónicas cualificadas

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

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

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

33) El artículo 37 se modifica como sigue:

a) se inserta el apartado 2 *bis* siguiente:

«2 *bis*. Se presumirá el cumplimiento de los requisitos de los sellos electrónicos avanzados mencionados en el artículo 36 y en el apartado 5 del presente artículo cuando un sello electrónico avanzado se ajuste a las normas a que hace referencia el apartado 4.»;

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

«4. En un plazo máximo de doce meses a contar desde la entrada en vigor del presente Reglamento, la Comisión establecerá, por medio de actos de ejecución, los números de referencia de las normas para los sellos electrónicos avanzados. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.».

34) El artículo 38 se modifica como sigue:

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

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

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

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

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

«Artículo 39 *bis*

Requisitos que debe cumplir un servicio cualificado para la gestión de dispositivos remotos de creación de sellos electrónicos

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

36) El artículo 42 se modifica como sigue:

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

«1 *bis*. Se presumirá el cumplimiento de los requisitos establecidos en el apartado 1 cuando la vinculación de la fecha y hora con los datos y la fuente de información temporal exacta se ajuste a las normas a que se refiere el apartado 2.»;

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

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

37) El artículo 44 se modifica como sigue:

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

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

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

«2. En un plazo máximo de doce meses a contar desde la entrada en vigor del presente Reglamento, la Comisión establecerá, por medio de actos de ejecución, los números de referencia de las normas para los procesos de envío y recepción de datos. Estos actos de ejecución se adoptarán

con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.».

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

«Artículo 45

Requisitos de los certificados cualificados de autenticación de sitios web

1. Los certificados cualificados de autenticación de sitios web cumplirán los requisitos establecidos en el anexo IV. Se presumirá el cumplimiento de los requisitos establecidos en el anexo IV cuando un certificado cualificado de autenticación de sitios web se ajuste a las normas a que se refiere el apartado 3.

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

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

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

«SECCIÓN 9

DECLARACIÓN ELECTRÓNICA DE ATRIBUTOS

Artículo 45 *bis*

Efectos jurídicos de la declaración electrónica de atributos

1. No se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a una declaración electrónica de atributos por el mero hecho de estar en formato electrónico.

2. Una declaración electrónica cualificada de atributos tendrá los mismos efectos jurídicos que las declaraciones lícitamente emitidas en formato impreso.

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

Artículo 45 *ter*

Declaración electrónica de atributos en servicios públicos

Cuando la legislación nacional exija una identificación electrónica utilizando un medio de identificación electrónica y una autenticación para acceder a un servicio en línea prestado por un organismo público, los datos de identificación personal

contenidos en la declaración electrónica de atributos no sustituirán a la identificación electrónica utilizando un medio de identificación electrónica y una autenticación para la identificación electrónica a menos que el Estado miembro o el organismo público lo autoricen expresamente. En tal caso, también se aceptarán las declaraciones electrónicas cualificadas de atributos procedentes de otros Estados miembros.

Artículo 45 *quater*

Requisitos que debe cumplir la declaración cualificada de atributos

1. La declaración electrónica cualificada de atributos cumplirá los requisitos establecidos en el anexo V. Se presumirá el cumplimiento de los requisitos establecidos en el anexo V cuando una declaración electrónica cualificada de atributos se ajuste a las normas a que se refiere el apartado 4.
2. Las declaraciones electrónicas cualificadas de atributos no estarán sometidas a ningún requisito obligatorio además de los requisitos establecidos en el anexo V.
3. Si una declaración electrónica cualificada de atributos ha sido revocada después de su emisión inicial, perderá su validez desde el momento de su revocación y no podrá en ninguna circunstancia recuperar su estado.
4. Dentro de los seis meses siguientes a la entrada en vigor del presente Reglamento, la Comisión establecerá números de referencia de normas para las declaraciones electrónicas cualificadas de atributos por medio de un acto de ejecución sobre la implantación de las carteras de identidad digital europea, tal como prevé el artículo 6 *bis*, apartado 10.

Artículo 45 *quinquies*

Cotejo de atributos con fuentes auténticas

1. Los Estados miembros garantizarán que, al menos para los atributos que se enumeran en el anexo VI, cuando tales atributos se basen en fuentes auténticas pertenecientes al sector público, se adopten medidas para permitir que los proveedores cualificados de declaraciones electrónicas de atributos verifiquen por medios electrónicos, a petición del usuario, la autenticidad del atributo, cotejándolo directamente con la correspondiente fuente auténtica a escala nacional o a través de intermediarios designados reconocidos a escala nacional de conformidad con el Derecho nacional o de la Unión.
2. Dentro de los seis meses siguientes a la entrada en vigor del presente Reglamento, la Comisión, teniendo en cuenta las normas internacionales aplicables, establecerá las especificaciones técnicas, normas y procedimientos mínimos en referencia al catálogo de atributos y sistemas para la declaración de atributos y los procedimientos de verificación de declaraciones electrónicas cualificadas de atributos, por medio de un acto de ejecución relativo a la implantación de la cartera de identidad digital europea, tal como prevé el artículo 6 *bis*, apartado 10.

Artículo 45 *sexties*

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

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

Artículo 45 *septies*

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

1. Los prestadores de servicios cualificados y no cualificados de declaración electrónica de atributos se abstendrán de combinar datos personales relacionados con la prestación de dichos servicios con datos personales obtenidos a través de otros servicios que ofrezcan.
2. Los datos personales relacionados con la prestación de servicios de declaración electrónica de atributos se conservarán en soporte lógico por separado de otros datos que se mantengan.
3. Los datos personales relacionados con la prestación de servicios cualificados de declaración electrónica de atributos se conservarán (tanto en soporte físico como lógico) por separado de otros datos que se mantengan.
4. Los prestadores de servicios cualificados de declaración electrónica de atributos prestarán dichos servicios bajo una entidad jurídica separada.

SECCIÓN 10

SERVICIOS CUALIFICADOS DE ARCHIVO ELECTRÓNICO

Artículo 45 *octies*

Servicios cualificados de archivo electrónico

Solo podrá prestar un servicio cualificado de archivo electrónico un prestador cualificado de servicios de confianza que utilice procedimientos y tecnologías capaces de ampliar la fiabilidad del documento electrónico más allá del período de validez tecnológico.

Dentro de los doce meses siguientes a la entrada en vigor del presente Reglamento, la Comisión establecerá, por medio de actos de ejecución, los números de referencia de las normas para los servicios de archivo electrónico. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

SECCIÓN 11

LIBROS MAYORES ELECTRÓNICOS

Artículo 45 *nonies*

Efectos jurídicos de los libros mayores electrónicos

1. No se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a un libro mayor electrónico por el mero hecho de estar en formato electrónico o de no cumplir los requisitos de los libros mayores electrónicos cualificados.
2. Un libro mayor electrónico cualificado gozará de la presunción de unicidad y autenticidad de los datos que contiene, de la exactitud de su fecha y hora y del orden cronológico secuencial interno del libro mayor.

Artículo 45 *decies*

Requisitos de los libros mayores electrónicos cualificados

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

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

   b) garantizar la unicidad, autenticidad y correcta secuenciación de las entradas de datos grabadas en el libro mayor;

   c) garantizar el orden cronológico secuencial correcto de los datos que contiene el libro mayor y la exactitud de la fecha y la hora de la entrada de datos;

   d) grabar datos de modo que sea posible detectar de forma inmediata cualquier modificación posterior de estos.

2. Se presumirá el cumplimiento de los requisitos establecidos en el apartado 1 cuando un libro mayor electrónico se ajuste a las normas a que se refiere el apartado 3.

3. La Comisión podrá establecer, por medio de actos de ejecución, números de referencia de normas para los procesos de ejecución y registro de un conjunto de datos en un libro mayor electrónico cualificado, así como para la creación de dicho libro mayor. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.».

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

«Artículo 48 *bis*

Requisitos de información

1. Los Estados miembros garantizarán la recopilación de estadísticas relativas al funcionamiento de las carteras de identidad digital europea y los servicios de confianza cualificados.

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

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

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

   c) incidencias y tiempo de interrupción de la infraestructura a escala nacional que impidan utilizar las aplicaciones de cartera de identidad digital.

3. Las estadísticas a las 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 en el mes de marzo, los Estados miembros presentarán a la Comisión un informe sobre las estadísticas recopiladas de conformidad con el apartado 2.».

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

«Artículo 49

Revisión

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

2. El informe de evaluación incluirá una evaluación de la disponibilidad y facilidad de uso de los medios de identificación contemplados en el ámbito de aplicación del presente Reglamento, en especial las carteras de identidad digital europea, y evaluarán si todos los prestadores de servicios privados en línea que se apoyan en servicios de identificación electrónica de terceros con fines de autenticación de los usuarios tienen la obligación de aceptar el uso de los medios de identificación electrónicos notificados.

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

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

«Artículo 51

Medidas transitorias

1. Los dispositivos de creación de firmas seguras cuya conformidad se haya determinado con arreglo al artículo 3, apartado 4, de la Directiva 1999/93/CE, continuarán considerándose dispositivos cualificados de creación de firmas electrónicas en virtud del presente Reglamento hasta el [fecha; DO sírvase insertar el período de cuatro años tras la entrada en vigor del presente Reglamento].

2. Los certificados cualificados expedidos a personas físicas en virtud de la Directiva 1999/93/CE seguirán considerándose certificados cualificados de firma electrónica en virtud del presente Reglamento hasta el [fecha; DO sírvase insertar el período de cuatro años tras la entrada en vigor del presente Reglamento].».

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

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

45) El anexo III se modifica de conformidad con el anexo III del presente Reglamento.

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

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

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

Artículo 2

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

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

Hecho en Bruselas, el

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

FICHA FINANCIERA LEGISLATIVA

1. MARCO DE LA PROPUESTA/INICIATIVA

1.1. Denominación de la propuesta/iniciativa

Reglamento del Parlamento Europeo y del Consejo relativo a un marco para la identidad digital europea, por el que se modifica el Reglamento eIDAS

1.2. Ámbito(s) político(s) afectado(s)

Ámbito de actuación: Mercado interior

Una Europa adaptada a la era digital

1.3. La propuesta/iniciativa se refiere a:

☐ **una acción nueva**

☐ **una acción nueva a raíz de un proyecto piloto / una acción preparatoria**[28]

☑**la prolongación de una acción existente**

☐ **una fusión o reorientación de una o más acciones hacia otra/una nueva acción**

1.4. Objetivo(s)

1.4.1. Objetivo(s) general(es)

El objetivo general de esta iniciativa es garantizar el correcto funcionamiento del mercado interior, particularmente en relación con la prestación y utilización de servicios transfronterizos e intersectoriales públicos y privados, basados en la disponibilidad y el uso de soluciones de identidad electrónica altamente seguras y fiables. Este objetivo se inscribe en los objetivos estratégicos propuestos en la Comunicación «Configurar el futuro digital de Europa».

1.4.2. Objetivo(s) específico(s)

Objetivo específico n.º 1

Proporcionar acceso a soluciones de identidad digital fiables y seguras que se puedan utilizar a través de las fronteras y que satisfagan las expectativas de los usuarios y la demanda del mercado.

Objetivo específico n.º 2

Garantizar que los servicios públicos y privados puedan apoyarse en soluciones de identidad digital fiables y seguras a través de las fronteras.

Objetivo específico n.º 3

Proporcionar a los ciudadanos pleno control sobre sus datos personales y garantizar su seguridad cuando utilicen soluciones de identidad digital.

Objetivo específico n.º 4

Garantizar la igualdad de condiciones para la prestación de servicios de confianza cualificados en la UE y su aceptación.

[28] Tal como se contempla en el artículo 58, apartado 2, letras a) o b), del Reglamento Financiero.

1.4.3. *Resultado(s) e incidencia esperados*

Especifíquense los efectos que la propuesta/iniciativa debería tener sobre los beneficiarios / la población destinataria.

En términos generales, los principales beneficiarios previstos de la iniciativa son los usuarios finales y ciudadanos, los prestadores de servicios en línea, los proveedores de aplicaciones de cartera y los prestadores públicos y privados de servicios de identidad digital. Se espera que la iniciativa proporcione acceso a soluciones de identidad digital fiables y seguras que se puedan utilizar a través de las fronteras y que satisfagan las expectativas de los usuarios y la demanda del mercado; garantice que los servicios públicos y privados puedan apoyarse en soluciones de identidad digital fiables y seguras a través de las fronteras; proporcione a los ciudadanos pleno control sobre sus datos personales y garantice su seguridad cuando utilicen soluciones de identidad digital; y garantice la igualdad de condiciones para la prestación de servicios de confianza cualificados en la UE y su aceptación.

Además de la facilidad de acceso a servicios públicos y privados, los ciudadanos y las empresas se beneficiarán directamente de la comodidad y facilidad de uso de la interfaz de autenticación de carteras y podrán realizar transacciones que requieran todos los niveles de seguridad (por ejemplo, desde el inicio de sesión en medios sociales hasta el uso de aplicaciones de sanidad electrónica).

Un enfoque reforzado de privacidad desde el diseño podría ofrecer beneficios adicionales, puesto que la cartera no requeriría intermediarios en el proceso de declaración de los atributos, lo cual permitiría a los ciudadanos comunicarse directamente con los proveedores de servicios y de credenciales. La seguridad reforzada de los datos que ofrece la cartera impediría la usurpación de identidad, evitando de ese modo pérdidas económicas a los ciudadanos y empresas europeos.

En lo que respecta al crecimiento económico, se espera que la introducción de un sistema basado en normas reduzca la incertidumbre para los agentes del mercado y que ejerza un efecto positivo en la innovación.

Un aspecto importante, asimismo, es que se prevé que proporcione un acceso más inclusivo a los servicios públicos y privados vinculados a bienes públicos como la educación y la salud, que en la actualidad ofrecen obstáculos para el acceso de determinados grupos sociales. Por ejemplo, algunos ciudadanos con discapacidad —a menudo las personas con movilidad reducida— o residentes en zonas rurales pueden gozar de un menor nivel de acceso a servicios que normalmente requieren presencia física en el caso de que no se presten localmente.

1.4.4. *Indicadores de resultados*

Especifíquense los indicadores que permiten realizar el seguimiento de los avances y logros.

Aspecto de seguimiento y evaluación y objetivos pertinentes	Indicador	Responsabilidad de la recopilación	Fuente(s)
Solicitud			

Proporcionar acceso a medios de identidad electrónica para todos los ciudadanos de la UE	Número de ciudadanos y empresas europeos a quienes se han expedido identidades electrónicas notificadas / carteras de identidad digital europea y número de credenciales de identidad (declaraciones de atributos) expedidas.	Comisión Europea y autoridades nacionales competentes (ANC)	Encuesta anual / datos de seguimiento y evaluación recopilados por las ANC
Proporcionar acceso a medios de identidad electrónica para todos los ciudadanos de la UE	Número de ciudadanos y empresas europeos que utilizan activamente identidades electrónicas notificadas / carteras de identidad digital europea y credenciales de identidad (declaraciones de atributos)	Comisión Europea y autoridades nacionales competentes (ANC)	Encuesta anual / datos de seguimiento y evaluación recopilados por las ANC
Aumentar el reconocimiento y la aceptación transfronterizos de los sistemas de identidad electrónica, aspirando a lograr la aceptación universal	Número de prestadores de servicios en línea que aceptan identidades electrónicas notificadas/carteras de identidad digital europea y credenciales de identidad (declaraciones de atributos)	Comisión Europea	Encuesta anual
Aumentar el reconocimiento y la aceptación transfronterizos de los sistemas de identidad electrónica, aspirando a lograr la aceptación universal	Número de transacciones en línea según identidades electrónicas notificadas/carteras de identidad digital europea y credenciales de identidad (declaraciones de atributos) (totales y transfronterizas)	Comisión Europea	Encuesta anual
Estimular la adopción por parte del sector privado y el desarrollo de nuevos servicios de identidad digital	Número de nuevos servicios de declaración de atributos de declaración privada que cumplen las normas de integración en la cartera de identidad digital europea	Comisión Europea y autoridades nacionales competentes (ANC)	Encuesta anual
Información contextual			
Estimular la adopción por parte del sector privado y el desarrollo de nuevos servicios de identidad digital	Tamaño del mercado de identidades digitales	Comisión Europea	Encuesta anual

Estimular la adopción por parte del sector privado y el desarrollo de nuevos servicios de identidad digital	Gasto en el marco de la adjudicación de contratos públicos vinculado a la identidad digital	Comisión Europea y autoridades nacionales competentes	Encuesta anual
Aumentar el reconocimiento y la aceptación transfronterizos de los sistemas de identidad electrónica, aspirando a lograr la aceptación universal	Porcentaje de empresas que realizan ventas de mercancías o servicios por medio del comercio electrónico	Comisión Europea	Eurostat
Aumentar el reconocimiento y la aceptación transfronterizos de los sistemas de identidad electrónica, aspirando a lograr la aceptación universal	Proporción de transacciones en línea que requieren una identificación reforzada del cliente (total)	Comisión Europea	Encuesta anual
Proporcionar acceso a medios de identidad electrónica para todos los ciudadanos de la UE	Porcentaje de particulares que realizan transacciones de comercio electrónico Porcentaje de particulares que acceden a servicios públicos en línea	Comisión Europea	Eurostat

1.5. Justificación de la propuesta/iniciativa

1.5.1. Necesidad(es) que debe(n) satisfacerse a corto o largo plazo, incluido un calendario detallado del despliegue de la aplicación de la iniciativa

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro. Los Estados miembros estarán obligados a expedir una cartera de identidad digital europea en un plazo (a título indicativo) de veinticuatro a cuarenta y ocho meses a contar desde la adopción del Reglamento. La Comisión estará facultada para adoptar actos de ejecución por los que se establezcan las especificaciones técnicas y las normas de referencia para la arquitectura técnica del Marco para una Identidad Digital Europea en un plazo (a título indicativo) de doce a veinticuatro meses a contar desde la adopción del Reglamento.

1.5.2. Valor añadido de la intervención de la Unión (puede derivarse de distintos factores, como mejor coordinación, seguridad jurídica, mejora de la eficacia o complementariedades). A efectos del presente punto, se entenderá por «valor añadido de la intervención de la Unión» el valor resultante de una intervención de la Unión que viene a sumarse al valor que se habría generado de haber actuado los Estados miembros de forma aislada.

Motivos para actuar a escala europea (*ex ante*)

Considerando la creciente demanda de soluciones de identidad digital seguras, fáciles de usar y que garanticen la privacidad por parte de los ciudadanos, las empresas y los prestadores de servicios en línea, una intervención más amplia a escala de la UE puede ofrecer un valor mayor que la acción de los Estados miembros a título individual, como demuestra la evaluación del Reglamento eIDAS.

Valor añadido de la Unión que se espera generar (*ex post*)

Un enfoque más armonizado a escala de la UE, basado en el cambio fundamental que supone pasar de la utilización exclusiva de soluciones de identidad digital a la provisión de declaraciones electrónicas de atributos, garantizará que los ciudadanos y las empresas puedan acceder a servicios públicos y privados en cualquier parte de Europa basándose en pruebas de identidad y atributos verificados. Los prestadores de servicios en línea podrán aceptar soluciones de identidad digital con independencia de dónde se hayan expedido, apoyándose en un enfoque común a escala europea con respecto a la confianza, la seguridad y la interoperabilidad. Tanto los usuarios como los prestadores de servicios podrán beneficiarse asimismo del mismo valor jurídico otorgado a las declaraciones electrónicas de atributos en toda la UE, un aspecto particularmente importante cuando sea necesaria una acción concertada, como en lo referente a los certificados sanitarios digitales. Los servicios de confianza que proporcionan declaraciones electrónicas de atributos también se beneficiarán de la disponibilidad de un mercado europeo para sus servicios. Por ejemplo, la recuperación de los costes que conlleva garantizar un entorno altamente fiable y seguro para la prestación de servicios de confianza cualificados resulta más sencilla a escala de la UE debido a las economías de escala. Solamente es posible garantizar una total portabilidad transfronteriza de identidades legales y declaraciones electrónicas de atributos vinculadas a ellas mediante un marco a escala de la UE que permita confiar en las declaraciones de identidad realizadas por otros Estados miembros.

1.5.3. Principales conclusiones extraídas de experiencias similares anteriores

El Reglamento n.º 910/2014 (Reglamento eIDAS) es el único marco transfronterizo que regula la identificación electrónica fiable de personas físicas y jurídicas y los servicios de confianza. Si bien el Reglamento eIDAS desempeña un papel indiscutible en el mercado interior, se han producido numerosos cambios desde su adopción en 2014. Dicho Reglamento está basado en sistemas nacionales de identidad electrónica que siguen normas diversas, y se centra en un segmento relativamente reducido de las necesidades de identificación electrónica de ciudadanos y empresas: el acceso seguro transfronterizo a servicios públicos. Los servicios contemplados interesan principalmente al 3 % de la población de la UE que reside en un Estado miembro distinto de aquel en el que nació.

Desde entonces, la digitalización de todas las funciones de la sociedad ha aumentado drásticamente. La pandemia de COVID-19 también ha tenido una incidencia muy

importante en la velocidad de la digitalización. Como resultado de todo ello, la prestación de servicios, tanto públicos como privados, se realiza cada vez más por medios digitales. Los ciudadanos y las empresas esperan un nivel alto de seguridad y comodidad en sus actividades en línea, como la presentación de declaraciones tributarias, la matriculación en una universidad extranjera, la apertura a distancia de cuentas bancarias o la solicitud de préstamos, el alquiler de automóviles, la creación de empresas en otro Estado miembro, la autenticación para realizar pagos en línea, la presentación de propuestas en el marco de licitaciones en línea, etc.

En consecuencia, la demanda de medios para identificarse y autenticarse en línea, así como para intercambiar por medios digitales información relativa a nuestra identidad y nuestros atributos o cualificaciones (identidad, direcciones, edad, pero también cualificaciones profesionales, permisos de conducción y otros permisos y sistemas de pago), de manera segura y con un nivel alto de protección de datos, ha aumentado radicalmente.

Esto ha provocado un cambio de paradigma hacia soluciones avanzadas y cómodas capaces de integrar diferentes datos y certificados verificables del usuario. Los usuarios esperan contar con un entorno autodeterminado en el que se puedan llevar y compartir credenciales y atributos diversos, como por ejemplo el documento nacional de identidad electrónico, certificados profesionales, bonos de transporte públicos o, en determinados casos, incluso entradas digitales para conciertos. Son las denominadas carteras de identidad soberana propia basadas en aplicaciones, que se gestionan a través de un dispositivo móvil del usuario y le permiten acceder de forma sencilla y segura a diferentes servicios públicos y privados con un control total.

1.5.4. Compatibilidad con el marco financiero plurianual y posibles sinergias con otros instrumentos adecuados

La iniciativa apoya los esfuerzos de recuperación europeos al proporcionar a ciudadanos y empresas las herramientas que necesitan para ayudarles a realizar sus actividades cotidianas en línea de manera segura y fiable, por ejemplo cómodos servicios de identificación electrónica y servicios de confianza. Por lo tanto, está plenamente en consonancia con los objetivos del marco financiero plurianual (MFP).

Los gastos de funcionamiento deben financiarse con cargo al objetivo específico 5 del programa Europa Digital. Se calcula que se adjudicarán contratos públicos por un importe de hasta 3 o 4 millones EUR para apoyar el desarrollo de normas y especificaciones técnicas, así como para sufragar el coste de mantenimiento de los pilares fundamentales de los servicios de identidad electrónica y de los servicios de confianza. La asignación exacta de este presupuesto deberá decidirse cuando se definan los futuros programas de trabajo. Las subvenciones que apoyarán la conexión de servicios públicos y privados al ecosistema de identidad digital contribuirán en gran medida al logro de los objetivos de la propuesta. El coste para un prestador de servicios de integrar la API necesaria de la cartera de identidad electrónica se estima en unos 25 000 EUR por prestador y se trataría de un coste puntual. Si se aprueba tras el debate de la distribución del presupuesto para el próximo programa de trabajo, un presupuesto para subvenciones de hasta 0,5 millones EUR por Estado miembro respaldaría la conexión de una masa crítica de servicios.

Los gastos asociados a las reuniones de grupos de expertos relacionadas con el desarrollo de los actos de ejecución se cargarán al apartado administrativo del programa Europa Digital por un importe total de hasta 0,5 millones EUR.

Sinergias con otros instrumentos

Esta iniciativa proporcionará un marco para la prestación de servicios de identidad electrónica y servicios de confianza en la UE, un marco en el que determinados sectores puedan apoyarse para cumplir los requisitos legales que les sean de aplicación, por ejemplo relacionados con documentos de viaje digitales, permisos de conducción digitales, etc. De manera similar, la propuesta está en consonancia con los objetivos del Reglamento 2019/1157, que fortalece la seguridad de los documentos de identidad y de residencia. En virtud del presente Reglamento, los Estados miembros están obligados a implantar nuevos documentos de identidad que ofrezcan las prestaciones de seguridad actualizadas a más tardar en agosto de 2021. Una vez desarrollados, los Estados miembros podrán modernizar los nuevos documentos de identidad para que puedan ser notificados como sistemas de identidad electrónica con arreglo a la definición recogida en el Reglamento eIDAS.

La iniciativa contribuirá asimismo a la transformación del ámbito aduanero a un entorno electrónico sin papel en el contexto de la iniciativa para el desarrollo de un entorno de ventanilla única de la UE para las aduanas. Es preciso señalar, además, que la futura propuesta contribuirá a las políticas europeas de movilidad, al facilitar el cumplimiento de los requisitos legales de información de los operadores marítimos definidos en el contexto del entorno europeo de ventanilla única europea marítima, que comenzará a aplicarse a partir del 15 de agosto de 2025. Lo anterior también es válido para la articulación con el Reglamento sobre información electrónica relativa al transporte de mercancías, que obliga a las autoridades de los Estados miembros a acepar información electrónica sobre los transportes de mercancías. La aplicación de la cartera de identidad digital europea también podrá gestionar las credenciales relacionadas con los conductores, los vehículos y las operaciones, exigidas en virtud del marco jurídico de la UE en el ámbito del transporte por carretera (por ejemplo, permisos de conducción digitales; Directiva 2006/126/CE). Las especificaciones se desarrollarán con mayor detalle en el contexto de este marco. La futura iniciativa podría contribuir asimismo a definir las iniciativas futuras en el terreno de la coordinación de la seguridad social, como el posible desarrollo de una tarjeta europea de seguridad social, que podría basarse en las características de confianza que ofrecen las identidades notificadas en el marco del Reglamento eIDAS.

Esta iniciativa apoya la aplicación del RGPD (Reglamento 2016/679), al otorgar al usuario pleno control sobre la forma en que se utilizan sus datos personales. Además, es fuertemente complementaria con el nuevo Reglamento sobre la Ciberseguridad y sus esquemas comunes de certificación de la ciberseguridad. Por otra parte, la necesidad que emana del Reglamento eIDAS de una identidad única en el contexto del internet de las cosas (IdC) garantiza la coherencia con el Reglamento sobre la Ciberseguridad y con la necesidad de englobar una mayor variedad de agentes además de a las personas y empresas, como máquinas, objetos, proveedores y dispositivos de IdC.

El Reglamento relativo a la pasarela digital única también incluye importantes puntos de conexión con esta iniciativa y está en consonancia con ella. El objetivo de dicho Reglamento es alcanzar la plena modernización de los servicios administrativos públicos y facilitar el acceso en línea a la información, los procedimientos administrativos y los servicios de asistencia que necesitan los ciudadanos y las empresas cuando residen o desarrollan actividades en otro país de la UE. Esta iniciativa proporciona una serie de elementos esenciales para respaldar los objetivos

de poner en práctica el principio de «solo una vez» en el marco de la pasarela digital única.

Además, es congruente con la Estrategia Europea de Datos y con la propuesta relativa a una Ley de Gobernanza de Datos, al proporcionar un marco para apoyar las aplicaciones impulsadas por datos en los casos en que se exija la transmisión de datos de identidad personales, puesto que permite que los usuarios mantengan el control sobre los datos y actúen de manera plenamente anonimizada.

1.5.5. Evaluación de las diferentes opciones de financiación disponibles, incluidas las posibilidades de reasignación

La iniciativa se apoyará en los pilares fundamentales de los servicios de identidad electrónica y los servicios de confianza desarrollados en el marco del Mecanismo «Conectar Europa» (MCE) y que se están integrando en el programa Europa Digital.

Los Estados miembros pueden solicitar además financiación al Mecanismo de Recuperación y Resiliencia (MRR) para la creación o mejora de la infraestructura necesaria.

1.6. Duración e incidencia financiera de la propuesta/iniciativa

☐ **duración limitada**

☐ en vigor desde [el] [DD.MM]AAAA hasta [el] [DD.MM]AAAA

☐ incidencia financiera desde AAAA hasta AAAA para los créditos de compromiso y desde AAAA hasta AAAA para los créditos de pago.

☑ **duración ilimitada**

Ejecución: fase de puesta en marcha desde AAAA hasta AAAA

y pleno funcionamiento a partir de la última fecha.

1.7. Modo(s) de gestión previsto(s)[29]

☑ **Gestión directa** a cargo de la Comisión

☑ por sus servicios, incluido su personal en las Delegaciones de la Unión;

☐ por las agencias ejecutivas

☐ **Gestión compartida** con los Estados miembros

☐ **Gestión indirecta** mediante delegación de tareas de ejecución presupuestaria en:

☐ terceros países o los organismos que estos hayan designado;

☐ organizaciones internacionales y sus agencias (especifíquense);

☐ el Banco Europeo de Inversiones (BEI) y el Fondo Europeo de Inversiones;

☐ los organismos a que se hace referencia en los artículos 70 y 71 del Reglamento Financiero;

☐ organismos de Derecho público;

☐ organismos de Derecho privado investidos de una misión de servicio público, en la medida en que presenten garantías financieras suficientes;

☐ organismos de Derecho privado de un Estado miembro a los que se haya encomendado la ejecución de una colaboración público-privada y que presenten garantías financieras suficientes;

☐ personas a quienes se haya encomendado la ejecución de acciones específicas en el marco de la política exterior y de seguridad común (PESC), de conformidad con el título V del Tratado de la Unión Europea, y que estén identificadas en el acto de base correspondiente.

Si se indica más de un modo de gestión, facilítense los detalles en el recuadro de observaciones.

Observaciones

[…]
[…]

[29] Las explicaciones sobre los modos de gestión y las referencias al Reglamento Financiero pueden consultarse en el sitio BudgWeb: https://myintracomm.ec.europa.eu/budgweb/ES/man/budgmanag/Pages/budgmanag.aspx.

2. MEDIDAS DE GESTIÓN

2.1. Disposiciones en materia de seguimiento e informes

Especifíquense la frecuencia y las condiciones de dichas disposiciones.

El Reglamento se revisará por primera vez dos años después de su plena aplicación y posteriormente cada cuatro años. La Comisión deberá informar sobre las constataciones al Parlamento Europeo y al Consejo.

Además, en el contexto de la aplicación de las medidas, los Estados miembros recopilarán estadísticas acerca del uso y funcionamiento de la cartera de identidad digital europea y los servicios de confianza cualificados. Estas estadísticas se recopilarán en un informe que se presentará a la Comisión con frecuencia anual.

2.2. Sistema(s) de gestión y de control

2.2.1. Justificación del modo o los modos de gestión, el mecanismo o los mecanismos de ejecución de la financiación, las modalidades de pago y la estrategia de control propuestos

El Reglamento establece normas más armonizadas para la prestación de servicios de identidad electrónica y de servicios de confianza en el mercado interior, garantizando al mismo tiempo el respeto de la confianza y el control de los usuarios sobre sus propios datos. Estas nuevas normas exigen desarrollar especificaciones técnicas y normas, así como supervisar y coordinar las actividades de las autoridades nacionales. Además, los pilares fundamentales conexos de la identidad electrónica, la firma electrónica, etc., se gestionarán y proporcionarán dentro del marco del programa Europa Digital. Es necesario tener en consideración, asimismo, los recursos necesarios para comunicarse con terceros países y negociar acuerdos con ellos sobre el reconocimiento mutuo de los servicios de confianza.

Para que puedan afrontar estas tareas, es necesario dotar de recursos apropiados a los servicios de la Comisión. Se calcula que la ejecución del nuevo Reglamento requerirá once trabajadores EJC; cuatro o cinco para tareas jurídicas, cuatro o cinco centrados en el trabajo técnico y dos para la coordinación, la difusión internacional y el apoyo administrativo.

2.2.2. Información relativa a los riesgos detectados y al sistema o sistemas de control interno establecidos para mitigarlos

Uno de los principales problemas causantes de las deficiencias del marco legislativo actualmente en vigor es la falta de armonización de los sistemas nacionales. Para superar este problema en la iniciativa actual se dará una gran importancia a las normas de referencia y las especificaciones técnicas que se definirán en los correspondientes actos de ejecución.

En la elaboración de dichos actos de ejecución, la Comisión contará con el apoyo de un grupo de expertos. Además, la Comisión iniciará con carácter inmediato una colaboración con los Estados miembros para alcanzar un acuerdo sobre la naturaleza técnica del futuro sistema, con objeto de prevenir una mayor fragmentación durante la negociación de la propuesta.

2.2.3. Estimación y justificación de la eficiencia de los controles (ratio «gastos de control ÷ valor de los correspondientes fondos gestionados») y evaluación del nivel esperado de riesgo de error (al pago y al cierre)

En lo relativo a los gastos de reuniones del grupo de expertos, debido al reducido valor por transacción (p. ej., el reembolso de los gastos de viaje de un delegado que participe en una reunión si esta es presencial), los procedimientos internos de control normalizados parecen suficientes.

De igual modo, los procedimientos normalizados de la Dirección General de Redes de Comunicación, Contenido y Tecnologías (DG CNECT) deberían ser suficientes para los proyectos piloto que se ejecuten en el marco del programa Europa Digital.

2.3. Medidas de prevención del fraude y de las irregularidades

Especifíquense las medidas de prevención y protección existentes o previstas, por ejemplo, en la estrategia de lucha contra el fraude.

Las medidas existentes de prevención del fraude aplicables a la Comisión cubrirán los créditos adicionales necesarios para el presente Reglamento.

3. INCIDENCIA FINANCIERA ESTIMADA DE LA PROPUESTA/INICIATIVA

3.1. Rúbrica(s) del marco financiero plurianual y línea(s) presupuestaria(s) de gastos afectada(s)

Líneas presupuestarias existentes

En el orden de las rúbricas del marco financiero plurianual y las líneas presupuestarias.

Rúbrica del marco financiero plurianual	Línea presupuestaria	Tipo de gasto	Contribución			
	Número	CD/CND[30]	de países de la AELC[31]	de países candidatos 32	de terceros países	a efectos de lo dispuesto en el artículo 21, apartado 2, letra b), del Reglamento Financiero
2	02 04 05 01 Despliegue	CD/	SÍ	NO	/NO	NO
2	02 01 30 01 Gasto de apoyo para el programa Europa Digital	ND				
7	20 02 06 Gastos administrativos	ND	NO			

Nuevas líneas presupuestarias solicitadas

En el orden de las rúbricas del marco financiero plurianual y las líneas presupuestarias.

Rúbrica del marco financiero plurianual	Línea presupuestaria	Tipo de gasto	Contribución			
	Número	CD/CND	de países de la AELC	de países candidatos	de terceros países	a efectos de lo dispuesto en el artículo 21, apartado 2, letra b), del Reglamento Financiero
	[XX.YY.YY.YY]		SÍ/NO	SÍ/NO	SÍ/NO	SÍ/NO

30 CD = créditos disociados / CND = créditos no disociados.

31 AELC: Asociación Europea de Libre Comercio.

32 Países candidatos y, en su caso, candidatos potenciales de los Balcanes Occidentales.

3.2. Incidencia financiera estimada de la propuesta en los créditos

3.2.1. Resumen de la incidencia estimada en los créditos de operaciones

☐ La propuesta/iniciativa no exige la utilización de créditos de operaciones

☑ La propuesta/iniciativa exige la utilización de créditos de operaciones, tal como se explica a continuación:

En millones EUR (al tercer decimal)

Rúbrica del marco financiero plurianual	Número	2

DG: CNECT			Año **2022**	Año **2023**	Año **2024**	Año **2025**	Año **2026**	Año **2027**		**TOTAL**
○Créditos de operaciones				La asignación del presupuesto se decidirá durante la formulación de los programas de trabajo. Las cantidades indicadas corresponden a los importes mínimos necesarios para el mantenimiento y la modernización[33].						
Línea presupuestaria[34] 02 04 05	Compromisos	(1a)	2,000	4,000	4,000	4,000	4,000	4,000		**22,000**
	Pagos	(2a)	1,000	3,000	4,000	4,000	4,000	4,000	2,000	**22,000**
Línea presupuestaria	Compromisos	(1b)								
	Pagos	(2b)								
Créditos de carácter administrativo financiados mediante la dotación de programas específicos[35]										
Línea presupuestaria 02 01 03 01		(3)	**0,048**	**0,144**	**0,144**	**0,072**	**0,072**	**0,072**		**0,552**
TOTAL de los créditos	Compromisos	= 1a + 1b +3	2,048	4,144	4,144	4,072	4,072	**4,072**		**22,552**

33 En el caso de que el coste real supere las cantidades indicadas, los costes se financiarán con cargo a 02 04 05 01.

34 Según la nomenclatura presupuestaria oficial.

35 Asistencia técnica o administrativa y gastos de apoyo a la ejecución de programas o acciones de la UE (antiguas líneas «BA»), investigación indirecta, investigación directa.

para la DG CNECT	Pagos	= 2a + 2b +3	1,048	3,144	4,144	4,072	4,072	**4,072**	**2,000**	**22,552**

○ TOTAL de los créditos de operaciones	Compromisos	(4)	2,000	4,000	4,000	4,000	4,000	4,000		**22,000**
	Pagos	(5)	1,000	3,000	4,000	4,000	4,000	4,000	2,000	**22,000**
○ TOTAL de los créditos de carácter administrativo financiados mediante la dotación de programas específicos		(6)	**0,048**	**0,144**	**0,144**	**0,072**	**0,072**	**0,072**		**0,552**
TOTAL de los créditos para la RÚBRICA 2 del marco financiero plurianual	Compromisos	= 4 + 6	2,048	4,144	4,144	4,072	4,072	**4,072**		**22,552**
	Pagos	= 5 + 6	0,048	4,144	4,144	4,072	4,072	**4,072**	**2,000**	**22,552**

Rúbrica del marco financiero plurianual	**7**	«Gastos administrativos»

Esta sección debe rellenarse utilizando los «datos presupuestarios de carácter administrativo» que deben introducirse primero en el anexo de la ficha financiera legislativa (anexo V de las normas internas), que se carga en DECIDE a efectos de consulta entre servicios.

En millones EUR (al tercer decimal)

		Año **2022**	Año **2023**	Año **2024**	Año **2025**	Año **2026**	Año **2027**	**TOTAL**
DG: CNECT								
○ Recursos humanos		0,776	1,470	1,470	1,470	1,470	1,318	**7,974**
○ Otros gastos administrativos		0,006	0,087	0,087	0,087	0,016	0,016	**0,299**
TOTAL para la DG CNECT	Créditos	0,782	1,557	1,557	1,557	1,486	1,334	**8,273**

TOTAL de los créditos para la RÚBRICA 7 del marco financiero plurianual	(Total de los compromisos = total de los pagos)	0,782	1,557	1,557	1,557	1,486	1,334	**8,273**

En millones EUR (al tercer decimal)

		Año **2022**	Año **2023**	Año **2024**	Año **2025**	Año **2026**	Año **2027**		**TOTAL**
TOTAL de los créditos para las RÚBRICAS 1 a 7 del marco financiero plurianual	Compromisos	2,830	5,701	5,701	5,629	5,558	5,408		**30,825**
	Pagos	1,830	4,701	5,701	5,629	5,558	5,406	2,000	**30,825**

3.2.2. Resultados estimados financiados con créditos de operaciones

Créditos de compromiso en millones EUR (al tercer decimal)

Indíquense los objetivos y los resultados ⇩			Año **2022**		Año **2023**		Año **2024**		Año **2025**		Año **2026**		Año **2027**		**TOTAL**	
	Tipo[36]	Coste medio	Nº.	Coste	Nº.	Coste	Nº.	Coste	Nº.	Coste	Nº.	Coste	Nº.	Coste	Número total	Coste total
OBJETIVO ESPECÍFICO N.º 1[37]…	Proporcionar acceso a soluciones de identidad digital fiables y seguras que se puedan utilizar a través de las fronteras y que satisfagan las expectativas de los usuarios y la demanda del mercado															
Encuestas/estudios anuales			1	0,050	1	0,050	1	0.050.	1	0,050	1	0,050	1	0,050	6	0,300
Subtotal del objetivo específico n.º 1			1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300
OBJETIVO ESPECÍFICO N.º 2	Garantizar que los servicios públicos y privados puedan apoyarse en soluciones de identidad digital fiables y seguras a través de las fronteras															
Encuestas/estudi			1	0,050	1	0,050	1	0.050.	1	0,050	1	0,050	1	0,050	6	0,300
Subtotal del objetivo específico n.º 2			1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300
OBJETIVO ESPECÍFICO N.º 3	Proporcionar a los ciudadanos pleno control sobre sus datos personales y garantizar su seguridad cuando utilicen soluciones de identidad digital															
Encuestas/estudi			1	0,050	1	0,050	1	0.050.	1	0,050	1	0,050	1	0,050	6	0,300
Subtotal del objetivo específico n.º 3			1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300

[36] Los resultados son productos y servicios que deben suministrarse (por ejemplo, número de intercambios de estudiantes financiados, número de kilómetros de carreteras construidos, etc.).

[37] Tal como se describe en el punto 1.4.2. «Objetivo(s) específico(s)…».

OBJETIVO ESPECÍFICO N.º 4			Garantizar la igualdad de condiciones para la prestación de servicios de confianza cualificados en la UE y su aceptación.												
Encuestas/estudi			1	0,050	1	0,050	1	0.050.	1	0,050	1	0,050	1	0,050	6	0,300
Subtotal del objetivo específico n.º 4			1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300
TOTAL			4	0,200	4	0,200	4	0,200	4	0,200	4	0,200	4	0,200	24	1,200

3.2.3. Resumen de la incidencia estimada en los créditos administrativos

☐ La propuesta/iniciativa no exige la utilización de créditos de carácter administrativo.

☑ La propuesta/iniciativa exige la utilización de créditos de carácter administrativo, tal como se explica a continuación:

En millones EUR (al tercer decimal)

	Año **2022**	Año **2023**	Año **2024**	Año **2025**	Año **2026**	Año **2027**	**TOTAL**
RÚBRICA 7 del marco financiero plurianual							
Recursos humanos	0,776	1,470	1,470	1,470	1,470	1,318	**7,974**
Otros gastos administrativos	0,006	0,087	0,087	0,087	0,0162	0,0162	**0,299**
Subtotal para la RÚBRICA 7 del marco financiero plurianual	0,782	1,557	1,557	1,557	1,486	1,334	**8,273**

al margen de la RÚBRICA 7[38] **del marco financiero plurianual**							
Recursos humanos							
Otros gastos de carácter administrativo Inclúyanse los costes administrativos en el programa Europa Digital	0,048	0,144	0,144	0,072	0,072	**0,072**	**0.552**
Subtotal al margen de la RÚBRICA 7 del marco financiero plurianual	0,048	0,144	0,144	0,072	0,072	**0,072**	**0.552**

TOTAL	**0,830**	**1,701**	**1,701**	**1,629**	**1,558**	**1,406**	**8,825**

Los créditos necesarios para recursos humanos y otros gastos de carácter administrativo se cubrirán mediante créditos de la DG ya asignados a la gestión de la acción o reasignados dentro de la DG, que se complementarán, en caso necesario, con cualquier dotación adicional que pudiera asignarse a la DG gestora en el marco del procedimiento de asignación anual y a la luz de los imperativos presupuestarios existentes.

[38] Asistencia técnica o administrativa y gastos de apoyo a la ejecución de programas o acciones de la UE (antiguas líneas «BA»), investigación indirecta, investigación directa.

3.2.4. Necesidades estimadas de recursos humanos

☐ La propuesta/iniciativa no exige la utilización de recursos humanos.

☑ La propuesta/iniciativa exige la utilización de recursos humanos, tal como se explica a continuación:

Estimación que debe expresarse en unidades de equivalente a jornada completa

		Año **2022**	Año **2023**	Año **2024**	Año **2025**	Año **2026**	Año **2027**
20 01 02 01 (Sede y Oficinas de Representación de la Comisión)		4	8	8	8	8	7
20 01 02 03 (Delegaciones)							
01 01 01 01 (Investigación indirecta)							
01 01 01 11 (Investigación directa)							
Otras líneas presupuestarias (especifíquense)							
20 02 01 (AC, ENCS, INT de la dotación global)		2	3	3	3	3	3
20 02 03 (AC, AL, ENCS, INT y JED en las Delegaciones)							
XX 01 xx **yy zz** [39]	- en la sede						
	- en las delegaciones						
01 01 01 02 (AC, ENCS, INT; investigación indirecta)							
01 01 01 12 (AC, INT, ENCS; investigación directa)							
Otras líneas presupuestarias (especifíquense)							
TOTAL		**6**	**11**	**11**	**11**	**11**	**10**

XX es el ámbito político o título presupuestario en cuestión.

Las necesidades en materia de recursos humanos las cubrirá el personal de la DG ya destinado a la gestión de la acción o reasignado dentro de la DG, que se complementará, en caso necesario, con cualquier dotación adicional que pudiera asignarse a la DG gestora en el marco del procedimiento de asignación anual y a la luz de los imperativos presupuestarios existentes.

Descripción de las tareas que deben llevarse a cabo:

Funcionarios y agentes temporales	Los funcionarios llevarán a cabo principalmente tareas jurídicas, actividades de coordinación y negociaciones con terceros países y organismos en relación con el reconocimiento mutuo de los servicios de confianza.
Personal externo	Los expertos nacionales deberán prestar apoyo en la configuración técnica y funcional del sistema. AC deberá prestar asistencia asimismo en tareas técnicas, incluida la gestión de los principales componentes del sistema.

[39] Por debajo del límite de personal externo con cargo a créditos de operaciones (antiguas líneas «BA»).

3.2.5. Compatibilidad con el marco financiero plurianual vigente

La propuesta/iniciativa:

☑ puede ser financiada en su totalidad mediante una redistribución dentro de la rúbrica correspondiente del marco financiero plurianual (MFP).

Explíquese la reprogramación requerida, precisando las líneas presupuestarias afectadas y los importes correspondientes. Facilite un cuadro Excel en el caso de que se lleve a cabo una importante reprogramación.

☐ requiere el uso del margen no asignado con cargo a la rúbrica pertinente del MFP o el uso de los instrumentos especiales tal como se define en el Reglamento del MFP.

Explíquese qué es lo que se requiere, precisando las rúbricas y líneas presupuestarias afectadas, los importes correspondientes y los instrumentos cuya utilización se propone.

☐ requiere una revisión del MFP.

Explíquese qué es lo que se requiere, precisando las rúbricas y líneas presupuestarias afectadas y los importes correspondientes.

3.2.6. Contribución de terceros

La propuesta/iniciativa:

☑ no prevé la cofinanciación por terceros

☐ prevé la cofinanciación por terceros que se estima a continuación:

Créditos en millones EUR (al tercer decimal)

	Año **N**[40]	Año **N+1**	Año **N+2**	Año **N+3**	Insértense tantos años como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6)			Total
Especifíquese el organismo de cofinanciación								
TOTAL de los créditos cofinanciados								

[40] El año N es el año de comienzo de la ejecución de la propuesta/iniciativa. Sustitúyase «N» por el primer año de aplicación previsto (por ejemplo: 2021). Hágase lo mismo con los años siguientes.

3.3. Incidencia estimada en los ingresos

☑ La propuesta/iniciativa no tiene incidencia financiera en los ingresos.

☐ La propuesta/iniciativa tiene la incidencia financiera que se indica a continuación:

☐ en los recursos propios

☐ en otros ingresos

indíquese si los ingresos se asignan a las líneas de gasto ☐

En millones EUR (al tercer decimal)

Línea presupuestaria de ingresos:	Créditos disponibles para el ejercicio presupuestario en curso	Incidencia de la propuesta/iniciativa[41]						
		Año **N**	Año **N+1**	Año **N+2**	Año **N+3**	Insértense tantos años como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6)		
Artículo …….								

En el caso de los ingresos asignados, especifíquese la línea o líneas presupuestarias de gasto en la(s) que repercutan.

[…]

Otras observaciones (por ejemplo, método/fórmula que se utiliza para calcular la incidencia en los ingresos o cualquier otra información).

[…]

[41] Por lo que se refiere a los recursos propios tradicionales (derechos de aduana, cotizaciones sobre el azúcar), los importes indicados deben ser importes netos, es decir, importes brutos una vez deducido el 20 % de los gastos de recaudación.

ANEXO
de la FICHA FINANCIERA LEGISLATIVA

Denominación de la propuesta/iniciativa:

Propuesta de Reglamento sobre un marco para la identidad digital europea, por el que se modifica el Reglamento eIDAS

1. NÚMERO Y COSTE DE LOS RECURSOS HUMANOS QUE SE CONSIDERAN NECESARIOS

2. COSTE DE LOS DEMÁS GASTOS ADMINISTRATIVOS

3. COSTES ADMINISTRATIVOS TOTALES

4. MÉTODOS DE CÁLCULO UTILIZADOS PARA LA ESTIMACIÓN DE LOS COSTES

4.1. Recursos humanos

4.2. Otros gastos administrativos

El presente anexo debe acompañar a la ficha financiera legislativa en el momento del lanzamiento de la consulta interservicios.

Los cuadros de datos se utilizan como fuente para los cuadros contenidos en la ficha financiera legislativa. Son únicamente para su uso interno dentro de la Comisión.

1) Coste de los recursos humanos que se consideran necesarios

☐ La propuesta/iniciativa no exige la utilización de recursos humanos

☑ La propuesta/iniciativa exige la utilización de recursos humanos, tal como se explica a continuación:

En millones EUR (al tercer decimal)

HEADING 7 of the multiannual financial framework		Year 2022		Year 2023		Year 2024		Year 2025		Year 2026		Year 2027		TOTAL	
		FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations
• Establishment plan posts (officials and temporary staff)															
20 01 02 01 - Headquarters and Representation offices	AD	4	608	7	1.064	7	1.064	7	1.064	7	1.064	6	912	38	5.776
	AST	0	-	1	152	1	152	1	152	1	152	1	152	5	760
20 01 02 03 - Union Delegations	AD														
	AST														
External staff [1]															
20 02 01 and 20 02 02 – External personnel – Headquarters and Representation offices	AC	1	82	1	82	1	82	1	82	1	82	1	82	6	492
	END	1	86	2	172	2	172	2	172	2	172	2	172	11	946
	INT														
20 02 03 – External personnel - Union Delegations	AC														
	AL														
	END														
	INT														
	JPD														
Other HR related budget lines (*specify*)															
Subtotal HR – HEADING 7		6	776	11	1.470	11	1.470	11	1.470	11	1.470	10	1.318	60	7.974

4.3. Las necesidades en materia de recursos humanos las cubrirá el personal de la DG ya destinado a la gestión de la acción o reasignado dentro de la DG, que se complementará, en caso necesario, con cualquier dotación adicional que pudiera asignarse a la DG gestora en el marco del procedimiento de asignación anual y a la luz de los imperativos presupuestarios existentes.

4.4.

4.5.

Al margen de la RÚBRICA 7 del marco financiero plurianual		**Año 2022**		**Año 2023**		**Año 2024**		**Año 2025**		**Año 2026**		**Año 2027**		**TOTAL**	
		EJC	Créditos	EJC	Créditos	EJC	Créditos	EJC	Créditos	EJC	Créditos	EJC	Créditos	EJC	Créditos
01 01 01 01 (investigación indirecta)[42] 01 01 01 11 (Investigación directa) Otra (especifíquese)	DA														
	AST														
Personal externo con cargo a créditos de operaciones (antiguas líneas «BA»).	- en la sede	CA													
		ENCS													
		INT													
	- en Delegaciones de la Unión	CA													
		AL													
		ENCS													
		INT													
		JPD													
01 01 01 02 (investigación indirecta) 01 01 01 12 (investigación directa) Otra (especifíquese)[43]	CA														
	ENCS														
	INT														

[42] Selecciónese la línea presupuestaria pertinente o especifíquese otra en caso necesario; si la propuesta afecta a más líneas presupuestarias, deberá diferenciarse el personal por cada línea presupuestaria afectada.

[43] Selecciónese la línea presupuestaria pertinente o especifíquese otra en caso necesario; si la propuesta afecta a más líneas presupuestarias, deberá diferenciarse el personal por cada línea presupuestaria afectada.

Otras líneas presupuestarias relacionadas con los recursos humanos (*especifíquense*)															
Subtotal RR. HH. al margen de la RÚBRICA 7															
Total RR. HH. (todas las rúbricas del MFP)		6	0,776	11	1,470	11	1,470	11	1,470	11	1,470	10	1,318	60	7,974

Las necesidades en materia de recursos humanos las cubrirá el personal de la DG ya destinado a la gestión de la acción o reasignado dentro de la DG, que se complementará, en caso necesario, con cualquier dotación adicional que pudiera asignarse a la DG gestora en el marco del procedimiento de asignación anual y a la luz de los imperativos presupuestarios existentes.

4.6. Coste de los demás gastos administrativos

4.7. ☐ La propuesta/iniciativa no exige la utilización de créditos administrativos

4.8. ☑ La propuesta/iniciativa exige la utilización de créditos administrativos, tal como se explica a continuación:

En millones EUR (al tercer decimal)

RÚBRICA 7 del marco financiero plurianual	Año 2022	Año 2023	Año 2024	Año 2025	Año 2026	Año 2027	Total
En la sede o dentro del territorio de la UE:							
20 02 06 01 - Gastos de misiones y de representación	0,006	0,015	0,015	0,015	0,015	0,015	**0,081**
20 02 06 02 - Gastos de conferencias y reuniones							
20 02 06 03 - Comités[44]		0,072	0,072	0,072	0,0012	0,012	**0,218**
20 02 06 04 - Estudios y consultas							
20 04 - Gasto en TI (institucional)[45]							
Otras líneas presupuestarias no relacionadas con los recursos humanos (*especifíquense cuando sea necesario*)							
En las Delegaciones de la Unión:							
20 02 07 01 - Gastos de misiones, conferencias y representación							
20 02 07 02 - Formación complementaria del personal							
20 03 05 - Infraestructura y logística							
Otras líneas presupuestarias no relacionadas con los recursos humanos (*especifíquense cuando sea necesario*)							
Subtotal Otros de la RÚBRICA 7 del marco financiero plurianual	0,006	0,087	0,087	0,087	0,016	0,016	**0,299**

44 Especifíquese el tipo de comité y el grupo al que pertenece.

45 Se requiere el dictamen del equipo de inversiones en TI de la DG DIGIT [véanse las Directrices sobre la financiación de TI, C(2020)6126 final de 10.9.2020, p. 7].

En millones EUR (al tercer decimal)

Al margen de la RÚBRICA 7 del marco financiero plurianual	**Año 2022**	**Año 2023**	**Año 2024**	**Año 2025**	**Año 2026**	**Año 2027**	**Total**
Gastos en asistencia técnica y administrativa (con exclusión del personal externo) con cargo a créditos operativos (antiguas líneas «BA»):	0,048	0,144	0,144	0,072	0,072	0,072	**0,552**
- en la sede							
- en Delegaciones de la Unión							
Otros gastos de gestión en el ámbito de la investigación							
Gasto estratégico en TI en programas operativos[46]							
Gasto institucional en TI en programas operativos[47]							
Otras líneas presupuestarias no relacionadas con los recursos humanos (*especifíquense cuando sea necesario*)							
Subtotal Otros al margen de la RÚBRICA 7 del marco financiero plurianual	0,048	0,144	0,144	0,072	0,072	0,072	**0,552**
Total Otros gastos administrativos (todas las rúbricas del MFP)	0,054	0,231	0,231	0,159	0,088	0,088	0,851

[46] Se requiere el dictamen del equipo de inversiones en TI de la DG DIGIT [véanse las Directrices sobre la financiación de TI, C(2020)6126 final de 10.9.2020, p. 7].

[47] Esta partida incluye sistemas administrativos locales y contribuciones a la cofinanciación de sistemas institucionales TI [véanse las Directrices sobre la financiación de TI, C(2020)6126 final de 10.9.2020].

5. COSTES ADMINISTRATIVOS TOTALES (TODAS LAS RÚBRICAS DEL MFP)

En millones EUR (al tercer decimal)

Resumen	Año 2022	Año 2023	Año 2024	Año 2025	Año 2026	Año 2027	Total
Rúbrica 7 - Recursos humanos	0,776	1,470	1,470	1,470	1,470	1,318	**7,974**
Rúbrica 7 - Otros gastos administrativos	0,006	0,087	0,087	0,087	0,016	0,016	**0,218**
Subtotal Rúbrica 7							
Al margen de la rúbrica 7 - Recursos humanos							
Al margen de la rúbrica 7 - Otros gastos administrativos	0,048	0,144	0,144	0,072	0,072	0,072	**0,552**
Subtotal para otras rúbricas							
1. TOTAL 2. RÚBRICA 7 y al margen de la RÚBRICA 7	0,830	1,701	1,701	1,629	1,558	1,406	**8,825**

1) Las necesidades en materia de créditos administrativos se cubrirán mediante los créditos ya destinados a la gestión de la acción o reasignados, que se complementarán en caso necesario con cualquier dotación adicional que pudiera asignarse a la DG gestora en el marco del procedimiento de asignación anual y a la luz de los imperativos presupuestarios existentes.

6. MÉTODOS DE CÁLCULO UTILIZADOS PARA LA ESTIMACIÓN DE LOS COSTES

a) Recursos humanos

En este apartado se expone el método de cálculo utilizado para estimar los recursos humanos considerados necesarios [hipótesis sobre carga de trabajo, incluidos los empleos específicos (perfiles de actividad Sysper 2), categorías de personal y costes medios conexos]

1. **RÚBRICA 7** del marco financiero plurianual
2. Nota: los costes medios correspondientes a cada categoría de personal en la Sede se encuentran disponibles en BudgWeb: 3. https://myintracomm.ec.europa.eu/budgweb/EN/pre/legalbasis/Pages/pre-040-020_preparation.aspx
4. O Funcionarios y agentes temporales 5. 7 funcionarios AD (incluido 1 procedente de CNECT/F.3 en 2023-2024) x 152 000 EUR/año en 2023-2027 (la mitad de dicho importe en 2022, puesto que la adopción está prevista a mediados de 2022); 6. 1 funcionario AST x 152 000 EUR/año en 2023-2027 (la mitad de dicho importe en 2022, puesto que la adopción está prevista a mediados de 2022) 7.
8. O Personal externo 9. CA: 1 x 82 000 EUR/año en 2023-2027 (la mitad de dicho importe en 2022, puesto que la adopción está prevista a mediados de 2022) (factor de indexación aplicado); 10. 2 funcionarios ENCS x 86 000 EUR/año en 2023-2027 (la mitad de dicho importe en 2022, puesto que la adopción está prevista a mediados de 2022) (factor de indexación aplicado); 11.

12. **Al margen de la RÚBRICA 7** del marco financiero plurianual
13. O Únicamente puestos financiados con cargo al presupuesto de investigación 14.
15. O Personal externo 16.

7. OTROS GASTOS ADMINISTRATIVOS

Describase detalladamente el método de cálculo utilizado para cada línea presupuestaria y, en particular, las hipótesis de base (p. ej., número de reuniones al año, costes medios, etc.)

17. **RÚBRICA 7** del marco financiero plurianual
18. Reuniones bimensuales de comités x 12 000 EUR/reunión en el período 2022-2024 para la adopción de actos de ejecución. Con posterioridad a dicho período, celebración de reuniones de comités para la adopción de actos de ejecución actualizados. 19. Las misiones son principalmente viajes de Luxemburgo y Bruselas, pero también incluyen la asistencia a conferencias y a reuniones con Estados miembros y con otras partes interesadas. 20.

21. **Al margen de la RÚBRICA 7** del marco financiero plurianual
22. Las reuniones del grupo de expertos deben cargarse a la línea administrativa del programa Europa Digital. **23.** Se prevé celebrar reuniones mensuales (con un coste de 12 000 EUR/reunión) durante la elaboración de actos de ejecución (desde mediados de 2022 hasta 2024) y, fuera del citado período, está previsto celebrar reuniones bimensuales para garantizar la coordinación de la aplicación técnica a escala de la UE.
24.