2024/2981

4.12.2024

REGLAMENTO DE EJECUCIÓN (UE) 2024/2981 DE LA COMISIÓN

de 28 de noviembre de 2024

por el que se establecen disposiciones de aplicación del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo en lo que respecta a la certificación de las carteras europeas de identidad digital

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto 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 y por el que se deroga la Directiva 1999/93/CE ([1]), y en particular su artículo 5 *quater*, apartado 6,

Considerando lo siguiente:

(1) De conformidad con el artículo 5 *quater* del Reglamento (UE) n.º 910/2014, la certificación de las carteras europeas de identidad digital (en lo sucesivo, «carteras») debe realizarse con arreglo a unos requisitos funcionales, de ciberseguridad y de protección de datos pertinentes a fin de garantizar un alto nivel de seguridad y confianza en las carteras. Estos requisitos de certificación deben armonizarse entre todos los Estados miembros para evitar la fragmentación del mercado y construir un marco sólido.

(2) El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo ([2]) y, en su caso, la Directiva 2002/58/CE del Parlamento Europeo y del Consejo ([3]) son aplicables a las actividades de tratamiento de datos personales en virtud del presente Reglamento.

(3) La Comisión evalúa periódicamente las nuevas tecnologías, prácticas, normas y especificaciones técnicas. Con el fin de garantizar el máximo nivel de armonización entre los Estados miembros para el desarrollo y la certificación de las carteras, las especificaciones técnicas establecidas en el presente Reglamento se basan en el trabajo realizado con arreglo a la Recomendación (UE) 2021/946 de la Comisión, de 3 de junio de 2021, sobre un conjunto de instrumentos común de la Unión para adoptar un enfoque coordinado de cara a un Marco para una Identidad Digital Europea ([4]), y en particular la arquitectura y el marco de referencia que forman parte de él. De conformidad con el considerando 75 del Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo ([5]), la Comisión debe revisar y, en caso necesario, actualizar el presente Reglamento de Ejecución, para mantenerlo en consonancia con la evolución mundial, la arquitectura y el marco de referencia, y seguir las mejores prácticas en el mercado interior.

(4) A fin de acreditar la conformidad con los requisitos de ciberseguridad incluidos en el marco de certificación, la certificación de las soluciones de cartera debe referirse a los esquemas europeos de certificación de la ciberseguridad establecidos en virtud del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo ([6]), cuando se disponga de ellos y sean pertinentes. En ausencia de tales esquemas, o cuando estos cubran solo parcialmente los requisitos de ciberseguridad, el presente Reglamento establece los requisitos generales aplicables a los esquemas nacionales de certificación, que comprenden requisitos funcionales, de ciberseguridad y de protección de datos.

([1]) DO L 257 de 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) 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, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([3]) Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (DO L 201 de 31.7.2002, p. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([4]) DO L 210 de 14.6.2021, p. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj.

([5]) Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital (DO L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

([6]) 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, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(5) De conformidad con el artículo 5 *bis*, apartado 11, del Reglamento (UE) n.º 910/2014, las carteras deben certificarse con respecto a un nivel de seguridad alto según lo establecido en el Reglamento (UE) n.º 910/2014, así como en el Reglamento de Ejecución (UE) 2015/1502 de la Comisión ([7]). Ese nivel de seguridad debe ser alcanzado por la solución de cartera en su conjunto. En virtud del presente Reglamento, algunos componentes de la solución de cartera pueden certificarse a un nivel de seguridad inferior, siempre que ello esté debidamente justificado y sin perjuicio del nivel de seguridad alto alcanzado globalmente por la solución.

(6) Todos los esquemas nacionales de certificación deben designar un dueño del esquema, que será responsable del desarrollo y el mantenimiento del esquema de certificación. El dueño del esquema puede ser un organismo de evaluación de la conformidad, un organismo o autoridad gubernamental, una asociación comercial, un grupo de organismos de evaluación de la conformidad o cualquier organismo apropiado, y puede ser distinto del organismo que gestione el funcionamiento del esquema nacional de certificación.

(7) El objeto de la certificación debe incluir los componentes de *software* de la solución de cartera, como la instancia de cartera. La aplicación criptográfica segura de cartera («ACSC»), el dispositivo criptográfico seguro de cartera («DCSC») y las plataformas en las que estos componentes de *software* se ejecutan, aunque forman parte del entorno operativo, únicamente deben incluirse en el objeto de la certificación cuando los proporcione la solución de cartera. En otros casos, y en particular cuando estos dispositivos y plataformas sean suministrados por usuarios finales, los proveedores deben establecer hipótesis sobre el entorno operativo de la solución de cartera, y en concreto sobre estos dispositivos y plataformas, y aplicar medidas para confirmar que estas hipótesis se verifican en la práctica. Con el fin de garantizar la protección de los activos críticos mediante el *hardware* y el *software* del sistema utilizados para gestionar y proteger las claves criptográficas creadas, almacenadas o procesadas por el DCSC, este debe ajustarse a las estrictas normas de certificación plasmadas en normas internacionales como los criterios comunes de la UE («EUCC»), establecidos en el Reglamento de Ejecución (UE) 2024/482 de la Comisión ([8]), con el nivel de evaluación EAL4 y el análisis metódico avanzado de vulnerabilidades, comparable al nivel AVA_VAN.5. Estas normas de certificación deben utilizarse a más tardar cuando la conformidad de las carteras se certifique según un esquema europeo de certificación de la ciberseguridad adoptado con arreglo al Reglamento (UE) 2019/881.

(8) Unas carteras totalmente móviles, seguras y fáciles de utilizar se sustentan en soluciones normalizadas y certificadas resistentes a las manipulaciones fraudulentas, como elementos seguros integrados, dispositivos externos como tarjetas inteligentes o plataformas SIM integradas en dispositivos móviles. Es importante garantizar el acceso oportuno de los medios de identificación electrónica nacionales y las carteras nacionales a elementos seguros integrados y coordinar los esfuerzos de los Estados miembros en este ámbito. El Grupo de Cooperación sobre la Identidad Digital Europea, creado en virtud del artículo 46 *sexies*, apartado 1, del Reglamento (UE) n.º 910/2014 (en lo sucesivo, «Grupo de Cooperación») debe, por tanto, crear un subgrupo específico a tal efecto. Previa consulta a las partes interesadas pertinentes, este subgrupo debe acordar una hoja de ruta conjunta para el acceso a elementos seguros integrados que se someterá a la consideración de la Comisión como parte del informe de revisión sobre el Reglamento (UE) n.º 910/2014. Con el fin de facilitar la penetración de la cartera a nivel nacional, la Comisión, en cooperación con los Estados miembros, debe además elaborar y mantener actualizado un manual para casos de uso en el marco de la arquitectura y el marco de referencia.

(9) El objeto de la certificación de los esquemas nacionales de certificación debe abarcar también los procesos que se utilizan para proporcionar la solución de cartera y gestionar su funcionamiento, aun cuando la definición o la ejecución de dichos procesos se subcontraten a terceros. Para demostrar que los procesos satisfacen los requisitos de los esquemas, se admite como prueba la información sobre la garantía, siempre que se determine mediante un análisis de la dependencia si esa información sobre la garantía es suficiente. La información sobre la garantía se presenta en múltiples formas distintas, como informes y certificados de conformidad, que pueden ser de ámbito privado, nacional, europeo o internacional, basados en normas o en especificaciones técnicas. El objetivo del análisis de la dependencia es evaluar la calidad de la información sobre la garantía disponible relativa a los componentes de una cartera.

([7]) Reglamento de Ejecución (UE) 2015/1502 de la Comisión, de 8 de septiembre de 2015, sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica con arreglo a lo dispuesto en el artículo 8, apartado 3, del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (DO L 235 de 9.9.2015, p. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

([8]) Reglamento de Ejecución (UE) 2024/482 de la Comisión, de 31 de enero de 2024, por el que se establecen disposiciones de aplicación del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo en lo concerniente a la adopción del esquema europeo de certificación de la ciberseguridad basado en los criterios comunes (EUCC) (DO L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg/2024/482/oj).

(10) Con arreglo a los procedimientos establecidos a tal efecto, el Grupo de Cooperación debe poder emitir dictámenes y recomendaciones sobre los proyectos de esquemas nacionales de certificación que se le presenten. Estos esquemas nacionales de certificación deben ser específicos para la arquitectura de la cartera, y deben existir perfiles específicos para cada arquitectura específica a la que se dé soporte.

(11) A fin de garantizar una comprensión común y un enfoque armonizado de la evaluación de los riesgos más críticos que pueden afectar al suministro y la gestión del funcionamiento de las carteras, debe elaborarse un registro de riesgos y amenazas que se tendrá presente al diseñar las soluciones de cartera, independientemente de su arquitectura específica. Los objetivos de ciberseguridad descritos en el Reglamento (UE) n.º 910/2014, como la confidencialidad, la integridad y la disponibilidad de la solución de cartera, así como la privacidad de los usuarios y de los datos, deben tenerse en cuenta al determinar qué riesgos han de incluirse en el registro. Los requisitos de los esquemas nacionales de certificación deben incorporar la consideración de los riesgos y amenazas incluidos en este registro. Para estar en consonancia con la continua evolución del panorama de amenazas, el registro de riesgos debe mantenerse y actualizarse periódicamente en colaboración con el Grupo de Cooperación.

(12) Al establecer sus esquemas de certificación, los dueños de estos esquemas deben realizar una evaluación de riesgos para precisar y completar los riesgos y las amenazas que figuren en el registro con otros que afecten de manera específica a la arquitectura o la ejecución de la solución de cartera. La evaluación de riesgos debe considerar cómo pueden tratarse adecuadamente los riesgos y amenazas correspondientes. Los proveedores de carteras deben completar la evaluación de riesgos del esquema indicando los riesgos y amenazas que afecten de manera específica a su ejecución y proponiendo medidas de tratamiento adecuadas para su evaluación por parte del organismo de certificación.

(13) A fin de demostrar que la arquitectura de una solución de cartera cumple los requisitos de seguridad aplicables, cada esquema o perfil específicos de la arquitectura debe contener al menos una descripción de la arquitectura de la solución de cartera, una lista de los requisitos de seguridad aplicables a esa arquitectura, un plan de evaluación para confirmar que una solución de cartera basada en esa arquitectura cumple dichos requisitos y una evaluación de riesgos. Los esquemas nacionales de certificación deben exigir a los proveedores de carteras que demuestren que el diseño de la solución de cartera que proporcionan se ajusta a la arquitectura de referencia y detalla los controles de seguridad y los planes de validación de la solución de cartera específica. Los esquemas nacionales de certificación deben definir también una actividad de evaluación de la conformidad para verificar que el diseño de la cartera refleja adecuadamente la arquitectura de referencia del perfil seleccionado. Los esquemas nacionales de certificación deben cumplir los requisitos establecidos en el artículo 51 del Reglamento (UE) 2019/881, excepto en lo que respecta a sus letras e) y f), en relación con el registro.

(14) En lo que respecta a la certificación de productos, debe permitirse el uso de los certificados de conformidad expedidos con arreglo al esquema de certificación de la ciberseguridad de la UE basado en los criterios comunes («EUCC»), y de los certificados de conformidad expedidos con arreglo a esquemas nacionales de certificación en el contexto del Acuerdo de Reconocimiento Mutuo (ARM) del Grupo de altos funcionarios sobre seguridad de los sistemas de información (SOG-IS). Además, para los componentes de productos menos sensibles debe permitirse el uso de otros esquemas nacionales de certificación, como los establecidos con arreglo a la norma CEN EN 17640 sobre metodología de evaluación de la ciberseguridad en tiempo fijo.

(15) La etiqueta de confianza de la UE para la cartera de identidad digital (en lo sucesivo, «etiqueta de confianza») debe utilizarse para indicar de manera clara, sencilla y reconocible que una cartera ha sido proporcionada de conformidad con el Reglamento (UE) n.º 910/2014. Por lo tanto, debe considerarse como etiqueta de conformidad para las soluciones de cartera certificadas con arreglo a los esquemas nacionales de certificación. Estos esquemas no deben definir ninguna otra etiqueta de conformidad.

(16) Con el fin de desincentivar el fraude, los esquemas nacionales de certificación deben definir las medidas que han de adoptarse cuando se declare de forma fraudulenta una certificación a su amparo.

(17) Para garantizar una gestión eficiente de las notificaciones de vulnerabilidad, los proveedores de soluciones de cartera y el sistema de identificación electrónica en el marco del cual se proporcionen deben definir y aplicar procesos para evaluar la gravedad y la posible repercusión de las vulnerabilidades. Los esquemas nacionales de certificación deben establecer un umbral por encima del cual se deba notificar al organismo de certificación. Este requisito de notificación no debe afectar a los criterios establecidos por la legislación en materia de protección de datos y las autoridades de protección de datos de los Estados miembros para la notificación de violaciones de la seguridad de los datos personales. Podrían establecerse posibles sinergias entre la notificación obligatoria de la violación o la puesta en peligro de las soluciones de cartera y la notificación de las violaciones de la seguridad de los datos personales de conformidad con el Reglamento (UE) 2016/679. La evaluación por el organismo de certificación de un informe de análisis de impacto de la vulnerabilidad debe entenderse sin perjuicio de la evaluación por una autoridad de protección de datos de una evaluación de impacto relativa a la protección de datos realizada con arreglo a los artículos 35 y 36 del Reglamento (UE) 2016/679.

(18) Los proveedores de soluciones de cartera y del sistema de identificación electrónica en el marco del cual las proporcionan deben notificar al dueño del esquema toda justificación de las excepciones a la evaluación de la vulnerabilidad exigida para la evaluación del DCSC y de la ACSC, tal como se establece en el anexo IV.

(19) La cancelación de un certificado de conformidad podría tener graves consecuencias, como la revocación de todas las unidades de cartera implantadas. Por lo tanto, los organismos de certificación solo deben considerar la cancelación si es probable que una vulnerabilidad no subsanada afecte significativamente a la fiabilidad de la solución de cartera o a la fiabilidad de otra solución de cartera.

(20) Debe establecerse un proceso específico para la actualización de los esquemas nacionales de certificación a fin de gestionar la transición entre las sucesivas versiones de los esquemas, en particular por lo que respecta a las medidas que debe adoptar en adelante el titular del certificado en relación con las evaluaciones, el mantenimiento, la renovación de la certificación y las evaluaciones especiales.

(21) Para facilitar la transparencia, los proveedores de carteras deben compartir públicamente la información sobre la seguridad de su solución de cartera.

(22) Cuando los esquemas nacionales de certificación se basen en información sobre la garantía procedente de otros esquemas o fuentes de certificación, debe realizarse un análisis de la dependencia para verificar que la documentación de la garantía, por ejemplo los informes de garantía y los certificados de conformidad, está disponible y es adecuada para la solución de cartera y el sistema de identificación electrónica en el marco del cual se proporciona. Este análisis de la dependencia debe basarse en la evaluación de riesgos de las soluciones de cartera y el sistema de identificación electrónica en el marco del cual se proporcionan. La evaluación debe determinar si la documentación de la garantía disponible para determinada solución de cartera y para el sistema de identificación electrónica en el marco del cual se proporciona es adecuada para ofrecer una garantía correspondiente al nivel de evaluación buscado. La evaluación debe actualizar también el análisis de la dependencia, o reevaluarlo por completo, en caso necesario.

(23) Los organismos de certificación deben expedir certificados de conformidad en los esquemas nacionales de certificación, junto con un informe de certificación a disposición del público, tal como se contempla en el artículo 5 *quinquies*, apartado 2, letra a), del Reglamento (UE) n.º 910/2014. El informe de evaluación de la certificación conexo debe ponerse a disposición del Grupo de Cooperación.

(24) Los esquemas nacionales de certificación deben establecer una evaluación de vigilancia anual para garantizar que los procesos asociados a la gestión y el mantenimiento de las carteras funcionan eficazmente, es decir, según lo definido en las políticas que regulan esos procesos. La evaluación bienal de la vulnerabilidad es un requisito derivado del Reglamento (UE) n.º 910/2014, para garantizar que la solución de cartera siga cubriendo adecuadamente los riesgos y amenazas de ciberseguridad indicados en el registro de riesgos, incluida cualquier evolución de la situación de amenazas. Los conceptos de evaluaciones de vigilancia, evaluaciones de renovación de la certificación y evaluaciones especiales deben ajustarse a la norma EN ISO/IEC 17021-1:2015.

(25) Un ciclo de certificación finaliza cuando expira el certificado de conformidad o cuando se expide un nuevo certificado de conformidad tras una evaluación satisfactoria de renovación de la certificación. La evaluación de renovación de la certificación debe abordar todos los componentes del objeto de la certificación, y en concreto evaluar la eficacia y, en su caso, la vulnerabilidad. Durante la renovación de la certificación, debe ser posible reutilizar los resultados de evaluaciones anteriores de los componentes que no hayan cambiado.

(26) Cuando se adopte un esquema europeo de certificación de la ciberseguridad, los esquemas nacionales de certificación con el mismo ámbito de aplicación deben dejar de expedir certificaciones tras un período transitorio definido, tal como se contempla en el artículo 57, apartado 1, del Reglamento (UE) 2019/881.

(27) Los esquemas nacionales de certificación deben basarse en los marcos existentes y reutilizar las pruebas, cuando proceda, a fin de garantizar la armonización y la interoperabilidad. Los Estados miembros podrán celebrar acuerdos para la reutilización transfronteriza de esquemas de certificación o partes de estos. La Comisión Europea y la ENISA, en cooperación con el Grupo de Cooperación, deben apoyar a los Estados miembros en la elaboración y el mantenimiento de sus esquemas nacionales de certificación, garantizando el intercambio de conocimientos y mejores prácticas.

(28) El Supervisor Europeo de Protección de Datos, al que se consultó de conformidad con el artículo 42, apartado 1, del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo ([9]), emitió su dictamen el 30 de septiembre de 2024.

(29) Las medidas previstas en el presente Reglamento se ajustan al dictamen del comité contemplado en el artículo 48, apartado 1, del Reglamento (UE) n.º 910/2014.

HA ADOPTADO EL PRESENTE REGLAMENTO:

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1

Objeto y ámbito de aplicación

El presente Reglamento establece normas de referencia, especificaciones y procedimientos a fin de construir un marco sólido para la certificación de las carteras, que debe actualizarse periódicamente para mantenerlo en consonancia con la evolución de la tecnología y las normas y con el trabajo realizado sobre la base de la Recomendación (UE) 2021/946, sobre un conjunto de instrumentos común de la Unión para adoptar un enfoque coordinado de cara a un Marco para una Identidad Digital Europea, y en particular la arquitectura y el marco de referencia.

Artículo 2

Definiciones

A los efectos del presente Reglamento, se entenderá por:

1) «solución de cartera»: combinación de *software*, *hardware*, servicios, ajustes y configuraciones, que incluye instancias de cartera, una o más aplicaciones criptográficas seguras de cartera y uno o más dispositivos criptográficos seguros de cartera;

2) «dueño del esquema»: organización responsable de elaborar y mantener un esquema de certificación;

3) «objeto de la certificación»: productos, procesos y servicios, o una combinación de estos, a los que se aplican unos requisitos especificados;

4) «aplicación criptográfica segura de cartera»: aplicación que gestiona activos críticos al estar vinculada a las funciones criptográficas y no criptográficas proporcionadas por el dispositivo criptográfico seguro de cartera y utilizarlas;

5) «instancia de cartera»: aplicación instalada y configurada en el dispositivo o el entorno de un usuario de una cartera, que forma parte de una unidad de cartera y que el usuario de la cartera utiliza para interactuar con la unidad de cartera;

([9]) 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, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

6) «dispositivo criptográfico seguro de cartera»: dispositivo resistente a las manipulaciones fraudulentas que proporciona un entorno vinculado a la aplicación criptográfica segura de cartera y utilizado por esta para proteger activos críticos y proporcionar funciones criptográficas para la ejecución segura de operaciones críticas;

7) «registro de riesgos»: registro de la información pertinente para el proceso de certificación sobre los riesgos detectados;

8) «proveedor de cartera»: persona física o jurídica que proporciona soluciones de cartera;

9) «organismo de certificación»: organismo tercero de evaluación de la conformidad que gestiona el funcionamiento de sistemas de certificación;

10) «unidad de cartera»: configuración única de una solución de cartera que incluye instancias de cartera, aplicaciones criptográficas seguras de cartera y dispositivos criptográficos seguros de cartera proporcionados por un proveedor de cartera a un usuario particular de una cartera;

11) «activos críticos»: activos contenidos en una unidad de cartera o relacionados con ella, de tan extraordinaria importancia que si su disponibilidad, confidencialidad o integridad se vieran comprometidas, el efecto sobre la capacidad para utilizar la unidad de cartera sería muy grave y debilitante;

12) «usuario de una cartera»: usuario que tiene el control sobre la unidad de cartera;

13) «incidente»: un incidente según se define en el artículo 6, punto 6, de la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo ([10]);

14) «política de divulgación incorporada»: conjunto de normas, incorporadas en una declaración electrónica de atributos por su proveedor, que indica las condiciones que debe cumplir una parte usuaria de la cartera para acceder a la declaración electrónica de atributos.

CAPÍTULO II

ESQUEMAS NACIONALES DE CERTIFICACIÓN

Artículo 3

Establecimiento de esquemas nacionales de certificación

1. Los Estados miembros designarán un dueño del esquema para cada esquema nacional de certificación.

2. El objeto de la certificación definido en los esquemas nacionales de certificación será el suministro y la gestión del funcionamiento de las soluciones de cartera y de los sistemas de identificación electrónica en el marco de los cuales se proporcionan.

3. De conformidad con el Reglamento de Ejecución (UE) 2015/1502, el objeto de la certificación en los esquemas nacionales de certificación incluirá los siguientes elementos:

a) los componentes de *software*, incluidos los ajustes y configuraciones de una solución de cartera y del sistema de identificación electrónica en el marco del cual se proporcionan las soluciones de cartera;

b) los componentes de *hardware* y las plataformas en las que funcionan o que utilizan los componentes de *software* mencionados en el punto b) para las operaciones críticas, en los casos en que sean proporcionados directa o indirectamente por la solución de cartera y el sistema de identificación electrónica en el marco del cual se proporciona y cuando se les exija que alcancen el nivel de seguridad deseado para dichos componentes de *software*. Cuando el proveedor de la cartera no proporcione los componentes de *hardware* y las plataformas, los esquemas nacionales de certificación formularán hipótesis para la evaluación de los componentes de *hardware* y las plataformas, en las cuales pueda proporcionarse resistencia contra atacantes con elevado potencial de ataque de conformidad con el Reglamento de Ejecución (UE) 2015/1502, y especificarán las actividades de evaluación para confirmar estas hipótesis, tal como se indica en el anexo IV;

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

c) los procesos que apoyan el suministro y la gestión del funcionamiento de una solución de cartera, incluido el proceso de incorporación de los usuarios a que se refiere el artículo 5 *bis* del Reglamento (UE) n.º 910/2014, cubriendo al menos la inscripción, la gestión de medios electrónicos y la organización de conformidad con las secciones 2.1, 2.2, y 2.4 del anexo I del Reglamento de Ejecución (UE) 2015/1502.

4. Los esquemas nacionales de certificación incluirán una descripción de la arquitectura específica de las soluciones de cartera y del sistema de identificación electrónica en el marco del cual se proporcionan. Cuando los esquemas nacionales de certificación abarquen más de una arquitectura específica, incluirán un perfil para cada una de ellas.

5. Para cada perfil, los esquemas nacionales de certificación establecerán, como mínimo, lo siguiente:

a) la arquitectura específica de una solución de cartera y del sistema de identificación electrónica en el marco del cual se proporciona;

b) los controles de seguridad asociados a los niveles de seguridad establecidos en el artículo 8 del Reglamento (UE) n.º 910/2014;

c) un plan de evaluación elaborado de conformidad con la sección 7.4.1 de la norma EN ISO/IEC 17065:2012;

d) los requisitos de seguridad necesarios para hacer frente a los riesgos y amenazas de ciberseguridad enumerados en el registro de riesgos establecido en el anexo I del presente Reglamento, hasta el nivel de seguridad requerido, y para cumplir, cuando proceda, los objetivos definidos en el artículo 51 del Reglamento (UE) 2019/881;

e) una puesta en correspondencia de los controles a que se refiere la letra b) del presente apartado con los componentes de la arquitectura;

f) una descripción de cómo los controles de seguridad, la puesta en correspondencia, los requisitos de seguridad y el plan de evaluación a que se refieren las letras b) y c) permiten a los proveedores de soluciones de cartera y del sistema de identificación electrónica en el marco del cual se proporcionan abordar adecuadamente los riesgos y amenazas de ciberseguridad indicados en el registro de riesgos a que se refiere la letra d), hasta el nivel de seguridad requerido basado en una evaluación de riesgos para precisar y completar los riesgos y las amenazas enumerados en el registro de riesgos con otros que afecten de manera específica a la arquitectura.

6. En el plan de evaluación a que se refiere el apartado 5, letra c), se indicarán las actividades de evaluación que deben incluirse en la evaluación de las soluciones de cartera y del sistema de identificación electrónica en cuyo marco se proporcionan.

7. La actividad de evaluación a que se refiere el apartado 6 exigirá a los proveedores de soluciones de cartera y del sistema de identificación electrónica en cuyo marco se proporcionan facilitar información que cumpla los requisitos que figuran en el anexo II.

Artículo 4

Requisitos generales

1. Los esquemas nacionales de certificación abarcarán los requisitos funcionales, de ciberseguridad y de protección de datos utilizando, cuando estén disponibles y sean aplicables, los siguientes esquemas de certificación:

a) los esquemas europeos de certificación de la ciberseguridad establecidos de conformidad con el Reglamento (UE) 2019/881, incluido el esquema de certificación de la ciberseguridad de la UE basado en los criterios comunes (EUCC);

b) los esquemas nacionales de certificación de la ciberseguridad cubiertos por el EUCC, de conformidad con el artículo 49 del Reglamento de Ejecución (UE) 2024/482.

2. Además, cuando estén disponibles y sean aplicables, los esquemas nacionales de certificación podrán hacer referencia a:

a) otros esquemas nacionales de certificación pertinentes;

b) normas internacionales, europeas y nacionales;

c) especificaciones técnicas que cumplan los requisitos establecidos en el anexo II del Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo ([11]).

3. Los esquemas nacionales de certificación:

a) especificarán los elementos enumerados en la sección 6.5 de la norma EN ISO/IEC 17067:2013;

b) se aplicarán como un esquema de tipo 6, de conformidad con la sección 5.3.8 de la norma EN ISO/IEC 17067:2013.

4. Los esquemas nacionales de certificación deberán cumplir los requisitos siguientes:

a) solo los proveedores a que se refiere el artículo 5 *bis*, apartado 2, del Reglamento (UE) n.º 910/2014 podrán expedir certificados con arreglo a los esquemas nacionales de certificación;

b) solo la etiqueta de confianza se utiliza como etiqueta de conformidad;

c) los proveedores de soluciones de cartera y del sistema de identificación electrónica con arreglo al cual se proporcionan incluyen referencias al Reglamento (UE) n.º 910/2014 y al presente Reglamento cuando se refieren al esquema;

d) los proveedores de soluciones de cartera y del sistema de identificación electrónica con arreglo al cual se proporcionan completan la evaluación de riesgos del esquema a que se refiere el artículo 3, apartado 5, letra f), para determinar los riesgos y las amenazas que afectan específicamente a su ejecución, y proponen medidas adecuadas para tratar todos los riesgos y amenazas pertinentes;

e) se han establecido las responsabilidades y las acciones legales e incluyen referencias a la legislación nacional aplicable, que define las responsabilidades y las posibles acciones legales en caso de uso fraudulento de la certificación en el marco del esquema.

5. La evaluación a que se refiere el apartado 4, letra d), se compartirá con el organismo de certificación para su evaluación.

Artículo 5

Gestión de incidentes y vulnerabilidades

1. Los esquemas nacionales de certificación contendrán requisitos de gestión de incidentes y vulnerabilidades de conformidad con lo dispuesto en los apartados 2 a 9.

2. El titular de un certificado de conformidad de una solución de cartera y del sistema de identificación electrónica en el marco del cual se proporciona notificará a su organismo de certificación, sin dilación indebida, cualquier violación o puesta en peligro de la solución de cartera, o del sistema de identificación electrónica en el marco del cual se proporciona, que sea probable que afecte a su conformidad con los requisitos de los esquemas nacionales de certificación.

3. El titular de un certificado de conformidad establecerá, mantendrá y aplicará una política y unos procedimientos de gestión de la vulnerabilidad, teniendo en cuenta los procedimientos establecidos en las normas europeas e internacionales vigentes, en particular la norma EN ISO/IEC 30111:2019.

4. El titular del certificado de conformidad notificará al organismo de certificación emisor las vulnerabilidades y los cambios que afecten a la solución de cartera, sobre la base de criterios definidos acerca de la repercusión de dichas vulnerabilidades y dichos cambios.

5. El titular del certificado de conformidad elaborará un informe de análisis de impacto de la vulnerabilidad para toda vulnerabilidad que afecte a los componentes de *software* de la solución de cartera. En él constará la siguiente información:

a) el impacto de la vulnerabilidad en la solución de cartera certificada;

b) los posibles riesgos asociados a la proximidad o probabilidad de un ataque;

([11]) Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre la normalización europea, por el que se modifican las Directivas 89/686/CEE y 93/15/CEE del Consejo y las Directivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE y 2009/105/CE del Parlamento Europeo y del Consejo y por el que se deroga la Decisión 87/95/CEE del Consejo y la Decisión n.º 1673/2006/CE del Parlamento Europeo y del Consejo (DO L 316 de 14.11.2012, p. 12, ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

c) si la vulnerabilidad puede subsanarse utilizando los medios disponibles;

d) en caso de que la vulnerabilidad pueda subsanarse utilizando los medios disponibles, posibles formas de subsanarla.

6. Cuando se requiera una notificación conforme al apartado 4, el titular del certificado de conformidad transmitirá, sin dilación indebida, el informe de análisis de impacto de la vulnerabilidad a que se refiere el apartado 5 al organismo de certificación.

7. El titular de un certificado de conformidad establecerá, mantendrá y aplicará una política de gestión de la vulnerabilidad que cumpla los requisitos establecidos en el anexo I del Reglamento de Ciberresiliencia ([12]).

8. Los esquemas nacionales de certificación establecerán los requisitos de divulgación de las vulnerabilidades aplicables a los organismos de certificación.

9. El titular de un certificado de conformidad divulgará y registrará cualquier vulnerabilidad públicamente conocida y subsanada en la solución de cartera o en uno de los repositorios en línea a que se refiere el anexo V.

Artículo 6

Mantenimiento de los esquemas nacionales de certificación

1. Los esquemas nacionales de certificación contendrán un proceso para la revisión periódica de su funcionamiento. Dicho proceso servirá para confirmar su idoneidad y determinar los aspectos que requieran mejoras, teniendo en cuenta las observaciones de las partes interesadas.

2. Los esquemas nacionales de certificación incluirán disposiciones relativas a su mantenimiento. Este proceso incluirá como mínimo los siguientes requisitos:

a) normas para la gobernanza de la definición y los requisitos de los esquemas nacionales de certificación;

b) el establecimiento de plazos para la expedición de certificados tras la adopción de versiones actualizadas de los esquemas nacionales de certificación, tanto para los nuevos certificados de conformidad como para los expedidos anteriormente;

c) una revisión periódica de los esquemas nacionales de certificación que garantice que sus requisitos se están aplicando de manera coherente, teniendo en cuenta al menos los siguientes aspectos:

— las solicitudes de aclaración sobre los requisitos del esquema nacional de certificación dirigidas al dueño del esquema,

— las observaciones formuladas por los participantes y otras partes interesadas,

— la capacidad de respuesta del dueño del esquema nacional de certificación a las solicitudes de información;

d) normas para el seguimiento de los documentos de referencia y procedimientos para la evolución de las versiones de referencia de los esquemas nacionales de certificación, en concreto, al menos, en los períodos transitorios;

e) un proceso que asegure que están cubiertos los riesgos y las amenazas de ciberseguridad más recientes incluidos en el registro de riesgos establecido en el anexo I del presente Reglamento;

f) un proceso para gestionar otros cambios en los esquemas nacionales de certificación.

([12]) Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE) n.º 168/2013 y el Reglamento (UE) 2019/1020 y la Directiva (UE) 2020/1828 (Reglamento de Ciberresiliencia) (DO L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

3. Los esquemas nacionales de certificación contendrán requisitos para la realización de evaluaciones sobre los productos ya certificados dentro de un determinado plazo tras la revisión del esquema, o tras la publicación de nuevas especificaciones o normas, o nuevas versiones de estas, que las soluciones de cartera y el sistema de identificación electrónica en el marco del cual se proporcionan deberán cumplir.

CAPÍTULO III

REQUISITOS RELATIVOS A LOS DUEÑOS DE LOS ESQUEMAS

Artículo 7

Requisitos generales

1. Los dueños de los esquemas elaborarán y mantendrán los esquemas nacionales de certificación y dirigirán su funcionamiento.

2. Los dueños de los esquemas podrán subcontratar todas sus tareas, o parte de ellas, a un tercero. Cuando subcontraten a una parte privada, los dueños de los esquemas establecerán mediante contrato las obligaciones y responsabilidades de todas las partes. Los dueños de los esquemas seguirán siendo responsables de todas las actividades subcontratadas realizadas por sus subcontratistas.

3. Los dueños de los esquemas llevarán a cabo su labor de supervisión, si procede, basándose al menos en la siguiente información:

a) la información procedente de los organismos de certificación, los organismos nacionales de acreditación y las autoridades de vigilancia del mercado pertinentes;

b) la información resultante de las auditorías e investigaciones realizadas por ellos mismos o por otra autoridad;

c) las reclamaciones y los recursos recibidos de conformidad con el artículo 15.

4. Los dueños de los esquemas informarán al Grupo de Cooperación de las revisiones de los esquemas nacionales de certificación. Al hacerlo, facilitarán información adecuada para que el Grupo de Cooperación les formule recomendaciones y emita dictámenes sobre los esquemas nacionales de certificación actualizados.

CAPÍTULO IV

REQUISITOS RELATIVOS A LOS PROVEEDORES DE SOLUCIONES DE CARTERA Y DE LOS SISTEMAS DE IDENTIFICACIÓN ELECTRÓNICA EN CUYO MARCO SE PROPORCIONAN

Artículo 8

Requisitos generales

1. Los esquemas nacionales de certificación contendrán requisitos de ciberseguridad basados en una evaluación de riesgos de cada arquitectura específica a la que den soporte. Dichos requisitos de ciberseguridad tendrán por objeto tratar los riesgos y amenazas de ciberseguridad detectados, tal como se establece en el registro de riesgos que figura en el anexo I.

2. De conformidad con el artículo 5 *bis*, apartado 23, del Reglamento (UE) n.º 910/2014, los esquemas nacionales de certificación exigirán que las soluciones de cartera y los sistemas de identificación electrónica en cuyo marco se proporcionen sean resistentes a atacantes con un elevado potencial de ataque para un nivel de seguridad alto, como se contempla en el Reglamento de Ejecución (UE) 2015/1502.

3. Los esquemas nacionales de certificación establecerán criterios de seguridad, que incluirán los siguientes requisitos:

a) el Reglamento de Ciberresiliencia, cuando proceda, o requisitos que cumplan los objetivos de seguridad establecidos en el artículo 51 del Reglamento (UE) 2019/881;

b) el establecimiento y la aplicación de políticas y procedimientos relativos a la gestión de los riesgos asociados al funcionamiento de una solución de cartera, incluidas la detección y la evaluación de los riesgos y la reducción de los riesgos detectados;

c) el establecimiento y la aplicación de políticas y procedimientos relacionados con la gestión de los cambios y las vulnerabilidades de conformidad con el artículo 5 del presente Reglamento;

d) el establecimiento y la aplicación de políticas y procedimientos de gestión de los recursos humanos, que incluyan requisitos en materia de conocimientos especializados, fiabilidad, experiencia, formación en seguridad y cualificaciones del personal que participe en la elaboración o la gestión del funcionamiento de la solución de cartera;

e) requisitos relativos al entorno operativo de la solución de cartera, también en forma de hipótesis sobre la seguridad de los dispositivos y las plataformas en los que funcionan los componentes de *software* de la solución de cartera, incluidos los DCSC y, cuando proceda, requisitos de evaluación de la conformidad para confirmar que dichas hipótesis se verifican en los dispositivos y las plataformas pertinentes;

f) para cada hipótesis que no esté respaldada por un certificado de conformidad u otra información sobre la garantía aceptable, una descripción del mecanismo que el proveedor de cartera utiliza para hacer que se cumpla la hipótesis, así como una justificación de que el mecanismo es suficiente para garantizar la verificación de la hipótesis;

g) el establecimiento y la aplicación de medidas para garantizar el uso de una versión actualmente certificada de la solución de cartera.

4. Los esquemas nacionales de certificación contendrán requisitos funcionales relativos a mecanismos de actualización para cada componente de *software* de las soluciones de cartera y del sistema de identificación electrónica en el marco del cual se proporcionan para las operaciones enumeradas en el anexo III.

5. Los esquemas nacionales de certificación exigirán que el solicitante de la certificación proporcione al organismo de certificación, o ponga de otro modo a su disposición, la siguiente información y documentación:

a) pruebas relacionadas con la información a que se refiere el anexo IV, punto 1, incluidos, en su caso, detalles sobre la solución de la cartera y su código fuente, y en concreto:

— *información sobre la arquitectura:* para cada componente de la solución de cartera (incluidos los componentes de producto, de proceso y de servicio), una descripción de sus propiedades de seguridad esenciales, incluidas sus dependencias externas,

— *controles y niveles de seguridad:* para cada control de seguridad de la solución de cartera, una descripción del control y del nivel de seguridad requerido, basada en el anexo del Reglamento de Ejecución (UE) 2015/1502, que establezca una serie de especificaciones técnicas y procedimientos aplicables a los diversos controles ejecutados por los medios de identificación electrónica,

— *puesta en correspondencia de los controles con los componentes de la arquitectura:* una descripción de cómo se ejecutan los controles de la cartera utilizando los diferentes componentes de la solución de cartera, sobre la base de una explicación de por qué se requiere un determinado nivel de seguridad, y cómo se ejecuta el control con todos los aspectos de seguridad requeridos al nivel adecuado,

— *explicación y justificación de la cobertura del riesgo:* una justificación de:

— la puesta en correspondencia de los controles con los componentes,

— la idoneidad del plan de evaluación propuesto para cubrir adecuadamente todos los controles,

— la cobertura proporcionada por los controles de los riesgos y amenazas de ciberseguridad indicados en el registro de riesgos, completada por los controles de los riesgos y las amenazas que afectan de manera específica a la ejecución, al nivel de seguridad adecuado;

b) la información mencionada en el anexo V;

c) una lista completa de los certificados de conformidad y otra información sobre la garantía utilizada como prueba durante las actividades de evaluación;

d) cualquier otra información pertinente para las actividades de evaluación.

CAPÍTULO V

REQUISITOS RELATIVOS A LOS ORGANISMOS DE CERTIFICACIÓN

Artículo 9

Requisitos generales

1. Los organismos de certificación estarán acreditados por organismos nacionales de acreditación designados con arreglo al Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo ([13]) de conformidad con la norma EN ISO/IEC 17065:2012, siempre que cumplan los requisitos establecidos en los esquemas nacionales de certificación de conformidad con el apartado 2.

2. A efectos de acreditación, los organismos de certificación cumplirán todos los requisitos de competencia siguientes:

a) conocimiento detallado y técnico de las arquitecturas pertinentes de una solución de cartera y del sistema de identificación electrónica en el marco del cual se proporciona, así como de las amenazas y los riesgos que afectan a esas arquitecturas;

b) conocimiento de las soluciones de seguridad disponibles y de sus propiedades de conformidad con el anexo del Reglamento de Ejecución (UE) 2015/1502;

c) conocimiento de las actividades realizadas en virtud de los certificados de conformidad aplicados a los componentes de la solución de cartera y del sistema de identificación electrónica en el marco del cual se proporciona, como objeto de la certificación;

d) conocimiento detallado del esquema nacional de certificación aplicable establecido de conformidad con el capítulo II.

3. Los organismos de certificación llevarán a cabo sus actividades de vigilancia basándose, en particular, en la siguiente información:

a) la información procedente de los organismos nacionales de acreditación y las autoridades de vigilancia del mercado pertinentes;

b) la información resultante de sus propias auditorías e investigaciones o de las realizadas por otra autoridad;

c) las reclamaciones y los recursos recibidos de conformidad con el artículo 15.

Artículo 10

Subcontratación

Los organismos de certificación podrán subcontratar a terceros las actividades de evaluación establecidas en el artículo 13. Cuando se subcontraten actividades de evaluación, los esquemas nacionales de certificación establecerán lo siguiente:

1) todos los subcontratistas del organismo de certificación que lleven a cabo actividades de evaluación cumplirán, según proceda y sea adecuado para las actividades que deban realizarse, los requisitos de normas armonizadas, como EN ISO/IEC 17025:2017 para los ensayos, EN ISO/IEC 17020:2012 para la inspección, EN ISO/IEC 17021-1:2015 para la auditoría, y EN ISO/IEC 17029:2019 para la validación y la verificación;

2) los organismos de certificación asumirán la responsabilidad de todas las actividades de evaluación externalizadas a otros organismos y demostrarán que han adoptado las medidas adecuadas durante su acreditación, incluso si se han basado en la propia acreditación de sus subcontratistas, cuando proceda;

3) el grado de aceptación previa de la externalización que se obtendrá de los dueños del esquema o del cliente cuya solución de cartera esté siendo certificada con arreglo al sistema de certificación.

([13]) Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos y por el que se deroga el Reglamento (CEE) n.º 339/93 (DO L 218 de 13.8.2008, p. 30, ELI: http://data.europa.eu/eli/reg/2008/765/oj).

Artículo 11

Notificación al organismo de supervisión

Los organismos de certificación notificarán al organismo de supervisión a que se refiere el artículo 46 *bis*, apartado 1, del Reglamento (UE) n.º 910/2014 la expedición, la suspensión y la cancelación de los certificados de conformidad de las soluciones de cartera y del sistema de identificación electrónica en el marco del cual se proporcionan.

Artículo 12

Gestión de incidentes y vulnerabilidades

1. Los organismos de certificación suspenderán, sin demora indebida, el certificado de conformidad de las soluciones de cartera y del sistema de identificación electrónica en el marco del cual se proporcionan una vez que confirmen que una violación o una puesta en peligro de la seguridad notificada afecta a la conformidad con los requisitos de los esquemas nacionales de certificación de la solución de cartera o del sistema de identificación electrónica en el marco del cual se proporciona.

2. Los organismos de certificación cancelarán el certificado de conformidad que haya sido suspendido a raíz de una violación o una puesta en peligro de la seguridad que no se hayan subsanado en tiempo útil.

3. Los organismos de certificación cancelarán los certificados de conformidad cuando una vulnerabilidad detectada no se haya subsanado oportunamente de manera proporcional a su gravedad y a su impacto potencial, de conformidad con el artículo 5 *quater*, apartado 4, y con el artículo 5 *sexies*, apartado 2, del Reglamento (UE) n.º 910/2014.

CAPÍTULO VI

ACTIVIDADES DE EVALUACIÓN DE LA CONFORMIDAD

Artículo 13

Actividades de evaluación

1. Los esquemas nacionales de certificación contendrán los métodos y procedimientos que deberán utilizar los organismos de evaluación de la conformidad cuando realicen sus actividades de evaluación con arreglo a la norma EN ISO/IEC 17065:2012, que comprenderán, como mínimo, los siguientes aspectos:

a) los métodos y los procedimientos para realizar las actividades de evaluación, incluidos los relacionados con el DCSC, tal como se establece en el anexo IV;

b) la auditoría de la ejecución de la solución de cartera y del sistema de identificación electrónica en el marco del cual se proporciona, basada en el registro de riesgos establecido en el anexo I y completado, en caso necesario, con los riesgos que afecten de manera específica a la ejecución;

c) las actividades de ensayo funcional, basadas, cuando estén disponibles y sean adecuadas, en series de pruebas definidas con arreglo a especificaciones o normas técnicas;

d) evaluación de la existencia de procesos de mantenimiento y de su idoneidad, y en particular, como mínimo, de la gestión de las versiones, las actualizaciones y las vulnerabilidades;

e) evaluación de la eficacia operativa de los procesos de mantenimiento, y en particular, como mínimo, de la gestión de las versiones, las actualizaciones y las vulnerabilidades;

f) análisis de la dependencia facilitado por el proveedor de cartera, incluida una metodología para evaluar la aceptabilidad de la información sobre la garantía, que comprenderá los elementos establecidos en el anexo VI;

g) evaluación de la vulnerabilidad, al nivel adecuado, que incluya:

— una revisión del diseño de la solución de cartera y, en su caso, de su código fuente,

— un ensayo de la resistencia de la solución de cartera frente a atacantes con elevado potencial de ataque para mantener un nivel de seguridad «alto» de conformidad con la sección 2.2.1 del anexo del Reglamento de Ejecución (UE) 2015/1502;

h) una evaluación de la evolución del entorno de amenazas y su repercusión en la cobertura de los riesgos por parte de la solución de cartera, a fin de determinar qué actividades de evaluación son necesarias para los distintos componentes de la solución de cartera.

2. Los esquemas nacionales de certificación contendrán una evaluación para determinar si la ejecución de las soluciones de cartera y del sistema de identificación electrónica en el marco del cual dichas soluciones se proporcionan se ajustan a la arquitectura establecida en el artículo 3, apartado 5, letra a), y una evaluación para determinar si el plan de evaluación propuesto junto con la ejecución se ajusta al plan de evaluación a que se refiere el artículo 3, apartado 5, letra c).

3. Los esquemas nacionales de certificación establecerán normas de muestreo para evitar la repetición de actividades de evaluación idénticas y centrarse en actividades que sean específicas de una variante determinada. Esas normas de muestreo harán que puedan realizarse ensayos funcionales y de seguridad solo sobre una muestra de variantes de un componente específico de una solución de cartera y del sistema de identificación electrónica en el marco del cual se proporciona y sobre una muestra de dispositivos específicos. Los esquemas nacionales de certificación exigirán a todos los organismos de certificación que justifiquen su uso del muestreo.

4. Los esquemas nacionales de certificación exigirán que el organismo de certificación evalúe la ACSC con arreglo a los métodos y procedimientos establecidos en el anexo IV.

Artículo 14

Actividades de certificación

1. Los esquemas nacionales de certificación establecerán una actividad de atestación a efectos de expedir un certificado de conformidad, de acuerdo con la sección V(a) de la Tabla 1 de EN ISO/IEC 17067:2013, que incluya los siguientes aspectos:

a) el contenido del certificado de conformidad según lo establecido en el anexo VII;

b) el modo en que deben comunicarse los resultados de la evaluación en el informe público de certificación, incluido al menos un resumen del plan preliminar de auditoría y validación, tal como se establece en el anexo VIII;

c) el contenido de los resultados de la evaluación comunicados en el informe de evaluación de la certificación, incluidos los elementos establecidos en el anexo VIII.

2. El informe de evaluación de la certificación podrá ponerse a disposición del Grupo de Cooperación y de la Comisión.

Artículo 15

Reclamaciones y recursos

Los esquemas nacionales de certificación contendrán procedimientos o referencias a la legislación nacional aplicable, que definan el mecanismo para presentar y tramitar eficazmente las reclamaciones y los recursos en relación con su ejecución del esquema de certificación o con un certificado de conformidad expedido. Estos procedimientos incluirán la comunicación al reclamante de información sobre el avance del procedimiento y sobre la decisión adoptada, así como de información sobre su derecho a una tutela judicial efectiva. Los esquemas nacionales de certificación exigirán que todas las reclamaciones y todos los recursos que no hayan sido resueltos o no puedan ser resueltos por el organismo de certificación se remitan al dueño del esquema para su evaluación y resolución.

Artículo 16

Actividades de vigilancia

1. Los esquemas nacionales de certificación exigirán a los organismos de certificación que lleven a cabo actividades de vigilancia consistentes en la evaluación de vigilancia de los procesos combinada con ensayos o inspecciones aleatorios.

2. Los esquemas nacionales de certificación contendrán requisitos para que los dueños de los esquemas supervisen el cumplimiento por parte de los organismos de certificación de sus obligaciones en virtud del Reglamento (UE) n.º 910/2014 y de los esquemas nacionales de certificación, si procede.

3. Los esquemas nacionales de certificación contendrán requisitos para que los organismos de certificación supervisen lo siguiente:

a) el cumplimiento, por parte de los titulares de un certificado de conformidad expedido en el marco de esquemas nacionales de certificación, de sus obligaciones en materia de certificación con arreglo al Reglamento (UE) n.º 910/2014 y a los esquemas nacionales de certificación;

b) el cumplimiento por la solución de cartera certificada de los requisitos establecidos en los esquemas nacionales de certificación.

Artículo 17

Consecuencias del incumplimiento

Los esquemas nacionales de certificación establecerán las consecuencias de la no conformidad de una solución de cartera certificada y del sistema de identificación electrónica en el marco del cual se proporciona con los requisitos establecidos en el presente Reglamento. Esas consecuencias incluirán los siguientes aspectos:

1) la obligación del organismo de certificación de informar al titular del certificado de conformidad y de solicitarle que aplique medidas correctoras;

2) la obligación del organismo de certificación de informar a otras autoridades de vigilancia del mercado pertinentes cuando la no conformidad afecte al Derecho de la Unión aplicable;

3) las condiciones para la adopción de medidas correctoras por parte del titular del certificado de conformidad;

4) las condiciones para la suspensión de un certificado de conformidad por el organismo de certificación y para el restablecimiento del certificado de conformidad una vez que se haya subsanado la no conformidad;

5) las condiciones para la cancelación de un certificado de conformidad por el organismo de certificación;

6) las consecuencias del incumplimiento por el organismo de certificación de los requisitos del esquema nacional de certificación.

CAPÍTULO VII

CICLO DE VIDA DE LA CERTIFICACIÓN

Artículo 18

Ciclo de vida de la certificación

1. La validez de los certificados de conformidad expedidos en el marco de los esquemas nacionales de certificación estará supeditada a las actividades de evaluación periódicas que el organismo de certificación llevará a cabo con arreglo a los requisitos establecidos en el anexo IX.

2. Los esquemas nacionales de certificación contendrán un proceso para la renovación de la certificación de las soluciones de cartera y del sistema de identificación electrónica en el marco del cual se proporcionan, cuando así lo solicite el titular del certificado de conformidad antes de que expire el certificado de conformidad inicial. Dicho proceso de renovación de la certificación comprenderá una evaluación completa de la solución de cartera y del sistema de identificación electrónica en el marco del cual se proporciona, incluida una evaluación de la vulnerabilidad, con arreglo a los principios establecidos en el anexo IX.

3. Los esquemas nacionales de certificación contendrán un proceso para gestionar los cambios en las soluciones de cartera y el sistema de identificación electrónica en el marco del cual se proporcionan. Ese proceso incluirá normas para determinar si un cambio debe estar cubierto por una evaluación especial como la contemplada en el apartado 4 o por la verificación de la eficacia operativa de los procesos de mantenimiento a que se refiere el anexo IV.

4. Los esquemas nacionales de certificación contendrán un proceso para evaluaciones especiales de conformidad con la norma EN ISO/IEC 17065:2012. Dicho proceso de evaluaciones especiales incluirá una selección de las actividades que se llevarán a cabo para abordar la cuestión específica que dio lugar a la evaluación especial.

5. Los esquemas nacionales de certificación establecerán normas relativas a la cancelación de un certificado de conformidad.

CAPÍTULO VIII

CONSERVACIÓN DE REGISTROS Y PROTECCIÓN DE LA INFORMACIÓN

Artículo 19

Conservación de registros

1. Los esquemas nacionales de certificación contendrán requisitos para los organismos de certificación relativos a un sistema de registro para toda la información pertinente producida a raíz de las actividades de evaluación de la conformidad realizadas por ellos, incluidos los datos expedidos y recibidos por los proveedores de las soluciones de cartera y los sistemas de identificación electrónica en el marco de los cuales se proporcionan. Los registros de esta información quedarán depositados de manera segura. Los registros podrán conservarse electrónicamente y permanecerán accesibles durante el tiempo que lo exija el Derecho de la Unión o el Derecho nacional, y durante al menos cinco años tras la cancelación o la expiración del certificado de conformidad pertinente.

2. Los esquemas nacionales de certificación establecerán requisitos para que el titular del certificado de conformidad almacene de forma segura, a efectos del presente Reglamento y durante al menos cinco años tras la cancelación o la expiración del certificado de conformidad pertinente, la siguiente información:

a) registros de la información facilitada al organismo de certificación o a cualquiera de sus subcontratistas durante el proceso de certificación;

b) muestras de los componentes de *hardware* que hayan sido incluidos en el ámbito de la certificación para la solución de cartera.

3. Los esquemas nacionales de certificación exigirán al titular del certificado de conformidad que ponga la información a que se refiere el apartado 1 a disposición del organismo de certificación o del organismo de supervisión a que se refiere el artículo 46 *bis*, apartado 1, del Reglamento (UE) n.º 910/2014, cuando se le solicite.

Artículo 20

Protección de la información

En el marco de los esquemas nacionales de certificación, se exigirá a todas las personas u organizaciones a las que se conceda acceso a información en la ejecución de actividades englobadas en el sistema nacional de certificación que garanticen la seguridad y la protección de los secretos comerciales y otra información confidencial, así como que preserven los derechos de propiedad intelectual e industrial, y que adopten las medidas técnicas y organizativas necesarias y adecuadas para garantizar esta confidencialidad.

CAPÍTULO IX

DISPOSICIONES FINALES

Artículo 21

Transición a un esquema europeo de certificación de la ciberseguridad

El presente Reglamento estará sujeto a revisión, cuando se adopte el primer esquema europeo de certificación de la ciberseguridad para soluciones de cartera y los sistemas de identificación electrónica en el marco de los cuales se proporcionan, con el objetivo de tener en cuenta la contribución de dicho esquema europeo de certificación de la ciberseguridad a la certificación general de esas soluciones de cartera y esos sistemas.

Artículo 22

Entrada en vigor

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

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

Hecho en Bruselas, el 28 de noviembre de 2024.

Por la Comisión
La Presidenta
Ursula VON DER LEYEN

ANEXO I

REGISTRO DE RIESGOS PARA LAS CARTERAS EUROPEAS DE IDENTIDAD DIGITAL

Introducción

El registro de riesgos describe los principales riesgos y amenazas para la seguridad y la privacidad que afectan a las carteras, y que deben ser adecuadamente tratados en todas las arquitecturas y ejecuciones de las carteras. Los **riesgos de nivel alto** (sección I) están relacionados con el uso de las carteras por los usuarios y por las partes usuarias, y están asociados a amenazas directas que afectan a los activos de las carteras. Además, se indican algunos **riesgos a nivel de sistema** (sección II) para las carteras, que normalmente serían el resultado de una combinación de amenazas dirigidas a todo el sistema de la cartera.

Tipo de riesgo	Identificador del riesgo	Denominaciones de los riesgos correspondientes
Riesgos de nivel alto para las carteras	R1	Creación o uso de una identidad electrónica existente
	R2	Creación o uso de una identidad electrónica falsa
	R3	Creación o uso de atributos falsos
	R4	Usurpación de identidad
	R5	Robo de datos
	R6	Divulgación de datos
	R7	Manipulación de datos
	R8	Pérdida de datos
	R9	Transacción no autorizada
	R10	Manipulación de transacciones
	R11	Repudio
	R12	Divulgación de datos de una transacción
	R13	Interrupción del servicio
	R14	Vigilancia
Riesgos relacionados con el sistema	SR1	Vigilancia integral
	SR2	Daño reputacional
	SR3	Incumplimiento de la normativa

El registro recoge también **amenazas técnicas** (sección III) dirigidas a la ejecución de la solución de cartera. Estas amenazas están relacionadas con los riesgos de nivel alto, en el sentido de que cada una de ellas puede utilizarse para provocar muchos riesgos de nivel alto.

Tipo de amenaza	Identificador de la amenaza	Denominaciones de las amenazas correspondientes	Subcategorías de amenazas
Amenaza técnica	TT1	Ataques físicos	1.1. *Robo*
			1.2. *Fuga de información*
			1.3. *Manipulación fraudulenta*
	TT2	Errores y fallos de configuración	2.1. *Errores cometidos al gestionar un sistema informático*
			2.2. *Errores a nivel de la aplicación o errores de uso*
			2.3. *Errores en la fase de desarrollo y fallos en la configuración del sistema*

Tipo de amenaza	Identificador de la amenaza	Denominaciones de las amenazas correspondientes	Subcategorías de amenazas
	TT3	Uso de recursos poco fiables	3.1. *Uso o configuración erróneos de los componentes de la cartera*
	TT4	Averías y cortes	4.1. *Avería o disfunción del equipo, los dispositivos o los sistemas*
			4.2. *Pérdida de recursos*
			4.3. *Pérdida de servicios de apoyo*
	TT5	Acciones malintencionadas	5.1. *Intercepción de información*
			5.2. *Captación ilegítima de datos confidenciales y suplantación*
			5.3. *Repetición de mensajes*
			5.4. *Ataque de fuerza bruta*
			5.5. *Vulnerabilidades del software*
			5.6. *Ataques a la cadena de suministro*
			5.7. *Programa malicioso*
			5.8. *Predicción de números aleatorios*

Por último, en el registro se enumeran **amenazas directas a las carteras**, cada una de ellas asociada a una selección (no exhaustiva) de riesgos (sección IV).

SECCIÓN I

Riesgos de nivel alto para las carteras

R1. Creación o uso de una identidad electrónica existente

La creación o el uso de una identidad electrónica existente se define como la creación, en una cartera, de una identidad electrónica que existe en el mundo real y está asignada a otro usuario. Por su naturaleza, este riesgo da lugar a los riesgos de usurpación de identidad (R4) y transacciones no autorizadas (R9).

R2. Creación o uso de una identidad electrónica falsa

La creación o el uso de una identidad electrónica falsa se define como la creación, en una cartera, de una identidad electrónica que no existe en el mundo real.

R3. Creación o uso de atributos falsos

La creación o el uso de atributos falsos se define como la creación o el uso de atributos que no pueden ser validados para su expedición por el supuesto proveedor y en los que no se puede confiar.

R4. Usurpación de identidad

La usurpación de identidad se define como la adquisición no autorizada de la unidad de cartera o la pérdida de factores de autenticación de modo que sea posible hacerse pasar por una persona.

R5. Robo de datos

El robo de datos se define como la extracción no autorizada de datos. El robo de datos está asociado también a amenazas, como la interceptación de datos (captura no autorizada de datos en tránsito) y el descifrado de datos (descodificación no autorizada de datos cifrados), que es probable que den lugar en algunos casos a la divulgación de datos (R6).

R6. Divulgación de datos

La divulgación de datos se define como la exposición no autorizada de datos personales, incluidas categorías especiales de datos personales. El riesgo de violación de la privacidad es muy similar si se considera desde el punto de vista de la privacidad y no de la seguridad.

R7. Manipulación de datos

La manipulación de datos se define como la alteración no autorizada de datos.

R8. Pérdida de datos

La pérdida de datos se define como la situación en que los datos almacenados en la cartera se pierden por un uso indebido o un acción maliciosa. Este riesgo suele ser un riesgo secundario de la manipulación de datos (R7) o de la interrupción del servicio (R13), cuando no pueden recuperarse los datos, o parte de ellos.

R9. Transacción no autorizada

Las transacciones no autorizadas se definen como actividades operativas realizadas sin el permiso o el conocimiento del usuario de una cartera. En muchos casos, una transacción no autorizada puede llevar a una usurpación de identidad (R4) o una divulgación de datos (R6). Está relacionado también con transacciones no autorizadas, como el uso indebido de claves criptográficas.

R10. Manipulación de transacciones

La manipulación de transacciones se define como la alteración no autorizada de operaciones de la cartera. La manipulación de transacciones es un ataque a la integridad y está relacionada con la violación de la integridad de los datos.

R11. Repudio

El repudio se define como una situación en la que una parte interesada puede negar haber realizado una acción o haber participado en una transacción, y otras partes interesadas no tienen pruebas adecuadas para contradecirla.

R12. Divulgación de datos de una transacción

La divulgación de datos de una transacción se define como la divulgación de información relacionada con información sobre una transacción entre partes interesadas.

R13. Interrupción del servicio

La interrupción del servicio se define como una interrupción o degradación del funcionamiento normal de la cartera. Un tipo específico de interrupción del servicio es el bloqueo del usuario, que se define como la incapacidad de un usuario para acceder a su cuenta o su cartera.

R14. Vigilancia

La vigilancia, o supervisión, se define como el seguimiento o la observación no autorizados de las actividades, la comunicación o los datos del usuario de una cartera. La vigilancia está a menudo relacionada con la inferencia, que se define como la deducción de información sensible o personal a partir de datos aparentemente inocuos.

SECCIÓN II

Riesgos relacionados con el sistema

Estos riesgos no figuran en la lista de amenazas, ya que suelen ser la consecuencia de múltiples amenazas, repetidas de manera que resulta afectado todo el sistema.

SR1. Vigilancia integral

La vigilancia integral se define como el seguimiento o la observación de las actividades de muchos usuarios a través de la comunicación o los datos de su cartera. La vigilancia integral está a menudo asociada a la vigilancia (R14) y la inferencia a escala mundial, cuando se combina la información sobre muchos usuarios para deducir datos sensibles o personales sobre ellos o para identificar tendencias estadísticas que pueden utilizarse para diseñar nuevos ataques.

SR2. Daño reputacional

El daño reputacional se define como el daño causado a la reputación de una organización o de un organismo público. El daño reputacional se deriva también de otros riesgos, cuando los medios de comunicación cubren una violación o un incidente y proyectan una imagen desfavorable de la organización afectada. A su vez, el daño reputacional puede conducir a otros riesgos, como la pérdida de confianza, derivada de las dudas razonables del usuario, y la pérdida de ecosistema, cuando es todo el ecosistema el que se derrumba.

SR3. Incumplimiento de la normativa

El incumplimiento de la normativa se define como una situación en la que no es posible acatar la legislación, los reglamentos o las normas aplicables. En el contexto de la cartera, puesto que la seguridad y la privacidad de la solución son requisitos normativos, es probable que todas las amenazas conduzcan a algún tipo de incumplimiento de la normativa.

SECCIÓN III

Amenazas técnicas

No todas las amenazas técnicas están vinculadas a riesgos específicos sobre las carteras, ya que muchas de ellas son medios que podrían utilizarse para llevar a cabo ataques correspondientes a muchos riesgos diferentes.

TT1. Ataques físicos

1.1. *Robo*

El robo se define como el robo de dispositivos que puede alterar el correcto funcionamiento de la cartera (en caso de que el dispositivo sea sustraído y la unidad de cartera no esté adecuadamente protegida). Este ataque puede propiciar numerosos riesgos, como la usurpación de identidad (R4), el robo de datos (R5) y las transacciones no autorizadas (R9).

1.2. *Fuga de información*

La fuga de información se define como el acceso no autorizado a información, su exposición o su divulgación tras un acceso físico a la cartera. Estas situaciones pueden contribuir en particular a la divulgación de datos (R6) y al robo de datos (R5).

1.3. *Manipulación fraudulenta*

La manipulación fraudulenta se define como la violación de la integridad de uno o múltiples componentes de la unidad de cartera, o de los componentes en los que se basa la unidad de cartera, como el dispositivo del usuario o su sistema operativo. Esto puede contribuir en particular a la manipulación de datos (R7), la pérdida de datos (R8) y la manipulación de transacciones (R10). Cuando la manipulación fraudulenta se dirige a componentes de *software*, puede contribuir a numerosos riesgos.

TT2. Errores y fallos de configuración

2.1. *Errores cometidos al gestionar un sistema informático*

Los errores cometidos al gestionar un sistema informático se definen como la fuga o divulgación de información, o los daños causados a la información, por un uso indebido de los activos informáticos por los usuarios (desconocimiento de las características de la aplicación) o por una configuración o gestión incorrectas de los activos informáticos.

2.2. *Errores a nivel de la aplicación o errores de uso*

Los errores a nivel de la aplicación o errores de uso se definen como disfunciones de la aplicación debidas a un error en la propia aplicación o a un error cometido por uno de los usuarios (usuarios de una cartera o partes usuarias de la cartera).

2.3. *Errores en la fase de desarrollo y fallos en la configuración del sistema*

Los errores en la fase de desarrollo y los fallos en la configuración del sistema se definen como disfunciones o vulnerabilidades causadas por el desarrollo o la configuración incorrectos de activos informáticos o procesos empresariales (especificaciones inadecuadas de los productos informáticos, insuficiente facilidad de uso, interfaces inseguras, flujos de políticas y de procedimientos incorrectos o errores de diseño).

TT3. Uso de recursos poco fiables

El uso de recursos poco fiables se define como una actividad que origina daños no intencionados causados por defectos en la definición de las relaciones de confianza, como el hecho de confiar en un proveedor tercero sin garantías suficientes.

3.1. *Uso o configuración erróneos de los componentes de la cartera*

El uso o la configuración erróneos de los componentes de la cartera se define como el hecho de causar daños no intencionados a los componentes de la cartera debido a un uso o una configuración erróneos por los usuarios de una cartera o por desarrolladores insuficientemente formados, o a falta de adaptación a los cambios acaecidos en el panorama de amenazas, normalmente asociados al uso de componentes de terceros o plataformas de tiempo de ejecución vulnerables.

TT4. Averías y cortes

4.1. *Avería o disfunción del equipo, los dispositivos o los sistemas*

Una avería o una disfunción del equipo se define como un daño no intencionado a los activos informáticos causado por una avería o una disfunción del equipo, incluidos la infraestructura del proveedor y los dispositivos del usuario.

4.2. *Pérdida de recursos*

La pérdida de recursos se define como un corte o una disfunción debidos a la no disponibilidad de esos recursos, por ejemplo, piezas de mantenimiento.

4.3. *Pérdida de servicios de apoyo*

La pérdida de servicios de apoyo se define como un corte o una disfunción debidos a la no disponibilidad de servicios de apoyo necesarios para el adecuado funcionamiento del sistema, incluida la conectividad a la red de la infraestructura del proveedor y del dispositivo del usuario.

TT5. Acciones malintencionadas

5.1. *Intercepción de información*

La intercepción de información se define como la captura de información incorrectamente protegida durante su transmisión, incluidos los ataques de intermediarios.

5.2. *Captación ilegítima de datos confidenciales y suplantación*

La captación ilegítima de datos confidenciales (*phishing*) se define como la captura de información proporcionada por el usuario a raíz de una interacción engañosa, a menudo asociada a la suplantación de medios de comunicación y sitios web legítimos. Estas amenazas están dirigidas al usuario y normalmente contribuyen a la usurpación de identidad (R4) y las transacciones no autorizadas (R9), a menudo a través del robo de datos (R5) o la divulgación de datos (R6).

5.3. *Repetición de mensajes*

La repetición de mensajes se define como la reutilización de mensajes previamente interceptados para llevar a cabo transacciones no autorizadas, a menudo a nivel de protocolo. Esta amenaza técnica contribuye principalmente a las transacciones no autorizadas, que a su vez pueden conducir a otros riesgos, dependiendo de la transacción.

5.4. *Ataque de fuerza bruta*

El ataque de fuerza bruta se define como una violación de la seguridad, a menudo de la confidencialidad, mediante la realización de un gran número de interacciones hasta que las respuestas proporcionan información valiosa.

5.5. *Vulnerabilidades del software*

La amenaza relacionada con las vulnerabilidades del *software* es una violación de la seguridad aprovechando una vulnerabilidad del *software* en los componentes de la cartera o en los componentes de *software* y *hardware* utilizados para la ejecución de la cartera, incluidas las vulnerabilidades que se han dado a conocer y las que no (día cero).

5.6. *Ataques a la cadena de suministro*

Un ataque a la cadena de suministro se define como una violación de la seguridad a través de ataques perpetrados contra el proveedor del proveedor de cartera o de sus usuarios para hacer posibles otros ataques en la propia cartera.

5.7. *Programa malicioso*

El programa malicioso se define como una violación de la seguridad a través de aplicaciones maliciosas que llevan a cabo acciones no deseadas e ilegítimas sobre la cartera.

5.8. *Predicción de números aleatorios*

La predicción de números aleatorios consiste en hacer posibles ataques de fuerza bruta mediante la predicción parcial o completa de números generados aleatoriamente.

SECCIÓN IV

Amenazas a las carteras

En esta última sección se presenta una selección de supuestos de amenaza característicos específicos de las carteras, que se ponen en correspondencia con los riesgos de nivel alto relacionados, enumerados más arriba. En esta lista se indican las amenazas que deben tratarse, pero no constituye una lista exhaustiva de amenazas, algo que depende en gran medida de la arquitectura de la solución de cartera seleccionada y de la evolución del entorno de amenazas. Además, en la evaluación del riesgo y las medidas propuestas, el proveedor de cartera solo puede ser responsable de los componentes incluidos en el ámbito de la certificación (*).

ID *Identificador*	Descripción de la amenaza *Descripción de la amenaza determinada (*)*	Denominación del riesgo *Riesgos relacionados*
TR1	Un atacante puede revocar seudónimos sin razón justificada.	Creación o uso de una identidad electrónica falsa (R2)
TR2	Un atacante puede expedir identidades electrónicas inventadas que no existen.	Creación o uso de una identidad electrónica falsa (R2)
TR3	Un atacante puede empezar a expedir datos de identificación de la persona no autorizados.	Creación o uso de una identidad electrónica falsa (R2)
TR4	Un atacante puede conseguir que un administrador introduzca un proveedor de datos de identidad de la persona equivocado en la lista de proveedores de datos de identidad de la persona de confianza.	Creación o uso de una identidad electrónica falsa (R2)
TR5	Un atacante puede eludir el servicio de acreditación de la identidad a distancia.	Creación o uso de una identidad electrónica existente (R1)/Creación o uso de una identidad electrónica falsa (R2)
TR6	Un atacante puede eludir el servicio de acreditación de la identidad física.	Creación o uso de una identidad electrónica existente (R1)/Creación o uso de una identidad electrónica falsa (R2)
TR7	Un atacante puede eludir los servicios de acreditación de la identidad relacionados con el uso de un certificado (cualificado) a distancia.	Creación o uso de una identidad electrónica existente (R1)/Creación o uso de una identidad electrónica falsa (R2)
TR8	Un atacante puede obtener acceso a una cartera que no está vinculada a una persona.	Creación o uso de una identidad electrónica existente (R1)/Creación o uso de una identidad electrónica falsa (R2)
TR9	Un atacante puede vencer los controles técnicos y procedimentales para crear datos de identidad de la persona erróneos.	Creación o uso de una identidad electrónica existente (R1)/Creación o uso de una identidad electrónica falsa (R2)
TR10	Un atacante puede activar una nueva cartera en un DCSC inválido.	Creación o uso de una identidad electrónica existente (R1)/Creación o uso de una identidad electrónica falsa (R2)
TR11	Un atacante puede eludir el servicio de acreditación de la identidad relacionado con el uso de medios de identificación electrónica existentes.	Creación o uso de una identidad electrónica existente (R1)/Usurpación de identidad (R4)/Transacción no autorizada (R9)
TR12	Un atacante puede sortear la verificación, por el proveedor de datos de identificación de la persona, del control de la cartera por el usuario y hacer que se expidan datos de identificación de la persona a una cartera en peligro que se encuentre bajo el control del atacante.	Creación o uso de una identidad electrónica existente (R1)/Usurpación de identidad (R4)/Transacción no autorizada (R9)

ID *Identificador*	Descripción de la amenaza *Descripción de la amenaza determinada* (*)	Denominación del riesgo *Riesgos relacionados*
TR13	Un atacante puede introducir datos de identificación de la persona válidos en una unidad de cartera inválida.	Creación o uso de una identidad electrónica existente (R1)/Usurpación de identidad (R4)/Transacción no autorizada (R9)
TR14	Un proveedor de datos de identificación de la persona puede expedir identidades inventadas que estén relacionadas con una persona existente.	Creación o uso de una identidad electrónica existente (R1)/Usurpación de identidad (R4)/Transacción no autorizada (R9)
TR15	Un atacante puede vincular datos de identificación de la persona con la cartera equivocada porque el proveedor de esos datos no es capaz de vincularlos con la cartera correcta.	Creación o uso de una identidad electrónica existente (R1)/Usurpación de identidad (R4)/Transacción no autorizada (R9)
TR16	Un atacante puede hacer que el usuario apruebe la activación de una nueva unidad/instancia de cartera controlada por el atacante, lo que conllevará también el control de las declaraciones.	Creación o uso de una identidad electrónica existente (R1)/Creación o uso de una identidad electrónica falsa (R2)/Usurpación de identidad (R4)/Transacción no autorizada (R9)
TR17	Un atacante puede expedir datos de identificación de la persona de otro Estado para acceder a los datos/activos digitales de los ciudadanos objetivo.	Creación o uso de una identidad electrónica existente (R1)/Usurpación de identidad (R4)/Transacción no autorizada (R9)
TR18	Un atacante puede vencer los controles técnicos y procedimentales para crear declaraciones electrónicas (cualificadas) de atributos falsas.	Creación o uso de atributos falsos (R3)
TR19	Un atacante puede presentar declaraciones electrónicas (cualificadas) de atributos que no le hayan sido expedidos de manera válida.	Creación o uso de atributos falsos (R3)
TR20	Un atacante puede atacar el mecanismo de vinculación criptográfica de la cartera entre los datos de identificación de la persona y una declaración electrónica (cualificada) de atributos que no se le debería haber expedido.	Creación o uso de atributos falsos (R3)
TR21	Un atacante puede utilizar una declaración electrónica (cualificada) de atributos en una cartera, aunque el correlato físico de esa declaración haya expirado o sea inválido.	Creación o uso de atributos falsos (R3)
TR22	Un atacante puede sortear la verificación por el proveedor de declaraciones electrónicas (cualificadas) de atributos del control de la cartera por el usuario y hacer que se expida una declaración electrónica (cualificada) de atributos a una cartera comprometida bajo el control del atacante.	Creación o uso de atributos falsos (R3)
TR23	Un atacante puede falsificar declaraciones electrónicas de atributos.	Creación o uso de atributos falsos (R3)
TR24	Un atacante puede inyectar declaraciones electrónicas de atributos falsificadas en una cartera.	Creación o uso de atributos falsos (R3)
TR25	La cartera puede presentar atributos a una parte usuaria sin la aprobación de un usuario.	Divulgación de datos (R6)
TR26	Se pueden presentar datos de identificación de la persona, declaraciones electrónicas (cualificadas) de atributos o seudónimos a una parte usuaria equivocada.	Divulgación de datos (R6)
TR27	Un atacante puede iniciar una renovación maliciosa de una declaración electrónica de atributos.	Divulgación de datos (R6)
TR28	Un atacante puede hacer que un usuario apruebe indebidamente una solicitud de declaraciones electrónicas de atributos (captación ilegítima de datos confidenciales u otros).	Divulgación de datos (R6)

ID *Identificador*	Descripción de la amenaza *Descripción de la amenaza determinada* (*)	Denominación del riesgo *Riesgos relacionados*
TR29	Un atacante puede filtrar atributos de la cartera e identificar a su usuario cuando la identificación no se exija o no esté permitida.	Divulgación de datos (R6)
TR30	Un atacante puede vencer los controles técnicos y procedimentales para extraer datos.	Divulgación de datos (R6)
TR31	Una solicitud puede ser filtrada a un atacante.	Divulgación de datos (R6)
TR32	Un atacante puede obtener información sobre la política de divulgación incorporada en materia de atributos y presentar atributos contenidos en la solicitud en curso de las unidades de cartera.	Divulgación de datos (R6)
TR33	Un atacante puede extraer registros, o partes de ellos.	Divulgación de datos (R6)
TR34	Un atacante puede saber si una cartera está instalada en el mismo dispositivo que él está utilizando, o en otro, y obtener información al respecto.	Divulgación de datos (R6)
TR35	Un atacante puede obtener un factor de conocimiento utilizado para la autenticación del usuario ante la ACSC.	Divulgación de datos (R6)
TR36	La declaración electrónica de atributos sobre una persona que se presenta en múltiples transacciones con una parte usuaria, o entre diferentes partes usuarias, permite involuntariamente vincular múltiples transacciones a la persona de la que se trate.	Divulgación de datos (R6)
TR37	Una lista pública de revocación de declaraciones o de partes usuarias puede contener información sobre el uso por el usuario de su declaración (por ejemplo, ubicación, dirección IP, etc.).	Divulgación de datos (R6)
TR38	Al no poder demostrar el consentimiento de los usuarios para que se compartan atributos, las partes usuarias pueden deteriorar la integridad de los registros.	Divulgación de datos (R6)
TR39	Un atacante puede rastrear ilegalmente a usuarios de una cartera utilizando identificadores únicos/rastreables.	Divulgación de datos (R6)/Vigilancia (R14)
TR40	Una parte usuaria que se compone de múltiples unidades/entidades, cada una de ellas con un ámbito diferente respecto de lo que se le permite solicitar/tratar, puede solicitar y tratar datos sin estar legalmente facultada para hacerlo.	Divulgación de datos (R6)/Transacción no autorizada (R9)
TR41	Un atacante puede alterar los controles de integridad y autenticidad que realiza la cartera de los datos de identificación de la persona a fin de obtener siempre una respuesta positiva.	Manipulación de datos (R7)
TR42	Un atacante puede eludir o trastocar los controles que realiza la cartera para verificar la integridad y la autenticidad de los atributos solicitados a fin de obtener siempre una respuesta positiva.	Manipulación de datos (R7)
TR43	Un atacante puede eludir o trastocar los controles que realiza la cartera para verificar que todos los atributos solicitados pertenecen al mismo usuario a fin de obtener siempre una respuesta positiva.	Manipulación de datos (R7)
TR44	Un atacante puede eludir o trastocar los controles que realiza la cartera para verificar que los datos de identificación de la persona son válidos y han sido expedidos por un proveedor fiable de dichos datos a fin de obtener siempre una respuesta positiva.	Manipulación de datos (R7)

ID *Identificador*	Descripción de la amenaza *Descripción de la amenaza determinada* (*)	Denominación del riesgo *Riesgos relacionados*
TR45	Un atacante puede eludir o trastocar los controles que realiza la cartera para verificar que una declaración electrónica cualificada de atributos es válida y ha sido expedida por un prestador cualificado de servicios de confianza, que está registrado para expedir dicha declaración, a fin de obtener siempre una respuesta positiva.	Manipulación de datos (R7)
TR46	Un atacante puede eludir o trastocar los controles que realiza la cartera para verificar si los datos de identificación de la persona han sido revocados por el proveedor de dichos datos a fin de obtener siempre una respuesta positiva.	Manipulación de datos (R7)
TR47	Un atacante puede eludir o trastocar los controles que realiza la cartera para verificar si la declaración electrónica (cualificada) de atributos ha sido revocada por el proveedor de dicha declaración a fin de obtener siempre una respuesta positiva.	Manipulación de datos (R7)
TR48	Un atacante puede modificar el contenido de los datos de la copia de seguridad y de recuperación que deben estar exclusivamente bajo control del usuario.	Manipulación de datos (R7)/Pérdida de datos (R8)
TR49	Un atacante puede modificar el historial de transacciones de una instancia de cartera determinada a partir de los registros de actividad.	Manipulación de datos (R7)/Pérdida de datos (R8)
TR50	Un atacante puede interceptar información durante la conexión de la cartera con las partes usuarias.	Robo de datos (R5)/Divulgación de datos (R6)
TR51	Un atacante puede convencer a un usuario para que comparta datos personales (por ejemplo, datos de identificación de la persona, declaraciones electrónicas de atributos, seudónimos, firmas electrónicas, registros y otros datos) con él o con un tercero con el que el usuario no tenía intención de hacerlo.	Robo de datos (R5)/Divulgación de datos (R6)
TR52	Un atacante puede leer el historial de transacciones de una instancia de cartera determinada a partir de los registros de actividad.	Robo de datos (R5)/Divulgación de datos (R6)
TR53	Un atacante puede exportar o extraer material de claves criptográficas fuera del DCSC.	Robo de datos (R5)/Divulgación de datos (R6)/Transacción no autorizada (R9)
TR54	Un atacante puede leer el contenido de los datos de la copia de seguridad y de recuperación que deben estar exclusivamente bajo el control del usuario.	Robo de datos (R5)/Divulgación de datos (R6)
TR55	Un atacante puede eludir el método de autenticación del usuario para utilizar un seudónimo generado por una unidad de cartera.	Usurpación de identidad (R4)
TR56	Un atacante puede proponer a los usuarios una aplicación que imite una cartera legítima específica.	Usurpación de identidad (R4)
TR57	Un atacante puede exportar datos de una cartera, incluidos datos de identificación de la persona, declaraciones electrónicas (cualificadas) de atributos o registros.	Usurpación de identidad (R4)
TR58	Un atacante puede exportar material de vinculación criptográfica.	Usurpación de identidad (R4)
TR59	Un atacante puede asumir identidades a través de las claves criptográficas de la cartera.	Usurpación de identidad (R4)
TR60	Un atacante puede duplicar la unidad de cartera personal de otro usuario en su dispositivo personal y utilizarla.	Usurpación de identidad (R4)/Creación o uso de una identidad electrónica existente (R1)

ID *Identificador*	Descripción de la amenaza *Descripción de la amenaza determinada* (*)	Denominación del riesgo *Riesgos relacionados*
TR61	Las autoridades de otro Estado pueden pedir al usuario que muestre o comparta todos los datos de la cartera en una situación de proximidad, por ejemplo cuando se atraviese la frontera de ese Estado.	Usurpación de identidad (R4)/Vigilancia (R14)
TR62	Los usuarios no pueden transferir sus registros de transacciones tras una avería de su dispositivo, lo que conlleva una pérdida de la trazabilidad de las transacciones previas en la nueva cartera.	Repudio (R11)
TR63	Los usuarios no pueden recuperar sus registros de transacciones tras una avería en su dispositivo, lo que conlleva una pérdida de la trazabilidad en la nueva cartera.	Repudio (R11)
TR64	Las partes usuarias pueden tener dificultades para demostrar el consentimiento cuando se trata de firmas electrónica a distancia.	Repudio (R11)
TR65	Un atacante puede inundar la(s) conexión(es) con solicitudes durante la conexión con las partes usuarias.	Interrupción del servicio (R13)
TR66	Un atacante puede inundar un servicio proveedor de estado con conexiones a las partes usuarias.	Interrupción del servicio (R13)
TR67	Un atacante puede hacer que la presentación de atributos aparezca como impugnada o denegada, pese a que la presentación de los atributos indique su validez.	Interrupción del servicio (R13)
TR68	Un atacante puede revocar datos de identificación de la persona sin razón justificada.	Interrupción del servicio (R13)
TR69	Un atacante puede revocar datos de identificación de la persona sin consentimiento del usuario.	Interrupción del servicio (R13)
TR70	Un atacante puede revocar una declaración electrónica (cualificada) de atributos sin razón justificada.	Interrupción del servicio (R13)
TR71	Un atacante puede revocar una declaración electrónica (cualificada) de atributos sin consentimiento del usuario.	Interrupción del servicio (R13)
TR72	Un atacante puede activar múltiples solicitudes de identificación sin que estas se reconozcan como solicitudes huérfanas intencionadas.	Interrupción del servicio (R13)
TR73	Un atacante puede enviar múltiples solicitudes a las que no siga después ninguna transacción.	Interrupción del servicio (R13)
TR74	Un atacante puede permitir que una parte usuaria solicite identificación sin una identificación correspondiente (respuesta) y control total.	Interrupción del servicio (R13)
TR75	Un atacante puede enviar una respuesta a una solicitud después de esta que haya expirado, o situaciones similares que den lugar a una interrupción del servicio.	Interrupción del servicio (R13)
TR76	Una parte usuaria puede enviar múltiples solicitudes inválidas.	Interrupción del servicio (R13)
TR77	Un atacante puede enviar múltiples solicitudes inválidas a un proveedor de cartera.	Interrupción del servicio (R13)
TR78	Un atacante puede hacer que un Estado miembro no pueda revocar a un proveedor de datos de identificación de la persona no confiable de la lista de confianza de proveedores de datos de identificación de la persona de confianza.	Interrupción del servicio (R13)
TR79	Un atacante puede impedir la suspensión o la revocación de una cartera.	Interrupción del servicio (R13)

ID *Identificador*	Descripción de la amenaza *Descripción de la amenaza determinada* (*)	Denominación del riesgo *Riesgos relacionados*
TR80	Un atacante puede bloquear las transacciones de las partes usuarias, los usuarios o el proveedor de datos de identificación de la persona.	Interrupción del servicio (R13)
TR81	Un atacante puede inutilizar o dejar indisponible un DCSC.	Interrupción del servicio (R13)
TR82	Un atacante puede hacer que el proveedor de datos de identificación de la persona sea incapaz de revocar o suspender esos datos.	Interrupción del servicio (R13)/Transacción no autorizada (R9)
TR83	Una parte usuaria puede hallar por deducción otros datos de identidad del usuario además de los datos compartidos con ella.	Vigilancia (R14)
TR84	Un grupo de partes usuarias o proveedores de datos de identificación de la persona que actúen en connivencia puede hallar por deducción otros datos de identidad del usuario además de los datos compartidos con ellos.	Vigilancia (R14)
TR85	Un atacante puede seguir y rastrear a un usuario utilizando los datos de identificación de la persona de ese usuario cuando no se requiera su identificación.	Vigilancia (R14)
TR86	Un atacante puede combinar una presentación «inventada» de combinaciones de declaraciones electrónicas (cualificadas) de atributos.	Manipulación de transacciones (R10)
TR87	Un atacante puede activar la cartera o hacerse con ella a distancia (por ejemplo, una aplicación bancaria que incorpore una solicitud de autenticación o declaración) sin el consentimiento explícito o el control exclusivo del usuario, en situaciones en las que este no es consciente (por ejemplo, mientras duerme) o no puede ver a la parte usuaria.	Manipulación de transacciones (R10)
TR88	Los atacantes pueden introducir cambios en los metadatos de una solicitud (nombre del servicio, usos, etc.).	Manipulación de transacciones (R10)
TR89	Los atacantes pueden introducir cambios en la información de las respuestas (estado del servicio, número de un solo uso, etc.).	Manipulación de transacciones (R10)
TR90	Los atacantes pueden introducir cambios en la información sobre los atributos de una solicitud (sobreabundancia de demandas, etc.).	Manipulación de transacciones (R10)
TR91	Una parte usuaria puede repetir en una sesión elementos de una sesión anterior.	Manipulación de transacciones (R10)
TR92	Un atacante puede sustituir o modificar los datos de identificación de la persona durante su transferencia del proveedor de esos datos a la unidad de cartera.	Manipulación de transacciones (R10)
TR93	Un atacante puede sustituir o modificar los datos de identificación de la persona durante su transferencia de la unidad de cartera a la parte usuaria en línea.	Manipulación de transacciones (R10)
TR94	Un atacante puede sustituir o modificar los datos de identificación de la persona durante su transferencia de la unidad de cartera a la parte usuaria fuera de línea.	Manipulación de transacciones (R10)
TR95	Un atacante puede expedir datos de identificación de la persona sin consentimiento del usuario.	Transacción no autorizada (R9)
TR96	Un atacante puede utilizar políticas de divulgación incorporadas revocadas o inválidas, posiblemente sin el conocimiento de las partes usuarias.	Transacción no autorizada (R9)
TR97	Un atacante puede amañar la cartera para que verifique firmas electrónicas erróneas.	Transacción no autorizada (R9)
TR98	Un atacante puede utilizar la cartera fuera del control del usuario.	Transacción no autorizada (R9)

ID *Identificador*	Descripción de la amenaza *Descripción de la amenaza determinada* (*)	Denominación del riesgo *Riesgos relacionados*
TR99	Un atacante puede convencer a un usuario para que autentique y apruebe transacciones con un atacante o un tercero no autorizado.	Transacción no autorizada (R9)
TR100	Un atacante puede hacer que un usuario firme electrónicamente sin presentarle antes el contenido o habiéndole presentado un contenido erróneo.	Transacción no autorizada (R9)
TR101	Un atacante puede eludir el control de acceso de la cuenta del usuario con el proveedor de cartera.	Transacción no autorizada (R9)
TR102	Un atacante puede hacerse pasar por las partes usuarias durante la conexión con las partes usuarias.	Transacción no autorizada (R9)/Divulgación de datos (R6)
TR103	El usuario que está tras la conexión de la parte usuaria con el navegador puede ser diferente del usuario que está tras la conexión de la parte usuaria con la cartera.	Transacción no autorizada (R9)/Divulgación de datos (R6)/Usurpación de identidad (R4)
TR104	Un atacante puede convencer al usuario para que revoque su cartera sin motivo.	Transacción no autorizada (R9)/Interrupción del servicio (R13)
TR105	Un atacante puede llevar a cabo ataques de intermediarios.	Transacción no autorizada (R9)/Divulgación de datos (R6)/Vigilancia (R14)
TR106	Un atacante puede presentar atributos inválidos o revocados de una cartera que no se conecta periódicamente a la red.	Efecto en diversos riesgos
TR107	Un atacante puede robar información de un usuario suplantando una cartera.	Efecto en diversos riesgos
TR108	Un atacante puede hacerse pasar por el usuario repitiendo o imitando una solicitud de datos (por ejemplo, autenticación), que parecería válida.	Efecto en diversos riesgos
TR109	Un atacante puede repetir una política de divulgación incorporada con respecto a un usuario, para imitar una solicitud aprobada.	Efecto en diversos riesgos
TR110	Un atacante puede aprovechar la falta de información de los usuarios de una cartera, o retrasos indebidos, tras una violación o puesta en peligro de la seguridad.	Efecto en diversos riesgos
TR111	Un atacante puede modificar una instancia de cartera legítima instalada previamente para añadir elementos maliciosos.	Efecto en diversos riesgos
TR112	Un atacante puede modificar una instancia de cartera legítima y proponérsela a los usuarios como legítima.	Efecto en diversos riesgos
TR113	Un atacante puede vencer el propio mecanismo de autenticación del usuario para eludir la autenticación del usuario de una cartera.	Efecto en diversos riesgos
TR114	Un atacante puede introducir un código malicioso o puertas traseras en el código de la cartera durante su implantación en el dispositivo del usuario.	Efecto en diversos riesgos
TR115	Un atacante puede introducir un código malicioso o puertas traseras en el código de la cartera durante su desarrollo.	Efecto en diversos riesgos
TR116	Un atacante puede manipular de forma fraudulenta la generación de números aleatorios con el fin de reducir su entropía lo suficiente para que puedan realizarse ataques.	Efecto en diversos riesgos

ID *Identificador*	Descripción de la amenaza *Descripción de la amenaza determinada* (*)	Denominación del riesgo *Riesgos relacionados*
TR117	Un atacante puede manipular fraudulentamente los dispositivos del usuario en la cadena de suministro para incluir códigos o configuraciones que no cumplan las condiciones de uso de la cartera.	Efecto en diversos riesgos
TR118	Un atacante puede activar una unidad de cartera utilizando un DCSC suplantado controlado por los atacantes.	Efecto en diversos riesgos
TR119	Un atacante puede leer información enviada a la ACSC o al DCSC.	Efecto en diversos riesgos
TR120	Un atacante puede enviar información arbitraria a la ACSC.	Efecto en diversos riesgos
TR121	Un atacante puede robar información interceptando los intercambios entre la ACSC y el DCSC.	Efecto en diversos riesgos
TR122	Un atacante puede enviar información arbitraria al DCSC.	Efecto en diversos riesgos
TR123	Un atacante puede enviar información al DCSC, sorteando la ACSC.	Efecto en diversos riesgos
TR124	Un atacante puede utilizar la captación ilegítima de datos confidenciales con el fin de conseguir usuarios para una falsa aplicación web de gestión de carteras y datos de identificación de la persona.	Efecto en diversos riesgos
TR125	Un atacante puede sustituir las claves de una cartera por otras para crear mensajes que se utilizarán en otro ataque.	Efecto en diversos riesgos
TR126	Un atacante puede modificar o destruir las claves de una cartera, haciendo que algunas funciones de la cartera queden inservibles.	Efecto en diversos riesgos
TR127	Un atacante puede controlar un programa malicioso para acceder a los datos almacenados en la cartera.	Efecto en diversos riesgos
TR128	Un atacante puede acceder a las pruebas generadas en la cartera.	Efecto en diversos riesgos
TR129	Los proveedores de cartera pueden acceder a objetos en la cartera.	Efecto en diversos riesgos
TR130	Los proveedores de cartera pueden acceder a pruebas generadas en la cartera.	Efecto en diversos riesgos
TR131	Un atacante puede robar un dispositivo de cartera no bloqueado.	Efecto en diversos riesgos
TR132	Un atacante puede manipular el sistema para impedir que determinados sucesos queden registrados.	Efecto en diversos riesgos
TR133	Un atacante puede interceptar la comunicación entre la instancia de cartera y la ACSC, o repetir o imitar a un usuario (por ejemplo, secuestrando el mecanismo de autenticación).	Efecto en diversos riesgos

ANEXO II

CRITERIOS PARA EVALUAR LA ACEPTABILIDAD DE LA INFORMACIÓN SOBRE LA GARANTÍA

Nombre	Objeto	Puntos de atención
Esquema europeo de certificación de la ciberseguridad basado en los criterios comunes (EUCC)	Productos de TIC	Sobre el emisor: ninguno (organismos de certificación acreditados) Sobre el ámbito de aplicación: — Comprobar el perfil de protección y el objetivo de seguridad — Comprobar el nivel de garantía de la evaluación (EAL) y los aumentos Sobre la garantía: — Comprobar las restricciones en la documentación dirigida a los usuarios — Para la composición, puede requerirse el acceso al informe técnico de evaluación
Esquema europeo de certificación de la ciberseguridad sobre servicios en la nube (EUCS) (cuando esté disponible)	Servicios en la nube	Sobre el emisor: ninguno (organismos de certificación acreditados) Sobre el ámbito de aplicación: — Comprobar la descripción del servicio en la nube — Comprobar el nivel de evaluación y los perfiles de extensión Sobre la garantía: — Comprobar la información sobre la transparencia y, si es necesario, sobre la composición
Esquemas de criterios comunes operativos en la UE, incluidos los esquemas SOG-IS	Productos de TIC	Sobre el emisor: ninguno (Estados miembros) Sobre el ámbito de aplicación: — Comprobar el perfil de protección y el objetivo de seguridad — Comprobar el nivel de garantía de la evaluación y los aumentos Sobre la garantía: — Comprobar las restricciones en la documentación dirigida a los usuarios — Para la composición, puede requerirse el acceso al informe técnico de evaluación
EN 17640:2018 (FITCEM, incluidos CSPN, BSZ, LINCE, BSZA)	Productos de TIC	Sobre el emisor: — Comprobar el esquema y los requisitos para los organismos de certificación Sobre el ámbito de aplicación: — Comprobar la descripción del producto — Comprobar las alegaciones de seguridad — Comprobar el nivel de garantía Sobre la garantía: — Comprobar las actividades realizadas y las conclusiones del informe
Esquemas de certificación de dispositivos cualificados de creación de firmas de conformidad con el artículo 30 del Reglamento (UE) n.º 910/2014	QSCD (dispositivo cualificado de creación de firma)	Sobre el emisor: — Comprobar el esquema y los requisitos para los organismos de certificación Sobre el ámbito de aplicación: — Comprobar la descripción del producto — Comprobar las alegaciones de seguridad — Comprobar el nivel de garantía Sobre la garantía: — Comprobar las actividades realizadas

Nombre	Objeto	Puntos de atención
EN ISO/IEC 27001:2022	SGSI	Sobre el emisor: ninguno (organismos de certificación acreditados) Sobre el ámbito de aplicación: — Comprobar la descripción del sistema de gestión — Comprobar la declaración de aplicabilidad Sobre la garantía: — Comprobar las actividades realizadas
SOC2	Organizaciones	Sobre el emisor: — Comprobar su estado como contable público Sobre el ámbito de aplicación: — Comprobar la declaración de gestión y la descripción de los controles — Comprobar la declaración de aplicabilidad Sobre la garantía: — Comprobar las conclusiones del informe — Comprobar las cartas puente si es necesario
MDSCert (Mobile Device Security Certification) (GSMA) (cuando esté disponible)	Dispositivos móviles	Sobre el emisor: — Comprobar los requisitos para los organismos de certificación Sobre el ámbito de aplicación: — Comprobar el nivel de garantía de seguridad — Comprobar los requisitos del esquema Sobre la garantía: — Comprobar las actividades y las conclusiones del informe
Otros esquemas	Cualquier componente	Sobre el esquema: — Comprobar la pertinencia y las disposiciones del esquema Sobre el emisor: — Comprobar los requisitos para los organismos de certificación Sobre el ámbito de aplicación: — Comprobar los requisitos del esquema — Comprobar el objetivo de seguridad o un documento similar en el que se describan los requisitos funcionales y de garantía por lo que respecta a la seguridad — Comprobar la descripción del producto y una selección de requisitos funcionales de seguridad Sobre la garantía: — Comprobar las actividades y las conclusiones del informe

ANEXO III

REQUISITOS FUNCIONALES PARA LAS SOLUCIONES DE CARTERA

De conformidad con el artículo 5 *bis*, apartados 4, 5, 8, y 14, del Reglamento (UE) n.º 910/2014, los criterios funcionales que deben cumplir una solución de cartera certificada y el sistema de identificación electrónica en el marco del cual se proporciona incluirán los requisitos funcionales aplicables a las operaciones indicadas en los siguientes actos:

1) Reglamento de Ejecución (UE) 2024/2979 de la Comisión ([1]), por el que se establecen disposiciones de aplicación del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo en lo que respecta a la integridad y las funcionalidades básicas;

2) Reglamento de Ejecución (UE) 2024/2982 de la Comisión ([2]), por el que se establecen disposiciones de aplicación del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo en lo que respecta a los protocolos y las interfaces que admitirá el marco europeo de identidad digital;

3) Reglamento de Ejecución (UE) 2024/2977 de la Comisión ([3]), por el que se establecen disposiciones de aplicación del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo en lo que respecta a los datos de identificación de la persona y las declaraciones electrónicas de atributos expedidos a carteras europeas de identidad digital.

([1]) Reglamento de Ejecución (UE) 2024/2979 de la Comisión, de 28 de noviembre de 2024, por el que se establecen disposiciones de aplicación del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo en lo que respecta a la integridad y las funcionalidades básicas (DO L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

([2]) Reglamento de Ejecución (UE) 2024/2982 de la Comisión, de 28 de noviembre de 2024, por el que se establecen disposiciones de aplicación del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo en lo que respecta a los protocolos y las interfaces que admitirá el marco europeo de identidad digital (DO L, 2024/2982, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

([3]) Reglamento de Ejecución (UE) 2024/2977 de la Comisión, de 28 de noviembre de 2024, por el que se establecen disposiciones de aplicación del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo en lo que respecta a los datos de identificación de la persona y las declaraciones electrónicas de atributos expedidos a carteras europeas de identidad digital (DO L, 2024/2977, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).

ANEXO IV

MÉTODOS Y PROCEDIMIENTOS PARA LAS ACTIVIDADES DE EVALUACIÓN

1. **Auditoría de la ejecución de una solución de cartera**

Una actividad de evaluación de la conformidad constará de una selección de actividades de evaluación específicas.

Los esquemas nacionales de certificación especificarán una actividad de evaluación para valorar la información facilitada, que comprenderá, como mínimo, lo siguiente:

a) un análisis de la información facilitada para confirmar que conviene a una de las arquitecturas especificadas en los esquemas nacionales de certificación;

b) un análisis de la cobertura, mediante los controles de seguridad descritos, de los riesgos y amenazas de ciberseguridad indicados en el registro de riesgos del anexo I.

Los análisis mencionados en las letras a) a b) se basarán en la explicación y la justificación facilitadas por el proveedor de cartera.

2. **Actividades de evaluación relacionadas con el dispositivo criptográfico seguro de cartera**

1) No es necesario que las operaciones críticas, incluidos los cálculos criptográficos, sean ejecutadas totalmente en el DCSC. No obstante, para la parte ejecutada en el DCSC, cuando este funcione como parte de la solución de cartera, se garantizará la protección de las operaciones críticas realizadas contra los atacantes con elevado potencial de ataque, de conformidad con el Reglamento de Ejecución (UE) 2015/1502 de la Comisión ([1]).

2) El DCSC o parte de él puede estar incluido en el objeto de la certificación cuando lo proporcione el titular o solicitante del certificado, o quedar fuera de su ámbito de aplicación cuando esté integrado en un dispositivo proporcionado por el usuario final. Además, los esquemas nacionales de certificación especificarán las actividades de evaluación para verificar la idoneidad del DCSC, en los dos casos siguientes:

   a) si la ACSC depende del DCSC concreto (es decir, si es necesario evaluarla como producto compuesto basado en el DCSC), la evaluación de la ACSC requerirá el acceso a información adicional relacionada con la certificación del DCSC, y en concreto a su informe técnico de evaluación;

   b) si una arquitectura contemplada en el esquema utiliza varios DCSC, o si algunas de las operaciones sobre activos críticos se realizan fuera del DCSC, los esquemas nacionales de certificación incluirán actividades de evaluación para garantizar que la solución en su conjunto ofrezca el nivel de seguridad esperado.

3) Como requisito previo para la certificación en el marco de los esquemas nacionales de certificación, el DCSC se evaluará con arreglo a los requisitos del nivel de seguridad alto según lo establecido en el Reglamento de Ejecución (UE) 2015/1502.

   a) Cuando se cumplan las condiciones del artículo 3, apartado 3, letra b), la evaluación del DCSC o de parte de él incluirá una evaluación de la vulnerabilidad, según la norma EN ISO/IEC 15408-3:2022 a nivel AVA_VAN.5, tal como se establece en el anexo I del Reglamento de Ejecución (UE) 2024/482 de la Comisión ([2]), a menos que se justifique debidamente al organismo de certificación que las características de seguridad de la ACSC permiten utilizar un nivel de evaluación inferior, manteniendo el mismo nivel de seguridad alto global según lo establecido en el Reglamento de Ejecución (UE) 2015/1502.

([1]) Reglamento de Ejecución (UE) 2015/1502 de la Comisión, de 8 de septiembre de 2015, sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica con arreglo a lo dispuesto en el artículo 8, apartado 3, del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (DO L 235 de 9.9.2015, p. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

([2]) Reglamento de Ejecución (UE) 2024/482 de la Comisión, de 31 de enero de 2024, por el que se establecen disposiciones de aplicación del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo en lo concerniente a la adopción del esquema europeo de certificación de la ciberseguridad basado en los criterios comunes (EUCC) (DO L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

4) Además, en la documentación relacionada con cada arquitectura específica, los esquemas nacionales de certificación formularán hipótesis para esta evaluación del DCSC, en las cuales se pueda proporcionar resistencia contra atacantes con elevado potencial de ataque de conformidad con el Reglamento de Ejecución (UE) 2015/1502, y especificarán las actividades de evaluación que servirán para confirmar estas hipótesis y confirmar que siguen verificándose después de la expedición del certificado. Los esquemas nacionales exigirán también a los candidatos a la certificación que perfeccionen estas hipótesis para su aplicación específica y que describan las medidas vigentes para garantizar que siguen verificándose a lo largo de todo el ciclo de vida de la certificación.

5) En todos los casos, los esquemas nacionales de certificación incluirán una actividad de evaluación para verificar que la información sobre la garantía disponible para el DCSC conviene a los fines de la solución de cartera, mediante un análisis de la información sobre la garantía, por ejemplo, el objetivo de seguridad para los certificados EUCC, que incluya las siguientes actividades:

   a) verificar que el ámbito de aplicación de la evaluación es el adecuado, lo que para los certificados EUCC, por ejemplo, significa verificar que el objetivo de seguridad se ajusta a uno de los perfiles de protección recomendados en el EUCC;

   b) verificar que las hipótesis sobre el entorno operativo son compatibles con la solución de cartera, lo que para los certificados EUCC, por ejemplo, significa que estas hipótesis están recogidas en el objetivo de seguridad;

   c) verificar que las recomendaciones de la guía o documentación del usuario son compatibles con las condiciones en las que se va a utilizar el DCSC en la solución de cartera;

   d) verificar que las hipótesis formuladas sobre los DCSC en el esquema nacional de certificación están verificadas y contempladas en la información sobre la garantía.

6) En los casos en que algunas de las verificaciones no sean totalmente concluyentes, los esquemas nacionales de certificación exigirán a los organismos de certificación que especifiquen requisitos compensatorios para la aplicación criptográfica segura de cartera (ACSC) basada en el DCSC, que se incluirán en la evaluación de dicha aplicación. Si esto no es posible, los esquemas nacionales de certificación considerarán que el DCSC es inadecuado, lo que implica que no se expedirá un certificado de conformidad a la solución de cartera.

3. **Actividades de evaluación relacionadas con la aplicación criptográfica segura de cartera (ACSC)**

1) Los esquemas nacionales de certificación exigirán que una ACSC, como parte de una solución de cartera, se evalúe con arreglo a los requisitos de al menos un nivel de seguridad alto, tal como se establece en el Reglamento de Ejecución (UE) 2015/1502.

2) Esta evaluación incluirá una evaluación de la vulnerabilidad, según lo dispuesto en la norma EN ISO/IEC 15408-3:2022 a nivel AVA_VAN.5, tal como se establece en el anexo I del Reglamento de Ejecución (UE) 2024/482, a menos que se justifique debidamente al organismo de certificación que las características de seguridad de la ACSC permiten utilizar un nivel de evaluación inferior, manteniendo el mismo nivel de seguridad alto global según lo establecido en el Reglamento de Ejecución de la Comisión (UE) 2015/1502.

3) Cuando la ACSC no sea proporcionada por el proveedor de la cartera, los esquemas nacionales de certificación formularán hipótesis para esta evaluación de la ACSC, en las cuales se pueda proporcionar resistencia contra atacantes con elevado potencial de ataque de conformidad con el Reglamento de Ejecución (UE) 2015/1502, y especificarán las actividades de evaluación que servirán para confirmar estas hipótesis y confirmar que siguen verificándose después de la expedición del certificado. Los esquemas nacionales exigirán también a los candidatos a la certificación que perfeccionen estas hipótesis para su aplicación específica y que describan las medidas vigentes para garantizar que siguen verificándose a lo largo de todo el ciclo de vida de la certificación.

4) En todos los casos, los esquemas nacionales de certificación incluirán una actividad de evaluación para verificar que la información sobre la garantía disponible para la ACSC conviene a los fines de la solución de cartera, mediante un análisis de la información sobre la garantía, por ejemplo, el objetivo de seguridad para los certificados EUCC, que incluya las siguientes actividades:

   a) verificar que el ámbito de aplicación de la evaluación es el adecuado, lo que para los certificados EUCC, por ejemplo, significa verificar que el objetivo de seguridad se ajusta a uno de los perfiles de protección recomendados en el EUCC;

   b) verificar que las hipótesis sobre el entorno operativo son compatibles con la solución de cartera, lo que para los certificados EUCC, por ejemplo, significa que estas hipótesis están recogidas en el objetivo de seguridad;

c) verificar que las recomendaciones de la guía o documentación del usuario son compatibles con las condiciones en las que se va a utilizar la ACSC en la solución de cartera;

d) verificar que las hipótesis formuladas sobre las ACSC en el esquema nacional de certificación están verificadas y contempladas en la información sobre la garantía.

5) Los esquemas nacionales de certificación exigirán que la evaluación de la ACSC abarque todos los controles de seguridad aplicados por dicha ACSC.

4. **Actividades de evaluación relacionadas con el dispositivo del usuario final**

Puesto que en el registro de riesgos, tal y como figura en el anexo I del presente Reglamento, se indican los riesgos directamente relacionados con la seguridad del dispositivo del usuario final, los esquemas nacionales de certificación deberán especificar requisitos de seguridad para los dispositivos del usuario final. No obstante, dado que estos dispositivos los proporciona el usuario final y no el proveedor de cartera, estos requisitos estarán formulados como hipótesis.

Para cada hipótesis, la solución de cartera incluirá un mecanismo que permita verificar, por lo que respecta a cada unidad de cartera, que el dispositivo del usuario final subyacente satisface la hipótesis. Estos mecanismos se considerarán controles de seguridad y estarán cubiertos por actividades de evaluación para comprobar su idoneidad y su eficacia al nivel de seguridad adecuado.

A continuación, se exponen dos ejemplos:

a) un dispositivo de un usuario final puede incluir un DCSC certificado, que debe comprobarse. Normalmente, esta comprobación se haría utilizando un mecanismo criptográfico para verificar que el DCSC certificado contiene un secreto criptográfico que solo está disponible en ese DCSC certificado. En este caso, el secreto criptográfico debe considerarse un activo crítico y debe estar cubierto por la certificación del DCSC o de la ACSC;

b) un requisito habitual para los dispositivos del usuario final sería que estos dispositivos deben recibir actualizaciones de seguridad. Puesto que este requisito está relacionado con la instancia de cartera, el mecanismo utilizado para verificar la disponibilidad de actualizaciones de seguridad solo debe ser objeto de actividades de evaluación al nivel de seguridad que sea adecuado para la instancia de cartera, especialmente porque es probable que esté integrado en la instancia de cartera.

5. **Actividades de evaluación relacionadas con la instancia de cartera**

1) En la evaluación de la instancia de cartera se tendrán en cuenta las dos dificultades principales siguientes:

a) es probable que la instancia de cartera exista en una serie de variantes de la misma aplicación básica, y que cada variante sea especializada para una determinada categoría de dispositivos del usuario final;

b) es probable que las diferentes variantes de la instancia de cartera precisen de actualizaciones frecuentes para seguir el desarrollo de la plataforma de seguridad subyacente, por ejemplo cuando se detecten vulnerabilidades que requieran cambios en las aplicaciones.

2) En la evaluación de la instancia de cartera se tendrán en cuenta estas dificultades específicas, una de cuyas consecuencias inmediatas es que el marco de criterios comunes puede no ser adecuado en todos los casos. Por lo tanto, se considerarán metodologías de evaluación alternativas cuando sea necesario. Los esquemas nacionales de certificación considerarán el uso de la metodología de la norma EN 17640:2018 para lo siguiente:

a) como parte del propio esquema;

b) a través de esquemas nacionales basados en la metodología;

c) a través de esquemas nacionales basados en principios similares pero creados antes de la elaboración de la metodología EN 17640:2018.

3) Además, dado que la realización de una evaluación específica completa de cada variante puede aportar escaso valor añadido, los esquemas nacionales de certificación considerarán la posibilidad de especificar criterios que permitan llevar a cabo un muestreo, a fin de evitar la repetición de actividades de evaluación idénticas y centrarse en las que sean específicas de una variante determinada. Los esquemas nacionales de certificación exigirán a todos los organismos de certificación que justifiquen su uso del muestreo.

4) Los esquemas nacionales de certificación incluirán actualizaciones de la instancia de cartera en el proceso general de gestión de cambios especificado para la solución de cartera. Asimismo, establecerán normas relativas a los procedimientos que deberá llevar a cabo el proveedor de cartera para cada actualización (por ejemplo, analizar la repercusión de los cambios en los controles de seguridad) y a las actividades de evaluación que deberá llevar a cabo el organismo de certificación sobre las actualizaciones en condiciones específicas (por ejemplo, evaluar la eficacia operativa de un control de seguridad modificado). El proceso de gestión de cambios es uno de los procesos cuya eficacia operativa debe comprobarse anualmente de conformidad con el artículo 18, apartado 3.

6. **Actividades de evaluación relacionadas con los servicios y procesos utilizados para el suministro de la solución de cartera y la gestión de su funcionamiento**

1) Para evaluar los servicios y procesos que intervienen en el suministro y la gestión del funcionamiento de la solución de cartera y el sistema de identificación electrónica en cuyo marco de proporciona, el equipo evaluador recogerá pruebas mediante actividades de evaluación que podrán incluir actividades de auditoría, inspección, verificación y validación.

2) El organismo de certificación confirmará que las pruebas son suficientes y adecuadas para ofrecer una garantía conveniente de que los servicios y procesos cumplen los requisitos de la certificación, comprobando lo siguiente:

   a) la exactitud de la información presentada en la descripción de los procesos y servicios;

   b) la idoneidad del diseño y de los controles de los procesos y servicios para cumplir los criterios de evaluación;

   c) la eficacia operativa de la aplicación de estos controles durante un período determinado antes de la evaluación.

3) La exactitud de la descripción y la eficacia operativa de una aplicación de controles pueden considerarse objetivos de verificación, a efectos de la norma ISO/IEC 17000:2020, de las correspondientes alegaciones del proveedor de la cartera (es decir, la confirmación de la imparcialidad de los sucesos ya acaecidos o de los resultados ya obtenidos), mientras que la idoneidad del diseño y los controles de los servicios y procesos para cumplir los criterios de evaluación puede considerarse un objetivo de validación, a efectos de la norma ISO/IEC 17000:2020, de la correspondiente alegación del proveedor de la cartera (es decir, la confirmación de la aceptabilidad en relación con un uso futuro proyectado o un resultado previsto).

4) Teniendo en cuenta que una solución de cartera no está autorizada para funcionar antes de ser certificada, la eficacia operativa no puede confirmarse sobre la base del funcionamiento efectivo de la solución. Por lo tanto, deberá confirmarse utilizando pruebas reunidas durante los ensayos o la fase experimental.

5) Es posible que ya existan esquemas nacionales de certificación para determinados servicios y procesos, por ejemplo para la incorporación de usuarios. Los esquemas nacionales de certificación considerarán, cuando proceda, su utilización.

7. **Actividades de evaluación relacionadas con los servicios de TIC utilizados para el suministro de la solución de cartera y la gestión de su funcionamiento**

1) Algunas arquitecturas de cartera pueden recurrir a servicios de TIC específicos, como los servicios en la nube para el suministro y la gestión del funcionamiento de una solución de cartera, y estos servicios pueden albergar datos sensibles y operaciones sensibles. En tal caso, los esquemas nacionales de certificación especificarán los requisitos de seguridad aplicables a estos servicios de TIC.

2) Existen ya numerosos esquemas de certificación para servicios de TIC, servicios en la nube y otras fuentes de información sobre la garantía, incluidos los mencionados en el anexo II. Los esquemas nacionales de certificación se basarán en los mecanismos existentes, cuando estén disponibles y sean aplicables, según uno de los siguientes procedimientos:

   a) exigiendo el uso de un esquema específico o de una selección de esquemas y especificando las condiciones en las que los servicios de TIC o en la nube se evaluarán con arreglo a ellos;

   b) dejando que el proveedor de cartera elija la evaluación y utilizando el análisis de la dependencia para analizar la idoneidad de la información sobre la garantía obtenida mediante esa evaluación.

3) En ambos casos, los esquemas nacionales de certificación especificarán las actividades de evaluación adicionales que sean necesarias para analizar o completar la información obtenida mediante estos esquemas.

ANEXO V

LISTA DE INFORMACIÓN PÚBLICAMENTE DISPONIBLE SOBRE LAS CARTERAS

1. La información que se hará pública de conformidad con el artículo 8, apartado 5, incluirá, como mínimo, lo siguiente:

   a) cualquier limitación de uso de una solución de cartera;

   b) las orientaciones y recomendaciones del proveedor de cartera para ayudar a los usuarios finales en la configuración, la instalación, la utilización, la gestión del funcionamiento y el mantenimiento seguros de las carteras;

   c) el período durante el cual se ofrecerá apoyo de seguridad a los usuarios finales, en particular en lo que se refiere a la disponibilidad de actualizaciones relacionadas con la ciberseguridad;

   d) los datos de contacto del fabricante o el proveedor y los métodos aceptados para recibir información sobre la vulnerabilidad remitida por los usuarios finales o investigadores en materia de seguridad;

   e) una referencia a los repositorios en línea en los que se enumeren las vulnerabilidades divulgadas públicamente en relación con las carteras y a cualquier asesoramiento pertinente sobre ciberseguridad.

2. La información a la que se refiere el apartado 1 se pondrá a disposición de cualquier persona que desee utilizar una solución de cartera de manera clara, completa y fácilmente accesible, en un espacio de acceso público.

ANEXO VI

METODOLOGÍA PARA EVALUAR LA ACEPTABILIDAD DE LA INFORMACIÓN SOBRE LA GARANTÍA

1. **Evaluación de la disponibilidad de documentación de la garantía**

Los evaluadores harán una relación de la documentación de la garantía disponible para cada componente pertinente de la solución de cartera y el sistema de identificación electrónica en el marco del cual se proporciona. A continuación, evaluarán la pertinencia general de cada documento de la garantía para la revisión de la dependencia.

En el análisis se tendrán en cuenta los siguientes aspectos:

1) sobre la propia documentación de la garantía:

   a) el tipo de documentación de la garantía, con todos los detalles requeridos

      [ejemplos de estos documentos son los certificados de conformidad con arreglo a la norma EN ISO/IEC 27001:2022 o los informes tipo 1 o tipo 2 para la Norma Internacional de Encargos de Aseguramiento (NIEA)];

   b) el período cubierto o el período de validez

      [este período puede completarse con una carta puente (un documento que cubra el período comprendido entre la fecha final del período de referencia del informe de la NIEA vigente y la publicación de un nuevo informe de la NIEA) o una declaración similar];

   c) el marco aplicable (por ejemplo, la norma vigente);

   d) si la documentación de la garantía incluye una puesta en correspondencia con los requisitos del esquema;

2) sobre la competencia profesional y la imparcialidad del emisor del informe de garantía:

   a) nombre del organismo de certificación y, en su caso, nombre del evaluador principal;

   b) pruebas de la competencia del organismo de certificación y del evaluador (por ejemplo, acreditación, certificación personal, etc.);

   c) pruebas de la imparcialidad del organismo de certificación y del evaluador (por ejemplo, acreditación, etc.).

2. **Evaluación de la garantía en relación con cada uno de los requisitos**

Los evaluadores verificarán que la documentación de la garantía disponible para la solución de cartera y el sistema de identificación electrónica en el marco del cual se proporciona es adecuada para determinar que la solución de cartera cumple las expectativas en relación con los distintos requisitos del esquema de certificación.

Esta evaluación se llevará a cabo para cada componente pertinente de la solución de cartera y del sistema de identificación electrónica en el marco del cual se proporciona, formulando una hipótesis sobre los controles de seguridad de la solución de cartera.

Para cada hipótesis de este tipo, el equipo evaluador determinará si la garantía que ofrece la documentación de la garantía disponible es adecuada o no.

La determinación de que la garantía es adecuada se basará en lo siguiente:

1) la documentación de la garantía ofrece la información necesaria, con el nivel de seguridad esperado;

2) la información disponible en la documentación de la garantía no abarca todo el ámbito del requisito, pero los controles adicionales o compensatorios (es decir, controles internos que reducen el riesgo de que existan o puedan existir deficiencias de control) aplicados en la solución de cartera o en el sistema de identificación electrónica en el marco del cual se proporciona permiten a los evaluadores determinar que la información es adecuada;

3) la información disponible en la documentación de la garantía no ofrece el nivel de seguridad esperado, pero los controles aplicados para evaluar y supervisar al proveedor de cartera permiten a los evaluadores determinar que la información es adecuada;

4) si la documentación de la garantía menciona incumplimientos en el diseño o la aplicación de los controles utilizados para cumplir una hipótesis, las medidas correctoras propuestas y aplicadas por el proveedor de cartera y revisadas por sus evaluadores serán adecuadas para asegurar que efectivamente se cumple la hipótesis.

ANEXO VII

CONTENIDO DEL CERTIFICADO DE CONFORMIDAD

1. Un identificador único asignado por el organismo de certificación que expide el certificado de conformidad.

2. Información relativa a la solución de cartera certificada y a los sistemas de identificación electrónica en el marco de los cuales se proporciona, y sobre el titular del certificado de conformidad, que incluya lo siguiente:
   a) nombre de la solución de cartera;
   b) nombre de los sistemas de identificación electrónica en el marco de los cuales se proporciona la solución de cartera,
   c) versión de la solución de cartera evaluada,
   d) nombre, dirección e información de contacto del titular del certificado de conformidad,
   e) enlace al sitio web del titular del certificado de conformidad que contiene la información que debe ponerse a disposición del público.

3. Información relativa a la evaluación y la certificación de la solución de cartera y de los sistemas de identificación electrónica en el marco de los cuales se proporciona, incluido lo siguiente:
   a) nombre, dirección e información de contacto del organismo de certificación que expidió el certificado de conformidad;
   b) cuando sea diferente del organismo de certificación, nombre del organismo de evaluación de la conformidad que haya realizado la evaluación, junto con información sobre su acreditación;
   c) nombre del dueño del esquema;
   d) referencias al Reglamento (UE) n.º 910/2014 y al presente Reglamento;
   e) una referencia al informe de certificación asociado al certificado de conformidad;
   f) una referencia al informe de evaluación de la certificación asociado al certificado de conformidad;
   g) una referencia a las normas utilizadas para la evaluación, incluidas sus versiones;
   h) la fecha de expedición del certificado de conformidad;
   i) el período de validez del certificado de conformidad.

ANEXO VIII

CONTENIDO DEL INFORME PÚBLICO DE CERTIFICACIÓN Y DEL INFORME DE EVALUACIÓN DE LA CERTIFICACIÓN

1. El informe público de certificación contendrá, al menos, los siguientes elementos:

   a) un resumen ejecutivo;

   b) una identificación de la solución de cartera y del sistema de identificación electrónica en el marco del cual se proporciona;

   c) una descripción de la solución de cartera y del sistema de identificación electrónica en el marco del cual se proporciona;

   d) la información sobre seguridad que debe ponerse a disposición del público, tal como se describe en el anexo V, o una remisión a dicha información;

   e) un resumen del plan preliminar de auditoría y validación;

   f) un resumen de la revisión y de la decisión de certificación.

2. El informe de evaluación de la certificación contendrá, como mínimo:

   a) una descripción del diseño de la solución de cartera, del sistema de identificación y del proceso de incorporación, junto con la evaluación de riesgos y el plan de validación específico;

   b) una descripción de cómo la solución de cartera cumple los requisitos del nivel de seguridad alto y de cómo lo demuestran los resultados de la evaluación de certificación de la solución de cartera realizada de conformidad con el presente Reglamento;

   c) una descripción del resultado de la evaluación de la conformidad de la solución de cartera y del sistema de identificación electrónica en el marco del cual se proporcionan las unidades de cartera correspondientes, y en particular la conformidad con lo siguiente:

      — los requisitos establecidos en el artículo 5 *bis*, apartados 4, 5 y 8, del Reglamento (UE) n.º 910/2014,

      — el requisito de separación lógica establecido en el artículo 5 *bis*, apartado 14, del Reglamento (UE) n.º 910/2014,

      — cuando proceda, las normas y especificaciones técnicas a que se refiere el artículo 5 *bis*, apartado 24, del Reglamento (UE) n.º 910/2014, junto con una descripción de cómo se relacionan estos requisitos con los correspondientes requisitos normativos especificados por los esquemas nacionales de certificación;

   d) un resumen del resultado de la realización del plan de validación, incluidos todos los incumplimientos detectados.

ANEXO IX

CALENDARIO DE LAS EVALUACIONES DE VIGILANCIA OBLIGATORIAS

1. El artículo 18 especifica los requisitos relativos al ciclo de vida de la certificación, en particular la realización de actividades de evaluación periódicas. Estas actividades incluirán, como mínimo, los siguientes elementos:

   a) una evaluación completa del objeto de la evaluación de la conformidad en la evaluación inicial y en cada evaluación de renovación de la certificación, incluida una función de actualización de cualquier componente del producto;

   b) una evaluación de la vulnerabilidad en la evaluación inicial y en cada evaluación de renovación de la certificación, y al menos cada dos años en las evaluaciones de vigilancia, que abarque al menos los cambios en el objeto de la evaluación de la conformidad y en el entorno de amenazas que se hayan producido desde la última evaluación de la vulnerabilidad;

   c) actividades adicionales, como las pruebas de penetración en caso de aumento del nivel de riesgo o de aparición de nuevas amenazas;

   d) una evaluación de la eficacia operativa de los procesos de mantenimiento al menos cada año en las evaluaciones de vigilancia y de renovación de la certificación, que abarque al menos los procesos de control de las versiones, actualización y gestión de las vulnerabilidades;

   e) tras una revisión satisfactoria y una decisión de certificación, la expedición de un certificado de conformidad después de la evaluación inicial y de cada evaluación de renovación de la certificación.

2. En el cuadro 1 se establece un calendario de referencia basado en un ciclo de cuatro años, en el que:

   a) el año 1 comienza cuando se expide por primera vez el certificado de conformidad, así como

   b) todas las actividades de evaluación se llevarán a cabo en un plazo de doce meses a partir de la evaluación del año anterior.

3. El calendario expuesto en el cuadro 1 es una recomendación para garantizar la renovación a tiempo de la certificación y evitar perturbaciones en el suministro de la solución de cartera. Pueden ser admisibles otros calendarios, siempre que la validez del certificado de conformidad no exceda de cinco años, tal como se establece en el artículo 5 *quater*, apartado 4, del Reglamento (UE) n.º 910/2014.

4. Además de las evaluaciones periódicas, podría iniciarse una evaluación especial a petición del organismo de certificación o del titular del certificado de conformidad, cuando se produzca una modificación significativa del objeto de la certificación o del entorno de amenazas.

5. Cualquier evaluación, incluidas las evaluaciones de vigilancia y las evaluaciones especiales, podría dar lugar a la expedición de un nuevo certificado de conformidad, en particular si se producen cambios significativos en el objeto de la certificación, pero con la misma fecha de expiración que el certificado de conformidad original.

Cuadro 1

Ciclo completo de evaluación de 4 años

Tiempo	Tipo de eval.	Actividades
Año 0	Inicial	— Evaluación completa del objeto de la certificación, incluida la evaluación de la vulnerabilidad — Incluida una función para realizar actualizaciones de cada componente de *software* — Evaluación de los procesos de mantenimiento, excluida su eficacia operativa — Expedición del certificado de conformidad e inicio del ciclo de cuatro años
Año 1	Vigilancia	— Evaluación de la eficacia operativa de los procesos de mantenimiento — Al menos comprobación de la versión, actualización y gestión de vulnerabilidades — Evaluación de los cambios que inciden en la seguridad del producto

Tiempo	Tipo de eval.	Actividades
Año 2	Vigilancia	— Evaluación de la vulnerabilidad de la solución completa — Evaluación de la eficacia operativa de los procesos de mantenimiento — Al menos control, actualización y gestión de vulnerabilidades de la versión — Evaluación de los cambios que inciden en la seguridad del producto
Año 3	Vigilancia	— Evaluación de la eficacia operativa de los procesos de mantenimiento — Al menos comprobación de la versión, actualización y gestión de vulnerabilidades — Evaluación de los cambios que inciden en la seguridad del producto
Año 4	Renovación de la certificación	1) Evaluación completa del objeto de la certificación, incluida la evaluación de la vulnerabilidad 2) Evaluación simplificada de las características o procesos que no hayan cambiado 3) Incluida una función para realizar actualizaciones de cada componente de *software* 4) Evaluación de los procesos de mantenimiento, incluida su eficacia operativa 5) Expedición de un nuevo certificado de conformidad