2025/847

7.5.2025

REGLAMENTO DE EJECUCIÓN (UE) 2025/847 DE LA COMISIÓN

de 6 de mayo de 2025

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 las reacciones a las violaciones de la seguridad 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 la que se deroga la Directiva 1999/93/CE ([1]), y, en particular, su artículo 5 *sexies*, apartado 5,

Considerando lo siguiente:

1) El marco europeo de identidad digital (en lo sucesivo, «el marco») establecido en el Reglamento (UE) n.º 910/2014 es un componente crucial para la creación de un ecosistema de identidad digital seguro e interoperable en toda la Unión. El objetivo de este marco, con las carteras europeas de identidad digital (en lo sucesivo, «carteras») como piedra angular, es facilitar el acceso a los servicios en todos los Estados miembros, garantizando al mismo tiempo la protección de los datos personales y de la privacidad.

2) Los Reglamentos (UE) 2016/679 ([2]) y (UE) 2018/1725 ([3]) del Parlamento Europeo y del Consejo y, en su caso, la Directiva 2002/58/CE del Parlamento Europeo y del Consejo ([4]) se aplican a las actividades de tratamiento de datos personales en virtud del presente Reglamento. Las normas sobre la evaluación y la facilitación de información establecidas en virtud del presente Reglamento se entienden sin perjuicio de la obligación de notificar las violaciones de la seguridad de los datos personales a la autoridad de control competente, cuando proceda, en virtud del Reglamento (UE) 2016/679 o del Reglamento (UE) 2018/1725, y de la obligación de comunicar las violaciones de la seguridad de los datos personales a los interesados, cuando proceda, en virtud de estos Reglamentos.

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 en virtud de la Recomendación (UE) 2021/946 de la Comisión ([5]), 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 ([6]), la Comisión debe revisar y, en caso necesario, actualizar el presente Reglamento, para mantenerlo en consonancia con la evolución mundial, la arquitectura y el marco de referencia, y seguir las mejores prácticas en el mercado interior.

([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]) 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).

([4]) 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).

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

([6]) 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).

4) En caso de violación o puesta en peligro de la seguridad de las soluciones de cartera o de los mecanismos de validación a que se refiere el artículo 5 *bis*, apartado 8, del Reglamento (UE) n.º 910/2014, o del sistema de identificación electrónica en virtud del cual se proporcionan las soluciones de cartera, es preciso que las reacciones a dichas violaciones y puestas en peligro de la seguridad se produzcan de manera rápida, coordinada y segura en todos los Estados miembros para proteger a los usuarios y mantener la confianza en el ecosistema de identidad digital. Esto se entiende sin perjuicio de la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo ([7]) y los Reglamentos (UE) 2019/881 ([8]) y (UE) 2024/2847 ([9]) del Parlamento Europeo y del Consejo, en particular por lo que respecta a la gestión de las incidencias o las vulnerabilidades y a su consideración como violaciones de la seguridad. Por consiguiente, los Estados miembros deben garantizar que se suspendan oportunamente la provisión y el uso de las carteras cuya seguridad haya sido violada o puesta en peligro o, cuando proceda, que se retiren.

5) A fin de asegurar que las reacciones a una violación o una puesta en peligro de la seguridad sean adecuadas, los Estados miembros deben evaluar si una violación o una puesta en peligro de la seguridad de una solución de cartera, de los mecanismos de validación a que se refiere el artículo 5 *bis*, apartado 8, del Reglamento (UE) n.º 910/2014, o del sistema de identificación electrónica en virtud del cual se proporciona una solución de cartera afecta a la fiabilidad de dicha solución de cartera o de otras soluciones de cartera. Esa evaluación debe basarse en criterios uniformes, como el número y la categoría de usuarios de una cartera, de personas físicas y de partes usuarias de la cartera afectadas, la naturaleza de los datos afectados, la duración de la puesta en peligro o la violación de la seguridad, la limitación de la disponibilidad de un servicio y las pérdidas financieras, y si se han visto comprometidos datos personales. Con arreglo a estos criterios los Estados miembros deben disponer de flexibilidad y discrecionalidad para determinar de manera proporcionada si la fiabilidad de una solución de cartera está afectada y si procede suspender la solución de cartera o, cuando la gravedad de la violación o la puesta en peligro lo justifique, retirarla. Estos criterios no deben desencadenar la retirada automática de una solución de cartera ni la suspensión automática de su provisión y su uso, sino que los Estados miembros deben tenerlos debidamente en cuenta a la hora de decidir si es necesario retirar una solución de cartera o suspender su provisión y su uso.

6) Debido a la repercusión y las molestias que conlleva la suspensión del uso de las soluciones de cartera, los Estados miembros deberán evaluar si la revocación de declaraciones de unidad de cartera u otras medidas adicionales son necesarias para reaccionar adecuadamente ante la violación o la puesta en peligro de la seguridad.

7) Para mantener informados a los usuarios de una cartera sobre el estado de sus carteras, se les deberá facilitar información adecuada sobre las violaciones o las puestas en peligro de la seguridad que afecten a estas. Dado que las partes usuarias de las carteras registradas en la Unión pueden verse asimismo afectadas por las violaciones y las puestas en peligro de la seguridad, se les debe transmitir también la información pertinente al respecto.

8) A fin de mejorar la transparencia y generar confianza en el ecosistema de identidad digital, conviene que la información sobre las violaciones o las puestas en peligro de la seguridad y sobre sus consecuencias comprenda, como mínimo, la información exigida en virtud del presente Reglamento. No obstante, la información relativa a violaciones o puestas en peligro de la seguridad transmitida a los usuarios de una cartera y a las partes usuarias de la cartera debe evaluarse cuidadosamente para prevenir y minimizar el riesgo de su explotación por atacantes.

([7]) 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).

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

([9]) 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).

9) Para que los usuarios puedan acceder de nuevo a sus unidades de cartera después de que se haya subsanado una violación o una puesta en peligro de la seguridad, el Estado miembro que haya proporcionado las soluciones de cartera deberá restablecer sin demora indebida la provisión y el uso de dichas soluciones. Esto podrá hacerse restableciendo las unidades de cartera, emitiendo unidades de cartera al amparo de una nueva versión de las soluciones de cartera o reemitiendo nuevas declaraciones de unidad de cartera válidas. Los usuarios de una cartera afectados, las partes usuarias de las carteras, los puntos de contacto únicos designados de conformidad con el artículo 46 *quater*, apartado 1, del Reglamento (UE) n.º 910/2014 y la Comisión deben ser informados en consecuencia.

10) A fin de garantizar la retirada de las carteras si la violación o la puesta en peligro de su seguridad no se han subsanado en un plazo de tres meses a partir de la suspensión, o cuando esté justificado por la gravedad de la violación o la puesta en peligro de la seguridad, el Estado miembro debe asegurar que las declaraciones de unidad de cartera pertinentes se revoquen y no puedan restituirse a un estado de validez ni expedirse o proporcionarse a unidades de cartera existentes. Además, no deben proporcionarse nuevas unidades de cartera en el marco de la solución de cartera afectada. Con fines de transparencia, los usuarios, las partes usuarias, los puntos de contacto únicos designados de conformidad con el artículo 46 *quater*, apartado 1, del Reglamento (UE) n.º 910/2014 y la Comisión deben ser informados de la retirada. Esta información incluirá una descripción de las posibles repercusiones para los usuarios de una cartera, en particular en lo que respecta a la gestión de las declaraciones expedidas, o para las partes usuarias de la cartera.

11) El período de tres meses a partir de la suspensión de la provisión y el uso de una solución de cartera, durante el cual debe subsanarse la violación o la puesta en peligro de la seguridad que haya dado lugar a dicha suspensión, debe constituir un plazo después del cual la solución de cartera deberá retirarse a menos que se haya aplicado una medida correctora adecuada. No obstante, los Estados miembros tienen libertad para exigir que la violación o la puesta en peligro de la seguridad se subsane en un plazo inferior a tres meses, teniendo en cuenta, en particular y cuando proceda, el alcance, la duración y las consecuencias de dicha violación o puesta en peligro. Cuando la violación o la puesta en peligro de la seguridad no se subsane o no se pueda subsanar en el plazo fijado por el Estado miembro, este podrá exigir que la solución de cartera se retire antes de que expire el período de tres meses. Los Estados miembros deben utilizar este período durante el cual ha de subsanarse una violación o una puesta en peligro de la seguridad que haya ocasionado la suspensión de la provisión y el uso de una solución de cartera para preparar la posible retirada de dicha solución de cartera y las comunicaciones conexas.

12) A fin de reducir la carga administrativa que puede suponer para ellos la transmisión de la información, de conformidad con el presente Reglamento, a la Comisión y a otros Estados miembros, los Estados miembros deben utilizar las herramientas de notificación existentes, como el sistema de notificación y análisis de incidentes cibernéticos (CIRAS), gestionado por la Agencia de la Unión Europea para la Ciberseguridad (ENISA). Por lo que respecta a la utilización de canales o medios alternativos para informar a los usuarios de una cartera afectados por una violación o una puesta en peligro de la seguridad y a las partes usuarias de la cartera, los Estados miembros deben asegurarse de que la información pertinente se facilite de manera clara, completa y fácilmente accesible. Los canales para facilitar dicha información a los usuarios de una cartera afectados y a las partes usuarias de la cartera deben incluir soluciones adecuadas para la retransmisión a través de sitios web, el seguimiento en tiempo real de las actualizaciones de los sitios web y la agregación de noticias.

13) El Supervisor Europeo de Protección de Datos, al que se consultó de conformidad con el artículo 42, apartado 1, del Reglamento (UE) 2018/1725, emitió su dictamen el 31 de enero de 2025.

14) Las medidas previstas en el presente Reglamento se ajustan al dictamen del comité establecido por el artículo 48 del Reglamento (UE) n.º 910/2014,

HA ADOPTADO EL PRESENTE REGLAMENTO:

Artículo 1

Objeto

El presente Reglamento establece normas sobre las reacciones a las violaciones de la seguridad de las carteras, de los mecanismos de validación a que se refiere el artículo 5 *bis*, apartado 8, del Reglamento (UE) n.º 910/2014 y del sistema de identificación electrónica en virtud del cual se proporcionan las carteras.

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

3) «parte usuaria de la cartera»: parte que tiene la intención de confiar en unidades de cartera para la prestación de servicios públicos o privados mediante interacción digital;

4) «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;

5) «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;

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

8) «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 carteras a un usuario particular de una cartera;

9) «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;

10) «declaración de unidad de cartera»: objeto de datos que describe los componentes de la unidad de cartera o permite la autenticación y la validación de esos componentes.

Artículo 3

Determinación de una violación o una puesta en peligro de la seguridad

1. Sin perjuicio de lo dispuesto en la Directiva (UE) 2022/2555 y en los Reglamentos (UE) 2019/881 y (UE) 2024/2847, los Estados miembros tendrán debidamente en cuenta los criterios establecidos en el anexo I del presente Reglamento para evaluar si una violación o una puesta en peligro de la seguridad de una solución de cartera, de los mecanismos de validación a que se refiere el artículo 5 *bis*, apartado 8, del Reglamento (UE) n.º 910/2014 o del sistema de identificación electrónica en virtud del cual se proporciona la solución de cartera afecta a su fiabilidad o a la de otras soluciones de cartera.

2. Cuando un Estado miembro determine, sobre la base de la evaluación establecida en el apartado 1, que una violación o una puesta en peligro de la seguridad está afectando a la fiabilidad de una solución de cartera y suspenda su provisión y su uso, adoptará las medidas establecidas en los artículos 4 y 5. Cuando un Estado miembro retire la solución de cartera, adoptará las medidas establecidas en los artículos 8 y 9.

3. Cuando un Estado miembro conozca información relativa a una posible violación o puesta en peligro de la seguridad que pueda afectar a la fiabilidad de una o varias soluciones de cartera proporcionadas por otro Estado miembro, ese Estado miembro lo comunicará sin demora indebida a la Comisión y a los puntos de contacto únicos de los Estados miembros afectados designados de conformidad con el artículo 46 *quater*, apartado 1, del Reglamento (UE) n.º 910/2014. Esta comunicación incluirá la información establecida en el artículo 5, apartado 2.

4. El Estado miembro que reciba información facilitada de conformidad con el apartado 3 adoptará sin demora indebida las medidas establecidas en los apartados 1 y 2.

Artículo 4

Suspensión de la provisión y el uso de carteras y otras medidas correctoras

1. Los Estados miembros se asegurarán de que no se proporcionen, utilicen ni activen unidades de cartera en el marco de la solución de cartera suspendida.

2. Los Estados miembros evaluarán si es necesario revocar las declaraciones de unidad de cartera de las unidades de cartera afectadas por la suspensión de una solución de cartera, o adoptar cualquier otra medida correctora, para reaccionar adecuadamente frente a la violación de la seguridad o su puesta en peligro.

3. Las medidas establecidas en los apartados 1 y 2 se adoptarán sin demora indebida y, en cualquier caso, a más tardar veinticuatro horas después de que se suspendan la provisión y el uso de la solución de cartera afectada por la violación o la puesta en peligro de la seguridad.

4. Las medidas establecidas en los apartados 1 y 2 no impedirán a los usuarios de una cartera afectados ejercer su derecho a la portabilidad de los datos establecido en el artículo 5 *bis*, apartado 4, letra g), del Reglamento (UE) n.º 910/2014. Esta disposición está sujeta a la condición de que los usuarios de la cartera puedan ejercer ese derecho sin menoscabo para la seguridad de los activos esenciales de las unidades de cartera afectadas, en particular teniendo en cuenta los motivos de la suspensión y la necesidad de garantizar la protección efectiva de dichos activos contra su uso indebido.

Artículo 5

Información sobre las suspensiones y las medidas correctoras

1. Sin demora indebida, y a más tardar veinticuatro horas después de la suspensión de la provisión y el uso de la solución de cartera, se facilitará información clara, completa y fácilmente accesible sobre dicha suspensión, a:

a) los puntos de contacto únicos designados con arreglo al artículo 46 *quater*, apartado 1, del Reglamento (UE) n.º 910/2014;

b) la Comisión;

c) los usuarios de la cartera afectados;

d) las partes usuarias de la cartera registradas de conformidad con el artículo 5 *ter* del Reglamento (UE) n.º 910/2014.

2. La información facilitada de conformidad con el apartado 1 incluirá al menos los siguientes elementos:

a) el nombre del proveedor de la solución de cartera cuya provisión y uso se hayan suspendido;

b) el nombre y el identificador de referencia de esa solución de cartera, tal y como esté indicado en la lista de carteras certificadas elaborada de conformidad con el artículo 5 *quinquies* del Reglamento (UE) n.º 910/2014 y, en su caso, las versiones de que se trate;

c) la fecha y la hora en que se detectó la violación o la puesta en peligro de la seguridad;

d) si se conocen, la fecha y la hora en que se hicieron efectivas la violación o la puesta en peligro de la seguridad, sobre la base de registros de redes o sistemas u otras fuentes de datos;

e) la fecha y hora de la suspensión de la solución de cartera;

f) los datos de contacto, indicando al menos una dirección de correo electrónico y un número de teléfono correspondientes al Estado miembro que efectúa la notificación y, cuando sea diferente, al proveedor de cartera a que se refiere la letra (a);

g) una descripción de la violación o la puesta en peligro de la seguridad;

h) una descripción de los datos que se han puesto en peligro, especificando, en su caso, las categorías de datos personales definidas en el artículo 9, apartado 1, y el artículo 10, del Reglamento (UE) 2016/679;

i) cuando sea posible, una estimación del número aproximado de usuarios de una cartera afectados y de otras personas físicas afectadas;

j) una descripción de las posibles repercusiones en las partes usuarias de una cartera o en los usuarios de una cartera y, en el caso de estos, cuando proceda, cualquier indicación de las medidas que puedan adoptar para mitigar esas posibles repercusiones;

k) una descripción de las medidas adoptadas o previstas para subsanar la violación o la puesta en peligro de la seguridad, junto con una planificación y un plazo para dicha subsanación;

l) cuando proceda, una descripción de las medidas adoptadas o previstas para trasladar a los usuarios de una cartera afectados a soluciones o servicios de cartera alternativos.

Artículo 6

Restablecimiento de la provisión y el uso de las carteras

Cuando sea necesario para garantizar el restablecimiento de la provisión, la activación y el uso de una solución de cartera, los Estados miembros, sin demora indebida:

1) restablecerán la provisión y el uso de las unidades de cartera proporcionadas en el marco de dicha solución de cartera mediante la emisión de una unidad de cartera proporcionada en el marco de una nueva versión de la solución a todos los usuarios afectados;

2) expedirán nuevas declaraciones de unidad de cartera a unidades de cartera nuevas o, en su caso, a unidades de cartera emitidas con anterioridad, siempre que dichas unidades de cartera cumplan los requisitos de seguridad vigentes una vez subsanada la violación o la puesta en peligro de la seguridad;

3) derogarán cualquier medida aplicada de conformidad con el artículo 4 del presente Reglamento que obstaculice la provisión de nuevas unidades de cartera en el marco de la solución de cartera afectada, cuando dicha medida estuviera vinculada únicamente a la violación o la puesta en peligro de la seguridad ya subsanada.

Artículo 7

Información sobre el restablecimiento

Cuando un Estado miembro restablezca una solución de cartera, dicho Estado miembro se asegurará de que:

1) se informe de ello sin demora indebida a todas las partes que hayan recibido información sobre la suspensión de la provisión y el uso de dicha solución de cartera de conformidad con el artículo 5, apartado 1;

2) la información facilitada de conformidad con el punto 1 incluya al menos los elementos a que se refiere el artículo 5, apartado 2, letras (a), (b) y (f) a (h) y los siguientes:

   a) la fecha y la hora en que se subsanó la violación o la puesta en peligro de la seguridad;

   b) la fecha y la hora del restablecimiento de la solución de cartera afectada y, en su caso, de las unidades de cartera afectadas proporcionadas en el marco de dicha solución;

   c) una descripción de las medidas adoptadas para subsanar la violación o la puesta en peligro de la seguridad;

   d) una descripción de las posibles repercusiones residuales en las partes usuarias de una cartera o en los usuarios de una cartera y, en el caso de estos, cuando proceda, cualquier indicación de las medidas que puedan adoptar para mitigar esas posibles repercusiones residuales.

Artículo 8

Retirada de las carteras

1. Si una violación o una puesta en peligro de la seguridad que haya dado lugar a la suspensión de la provisión y el uso de una solución de cartera no se subsana en un plazo de tres meses a partir de la fecha de dicha suspensión, el Estado miembro que haya proporcionado esa solución de cartera se asegurará de que la solución de cartera afectada se retire y de que se revoque su validez, sin demora indebida y, en cualquier caso, en un plazo de setenta y dos horas tras la expiración del período de tres meses.

2. Cuando un Estado miembro retire una solución de cartera, se asegurará de que:

a) se revoquen las declaraciones de unidad de cartera de la unidad de cartera de la solución de cartera afectada;

b) las declaraciones de unidad de cartera no puedan revertirse al estado de validez;

c) no pueda expedirse ninguna nueva declaración de unidad de cartera a las unidades de cartera existentes proporcionadas en el marco de la solución de cartera afectada;

d) no pueda proporcionarse ninguna nueva unidad de cartera en el marco de la solución de cartera afectada.

3. Las medidas establecidas en los apartados 1 y 2 no impedirán a los usuarios de una cartera afectados ejercer su derecho a la portabilidad de los datos establecido en el artículo 5 *bis*, apartado 4, letra g), del Reglamento (UE) n.º 910/2014. Esta disposición está sujeta a la condición de que los usuarios de la cartera puedan ejercer ese derecho sin menoscabo para la seguridad de los activos esenciales de las unidades de cartera afectadas, en particular teniendo en cuenta los motivos de la retirada y la necesidad de garantizar la protección efectiva de dichos activos contra su uso indebido.

Artículo 9

Información sobre la retirada

1. Sin demora indebida, y a más tardar veinticuatro horas después de la retirada de la solución de cartera, se facilitará información clara, completa y fácilmente accesible sobre dicha retirada, a:

a) los puntos de contacto únicos designados con arreglo al artículo 46 *quater*, apartado 1, del Reglamento (UE) n.º 910/2014;

b) la Comisión;

c) los usuarios de la cartera afectados;

d) las partes usuarias de la cartera registradas de conformidad con el artículo 5 ter del Reglamento (UE) n.º 910/2014.

2. La información facilitada de conformidad con el apartado 1 incluirá al menos los siguientes elementos:

a) el nombre del proveedor de la solución de cartera que haya sido retirada;

b) el nombre y el identificador de referencia de esa solución de cartera, tal y como esté indicado en la lista de carteras certificadas elaborada de conformidad con el artículo 5 *quinquies* del Reglamento (UE) n.º 910/2014 y, en su caso, las versiones de que se trate;

c) la fecha y la hora en que se detectó la violación o la puesta en peligro de la seguridad que dio lugar a la retirada de la solución de cartera afectada debido a su gravedad o a que no se había subsanado en el plazo de tres meses;

d) si se conocen, la fecha y la hora en que se hicieron efectivas la violación o la puesta en peligro de la seguridad, sobre la base de registros de redes o sistemas u otras fuentes de datos;

e) la fecha y hora de la retirada de la solución de cartera y de la revocación efectiva de las declaraciones de unidad de cartera de las unidades de cartera proporcionadas en el marco de la solución de cartera;

f) si la retirada es el resultado de la gravedad de la violación o la puesta en peligro de la seguridad o es consecuencia de que no se haya subsanado la violación o la puesta en peligro de la seguridad;

g) los datos de contacto, indicando al menos una dirección de correo electrónico y un número de teléfono correspondientes al Estado miembro que efectúa la notificación y, cuando sea diferente, al proveedor de cartera a que se refiere la letra (a);

h) una descripción de la violación o la puesta en peligro de la seguridad;

i) una descripción de los datos que se han puesto en peligro, indicando, en su caso, las categorías de datos personales especificadas en el artículo 9, apartado 1, y en el artículo 10, del Reglamento (UE) 2016/679;

j) cuando sea posible, una estimación del número aproximado de usuarios de la cartera afectados y de otras personas físicas afectadas;

k) una descripción de las posibles repercusiones en las partes usuarias de una cartera o en los usuarios de una cartera y, en el caso de estos, cuando proceda, cualquier indicación de las medidas que puedan adoptar para mitigar esas posibles repercusiones;

l) una descripción de las medidas adoptadas o previstas para trasladar a los usuarios de una cartera afectados a soluciones de cartera alternativas o, cuando sea posible y adecuado, a servicios alternativos.

Artículo 10

Sistema de información

Los Estados miembros enviarán la información establecida en los artículos 3, 5, 7 y 9 a la Comisión y a los puntos de contacto únicos de los Estados miembros designados de conformidad con el artículo 46 *quater*, apartado 1, del Reglamento (UE) n.º 910/2014, a través del sistema CIRAS gestionado por la ENISA o de un sistema equivalente acordado por los Estados miembros y la Comisión.

Artículo 11

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, con excepción del artículo 10, que será aplicable a partir del 7 de mayo de 2026.

Hecho en Bruselas, el 6 de mayo de 2025.

Por la Comisión
La Presidenta
Ursula VON DER LEYEN

ANEXO

Criterios para la evaluación de una violación o una puesta en peligro de la seguridad

1. Los Estados miembros basarán su evaluación de una violación o una puesta en peligro de la seguridad en los siguientes criterios:

a) la violación o la puesta en peligro ha causado o puede causar la muerte de una persona física o daños considerables a la salud de una persona física;

b) se ha producido, o puede producirse, un acceso presuntamente malintencionado o no autorizado a la red y los sistemas de información de un proveedor de carteras, del proveedor de mecanismos de validación a que se refiere el artículo 5 *bis*, apartado 8, del Reglamento (UE) n.º 910/2014, o de un proveedor del sistema de identificación electrónica en virtud del cual se proporciona una solución de cartera («entidades afectadas»), de tal manera que puede causar graves perturbaciones operativas, y esos sistemas son componentes esenciales de la solución de cartera afectada, de los mecanismos de validación a que se refiere el artículo 5 *bis*, apartado 8, del Reglamento (UE) n.º 910/2014 afectados o del sistema de identificación electrónica en virtud del cual se proporciona una solución de cartera afectado;

c) una solución de cartera, un mecanismo de validación contemplado en el artículo 5 *bis*, apartado 8, del Reglamento (UE) n.º 910/2014, o un sistema de identificación electrónica en virtud del cual se proporciona una solución de cartera, o una parte de ellos:

— está completamente indisponible para los usuarios de una cartera o las partes usuarias de una cartera durante más de doce horas consecutivas, o se prevé que vaya a estarlo;

— está indisponible para los usuarios de una cartera o las partes usuarias de una cartera durante más de dieciséis horas calculadas sobre la base de una semana natural, o se prevé que vaya a estarlo;

d) se sospecha que más del 1 % de los usuarios de una cartera o de las partes usuarias de una cartera está afectado o se prevé que vaya a estar afectado por una limitación de la disponibilidad de la solución de cartera o de los servicios prestados por las entidades afectadas en lo que respecta a la solución de cartera;

e) existe la capacidad de poner en peligro, o se ha puesto en peligro, la restricción del acceso físico al personal de confianza de las entidades afectadas, o la protección de dicho acceso físico, a una o varias de las ubicaciones de la red y de los sistemas de información que dan soporte a la solución de cartera, a la provisión de los mecanismos de validación a que se refiere el artículo 5 *bis*, apartado 8, del Reglamento (UE) n.º 910/2014 asociados a una solución de cartera, o al sistema de identificación electrónica en virtud del cual se proporciona una solución de cartera;

f) la privacidad, la integridad, la confidencialidad o la autenticidad de los datos almacenados, transmitidos o tratados en la solución de la cartera están en peligro, o pueden estar en peligro, de una o varias de las siguientes maneras:

— con repercusión en más del 1 % de los usuarios de la cartera de la solución de cartera afectada o en más de 100 000 de dichos usuarios, si este número es menor;

— como resultado de una actividad presuntamente malintencionada que ha logrado su objetivo;

— como resultado de una o varias vulnerabilidades conocidas, incluidas las gestionadas de conformidad con el Reglamento de Ejecución (UE) 2024/2981 de la Comisión ([1]), o si existe la probabilidad de que se produzca ese resultado;

— existe la probabilidad de que repercuta en los datos personales de manera que pueda suponer un riesgo para los derechos y libertades de las personas físicas afectadas y, en particular, en caso de violación de la seguridad de los datos personales tal como se define en el artículo 9, apartado 1, y en el artículo 10 del Reglamento (UE) 2016/679;

([1]) 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 (DO L, 2024/2981, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2981/oj).

— es probable que afecte a las comunicaciones electrónicas personales;

— es probable que entrañe un alto riesgo para los derechos y libertades de las personas físicas;

— es probable que afecte a personas físicas vulnerables;

g) la certificación de la solución de cartera ha sido cancelada o se prevé que sea cancelada;

h) la violación o la puesta en peligro ha causado o puede causar a la entidad afectada pérdidas financieras directas superiores a 500 000 EUR o, cuando proceda, al 5 % de su volumen de negocios total anual en el ejercicio financiero anterior, si esta cifra es inferior.

2. Los Estados miembros no tendrán en cuenta las consecuencias previstas de una operación de mantenimiento realizada por las entidades afectadas o en su nombre, siempre que dicha operación de mantenimiento:

a) se haya notificado previamente a los usuarios de una cartera, a las partes usuarias de la cartera y a los organismos de supervisión competentes potencialmente afectados;

b) no cumpla ninguno de los criterios establecidos en el punto 1 del presente anexo.

3. Por lo que se refiere al punto 1, letra c), la duración de un incidente que afecte a la disponibilidad se medirá desde el momento en que se interrumpa la prestación adecuada del servicio afectado hasta el momento en que el servicio se restablezca y vuelva a funcionar. Cuando una entidad afectada no pueda determinar el momento en que se produjo la interrupción, la duración del incidente se medirá desde el momento en que este fue detectado o desde el momento en que se dejó constancia de él en el registro de la red o del sistema o en otras fuentes de datos, si esto ocurriera antes. La indisponibilidad total de un servicio se medirá desde el momento en que el servicio quede completamente indisponible para los usuarios hasta el momento en que las actividades u operaciones habituales se hayan restablecido al mismo nivel de servicio que se prestaba antes del incidente. Cuando una entidad afectada no pueda determinar el momento en que se inició la indisponibilidad total de un servicio, esta se medirá a partir del momento en que fue detectada por dicha entidad.

4. Por lo que se refiere al punto 1, letra d), se considera que la disponibilidad de un servicio es limitada, en particular, cuando el tiempo de respuesta de ese servicio es considerablemente más lento que su tiempo medio de respuesta o cuando no están disponibles todas sus funcionalidades. Cuando sea posible, deberán utilizarse criterios objetivos basados en los tiempos medios de respuesta de los servicios para evaluar los retrasos en el tiempo de respuesta.

5. Para determinar las pérdidas financieras directas resultantes de una violación o una puesta en peligro de la seguridad a que se refiere el punto 1, letra h), las entidades afectadas tendrán en cuenta todas las pérdidas financieras que hayan sufrido como consecuencia del incidente, como los costes de sustitución o reubicación de *software*, *hardware* o infraestructuras, los costes de personal, incluidos los costes asociados a la sustitución o reubicación del personal, la contratación de personal adicional, la remuneración de las horas extraordinarias y la recuperación de las capacidades perdidas o deterioradas, los desembolsos por incumplimiento de las obligaciones contractuales, los costes de reparación y compensación a los clientes, las pérdidas por lucro cesante, los costes asociados a la comunicación interna y externa, y los costes de asesoramiento, incluidos los asociados al asesoramiento jurídico, a los servicios forenses y a los servicios de reparación. Los costes necesarios para el funcionamiento cotidiano de la empresa, como los costes de mantenimiento general de infraestructuras, equipos, *hardware* y *software*, las mejoras y las iniciativas de evaluación de riesgos, y las primas de seguros, no se considerarán pérdidas financieras derivadas de un incidente. Las entidades afectadas calcularán los importes de las pérdidas financieras basándose en los datos disponibles y, si no pueden determinarse los importes reales de las pérdidas financieras, harán una estimación de dichos importes.