►**B** **REGLAMENTO (UE) 2025/38 DEL PARLAMENTO EUROPEO Y DEL CONSEJO**

de 19 de diciembre de 2024

por el que se establecen medidas destinadas a reforzar la solidaridad y las capacidades en la Unión a fin de detectar ciberamenazas e incidentes, prepararse y responder a ellos y por el que se modifica el Reglamento (UE) 2021/694 (Reglamento de Cibersolidaridad)

(DO L 38 de 15.1.2025, p. 1)

Rectificado por:

►**C1** Rectificación, DO L 90063 de 24.1.2025, p. 1 (2025/38)

▼B

REGLAMENTO (UE) 2025/38 DEL PARLAMENTO EUROPEO Y DEL CONSEJO

de 19 de diciembre de 2024

por el que se establecen medidas destinadas a reforzar la solidaridad y las capacidades en la Unión a fin de detectar ciberamenazas e incidentes, prepararse y responder a ellos y por el que se modifica el Reglamento (UE) 2021/694 (Reglamento de Cibersolidaridad)

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1

Objeto y objetivos

1. El presente Reglamento establece medidas para reforzar las capacidades de la Unión a fin de detectar amenazas e incidentes de ciberseguridad, prepararse para ellos y responder a ellos, en particular mediante la creación:

a) de una red paneuropea de centros cibernéticos (en lo sucesivo, «Sistema Europeo de Alerta de Ciberseguridad») a fin de desarrollar y mejorar las capacidades coordinadas de detección y la conciencia situacional común;

b) de un Mecanismo de Emergencia en materia de Ciberseguridad para ayudar a los Estados miembros a prepararse para incidentes de ciberseguridad significativos, a gran escala y equivalentes a gran escala, y a responder a ellos, atenuar sus repercusiones y e iniciar la recuperación de ellos, así como ayudar a otros usuarios a responder a incidentes de ciberseguridad significativos y equivalentes a gran escala;

c) de un Mecanismo Europeo de Revisión de Incidentes de Ciberseguridad para revisar y evaluar incidentes de ciberseguridad significativos o a gran escala.

2. El presente Reglamento persigue los objetivos generales de reforzar la posición competitiva de la industria y los servicios en la Unión en toda la economía digital, incluidas las microempresas y las pequeñas y medianas empresas, así como las empresas emergentes, y de contribuir a la soberanía tecnológica de la Unión y a su autonomía estratégica abierta en el ámbito de la ciberseguridad, en particular impulsando la innovación en el mercado único digital. Persigue dichos objetivos reforzando la solidaridad a escala de la Unión, consolidando el ecosistema de ciberseguridad, mejorando la ciberresiliencia de los Estados miembros y desarrollando las capacidades, los conocimientos técnicos, las habilidades y las competencias de la mano de obra en relación con la ciberseguridad.

3. Los objetivos generales a que se refiere el apartado 2 se alcanzarán mediante los siguientes objetivos específicos:

a) reforzar las capacidades coordinadas comunes de detección de la Unión y la conciencia situacional común de ciberamenazas e incidentes;

▼B

b) consolidar la preparación de las entidades que operan en sectores de alta criticidad y de entidades que operen en otros sectores críticos en toda la Unión y reforzar la solidaridad mediante el desarrollo de pruebas coordinadas de preparación y capacidades mejoradas de respuesta y recuperación con vistas a gestionar incidentes de ciberseguridad significativos, a gran escala o equivalentes a gran escala, incluida la posibilidad de poner el apoyo de la Unión a la respuesta a incidentes de ciberseguridad a disposición de terceros países asociados al Programa Europa Digital;

c) mejorar la resiliencia de la Unión y contribuir a una respuesta eficaz frente a los incidentes mediante la revisión y evaluación de incidentes de ciberseguridad significativos o a gran escala, incluida la extracción de conclusiones y, en su caso, la formulación de recomendaciones.

4. Las acciones con arreglo al presente Reglamento deben llevarse a cabo dentro del debido respeto de las competencias de los Estados miembros y deben ser complementarias de las actividades que llevan a cabo la red de CSIRT, la EU-CyCLONe y el Grupo de Cooperación.

5. El presente Reglamento se entiende sin perjuicio de las funciones estatales esenciales de los Estados miembros, incluida la garantía de la integridad territorial del Estado, el mantenimiento del orden público y la salvaguardia de la seguridad nacional. En particular, la seguridad nacional seguirá siendo responsabilidad exclusiva de cada Estado miembro.

6. La puesta en común o el intercambio de información con arreglo al presente Reglamento que sea confidencial en virtud de las normas de la Unión o nacionales se limitará a aquella que sea pertinente y proporcionada en cuanto a la finalidad de dicha puesta en común o intercambio. Tal puesta en común o intercambio de información preservará la confidencialidad de la información y protegerá los intereses comerciales y de seguridad de las entidades afectadas. Ello no implicará facilitar información cuya divulgación sea contraria a los intereses esenciales de los Estados miembros en materia de seguridad nacional, seguridad pública o defensa.

Artículo 2

Definiciones

A los efectos del presente Reglamento, se entenderá por:

1) «centro cibernético transfronterizo»: una plataforma plurinacional creada mediante un acuerdo de consorcio escrito que reúne en una estructura de red coordinada a los centros cibernéticos nacionales de al menos tres Estados miembros, y que se ha concebido para mejorar el seguimiento, la detección y el análisis de las ciberamenazas, prevenir los incidentes y apoyar la producción de inteligencia sobre ciberamenazas, en particular mediante el intercambio de datos e información pertinentes, en su caso anonimizados, así como mediante la puesta en común de herramientas de vanguardia y el desarrollo conjunto de capacidades de detección, análisis y de prevención y protección cibernéticos en un entorno de confianza;

▼B

2) «consorcio anfitrión»: un consorcio compuesto por Estados participantes, que han acordado establecer y contribuir a la adquisición de herramientas, infraestructuras y servicios para un centro cibernético transfronterizo y a su funcionamiento;

3) «CSIRT»: un CSIRT designado o establecido con arreglo al artículo 10, de la Directiva (UE) 2022/2555;

4) «entidad»: una entidad según se define en el artículo 6, punto 38, de la Directiva (UE) 2022/2555;

5) «entidades que operan en sectores de alta criticidad»: el tipo de entidades enumeradas en el anexo I de la Directiva (UE) 2022/2555;

6) «entidades que operan en otros sectores críticos»: el tipo de entidades enumeradas en el Anexo II de la Directiva (UE) 2022/2555

7) «riesgo»: un riesgo según se define en el artículo 6, punto 9, de la Directiva (UE) 2022/2555;

8) «ciberamenaza»: una ciberamenaza según se define en el artículo 2, punto 8, del Reglamento (UE) 2019/881;

9) «incidente»: incidente según se define en el artículo 6, punto 6, de la Directiva (UE) 2022/2555;

10) «incidente de ciberseguridad significativo»: un incidente que cumple los criterios establecidos en el artículo 23, apartado 3, de la Directiva (UE) 2022/2555;

11) «incidente grave»: un incidente grave según se define en el artículo 3, punto 8, del Reglamento (UE, Euratom) 2023/2841 del Parlamento Europeo y del Consejo ([1]);

12) «incidente de ciberseguridad a gran escala»: un incidente de ciberseguridad a gran escala según se define en el artículo 6, punto 7, de la Directiva (UE) 2022/2555;

13) «incidente de ciberseguridad equivalente a gran escala»: en el caso de las instituciones, órganos y organismos de la Unión, un incidente grave y, en el caso de los terceros países asociados al Programa Europa Digital, un incidente que cause un nivel de perturbación que supere la capacidad para responder a él del tercer país asociado al Programa Europa Digital afectado;

([1]) Reglamento (UE, Euratom) 2023/2841 del Parlamento Europeo y del Consejo, de 13 de diciembre de 2023, por el que se establecen medidas destinadas a garantizar un elevado nivel común de ciberseguridad en las instituciones, los órganos y los organismos de la Unión (DO L, 2023/2841, 18.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2841/oj).

▼B

14) «tercer país asociado al Programa Europa Digital»: un tercer país que es parte en un acuerdo con la Unión que permite su participación en el Programa Europa Digital en virtud del artículo 10 del Reglamento (UE) 2021/694;

15) «órgano de contratación»: la Comisión o, en la medida en que el funcionamiento y la administración de la Reserva de Ciberseguridad de la UE se hayan encomendado a ENISA en virtud del artículo 14, apartado 5, ENISA;

16) «proveedor de servicios de seguridad gestionados»: un proveedor de servicios de seguridad gestionados tal como se define en el artículo 6, punto 40, de la Directiva (UE) 2022/2555;

17) «proveedores de servicios de seguridad gestionados de confianza»: los proveedores de servicios de seguridad gestionados seleccionados para formar parte de la Reserva de Ciberseguridad de la UE de conformidad con el artículo 17.

CAPÍTULO II

SISTEMA EUROPEO DE ALERTA DE CIBERSEGURIDAD

Artículo 3

Establecimiento del Sistema Europeo de Alerta de Ciberseguridad

1. Se creará una red paneuropea de infraestructuras integrada por los centros cibernéticos nacionales y los centros cibernéticos transfronterizos que voluntariamente se integren en ella, el Sistema Europeo de Alerta de Ciberseguridad, para apoyar el desarrollo de capacidades avanzadas a fin de que la Unión mejore las capacidades de detección, análisis y tratamiento de datos en relación con las ciberamenazas y la prevención de incidentes en la Unión.

2. El Sistema Europeo de Alerta de Ciberseguridad:

a) contribuirá a una mejor protección y respuesta frente a las ciberamenazas a través del apoyo, la cooperación con y el refuerzo de las capacidades de las entidades pertinentes, en particular, los CSIRT, la red de CSIRT, la EU-CyCLONe y las autoridades competentes designadas o establecidas de conformidad con el artículo 8, apartado 1 de la Directiva (UE) 2022/2555;

b) agrupará y pondrá en común datos e información pertinentes sobre ciberamenazas e incidentes procedentes de diversas fuentes dentro de los centros cibernéticos transfronterizos y compartirá información analizada o agregada a través de los centros cibernéticos transfronterizos, cuando proceda, con la red de CSIRT;

c) recogerá e impulsará la producción de información de alta calidad y ejecutable y de inteligencia sobre ciberamenazas, mediante el uso de herramientas de vanguardia y de tecnologías avanzadas, y pondrá en común dicha información e inteligencia sobre ciberamenazas;

▼B

d) contribuirá a mejorar la detección coordinada de ciberamenazas y la conciencia situacional común en toda la Unión, así como a la emisión de alertas, en particular, cuando proceda, formulando recomendaciones concretas a las entidades;

e) prestará servicios a la comunidad de ciberseguridad de la Unión y llevará a cabo actividades para dicha comunidad, incluida la contribución al desarrollo de herramientas y tecnologías avanzadas, como las de inteligencia artificial y análisis de datos.

3. Las medidas por las que se aplique el Sistema Europeo de Alerta de Ciberseguridad recibirán financiación del Programa Europa Digital y se ejecutarán de conformidad con el Reglamento (UE) 2021/694, en particular, con su objetivo específico 3.

Artículo 4

Centros cibernéticos nacionales

1. Cuando un Estado miembro decida participar en el Sistema Europeo de Alerta de Ciberseguridad, designará o, en su caso, establecerá un centro cibernético nacional a efectos del presente Reglamento.

2. El centro cibernético nacional será una entidad única que actuará bajo la autoridad de su Estado miembro. Podrá ser un CSIRT o, en su caso, una autoridad de gestión de crisis de ciberseguridad u otra autoridad competente designada o establecida en virtud del artículo 8, apartado 1, de la Directiva (UE) 2022/2555, u otra entidad. El centro cibernético nacional:

a) tendrá la capacidad de actuar como punto de referencia y pasarela a otras organizaciones públicas y privadas a nivel nacional para recoger y analizar información sobre ciberamenazas e incidentes y para contribuir a un centro cibernético transfronterizo, a que se refiere el artículo 5, y

b) será capaz de detectar, agregar y analizar datos e información pertinentes para las ciberamenazas e incidentes, como la inteligencia sobre ciberamenazas, utilizando en particular tecnologías de vanguardia, con el objetivo de prevenir incidentes.

3. Como parte de las funciones a que se refiere el apartado 2 del presente artículo, los centros cibernéticos nacionales podrán cooperar con entidades del sector privado para intercambiar datos e información pertinentes con el fin de detectar y prevenir ciberamenazas e incidentes, en particular con comunidades sectoriales e intersectoriales de entidades esenciales e importantes a que se refiere el artículo 3 de la Directiva (UE) 2022/2555. Cuando proceda, y de conformidad con el Derecho de la Unión y nacional, la información solicitada o recibida por los centros cibernéticos nacionales podrá incluir datos de telemetría, sensores y registro.

4. Los Estados miembros seleccionados de conformidad con el artículo 9, apartado 1, se comprometerán a solicitar que sus respectivos centros cibernéticos nacionales participen en un centro cibernético transfronterizo.

▼B

Artículo 5

Centros cibernéticos transfronterizos

1. Cuando al menos tres Estados miembros se comprometan a garantizar que sus centros cibernéticos nacionales colaboren para coordinar sus actividades de ciberdetección y seguimiento de amenazas, dichos Estados miembros podrán crear un consorcio anfitrión a efectos del presente Reglamento.

2. Un consorcio anfitrión estará compuesto por al menos tres Estados miembros participantes que hayan acordado establecer y contribuir a la adquisición de herramientas, infraestructuras y servicios para un centro cibernético transfronterizo y su funcionamiento de conformidad con el apartado 4.

3. Cuando se seleccione un consorcio anfitrión de conformidad con el artículo 9, apartado 3, sus miembros celebrarán un acuerdo de consorcio por escrito por el que:

a) se establecerán las disposiciones internas para la aplicación del acuerdo de alojamiento y uso a que se refiere el artículo 9, apartado 3;

b) se creará el centro cibernético transfronterizo del consorcio anfitrión, y

c) se incluirán las cláusulas específicas exigidas en virtud del artículo 6, apartados 1 y 2.

4. Un centro cibernético transfronterizo consistirá en una plataforma de múltiples países creada mediante un acuerdo de consorcio escrito al que se refiere el apartado 3. Reunirá en una estructura de red coordinada los centros cibernéticos nacionales de los Estados miembros del consorcio anfitrión. Deberá estar diseñado para mejorar el seguimiento, la detección y el análisis de ciberamenazas, prevenir incidentes y apoyar la producción de inteligencia sobre ciberamenazas, en particular, mediante el intercambio de datos e información pertinentes, anonimizados cuando proceda, así como mediante la puesta en común de herramientas de vanguardia, y el desarrollo conjunto de capacidades de detección, análisis y de prevención y protección cibernéticos en un entorno de confianza.

5. El centro cibernético transfronterizo estará representado a efectos jurídicos por un miembro del consorcio anfitrión en calidad de coordinador, o por el consorcio anfitrión si este tiene personalidad jurídica. La responsabilidad del cumplimiento del presente Reglamento y el acuerdo de alojamiento y uso por parte del centro cibernético transfronterizo se asignará en el acuerdo de consorcio escrito a que se refiere el apartado 3.

6. Un Estado miembro podrá adherirse a un consorcio anfitrión existente con el acuerdo de los miembros de dicho consorcio. El acuerdo de consorcio escrito a que se refiere el apartado 3 y el acuerdo de alojamiento y uso se modificarán en consecuencia. Esto no afectará a los derechos de propiedad del Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad (ECCC) sobre las herramientas, infraestructuras o servicios ya adquiridos conjuntamente con dicho consorcio anfitrión.

▼B

Artículo 6

Cooperación y puesta en común de información dentro de los centros cibernéticos transfronterizos y entre ellos

1. Los miembros de un consorcio anfitrión garantizarán que sus centros cibernéticos nacionales pongan en común, de conformidad con el acuerdo de consorcio al que se refiere el artículo 5, apartado 3, dentro del centro cibernético transfronterizo, la información pertinentes, anonimizados cuando proceda, como, por ejemplo, información relativa a ciberamenazas, cuasiincidentes, vulnerabilidades, técnicas y procedimientos, indicadores de compromiso, tácticas de los adversarios, información específica del agente de riesgo, alertas de ciberseguridad y recomendaciones relativas a la configuración de las herramientas de ciberseguridad para detectar ciberataques, siempre que dicha puesta en común de información:

a) fomente y mejore la detección de ciberamenazas y refuerce las capacidades de la red de CSIRT para prevenir y responder a incidentes o atenuar su repercusión;

b) refuerce el nivel de ciberseguridad, por ejemplo, concienciando sobre las ciberamenazas, limitando o anulando la capacidad de tales amenazas de propagarse, respaldando una batería de capacidades de defensa, corrección y divulgación de las vulnerabilidades, técnicas de detección, contención y prevención de amenazas, estrategias paliativas, etapas de respuesta y recuperación, o fomentando la investigación de amenazas en colaboración con entidades públicas y privadas.

2. El acuerdo de consorcio escrito a que se refiere el artículo 5, apartado 3, establecerá:

a) el compromiso de poner en común entre los miembros del consorcio anfitrión la información a que se refiere el apartado 1 y las condiciones en las que se pondrá en común dicha información;

b) un marco de gobernanza que aclare e incentive la puesta en común de información pertinente, en su caso anonimizada, a que se refiere el apartado 1 entre todos los participantes;

c) objetivos para la contribución al desarrollo de herramientas y tecnologías avanzadas, tales como herramientas de inteligencia artificial y análisis de datos.

El acuerdo de consorcio escrito podrá especificar que la información a que se refiere el apartado 1 se pondrá en común de conformidad con el Derecho de la Unión y nacional.

3. Los centros cibernéticos transfronterizos celebrarán acuerdos de cooperación entre sí, especificando los principios de interoperabilidad y puesta en común de información entre ellos. Los centros cibernéticos transfronterizos informarán a la Comisión de los acuerdos de cooperación celebrados.

▼B

4. El intercambio de información a que se refiere el apartado 1 entre centros cibernéticos transfronterizos estará garantizado por un alto nivel de interoperabilidad. Para apoyar dicha interoperabilidad ENISA, en estrecha concertación con la Comisión, sin demora indebida y a más tardar el 5 de febrero de 2026, emitirá directrices de interoperabilidad en las que se especifiquen, en particular, los formatos y protocolos de puesta en común de información, teniendo en cuenta las normas y mejores prácticas internacionales, así como el funcionamiento de cualquier centro cibernético transfronterizo existente. Los requisitos de interoperabilidad previstos en los acuerdos de cooperación de los centros cibernéticos transfronterizos se basarán en las directrices publicadas por ENISA.

Artículo 7

Cooperación y puesta en común de información con redes a escala de la Unión

1. Los centros cibernéticos transfronterizos y la red de CSIRT deben cooperar estrechamente, en particular para poner en común información. A tal fin, acordarán disposiciones de procedimiento en materia de cooperación y puesta en común de información pertinente y, sin perjuicio de lo dispuesto en el apartado 2, los tipos de información que se pondrán en común.

2. Cuando los centros de ciberseguridad transfronterizos obtengan información relativa a un incidente de ciberseguridad a gran escala potencial o en curso, garantizarán, a efectos de conciencia situacional común, que se faciliten a las autoridades de los Estados miembros y a la Comisión la información pertinente y las alertas tempranas a través de la EU-CyCLONe y de la red de CSIRT, sin demora indebida.

Artículo 8

Seguridad

1. Los Estados miembros que participen en el Sistema Europeo de Alerta de Ciberseguridad garantizarán un alto nivel de ciberseguridad, incluida la confidencialidad y seguridad de los datos, así como de seguridad física de la infraestructura del Sistema Europeo de Alerta de Ciberseguridad, y velarán por que la red se gestione y controle adecuadamente, de tal manera que se proteja de las amenazas y se garantice su seguridad y la de los sistemas, incluidos los datos e información puestos en común a través de la red.

2. Los Estados miembros que participen en el Sistema Europeo de Alerta de Ciberseguridad velarán por que la puesta en común de información a que se refiere el artículo 6, apartado 1, dentro del Sistema Europeo de Alerta de Ciberseguridad con cualquier entidad que no sea una autoridad u organismo público de un Estado miembro no afecte negativamente a los intereses de seguridad de la Unión o de los Estados miembros.

Artículo 9

Financiación del Sistema Europeo de Alerta de Ciberseguridad

1. Tras una convocatoria de manifestaciones de interés, el ECCC seleccionará de entre los Estados miembros que tengan la intención de participar en el Sistema Europeo de Alerta de Ciberseguridad a aquellos que participarán con el ECCC en una contratación conjunta de herramientas, infraestructuras o servicios, con el fin de crear, o mejorar

▼B

las capacidades de los centros cibernéticos nacionales designados o establecidos en virtud del artículo 4, apartado 1. El ECCC podrá conceder subvenciones a los Estados miembros seleccionados para financiar el funcionamiento de tales herramientas, infraestructuras y servicios. La contribución financiera de la Unión sufragará hasta el 50 % de los costes de adquisición de las herramientas, infraestructuras o servicios, y hasta el 50 % de los costes de funcionamiento. Los Estados miembros seleccionados sufragarán los costes restantes. Antes de iniciar el procedimiento para la adquisición de las herramientas, infraestructuras o servicios, el ECCC y los Estados miembros seleccionados celebrarán un acuerdo de alojamiento y uso que regule el uso de las herramientas, infraestructuras o servicios.

2. Si el centro cibernético nacional de un Estado miembro no participa en un centro cibernético transfronterizo en el plazo de dos años a partir de la fecha en que se adquieran las herramientas, infraestructuras y servicios, o de la fecha en que reciba la financiación mediante subvenciones, si dicha fecha fuera anterior, el Estado miembro no podrá beneficiarse de otro apoyo de la Unión previsto en el presente capítulo hasta que no se adhiera a un centro cibernético transfronterizo.

3. Tras una convocatoria de manifestaciones de interés, el ECCC seleccionará un consorcio anfitrión para que participe con él en una contratación conjunta de herramientas, infraestructuras o servicios. El ECCC podrá conceder al consorcio anfitrión una subvención para financiar el funcionamiento de dichas herramientas, infraestructuras o servicios. La contribución financiera de la Unión sufragará hasta el 75 % de los costes de adquisición de las herramientas, infraestructuras o servicios, y hasta el 50 % de los costes de funcionamiento. El consorcio anfitrión sufragará los costes restantes. Antes de iniciar el procedimiento para la adquisición de las herramientas, infraestructuras y servicios, el ECCC y el consorcio anfitrión celebrarán un acuerdo de alojamiento y uso que regule el uso de las herramientas, infraestructuras o servicios.

4. El ECCC preparará, al menos cada dos años, una cartografía de las herramientas, infraestructuras o servicios necesarios y de calidad adecuada para crear o mejorar las capacidades de los centros cibernéticos nacionales y los centros cibernéticos transfronterizos, así como su disponibilidad, también por parte de entidades jurídicas establecidas o que se consideren establecidas en los Estados miembros y controladas por los Estados miembros o por nacionales de los Estados miembros. Al preparar la cartografía, el ECCC consultará a la red de CSIRT, a cualquier centro cibernético transfronterizo existente, a ENISA y a la Comisión.

CAPÍTULO III

MECANISMO DE EMERGENCIA EN MATERIA DE CIBERSEGURIDAD

Artículo 10

Creación del Mecanismo de Emergencia en materia de Ciberseguridad

1. Se crea un Mecanismo de Emergencia en materia de Ciberseguridad para apoyar la mejora de la resiliencia de la Unión ante las ciberamenazas, prepararla para los efectos a corto plazo de los incidentes de ciberseguridad significativos, a gran escala y equivalentes a gran escala, y paliar dichos efectos, en un espíritu de solidaridad.

▼B

2. En el caso de los Estados miembros, las acciones en el marco del Mecanismo de Emergencia en materia de Ciberseguridad se llevarán a cabo previa solicitud y complementarán los esfuerzos y acciones de los Estados miembros para prepararse ante incidentes, responder a ellos y recuperarse de ellos.

3. Las acciones por las que se aplica el Mecanismo de Emergencia en materia de Ciberseguridad recibirán financiación del Programa Europa Digital y se ejecutarán de conformidad con el Reglamento (UE) 2021/694, en particular, con su objetivo específico 3.

4. Las acciones en el marco del Mecanismo de Emergencia en materia de Ciberseguridad se ejecutarán principalmente a través del ECCC de conformidad con el Reglamento (UE) 2021/887. Sin embargo, las acciones de ejecución de la Reserva de Ciberseguridad de la UE, a que se refiere el artículo 11, letra b), del presente Reglamento que se ejecutarán por la Comisión y ENISA.

Artículo 11

Tipos de acciones

El Mecanismo de Emergencia en materia de Ciberseguridad apoyará los siguientes tipos de acciones:

a) acciones de preparación, a saber:

   i) las pruebas coordinadas de preparación de las entidades que operan en sectores de alta criticidad en toda la Unión, tal como se especifica en el artículo 12;

   ii) otras acciones de preparación para las entidades que operan en sectores de alta criticidad o entidades que operan en otros sectores críticos, tal como se especifica en el artículo 13;

b) acciones que apoyen la respuesta a incidentes de ciberseguridad significativos, a gran escala y equivalentes a gran escala, e inicien la recuperación de ellos, de las que se ocuparán los proveedores de servicios de seguridad gestionados de confianza que participen en la Reserva de Ciberseguridad de la UE establecida en virtud del artículo 14;

c) acciones de apoyo a la asistencia mutua, tal como se contempla en el artículo 18.

Artículo 12

Pruebas coordinadas de preparación de las entidades

1. El Mecanismo de Emergencia en materia de Ciberseguridad apoyará las pruebas coordinadas de preparación de las entidades que operan en sectores de alta criticidad.

2. Las pruebas coordinadas de preparación podrán consistir en actividades de preparación, tales como pruebas de penetración y evaluación de amenazas.

▼B

3. El apoyo a las acciones de preparación con arreglo al presente artículo se prestará a los Estados miembros principalmente en forma de subvenciones y en las condiciones previstas en los programas de trabajo pertinentes a que se refiere el artículo 24 del Reglamento (UE) 2021/694.

4. Con el fin de apoyar las pruebas coordinadas de preparación de las entidades a que se refiere el artículo 11, letra a), inciso i), del presente Reglamento en toda la Unión, la Comisión, previa consulta al Grupo de Cooperación, a la EU-CyCLONe y a ENISA, determinará, a partir de los sectores de alta criticidad enumerados en el anexo I de la Directiva (UE) 2022/2555, los sectores o subsectores afectados para los que se pueda publicar una convocatoria de propuestas para la concesión de subvenciones. La participación de los Estados miembros en dichas convocatorias de propuestas es voluntaria.

5. Para determinar los sectores o subsectores contemplados en el apartado 4, la Comisión tendrá en cuenta las evaluaciones de riesgos coordinadas y las pruebas de resiliencia a escala de la Unión, así como sus resultados.

6. El Grupo de Cooperación, en colaboración con la Comisión, el Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad (en lo sucesivo, «Alto Representante») y ENISA, y en el marco de su mandato, la EU-CyCLONe, elaborará escenarios de riesgo y metodologías comunes para las pruebas de preparación coordinadas a que se refiere el artículo 11, letra a), inciso i), y, cuando proceda, para otras acciones de preparación a que se refiere la letra a), inciso ii), de dicho artículo.

7. Cuando una entidad que opere en un sector de alta criticidad participe voluntariamente en pruebas de preparación coordinadas y estas den lugar a recomendaciones de medidas específicas, que la entidad participante podrá integrar en un plan corrector, la autoridad del Estado miembro responsable de las de pruebas de preparación coordinadas revisará, cuando proceda, el seguimiento de dichas medidas por parte de las entidades participantes con vistas a reforzar la preparación.

Artículo 13

Otras acciones de preparación

1. El Mecanismo de Emergencia en materia de Ciberseguridad apoyará las acciones de preparación no contempladas en el artículo 12. Tales acciones incluirán acciones de preparación para entidades de sectores no identificados para pruebas de preparación coordinadas en virtud del artículo 12. Estas acciones pueden apoyar el seguimiento de vulnerabilidades y de riesgos, los ejercicios y la formación.

2. El apoyo a las acciones de preparación con arreglo al presente artículo se prestará a los Estados miembros principalmente en forma de subvenciones a reserva de las condiciones definidas en los programas de trabajo pertinentes a que se refiere el artículo 24 del Reglamento (UE) 2021/694.

▼B

Artículo 14

Creación de la Reserva de Ciberseguridad de la UE

1. Se crea una reserva de ciberseguridad de la UE para ayudar, previa solicitud, a los usuarios a que se refiere el apartado 3 a responder o a prestar apoyo para responder a incidentes de ciberseguridad significativos, a gran escala o equivalentes a gran escala, y para iniciar la recuperación de tales incidentes.

2. La Reserva de Ciberseguridad de la UE consistirá en servicios de respuesta prestados por proveedores de servicios de seguridad gestionados de confianza seleccionados de conformidad con los criterios establecidos en el artículo 17, apartado 2. La Reserva de Ciberseguridad de la UE podrá incluir servicios objeto de compromiso previo. Los servicios objeto de compromiso previo de un proveedor de servicios de seguridad gestionados de confianza podrán convertirse en servicios de preparación relacionados con la prevención y respuesta a incidentes, en caso de que dichos servicios objeto de compromiso previo no se utilicen para la respuesta a incidentes durante el período en el que se hayan sido objeto de compromiso previo. La Reserva de Ciberseguridad de la UE podrá desplegarse, previa solicitud, en todos los Estados miembros, en las instituciones, órganos y organismos de la Unión, y en los terceros países asociados al Programa Europa Digital a que se refiere el artículo 19, apartado 1.

3. Los usuarios de los servicios de la Reserva de Ciberseguridad de la UE comprenderán los siguientes:

a) las autoridades de gestión de crisis de ciberseguridad de los Estados miembros y los CSIRT a que se refieren, respectivamente, el artículo 9, apartados 1 y 2, y el artículo 10 de la Directiva (UE) 2022/2555;

b) el CERT-EU, de conformidad con el artículo 13 del Reglamento (UE, Euratom) 2023/2841;

c) las autoridades competentes, como los equipos de respuesta a incidentes de seguridad informática y las autoridades de gestión de crisis de ciberseguridad de terceros países asociados al Programa Europa Digital, de conformidad con el artículo 19, apartado 8.

4. La Comisión tendrá la responsabilidad general de la ejecución de la Reserva de Ciberseguridad de la UE. La Comisión, junto con el Grupo de Cooperación, determinará las prioridades y la evolución de la Reserva de Ciberseguridad de la UE, en consonancia con los requisitos de los usuarios a que se refiere el apartado 3, supervisará su aplicación y garantizará la complementariedad, la coherencia, las sinergias y los vínculos con otras acciones de apoyo con arreglo al presente Reglamento, así como con otras acciones y programas de la Unión. Esas prioridades serán evaluadas, y si procede, revisadas cada dos años. La Comisión informará al Parlamento Europeo y al Consejo de dichas prioridades y sus revisiones.

▼B

5. Sin perjuicio de la responsabilidad general de la Comisión en la ejecución de la Reserva de Ciberseguridad de la UE a que se refiere el apartado 4 del presente artículo y a reserva de un convenio de contribución, tal como se define en el artículo 2, punto 19, del Reglamento (UE, Euratom) 2024/2509, la Comisión encomendará el funcionamiento y la administración de la Reserva de Ciberseguridad de la UE, total o parcialmente, a ENISA. Los aspectos no encomendados a ENISA seguirán siendo objeto de gestión directa por parte de la Comisión.

6. ENISA preparará, al menos cada dos años, una cartografía de los servicios que necesitan los usuarios a que se refiere el apartado 3, letras a) y b), del presente artículo. La cartografía incluirá asimismo la disponibilidad de tales servicios, también por parte de entidades jurídicas establecidas o que se consideren establecidas en los Estados miembros y controladas por los Estados miembros o por nacionales de los Estados miembros. Al elaborar la cartografía respecto de dicha disponibilidad, ENISA evaluará las competencias y capacidades de la mano de obra de la Unión en el ámbito de la ciberseguridad pertinentes para alcanzar los objetivos de la Reserva de Ciberseguridad de la UE. Para preparar la cartografía, ENISA consultará al Grupo de Cooperación, a la EU-CyCLONe, la Comisión y, en su caso, el Consejo Interinstitucional de Ciberseguridad, creado en virtud del artículo 10 del Reglamento (UE, Euratom) 2023/2841. Al elaborar la cartografía respecto de la disponibilidad de servicios, ENISA también consultará a las partes interesadas pertinentes del sector de la ciberseguridad, como los proveedores de servicios de seguridad gestionados. ENISA preparará una cartografía similar, tras informar al Consejo y tras consultar a la EU-CyCLONe, a la Comisión y, cuando proceda, al Alto Representante, para determinar las necesidades de los usuarios a que se refiere el apartado 3, letra c) del presente artículo.

7. La Comisión estará facultada para adoptar actos delegados, con arreglo al artículo 23, para completar el presente Reglamento especificando los tipos y el número de servicios de respuesta necesarios para la Reserva de Ciberseguridad de la UE. Al preparar dichos actos delegados, la Comisión tendrá en cuenta la cartografía a que se refiere el apartado 6 del presente artículo, y podrá intercambiar asesoramiento y cooperar con el Grupo de Cooperación y ENISA.

Artículo 15

Solicitudes de apoyo de la Reserva de Ciberseguridad de la UE

1. Los usuarios a que se refiere el artículo 14, apartado 3, podrán solicitar los servicios de la Reserva de Ciberseguridad de la UE para apoyar la respuesta a incidentes de ciberseguridad significativos, a gran escala o equivalentes a gran escala e iniciar la recuperación de tales incidentes.

2. Para recibir el apoyo de la Reserva de Ciberseguridad de la UE, los usuarios a que se refiere el artículo 14, apartado 3, tomarán todas las medidas apropiadas para atenuar los efectos del incidente para el que se solicite el apoyo, incluida, cuando proceda, la prestación de asistencia técnica directa, y otros recursos para ayudar a la respuesta y a los esfuerzos de recuperación.

▼B

3. Las solicitudes de apoyo se transmitirán al órgano de contratación como sigue:

a) en el caso de los usuarios a que se refiere el artículo 14, apartado 3, letra a), del presente Reglamento, a través del punto de contacto único designado o establecido en virtud del artículo 8, apartado 3, de la Directiva (UE) 2022/2555;

b) en el caso del usuario a que se refiere el artículo 14, apartado 3, letra b), por dicho usuario;

c) en el caso de los usuarios a que se refiere el artículo 14, apartado 3, letra c), a través del punto de contacto único a que se refiere el artículo 19, apartado 9.

4. En el caso de las solicitudes de los usuarios a que se refiere el artículo 14, apartado 3, letra a), los Estados miembros informarán a la red de CSIRT y, cuando proceda, a la EU-CyCLONe, de sus solicitudes de apoyo de usuarios para la respuesta a incidentes y la recuperación inicial con arreglo al presente artículo.

5. Las solicitudes de apoyo para la respuesta a incidentes y la recuperación inicial incluirán:

a) información adecuada sobre la entidad afectada y las posibles repercusiones del incidente sobre lo siguiente:

   i) en el caso de los usuarios a que se refiere el artículo 14, apartado 3, letra a), los Estados miembros y usuarios afectados, incluido el riesgo de contagio a otro Estado miembro;

   ii) en el caso del usuario a que se refiere el artículo 14, apartado 3, letra b), las instituciones, órganos u organismos de la Unión afectados;

   iii) en el caso de los usuarios a que se refiere el artículo 14, apartado 3, letra c), los países asociados al Programa Europa Digital afectados;

b) información sobre el servicio solicitado, además del uso previsto y el apoyo requerido, incluida una indicación de las necesidades estimadas;

c) información apropiada sobre las medidas tomadas para paliar el incidente para el que se solicite el apoyo, tal como se contempla en el apartado 2;

d) en su caso, información disponible sobre otras formas de apoyo a disposición de la entidad afectada.

6. ENISA, en cooperación con la Comisión y la EU-CyCLONe, elaborará una plantilla para facilitar la presentación de solicitudes de apoyo de la Reserva de Ciberseguridad de la UE.

▼B

7. La Comisión podrá especificar, mediante actos de ejecución, las disposiciones de procedimiento detalladas sobre la manera en que se deberá solicitar los servicios de apoyo de la Reserva de Ciberseguridad de la UE y la manera en que se deberá responder a dichas solicitudes en virtud del presente artículo, el artículo 16, apartado 1, y el artículo 19, apartado 10, así como las disposiciones para la presentación de tales solicitudes y la entrega de las respuestas y los modelos para los informes a que se refiere el artículo 16, apartado 9. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 24, apartado 2.

Artículo 16

Ejecución del apoyo de la Reserva de Ciberseguridad de la UE

1. En el caso de las solicitudes de los usuarios a que se refiere el artículo 14, apartado 3, letras a) y b), las solicitudes de apoyo de la Reserva de Ciberseguridad de la UE serán evaluadas por el órgano de contratación. Se transmitirá una respuesta a los usuarios a que se refiere el artículo 14, apartado 3, letras a) y b), sin demora y, en cualquier caso, en un plazo máximo de cuarenta y ocho horas a partir de la presentación de la solicitud para garantizar la eficacia del apoyo. El órgano de contratación informará al Consejo y a la Comisión de los resultados del proceso.

2. Por lo que se refiere a la información puesta en común durante la solicitud y la prestación de los servicios de la Reserva de Ciberseguridad de la UE, todas las partes implicadas en la aplicación del presente Reglamento:

a) limitarán el uso y la puesta en común de dicha información a lo estrictamente necesario para cumplir sus obligaciones o funciones con arreglo al presente Reglamento;

b) utilizarán y pondrán en común toda información confidencial o clasificada en virtud del Derecho de la Unión y nacional únicamente de conformidad con dicho Derecho, y

c) garantizarán un intercambio de información eficaz, eficiente y seguro, cuando proceda, utilizando y respetando los protocolos pertinentes, como el TLP para la puesta en común de información.

3. Al evaluar las solicitudes individuales con arreglo al artículo 16, apartado 1, y al artículo 19, apartado 10, el órgano de contratación o la Comisión, según proceda, evaluará en primer lugar si se cumplen los criterios mencionados en el artículo 15, apartados 1 y 2. En tal caso, evaluará la adecuación de la duración y la naturaleza del apoyo, teniendo en cuenta el objetivo recogido en el artículo 1, apartado 3, letra b), y los siguientes criterios, cuando proceda:

a) la magnitud y la gravedad del incidente;

b) el tipo de entidad afectada, dando mayor prioridad a los incidentes que afecten a entidades esenciales según se contemplan en el artículo 3, apartado 1, de la Directiva (UE) 2022/2555;

▼B

c) la repercusión potencial del incidente en el Estado miembro o Estados miembros, las instituciones, órganos u organismos de la Unión o los terceros países asociados al Programa Europa Digital;

d) el posible carácter transfronterizo del incidente y el riesgo de contagio a otros Estados miembros o instituciones, órganos u organismos de la Unión o terceros países asociados al Programa Europa Digital;

e) las medidas tomadas por el usuario para ayudar a la respuesta y los esfuerzos de recuperación iniciales a que se refieren el artículo 15, apartado 2.

4. Para establecer el orden de prioridad de las solicitudes, en el caso de solicitudes simultáneas de los usuarios a que se refiere el artículo 14, apartado 3, se tendrán en cuenta, cuando proceda, los criterios a que se refiere el apartado 3 del presente artículo, sin perjuicio del principio de cooperación leal entre los Estados miembros y las instituciones, órganos y organismos de la Unión. Cuando dos o más solicitudes se consideren iguales con arreglo a los dichos criterios se dará mayor prioridad a las solicitudes de los usuarios de los Estados miembros. Cuando el funcionamiento y la administración de la Reserva de Ciberseguridad de la UE se hayan encomendado, total o parcialmente, a ENISA en virtud del artículo 14, apartado 5, ENISA y la Comisión cooperarán estrechamente para establecer el orden de prioridad de las solicitudes de conformidad con el presente apartado.

5. Los servicios de la Reserva de Ciberseguridad de la UE se prestarán de conformidad con acuerdos específicos entre el proveedor de servicios de seguridad gestionados de confianza y el usuario al que se preste el apoyo en el marco de la Reserva de Ciberseguridad de la UE. Dichos servicios podrán prestarse de conformidad con acuerdos específicos entre el proveedor de servicios de seguridad gestionados de confianza, el usuario y la entidad afectada. Todos los acuerdos a que se refiere el presente apartado incluirán, entre otras cosas, condiciones en materia de responsabilidad.

6. Los acuerdos a que se refiere el apartado 5 se basarán en plantillas preparadas por ENISA, previa consulta a los Estados miembros y, cuando proceda, a otros usuarios de la Reserva de Ciberseguridad de la UE.

7. La Comisión, ENISA y los usuarios de la Reserva de Ciberseguridad de la UE no asumirán responsabilidad contractual alguna por los daños causados a terceros por los servicios prestados en el marco de la ejecución de la Reserva de Ciberseguridad de la UE.

8. Los usuarios podrán utilizar los servicios de la Reserva de Ciberseguridad de la UE prestados en respuesta a una solicitud con arreglo al artículo 15, apartado 1, únicamente para apoyar la respuesta a incidentes de ciberseguridad significativos, a gran escala o equivalentes a gran escala e iniciar la recuperación de ellos. Solo podrán utilizar dichos servicios con respecto a:

a) entidades que operan en sectores de alta criticidad o entidades que operan en otros sectores críticos, en el caso de los usuarios a que se refiere el artículo 14, apartado 3, letra a), y entidades equivalentes en el caso de los usuarios a que se refiere el artículo 14, apartado 3, letra c), y

▼B

b) instituciones, órganos y organismos de la Unión, en el caso del usuario a que se refiere el artículo 14, apartado 3, letra b).

9. En el plazo de dos meses a partir del fin del apoyo, todo usuario que haya recibido apoyo facilitará un informe resumido sobre el servicio prestado, los resultados obtenidos y las conclusiones extraídas:

a) a la Comisión, ENISA, la red de CSIRT y la EU-CyCLONe, en el caso de los usuarios a que se refiere el artículo 14, apartado 3, letra a);

b) a la Comisión, a ENISA y al Consejo Interinstitucional de Ciberseguridad, en el caso del usuario a que se refiere el artículo 14, apartado 3, letra b);

c) a la Comisión, en el caso de los usuarios a que se refiere el artículo 14, apartado 3, letra c).

La Comisión transmitirá los informes resumidos recibidos de los usuarios a que se refiere el artículo 14, apartado 3, en virtud de la letra c), párrafo primero, del presente apartado al Consejo y al Alto Representante.

10. Cuando el funcionamiento y la administración de la Reserva de Ciberseguridad de la UE se hayan encomendado, total o parcialmente, a ENISA con arreglo al artículo 14, apartado 5, del presente Reglamento, ENISA informará a la Comisión y le consultará periódicamente a este respecto. En este contexto, ENISA enviará inmediatamente a la Comisión todas las solicitudes que reciba de los usuarios a que se refiere el artículo 14, apartado 3, letra c), del presente Reglamento, y, cuando sea necesario a efectos de priorización con arreglo al presente artículo, cualquier solicitud que haya recibido de los usuarios a que se refiere el artículo 14, apartado 3, letras a) o b), del presente Reglamento. Las obligaciones establecidas en el presente apartado se entenderán sin perjuicio de lo dispuesto en el artículo 14 del Reglamento (UE) 2019/881.

11. En el caso de los usuarios a que se refiere el artículo 14, apartado 3, letras a) y b), el órgano de contratación informará al Grupo de Cooperación, de forma periódica y al menos dos veces al año, sobre el uso y los resultados del apoyo.

12. En el caso de los usuarios a que se refiere el artículo 14, apartado 3, letra c), la Comisión informará al Consejo y comunicará periódicamente al Alto Representante, al menos dos veces al año, sobre el uso y los resultados del apoyo.

Artículo 17

Proveedores de servicios de seguridad gestionados de confianza

1. En los procedimientos de contratación pública destinados a crear la Reserva de Ciberseguridad de la UE, el órgano de contratación actuará de conformidad con los principios establecidos en el Reglamento (UE, Euratom) 2024/2509 y con los principios siguientes:

▼B

a) garantizar que los servicios incluidos en la Reserva de Ciberseguridad de la UE, cuando sean considerados en su conjunto, sean tales que la Reserva de Ciberseguridad de la UE incluya servicios que puedan prestarse en todos los Estados miembros, teniendo en cuenta, en particular, los requisitos nacionales para la prestación de tales servicios, incluidas las lenguas y la certificación o acreditación;

b) garantizar la protección de los intereses esenciales de seguridad de la Unión y de sus Estados miembros;

c) garantizar que la Reserva de Ciberseguridad de la UE aporte valor añadido de la Unión, al contribuir a los objetivos establecidos en el artículo 3 del Reglamento (UE) 2021/694, en particular promoviendo el desarrollo de capacidades de ciberseguridad en la Unión.

2. Al contratar servicios para la Reserva de Ciberseguridad de la UE, el órgano de contratación incluirá en los pliegos de la contratación los siguientes criterios y requisitos:

a) el proveedor demostrará que su personal tiene el máximo grado de integridad profesional, independencia y responsabilidad y la competencia técnica necesaria para llevar a cabo las actividades en su ámbito específico, y garantizará la permanencia y continuidad de los conocimientos especializados, así como los recursos técnicos necesarios;

b) el proveedor, y todas las filiales y subcontratistas pertinentes, cumplirán las normas aplicables en materia de protección de la información clasificada y habrán establecido las medidas adecuadas, como, en su caso, acuerdos entre sí, para proteger la información confidencial relacionada con el servicio y, en particular, las pruebas, conclusiones e informes;

c) el proveedor deberá aportar pruebas suficientes de la transparencia de su estructura de gobierno y de la improbabilidad de que esta ponga en peligro su imparcialidad y la calidad de sus servicios o cause conflictos de intereses;

d) el proveedor dispondrá de la habilitación de seguridad adecuada, al menos para el personal destinado a participar en la prestación de servicios, cuando así lo exija el Estado miembro;

e) el proveedor dispondrá del nivel de seguridad pertinente para sus sistemas informáticos;

f) el proveedor estará equipado con el *hardware* y *software* necesarios para prestar el servicio solicitado, sin vulnerabilidades aprovechables conocidas, que incluirán las últimas actualizaciones de seguridad y cumplirán, en todo caso, toda disposición aplicable del Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo ([2]);

([2]) 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).

▼B

g) el proveedor deberá poder demostrar que tiene experiencia en la prestación de servicios similares a las autoridades nacionales pertinentes, a las entidades que operan en sectores de alta criticidad o entidades que operan en otros sectores críticos;

h) el proveedor deberá poder prestar el servicio en un plazo breve en los Estados miembros en los que pueda prestar el servicio;

i) el proveedor deberá poder prestar el servicio en una o varias lenguas oficiales de las instituciones de la Unión o de un Estado miembro según lo exija, en su caso, el Estado o Estados miembros o los usuarios a que se refieren los artículos 14, apartado 3, letras b) y c), en los que el proveedor pueda prestar el servicio;

j) una vez que se haya establecido un esquema europeo de certificación de la ciberseguridad para los servicios de seguridad gestionados con arreglo al Reglamento (UE) 2019/881, el proveedor será certificado de conformidad con dicho esquema en dos años a partir de la fecha de aplicación del esquema;

k) el proveedor incluirá en la oferta las condiciones de conversión de cualquier servicio de respuesta a incidentes no utilizado que pueda convertirse en servicios de preparación estrechamente relacionados con la respuesta a incidentes, como ejercicios o formaciones.

3. A efectos de la contratación de servicios para la Reserva de Ciberseguridad de la UE, el órgano de contratación podrá, cuando proceda, añadir criterios y requisitos a los que figuran en el apartado 2, en estrecha cooperación con los Estados miembros.

Artículo 18

Acciones de apoyo para la asistencia mutua

1. El Mecanismo de Emergencia en materia de Ciberseguridad debe apoyar la asistencia técnica prestada por un Estado miembro a otro Estado miembro afectado por un incidente de ciberseguridad significativo o a gran escala, también en los casos a que se refiere el artículo 11, apartado 3, letra f), de la Directiva (UE) 2022/2555.

2. El apoyo para la asistencia técnica mutual a que hace referencia el apartado 1 se prestará en forma de subvenciones a reserva de las condiciones definidas en los programas de trabajo pertinentes a que se refiere el artículo 24 del Reglamento (UE) 2021/694.

▼B

Artículo 19

Apoyo a terceros países asociados al Programa Europa Digital

1. El tercer país asociado al Programa Europa Digital podrá solicitar apoyo de la Reserva de Ciberseguridad de la UE cuando el acuerdo por el que esté asociado al Programa Europa Digital prevea la participación en la Reserva de Ciberseguridad de la UE. Dicho acuerdo contendrá disposiciones que exijan al tercer país asociado al Programa Europa Digital cumplir las obligaciones establecidas en los apartados 2 y 9 del presente artículo. A efectos de la participación de un tercer país en la Reserva de Ciberseguridad de la UE, un tercer país asociado al Programa Europa Digital parcialmente podrá incluir una asociación limitada al objetivo operativo a que se refiere el artículo 6, apartado 1, letra g), del Reglamento (UE) 2021/694.

2. En un plazo de tres meses desde la celebración del acuerdo al que se refiere el apartado 1 y, en todo caso, antes de recibir el apoyo de la Reserva de Ciberseguridad de la UE, el tercer país asociado al Programa Europa Digital facilitarán a la Comisión información sobre sus capacidades de ciberresiliencia y gestión de riesgos, incluida, como mínimo, información sobre las medidas nacionales adoptadas para prepararse frente a incidentes de ciberseguridad significativos, o equivalentes a gran escala, así como información sobre las entidades nacionales responsables, incluidos los equipos de respuesta a incidentes de seguridad informática o entidades equivalentes, sus capacidades y los recursos que tienen asignados. El tercer país asociado al Programa Europa Digital facilitará actualizaciones de esa información de forma periódica y al menos una vez al año. La Comisión suministrará dicha información al Alto Representante y a ENISA a fin de facilitar la aplicación del apartado 11.

3. La Comisión evaluará periódicamente, y al menos una vez al año, los siguientes criterios con respecto a cada tercer país asociado al Programa Europa Digital a que se refiere el apartado 1:

a) si dicho país cumple las condiciones del acuerdo a que se refiere el apartado 1, en la medida en que dichas condiciones se refieran a la participación en la Reserva de Ciberseguridad de la UE;

b) si dicho país ha adoptado medidas adecuadas para prepararse ante incidentes de ciberseguridad significativos o equivalentes a gran escala, sobre la base de la información a que se refiere el apartado 2, y

c) si la prestación de apoyo es coherente con la política y las relaciones generales de la Unión con ese país y si es coherente con otras políticas de la Unión en el ámbito de la seguridad.

La Comisión consultará al Alto Representante cuando lleve a cabo la evaluación a que se refiere el párrafo primero, en relación con el criterio contemplado en la letra c) de dicho párrafo.

▼B

Cuando la Comisión concluya que un tercer país asociado al Programa Europa Digital cumple todas las condiciones a que se refiere el párrafo primero, presentará una propuesta al Consejo para adoptar un acto de ejecución de conformidad con el apartado 4 por el que se autorice la prestación de apoyo de la Reserva de Ciberseguridad de la UE a dicho país.

4. El Consejo podrá adoptar los actos de ejecución a que se refiere el apartado 3. Estos actos de ejecución se aplicarán como máximo durante un año y serán renovables. Podrán incluir un límite, no inferior a setenta y cinco días, sobre el número de días para los que puede prestarse apoyo en respuesta a una única solicitud.

A efectos del presente artículo, el Consejo actuará con celeridad y adoptará, por regla general, los actos de ejecución a que se refiere el presente apartado en las ocho semanas siguientes a la adopción de la propuesta pertinente de la Comisión en virtud del apartado 3, párrafo tercero.

5. El Consejo podrá modificar o derogar un acto de ejecución adoptado en virtud del apartado 4 en cualquier momento, a propuesta de la Comisión.

Si el Consejo considera que se ha producido un cambio significativo en relación con el criterio a que se refiere el apartado 3, párrafo primero, letra c), podrá modificar o derogar un acto de ejecución adoptado en virtud del apartado 4, por iniciativa debidamente motivada de uno o varios Estados miembros.

6. En el ejercicio de sus competencias de ejecución en virtud del presente artículo, el Consejo aplicará los criterios a que se refiere el apartado 3 y explicará su valoración de dichos criterios. En particular, cuando actúe por propia iniciativa en virtud del apartado 5, párrafo segundo, el Consejo explicará el cambio significativo a que se refiere dicho párrafo.

7. El apoyo de la Reserva de Ciberseguridad de la UE a un tercer país asociado al Programa Europa Digital se ajustará a lo dispuesto en el acuerdo a que se refiere el apartado 1.

8. Entre los usuarios de los terceros países asociados al Programa Europa Digital que puedan optar a recibir los servicios de la Reserva de Ciberseguridad de la UE figurarán las autoridades competentes, como los equipos de respuesta a incidentes de seguridad informática o entidades equivalentes y las autoridades de gestión de crisis de ciberseguridad.

9. Cada tercer país asociado al Programa Europa Digital que pueda optar al apoyo de la Reserva de Ciberseguridad de la UE designará a una autoridad para que actúe como punto de contacto único a efectos del presente Reglamento.

10. Las solicitudes de apoyo de la Reserva de Ciberseguridad de la UE en virtud del presente artículo deben ser evaluadas por la Comisión. El órgano de contratación solo podrá prestar apoyo a un tercer país cuando, y en la medida en que, esté en vigor el acto de ejecución del Consejo por el que se autorice dicho apoyo con respecto a dicho país, adoptado en virtud del apartado 4, del presente artículo. Se transmitirá una respuesta a los usuarios a que se refiere el artículo 14, apartado 3, letra c), sin demora indebida.

▼B

11. Tras la recepción de una solicitud de ayuda con arreglo al presente artículo, la Comisión informará inmediatamente al Consejo. La Comisión mantendrá informado al Consejo de la evaluación de la solicitud. La Comisión también coordinará con el Alto Representante las solicitudes recibidas y la ejecución del apoyo de la Reserva de Ciberseguridad de la UE concedido a terceros países asociados al Programa Europa Digital. Además, la Comisión también debe tener en cuenta todo punto de vista facilitado por ENISA respecto a esas mismas solicitudes.

Artículo 20

Coordinación con los mecanismos de gestión de crisis de la Unión

1. Si un incidente de ciberseguridad significativo, a gran escala o equivalente a gran escala se produce a raíz de catástrofes o den lugar a catástrofes, tal como se definen en el artículo 4, punto 1, de la Decisión 1313/2013/UE, el apoyo en virtud del presente Reglamento para responder a tales incidentes complementará las acciones previstas en la Decisión 1313/2013/UE sin perjuicio de lo dispuesto en dicha Decisión.

2. En caso de un incidente de ciberseguridad a gran escala o equivalente a gran escala en el que se active el dispositivo de la UE de respuesta política integrada a las crisis con arreglo a la Decisión de Ejecución (UE) 2018/1993 (DIRPC), el apoyo en virtud del presente Reglamento para responder a dicho incidente se gestionará de conformidad con los protocolos y procedimientos pertinentes en el marco del DIRPC.

CAPÍTULO IV

MECANISMO EUROPEO DE REVISIÓN DE INCIDENTES DE CIBERSEGURIDAD

Artículo 21

Mecanismo Europeo de Revisión de Incidentes de Ciberseguridad

1. A petición de la Comisión o de la EU-CyCLONe, ENISA, con el apoyo de la red de CSIRT y la aprobación del Estado miembro afectado, revisará y evaluará las ciberamenazas, vulnerabilidades aprovechables conocidas y medidas paliativas con respecto a un incidente de ciberseguridad significativo específico o a gran escala. Una vez finalizada la revisión y evaluación de un incidente, ENISA presentará un informe de revisión del incidente con el objetivo de extraer conclusiones que permitan evitar o paliar futuros incidentes, a EU-CyCLONe, a la red de CSIRT, a los Estados miembros afectados y a la Comisión para ayudarlos en el desempeño de sus cometidos, en particular a la luz de los establecidos en los artículos 15 y 16 de la Directiva (UE) 2022/2555. Si un incidente afecta a un tercer país asociado al Programa Europa Digital, ENISA facilitará el informe al Consejo. En tales casos, la Comisión entregará el informe al Alto Representante.

▼B

2. Para preparar el informe de revisión del incidente a que se refiere el apartado 1 del presente artículo, ENISA cooperará con todas las partes interesadas pertinentes y recopilará sus observaciones, incluidos los representantes de los Estados miembros, la Comisión, otras instituciones, órganos y organismos pertinentes de la Unión, de la industria, incluidos los proveedores de servicios de seguridad gestionados, y de los usuarios de servicios de ciberseguridad. Cuando proceda, ENISA, en cooperación con los CSIRT y, en su caso, las autoridades competentes designadas o creadas en virtud del artículo 8, apartado 1, de la Directiva (UE) 2022/2555, también cooperará con las entidades afectadas por incidentes de ciberseguridad significativos o a gran escala. Los representantes consultados revelarán cualquier posible conflicto de intereses.

3. El informe de revisión del incidente a que se refiere el apartado 1 del presente artículo incluirá una revisión y un análisis del incidente de ciberseguridad significativo específico o a gran escala, incluidas las principales causas, vulnerabilidades aprovechables conocidas y conclusiones extraídas. ENISA garantizará que el informe cumple la legislación nacional o de la Unión relativa a la protección de la información sensible o clasificada. Si el Estado o Estados miembros pertinentes u otros usuarios a que se refiere el artículo 14, apartado 3, afectados por el incidente, así lo solicitan, los datos e información que figuren en el informe estarán anonimizados. No incluirá ningún dato sobre las vulnerabilidades aprovechadas activamente que permanezcan sin subsanar.

4. Cuando proceda, el informe de revisión del incidente formulará recomendaciones para mejorar la posición de la Unión en materia cibernética y podrá incluir las mejores prácticas y las conclusiones extraídas de las partes interesadas pertinentes.

5. ENISA podrá publicar una versión del informe accesible al público. Dicha versión del informe solo incluirá información pública fiable u otra información con el consentimiento de los Estados miembros afectados y, por lo que respecta a la información relativa a un usuario a que se refiere el artículo 14, apartado 3, letras b) o c), con el consentimiento de dicho usuario.

CAPÍTULO V

DISPOSICIONES FINALES

Artículo 22

Modificaciones del Reglamento (UE) 2021/694

El Reglamento (UE) 2021/694 se modifica como sigue:

1) el artículo 6 se modifica como sigue:

a) el apartado 1 se modifica como sigue:

i) se inserta la letra siguiente:

▼B

«a *bis*) apoyar el desarrollo de un Sistema Europeo de Alerta de Ciberseguridad establecido en el artículo 3 del Reglamento (UE) 2025/38 del Parlamento Europeo y del Consejo (*) (en lo sucesivo, “Sistema Europeo de Alerta de Ciberseguridad”) incluido el desarrollo, implantación y funcionamiento de centros cibernéticos nacionales y transfronterizas que contribuyan a la conciencia situacional en la Unión y a la mejora de las capacidades de inteligencia sobre ciberamenazas de la Unión;

(*) Reglamento (UE) 2025/38 del Parlamento Europeo y del Consejo, de 19 de diciembre de 2024, por el que se establecen medidas destinadas a reforzar la solidaridad y las capacidades en la Unión a fin de detectar ciberamenazas e incidentes, prepararse y responder a ellos y por el que se modifica el Reglamento (UE) 2021/694 (Reglamento de Cibersolidaridad) (DO L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).»;

ii) se añade la letra siguiente:

«g) establecer y gestionar el Mecanismo de Emergencia en materia de Ciberseguridad, establecido por el artículo 10 del Reglamento (UE) 2025/38 incluida la Reserva de Ciberseguridad de la UE, establecida por el artículo 14 de dicho Reglamento (en lo sucesivo, “Reserva de Ciberseguridad de la UE”) para ayudar a los Estados miembros a prepararse ante incidentes de ciberseguridad significativos y a gran escala, y darles respuesta, como complemento de los recursos y capacidades nacionales y otras formas de apoyo disponibles a escala de la Unión, y dar apoyo a otros usuarios en su respuesta a incidentes de ciberseguridad significativos y equivalentes a gran escala;»;

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

«2. Las acciones correspondientes al objetivo específico 3 se ejecutarán principalmente a través del Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y la Red de Centros Nacionales de Coordinación, de conformidad con el Reglamento (UE) 2021/887 del Parlamento Europeo y del Consejo (*). Sin embargo, la Reserva de Ciberseguridad de la UE, deberá ser ejecutada por la Comisión y, de conformidad con el artículo 14, apartado 6, del Reglamento (UE) 2025/38, por ENISA.

(*) Reglamento (UE) 2021/887 del Parlamento Europeo y del Consejo, de 20 de mayo de 2021, por el que se establecen el Centro Europeo de Competencia Industrial Tecnológica y de Investigación en Ciberseguridad y la Red de Centros Nacionales de Coordinación (DO L 202 de 8.6.2021, p. 1).».

▼B

2) el artículo 9 se modifica como sigue:

a) en el apartado 2, las letras b), c) y d) se sustituyen por el texto siguiente:

«b) 1 760 806 000 EUR para el objetivo específico 2 – Inteligencia artificial;

c) 1 372 020 000 EUR para el objetivo específico 3 – Ciberseguridad y confianza;

d) 482 640 000 EUR para el objetivo específico 4 – Capacidades digitales avanzadas;»;

b) se añade el apartado siguiente:

«8. Como excepción a lo dispuesto en el artículo 12, apartado 1, del Reglamento Financiero, los créditos de compromiso y de pago no utilizados para acciones emprendidas en el contexto de la ejecución de la Reserva de Ciberseguridad de la UE y las acciones que apoyen la asistencia mutua con arreglo al Reglamento 2025/38 que persigan los objetivos establecidos en el artículo 6, apartado 1, letra g), del presente Reglamento se prorrogarán automáticamente y podrán ser comprometidos y abonados hasta el 31 de diciembre del ejercicio siguiente. Deberá informarse al Parlamento y al Consejo de los créditos prorrogados de en virtud del artículo 12, apartado 6, del Reglamento Financiero.».

3) el artículo 12 se modifica como sigue:

a) se insertan los apartados siguientes:

«5 *bis)*. El apartado 5 no se aplicará, en lo que respecta a las entidades jurídicas establecidas en la Unión pero controladas desde terceros países, a ninguna acción por la que se aplique el Sistema Europeo de Alerta de Ciberseguridad cuando se cumplan las dos condiciones siguientes en relación con la acción en cuestión:

a) existe un riesgo real, teniendo en cuenta los resultados de la cartografía efectuada en virtud del artículo 9, apartado 4, del Reglamento (UE) 2025/38, de que las entidades jurídicas establecidas o que se consideren establecidas en los Estados miembros y controladas por Estados miembros o por nacionales de los Estados miembros no dispongan de las herramientas, infraestructuras o servicios necesarios y suficientes para que dicha acción contribuya adecuadamente al objetivo del Sistema Europeo de Alerta de Ciberseguridad;

b) el riesgo para la seguridad derivado de la contratación a dichas entidades jurídicas dentro del Sistema Europeo de Alerta de Ciberseguridad es proporcional a los beneficios y no socava los intereses esenciales de seguridad de la Unión y de sus Estados miembros.

▼B

5 *ter*. El apartado 5 no se aplicará, en lo que respecta a las entidades jurídicas establecidas en la Unión pero controladas desde terceros países, a las acciones de ejecución de la Reserva de Ciberseguridad de la UE, cuando se cumplan, con respecto a esas acciones, las dos condiciones siguientes:

a) existe un riesgo real, teniendo en cuenta los resultados de la cartografía con arreglo al artículo 14, apartado 6, del Reglamento (UE) 2025/38, de que las entidades jurídicas establecidas o que se consideren establecidas en los Estados miembros y controladas por los Estados miembros o por nacionales de los Estados miembros no dispongan de la tecnología, los conocimientos especializados o la capacidad necesarios y suficientes para que la Reserva de Ciberseguridad de la UE pueda funcionar adecuadamente;

b) el riesgo para la seguridad de la inclusión de dichas entidades jurídicas en la Reserva de Ciberseguridad de la UE es proporcional a los beneficios y no socava los intereses esenciales de seguridad de la Unión y de sus Estados miembros.»;

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

«6. En caso de que existan motivos de seguridad debidamente justificados, el programa de trabajo también podrá estipular que las entidades jurídicas establecidas en países asociados y las entidades jurídicas establecidas en la Unión pero controladas desde terceros países puedan optar a participar en la totalidad o en una parte de las acciones en el marco de los objetivos específicos 1 y 2 únicamente si cumplen los requisitos que han de cumplir estas entidades jurídicas para garantizar la protección de los intereses esenciales de seguridad de la Unión y los Estados miembros y para garantizar la protección de la información de los documentos clasificados. Dichos requisitos se establecerán en el programa de trabajo.

El párrafo primero del presente apartado se aplicará, en lo que respecta a las entidades jurídicas establecidas en la Unión, pero controladas desde terceros países, a las acciones contempladas en el objetivo específico 3:

a) ejecutar el Sistema Europeo de Alerta de Ciberseguridad en los casos en que sea de aplicación el apartado 5 *bis*, y

b) ejecutar la Reserva de Ciberseguridad de la UE en los casos en que sea de aplicación el apartado 5 *ter*.».

4) en el artículo 14, el apartado 2 se sustituye por el texto siguiente:

«2. El Programa podrá proporcionar financiación en cualquiera de las formas establecidas en el Reglamento Financiero, en particular mediante contratación principalmente, así como subvenciones y premios.

▼B

Cuando el logro del objetivo de una acción requiera la contratación de bienes y servicios innovadores, podrán concederse subvenciones solo a los beneficiarios que sean poderes adjudicadores o entidades adjudicadoras como se definen en las Directivas 2014/24/UE (*) y 2014/25/UE (**) del Parlamento Europeo y del Consejo.

Cuando el suministro de bienes o servicios innovadores que aún no estén disponibles sobre una base comercial a gran escala sea necesario para el logro de los objetivos de una acción, el poder adjudicador o la entidad adjudicadora podrá autorizar la adjudicación de contratos múltiples dentro del mismo procedimiento de contratación.

Por motivos de seguridad pública debidamente justificados, el poder adjudicador o la entidad adjudicadora podrá solicitar que el lugar de ejecución del contrato esté situado en territorio de la Unión.

Al ejecutar los procedimientos de contratación para la Reserva de Ciberseguridad de la UE, la Comisión y ENISA podrán actuar como central de compras para la contratación en nombre de terceros países asociados al Programa, o por cuenta de ellos, de conformidad con el artículo 10 del presente Reglamento. La Comisión y ENISA también podrán actuar como mayoristas, comprando, almacenando, revendiendo o donando suministros y servicios, incluidos los alquileres, a esos terceros países. Como excepción a lo dispuesto en el artículo 168, apartado 3, del Reglamento (UE, Euratom) 2024/2509 del Parlamento Europeo y del Consejo (***), la solicitud de un único tercer país será suficiente para otorgar un mandato a la Comisión o a ENISA para que actúen.

Al ejecutar los procedimientos de contratación pública para la Reserva de Ciberseguridad de la UE, la Comisión y ENISA podrán actuar como central de compras para la contratación en nombre de las instituciones, órganos u organismos de la Unión, o por cuenta de estos. La Comisión y ENISA también podrán actuar como mayoristas, comprando, almacenando, revendiendo o donando suministros y servicios, incluidos los alquileres, a las instituciones, órganos u organismos de la Unión. Como excepción a lo dispuesto en el artículo 168, apartado 3, del Reglamento (UE, Euratom) 2024/2509, la solicitud de una única institución, órgano u organismo de la Unión es suficiente para otorgar un mandato a la Comisión o a ENISA para que actúen.

El Programa también podrá proporcionar financiación en forma de instrumentos financieros en el marco de operaciones de financiación mixta.

(*) Directiva 2014/24/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, sobre contratación pública y por la que se deroga la Directiva 2004/18/CE (DO L 94 de 28.3.2014, p. 65).

(**) Directiva 2014/25/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, relativa a la contratación por entidades que operan en los sectores del agua, la energía, los transportes y los servicios postales y por la que se deroga la Directiva 2004/17/CE (DO L 94 de 28.3.2014, p. 243).

(***) Reglamento (UE, Euratom) 2024/2509 del Parlamento Europeo y del Consejo, de 23 de septiembre de 2024, sobre las normas financieras aplicables al presupuesto general de la Unión, (versión refundida) (DO L, 2024/2509, 26.9.2024, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).».

▼B

5) se inserta el artículo siguiente:

«Artículo 16 bis

Conflicto de normas

En el caso de las acciones de ejecución del Sistema Europeo de Alerta de Ciberseguridad, las normas aplicables serán las establecidas en los artículos 4, 5 y 9 del Reglamento UE) 2025/38. En caso de conflicto entre las disposiciones del presente Reglamento y los artículos 4, 5 y 9 del Reglamento 2025/38, estos últimos prevalecerán y se aplicarán a dichas acciones específicas.

En el caso de la Reserva de Ciberseguridad, las normas específicas para la participación de terceros países asociados al Programa se establecen en el artículo 19 del Reglamento (UE) 2025/38. En caso de conflicto entre las disposiciones del presente Reglamento y el artículo 19 del Reglamento (UE) 2025/38, este último prevalecerá y se aplicará a dichas acciones específicas.».

6) el artículo 19 se sustituye por el texto siguiente:

«Artículo 19

Subvenciones

Las subvenciones en el marco del Programa se concederán y gestionarán de conformidad con el título VIII del Reglamento Financiero y podrán cubrir hasta el 100 % de los costes admisibles, sin perjuicio del principio de cofinanciación establecido en el artículo 190 del Reglamento Financiero. Tales subvenciones se concederán y gestionarán conforme a lo especificado para cada objetivo específico.

El apoyo en forma de subvenciones podrá ser concedido directamente por el ECCC sin convocatoria de propuestas a los Estados miembros seleccionados en virtud del artículo 9 del Reglamento (UE) 2025/38, y el consorcio anfitrión a que se refiere el artículo 5 del Reglamento (UE) 2025/38, de conformidad con el artículo 195, apartado 1, letra d), del Reglamento Financiero.

El apoyo en forma de subvenciones para el Mecanismo de Emergencia en materia de Ciberseguridad, podrá ser concedido directamente por el ECCC a los Estados miembros sin convocatoria de propuestas, de conformidad con el artículo 195, apartado 1, letra d), del Reglamento Financiero.

Por lo que respecta a las acciones de apoyo para la asistencia mutua previstas en el artículo 18 del Reglamento (UE) 2025/38, el ECCC informará a la Comisión y a ENISA sobre las solicitudes de subvenciones directas de los Estados miembros sin convocatoria de propuestas.

Por lo que respecta a las acciones de apoyo para la asistencia mutua previstas en el artículo 18 del Reglamento (UE) 2025/38 y de conformidad con el artículo 193, apartado 2, párrafo segundo, letra a), del Reglamento Financiero, en casos debidamente justificados, los costes podrán considerarse subvencionables aunque se haya incurrido en ellos antes de la presentación de la solicitud de subvención.».

▼B

7) los anexos I y II se modifican de conformidad con lo dispuesto en el anexo del presente Reglamento.

Artículo 23

Ejercicio de la delegación

1. Se otorgan a la Comisión los poderes para adoptar actos delegados en las condiciones establecidas en el presente artículo.

2. Los poderes para adoptar actos delegados mencionados en el artículo 14, apartado 7, se otorgan a la Comisión por un período de cinco años a partir del 5 de febrero de 2025. La Comisión elaborará un informe sobre la delegación de poderes a más tardar nueve meses antes de que finalice el período de cinco años. La delegación de poderes se prorrogará tácitamente por períodos de idéntica duración, excepto si el Parlamento Europeo o el Consejo se oponen a dicha prórroga a más tardar tres meses antes del final de cada período.

3. La delegación de poderes mencionada en el artículo 14, apartado 7, podrá ser revocada en cualquier momento por el Parlamento Europeo o por el Consejo. La decisión de revocación pondrá término a la delegación de los poderes que en ella se especifiquen. La decisión surtirá efecto el día siguiente al de su publicación en el *Diario Oficial de la Unión Europea* o en una fecha posterior indicada en ella. No afectará a la validez de los actos delegados que ya estén en vigor.

4. Antes de la adopción de un acto delegado, la Comisión consultará a los expertos designados por cada Estado miembro de conformidad con los principios establecidos en el Acuerdo interinstitucional de 13 de abril de 2016 sobre la mejora de la legislación.

5. Tan pronto como la Comisión adopte un acto delegado lo notificará simultáneamente al Parlamento Europeo y al Consejo.

6. Los actos delegados adoptados en virtud del artículo 14, apartado 7, entrarán en vigor únicamente si, en un plazo de dos meses a partir de su notificación al Parlamento Europeo y al Consejo, ninguna de estas instituciones formula objeciones o si, antes del vencimiento de dicho plazo, ambas informan a la Comisión de que no las formularán. El plazo se prorrogará dos meses a iniciativa del Parlamento Europeo o del Consejo.

Artículo 24

Procedimiento de comité

1. La Comisión estará asistida por el Comité de Coordinación del Programa Europa Digital a que se refiere el artículo 31, apartado 1 del Reglamento (UE) 2021/694. Dicho comité será un comité en el sentido del Reglamento (UE) n.º 182/2011.

2. En los casos en que se haga referencia al presente apartado, se aplicará el artículo 5 del Reglamento (UE) n.º 182/2011.

▼B

Artículo 25

Evaluación y revisión

1. A más tardar el 5 de febrero de 2027 y, posteriormente, al menos cada cuatro años, la Comisión evaluará el funcionamiento de las medidas establecidas en el presente Reglamento y presentará un informe al Parlamento Europeo y al Consejo.

2. La evaluación a que se refiere el apartado 1 analizará, en particular:

a) el número de centros cibernéticos nacionales y de centros cibernéticos transfronterizos creados, el alcance de la información puesta en común, incluido, si es posible, los efectos en el trabajo de la red de CSIRT, y la medida en que dichos centros han contribuido a reforzar la detección y la conciencia situacional común de la Unión en materia de ciberamenazas e incidentes y a desarrollar tecnologías de vanguardia; y el uso de la financiación del Programa Europa Digital para herramientas, infraestructuras o servicios de ciberseguridad contratados conjuntamente; y, si se dispone de información, el nivel de cooperación entre los centros cibernéticos nacionales y las comunidades sectoriales e intersectoriales de entidades esenciales e importantes a que se refiere el artículo 3 de la Directiva (UE) 2022/2555;

b) el uso y la eficacia de las acciones en el marco del Mecanismo de Emergencia en materia de Ciberseguridad que apoyen la preparación, incluida la formación, la respuesta a incidentes de ciberseguridad significativos, a gran escala y equivalentes a gran escala, y la recuperación inicial con respecto de estos. incluido el uso de la financiación del Programa Europa Digital, así como las conclusiones extraídas y las recomendaciones derivadas de la ejecución del Mecanismo de Emergencia en materia de Ciberseguridad;

c) el uso y la eficacia de la Reserva de Ciberseguridad de la UE en relación con el tipo de usuarios, incluido el uso de la financiación del Programa Europa Digital, la adopción de servicios, incluido su tipo, el tiempo medio de respuesta a las solicitudes y de implantación de la Reserva de Ciberseguridad de la UE, el porcentaje de servicios convertidos en servicios de preparación relacionados con la prevención y respuesta a incidentes, así como las conclusiones extraídas y las recomendaciones derivadas de la aplicación de la Reserva de Ciberseguridad de la UE;

d) la contribución del presente Reglamento al refuerzo de la posición competitiva de la industria y los servicios en la Unión en toda la economía digital, incluidas las microempresas y las pequeñas y medianas empresas, así como las empresas emergentes, y la contribución al objetivo general de reforzar las competencias y capacidades en materia de ciberseguridad de la mano de obra.

3. A partir del informe mencionado en el apartado 1, la Comisión presentará, si procede, una propuesta legislativa al Parlamento Europeo y al Consejo para modificar el presente Reglamento.

▼B

Artículo 26

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.

▼B

ANEXO

El Reglamento (UE) 2021/694 se modifica como sigue:

1) En el anexo I, la sección «Objetivo específico 3 – Ciberseguridad y confianza» se sustituye por el texto siguiente:

«Objetivo específico 3 – Ciberseguridad y confianza

El Programa estimulará el refuerzo, la creación y la adquisición de la capacidad esencial para proteger la economía digital, la sociedad y la democracia de la Unión reforzando el potencial industrial y la competitividad en materia de ciberseguridad de la Unión, así como mejorando las capacidades de los sectores público y privado para proteger a los ciudadanos y empresas de ciberamenazas, incluido el apoyo a la aplicación de la Directiva (UE) 2016/1148.

Las acciones iniciales y, cuando proceda, posteriores, en el marco del presente objetivo, incluirán:

1. La coinversión con los Estados miembros en equipamiento avanzado de ciberseguridad, infraestructuras y conocimientos especializados que son esenciales para proteger las infraestructuras críticas y el mercado único digital en general. Dicha coinversión podría incluir inversiones en instalaciones cuánticas y recursos de datos para la ciberseguridad, conciencia situacional en el ciberespacio, incluidos los centros cibernéticos nacionales y los centros cibernéticos transfronterizos que forman el Sistema Europeo de Alerta de Ciberseguridad, así como otras herramientas que se pondrán a disposición de los sectores público y privado en toda Europa.

2. La ampliación de la capacidad tecnológica existente y la integración en red de los centros de competencia de los Estados miembros y la garantía de que esa capacidad responda a las necesidades del sector público y de la industria, en particular en el caso de los productos y servicios que refuercen la ciberseguridad y la confianza en el mercado único digital.

3. La garantía de una amplia implantación de soluciones de vanguardia eficaces en materia de ciberseguridad y confianza en los Estados miembros. Dicha implantación incluye el refuerzo de la seguridad y la protección de los productos desde su diseño hasta su comercialización.

4. Un apoyo para solucionar el déficit de capacidades en materia de ciberseguridad, teniendo en cuenta el equilibrio de género, por ejemplo, alineando los programas de capacidades en materia de ciberseguridad, adaptándolos a las necesidades sectoriales específicas y facilitando el acceso a una formación especializada específica.

5. La promoción de la solidaridad entre los Estados miembros por lo que respecta a la preparación frente a incidentes de ciberseguridad significativos y de incidentes de ciberseguridad a gran escala y la respuesta a ellos mediante la prestación de servicios de ciberseguridad a través de las fronteras, incluido el apoyo a la asistencia mutua entre las autoridades públicas y el establecimiento de una reserva de proveedores de ciberseguridad de confianza de servicios de seguridad gestionados a escala de la Unión.».

▼B

2) En el anexo II, la sección «Objetivo específico 3 – Ciberseguridad y confianza» se sustituye por el texto siguiente:

«Objetivo específico 3 – Ciberseguridad y confianza

3.1. Número de infraestructuras o herramientas de ciberseguridad, o ambas contratadas conjuntamente, también en el contexto del Sistema Europeo de Alerta de Ciberseguridad

3.2. Número de usuarios y de comunidades de usuarios con acceso a instalaciones europeas de ciberseguridad

3.3 Número de acciones de apoyo a la preparación frente a incidentes de ciberseguridad y la respuesta a ellos en el marco del Mecanismo de Emergencia en materia de Ciberseguridad».

▼C1

Se ha realizado una declaración con respecto a este acto y se puede encontrar en el DO C, C/2025/310, 15.1.2025, ELI: http://data.europa.eu/eli/C/2025/310/oj.