Consejo de la Unión Europea

Bruselas, 20 de abril de 2023
(OR. en)

8512/23

Expediente interinstitucional: 2023/0109(COD)

CYBER 92
TELECOM 108
CADREFIN 51
FIN 448
BUDGET 6
IND 181
JAI 471
MI 314
DATAPROTECT 110
RELEX 481
CODEC 662

PROPUESTA

De:	Por la secretaria general de la Comisión Europea, D.ª Martine DEPREZ, directora
Fecha de recepción:	19 de abril de 2023
A:	D.ª Thérèse BLANCHET, secretaria general del Consejo de la Unión Europea
N.° doc. Ción.:	COM(2023) 209 final
Asunto:	Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO por el que se establecen medidas destinadas a reforzar la solidaridad y las capacidades en la Unión a fin de detectar amenazas e incidentes de ciberseguridad, prepararse para ellos y responder a ellos

Adjunto se remite a las Delegaciones el documento – COM(2023) 209 final.

Adj.: COM(2023) 209 final

COMISIÓN
EUROPEA

Estrasburgo, 18.4.2023
COM(2023) 209 final

2023/0109 (COD)

Propuesta de

REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO

por el que se establecen medidas destinadas a reforzar la solidaridad y las capacidades en la Unión a fin de detectar amenazas e incidentes de ciberseguridad, prepararse para ellos y responder a ellos

EXPOSICIÓN DE MOTIVOS

1. CONTEXTO DE LA PROPUESTA

• Razones y objetivos de la propuesta

La presente exposición de motivos acompaña a la propuesta de Ley de Cibersolidaridad. La utilización de las tecnologías de la información y la comunicación, así como la dependencia de las mismas, constituyen un elemento esencial en todos los sectores de actividad económica, ya que tanto nuestras administraciones públicas como nuestras empresas y ciudadanos están más interconectados y son más interdependientes que nunca, en todos los sectores y por encima de todas las fronteras. Esta mayor implantación de las tecnologías digitales aumenta la exposición a incidentes de ciberseguridad y a sus posibles repercusiones. Al mismo tiempo, los Estados miembros se enfrentan a riesgos crecientes en materia de ciberseguridad y a un panorama general de amenazas complejo, con un claro riesgo de propagación rápida de ciberincidentes de un Estado miembro a otros.

Además, las ciberoperaciones se integran cada vez más en estrategias híbridas y de guerra, con efectos significativos en el objetivo. En particular, la agresión militar de Rusia contra Ucrania fue precedida y va acompañada de una estrategia de ciberoperaciones hostiles, lo que supone un punto de inflexión para la percepción y la evaluación de la preparación de la UE para la gestión colectiva de crisis de ciberseguridad y un llamamiento a la adopción de medidas urgentes. La amenaza de un posible incidente a gran escala que provoque perturbaciones y daños significativos en las infraestructuras críticas exige una mayor preparación a todos los niveles del ecosistema de ciberseguridad de la UE. Esa amenaza va más allá de la agresión militar de Rusia a Ucrania e incluye ciberamenazas continuas de agentes estatales y no estatales que probablemente persistirán, dada la multiplicidad de agentes alineados con Estados, criminales y *hacktivistas* implicados en las tensiones geopolíticas actuales. En los últimos años, el número de ciberataques ha aumentado significativamente, incluidos los ataques a la cadena de suministro con fines de ciberespionaje, secuestro de archivos o perturbación. En 2020, el ataque a la cadena de suministro de SolarWinds afectó a más de 18 000 organizaciones de todo el mundo, incluidas agencias gubernamentales y grandes empresas. Los incidentes de ciberseguridad graves pueden resultar demasiado perturbadores como para que uno o varios Estados miembros afectados puedan hacerles frente por sí solos. Por este motivo, se requiere una solidaridad reforzada a escala de la Unión a fin de detectar las amenazas e incidentes de ciberseguridad, prepararse para ellos y responder a ellos en mejores condiciones.

Por lo que se refiere a la detección de ciberamenazas y ciberincidentes, urge aumentar los intercambios de información y mejorar nuestras capacidades colectivas a fin de reducir considerablemente el tiempo necesario para detectar las ciberamenazas antes de que puedan causar daños y costes a gran escala[1]. Aunque muchas de las amenazas e incidentes de

[1] Según un informe de Ponemon Institute e IBM Security, el tiempo medio para detectar una violación de la seguridad en 2022 fue de 207 días, a los que se suman unos 70 días adicionales para contenerla. Al mismo tiempo, en 2022, las violaciones de la seguridad de los datos con un ciclo de vida superior a 200 días tuvieron un coste medio de 4,86 millones EUR, frente al de 3,74 millones EUR cuando se

ciberseguridad tienen una posible dimensión transfronteriza debido a la interconexión de las infraestructuras digitales, el intercambio de información pertinente entre los Estados miembros sigue siendo limitado. La creación de una red de centros de operaciones de seguridad (COS) transfronterizos para mejorar las capacidades de detección y respuesta tiene por objeto ayudar a abordar esta cuestión.

Por lo que se refiere a la preparación frente a incidentes de ciberseguridad y la respuesta a ellos, el apoyo a escala de la Unión y la solidaridad entre los Estados miembros son actualmente limitados. Las Conclusiones del Consejo de octubre de 2021 destacaron la necesidad de subsanar estas lagunas, pidiendo a la Comisión que presentara una propuesta sobre un nuevo Fondo de Respuesta de Emergencia para la Ciberseguridad[2].

El presente Reglamento también aplica la Estrategia de Ciberseguridad de la UE adoptada en diciembre de 2020[3], que anunció la creación de un escudo cibernético europeo y el refuerzo de las capacidades de detección de ciberamenazas y de intercambio de información en la Unión Europea a través de una federación de COS nacionales y transfronterizos.

El presente Reglamento se basa en los primeros pasos ya dados en estrecha colaboración con las principales partes interesadas y respaldados por el programa Europa Digital. En particular y por lo que respecta a los COS, en el marco del programa de trabajo sobre ciberseguridad 2021-2022 del programa Europa Digital, se celebró una convocatoria de manifestaciones de interés para la adquisición conjunta de herramientas e infraestructuras con el fin de establecer COS transfronterizos, y una convocatoria de subvenciones para permitir el desarrollo de capacidades de los COS que están al servicio de organizaciones públicas y privadas. Por lo que se refiere a la preparación para los incidentes y la respuesta a estos, la Comisión ha establecido un programa a corto plazo para apoyar a los Estados miembros, mediante financiación adicional asignada a la Agencia de la Unión Europea para la Ciberseguridad (ENISA), con el fin de reforzar inmediatamente la preparación y las capacidades para responder a ciberincidentes graves. Ambas acciones se han preparado en estrecha coordinación con los Estados miembros. El presente Reglamento aborda las deficiencias e integra información de dichas acciones.

Por último, la presente propuesta responde al compromiso, en consonancia con la Comunicación conjunta sobre ciberdefensa[4] adoptada el 10 de noviembre, de preparar una propuesta para una Iniciativa de Cibersolidaridad de la UE con los siguientes objetivos: reforzar las capacidades comunes de detección, conciencia situacional y respuesta de la UE con el fin de crear gradualmente una reserva de ciberseguridad a escala de la UE con servicios de proveedores privados de confianza y de apoyar las pruebas de las entidades críticas.

---

detectaron en menos de 200 días. [«Cost of a data breach 2022» (Coste de una violación de la seguridad de los datos 2022), https://www.ibm.com/reports/data-breach].

2 Conclusiones del Consejo en relación con el afianzamiento de una posición de la Unión Europea en materia cibernética, aprobadas por el Consejo en su sesión de 23 de mayo de 2022 (9364/22).

3 Comunicación conjunta al Parlamento Europeo y al Consejo, La Estrategia de Ciberseguridad de la UE para la Década Digital, JOIN(2020) 18 final.

4 Comunicación conjunta al Parlamento Europeo y al Consejo, Política de ciberdefensa de la UE, JOIN(2022) 49 final.

En este contexto, la Comisión propone la presente Ley de Cibersolidaridad para reforzar la solidaridad a escala de la Unión con el fin de mejorar la detección de las amenazas e incidentes de ciberseguridad, la preparación frente a ellos y la respuesta a ellos a través de los siguientes objetivos específicos:

- reforzar las capacidades comunes de la UE de detección y conciencia situacional de las ciberamenazas y ciberincidentes, contribuyendo así a la soberanía tecnológica europea en el ámbito de la ciberseguridad;
- afianzar la preparación de las entidades críticas en toda la UE y reforzar la solidaridad mediante el desarrollo de capacidades comunes de respuesta frente a incidentes de ciberseguridad significativos o a gran escala, en particular poniendo el apoyo a la respuesta a incidentes de ciberseguridad a disposición de terceros países asociados al programa Europa Digital;
- aumentar la resiliencia de la Unión y contribuir a una respuesta eficaz mediante la revisión y evaluación de incidentes significativos o a gran escala, incluida la extracción de conclusiones y, en su caso, la formulación de recomendaciones.

Estos objetivos se alcanzarán a través de las siguientes acciones:

- El despliegue de una infraestructura paneuropea de COS (el «Ciberescudo Europeo») para desarrollar y mejorar las capacidades comunes de detección y conciencia situacional.
- La creación de un Mecanismo de Ciberemergencia para ayudar a los Estados miembros a prepararse ante incidentes de ciberseguridad significativos y a gran escala, a responder a ellos y a recuperarse inmediatamente de ellos. El apoyo a la respuesta a incidentes también se pondrá a disposición de las instituciones, órganos y organismos de la Unión.
- El establecimiento de un Mecanismo Europeo de Revisión de Incidentes de Ciberseguridad para examinar y evaluar incidentes significativos o a gran escala.

El Ciberescudo Europeo y el Mecanismo de Ciberemergencia recibirán financiación del programa Europa Digital, que el presente instrumento legislativo modificará para establecer las acciones mencionadas, proporcionar apoyo financiero para su ejecución y aclarar las condiciones necesarias para recibir la ayuda financiera.

• Coherencia con las disposiciones existentes en la misma política sectorial

El marco de la UE comprende varios actos legislativos ya vigentes o propuestos a escala de la Unión para reducir las vulnerabilidades, aumentar la resiliencia de las entidades críticas frente a los riesgos de ciberseguridad y apoyar la gestión coordinada de los incidentes y crisis de ciberseguridad a gran escala, en particular la Directiva relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la

Unión (SRI 2)[5], el Reglamento sobre la Ciberseguridad[6], la Directiva relativa a los ataques contra los sistemas de información[7] y la Recomendación (UE) 2017/1584 de la Comisión sobre la respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala[8].

Las acciones propuestas en el marco de la Ley de Cibersolidaridad abarcan la conciencia situacional, el intercambio de información y el apoyo a la preparación ante ciberincidentes y la respuesta a ellos. Estas acciones son coherentes con los objetivos del marco regulador vigente a escala de la Unión y los respaldan, en particular en virtud de la Directiva (UE) 2022/2555 (en lo sucesivo, «Directiva SRI 2»). La Ley de Cibersolidaridad se basará especialmente en los marcos existentes de cooperación operativa y gestión de crisis en materia de ciberseguridad y apoyará dichos marcos, en particular la red europea de organizaciones de enlace para las crisis de ciberseguridad (EU-CyCLONe) y la red de equipos de respuesta a incidentes de seguridad informática (CSIRT).

Las plataformas de COS transfronterizos deben constituir una nueva capacidad que sea complementaria de la red de CSIRT, mediante la puesta en común y el intercambio de datos sobre las amenazas a la ciberseguridad para las entidades públicas y privadas, aumentando el valor de dichos datos mediante el análisis de expertos y las herramientas más avanzadas, y contribuyendo al desarrollo de las capacidades y la soberanía tecnológica de la Unión.

Por último, la presente propuesta es coherente con la Recomendación del Consejo sobre un enfoque coordinado a escala de la Unión para reforzar la resiliencia de las infraestructuras críticas[9], que invita a los Estados miembros a tomar medidas urgentes y eficaces y a cooperar de manera leal, eficiente, solidaria y coordinada entre sí, con la Comisión y otras autoridades públicas pertinentes, así como con las entidades afectadas, a fin de aumentar la resiliencia de las infraestructuras críticas utilizadas para prestar servicios esenciales en el mercado interior.

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

[5] 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).

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

[7] Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo.

[8] Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE) 2019/1020, COM(2022) 454 final.

[9] Recomendación del Consejo, de 8 de diciembre de 2022, sobre un enfoque coordinado en toda la Unión para reforzar la resiliencia de las infraestructuras críticas (Texto pertinente a efectos del EEE) 2023/C 20/01.

La propuesta es coherente con otros mecanismos y protocolos de emergencia en caso de crisis, como el Dispositivo de la UE de Respuesta Política Integrada a las Crisis (Dispositivo RPIC). La Ley de Cibersolidaridad completará estos marcos y protocolos de gestión de crisis proporcionando apoyo específico para la preparación ante incidentes de ciberseguridad y la respuesta a ellos. La propuesta también será coherente con la acción exterior de la UE en respuesta a incidentes a gran escala en el marco de la política exterior y de seguridad común (PESC), en particular a través del conjunto de instrumentos de ciberdiplomacia de la UE. La propuesta complementará las acciones ejecutadas en el contexto del artículo 42, apartado 7, del Tratado de la Unión Europea o en las situaciones definidas en el artículo 222 del Tratado de Funcionamiento de la Unión Europea.

También complementa el Mecanismo de Protección Civil de la Unión (UCPM, por sus siglas en inglés)[10], creado en diciembre de 2013 y completado con un nuevo reglamento adoptado en mayo de 2021[11], que refuerza los pilares de prevención, preparación y respuesta del UCPM, dota a la UE de capacidades adicionales para responder a nuevos riesgos en Europa y en el mundo e impulsa la reserva rescEU.

2. BASE JURÍDICA, SUBSIDIARIEDAD Y PROPORCIONALIDAD

• Base jurídica

La base jurídica de esta propuesta la constituyen el artículo 173, apartado 3, y el artículo 322, apartado 1, letra a), del Tratado de Funcionamiento de la Unión Europea (TFUE). El artículo 173 del TFUE establece que la Unión y los Estados miembros deben asegurar la existencia de las condiciones necesarias para la competitividad de la industria de la Unión. El presente Reglamento tiene por objeto afianzar la posición competitiva de la industria y los sectores de servicios en Europa en el conjunto de la economía digitalizada y apoyar su transformación digital reforzando el nivel de ciberseguridad en el mercado único digital. Pretende, en particular, aumentar la resiliencia de los ciudadanos, las empresas y las entidades que operan en sectores críticos y muy críticos frente a las crecientes amenazas a la ciberseguridad, que pueden tener repercusiones sociales y económicas devastadoras.

La propuesta se basa también en el artículo 322, apartado 1, letra a), del TFUE porque contiene normas específicas de prórroga que establecen excepciones al principio de anualidad establecido en el Reglamento (UE, Euratom) 2018/1046 del Parlamento Europeo y del Consejo (el «Reglamento Financiero»)[12]. A efectos de una buena gestión financiera y teniendo en cuenta el carácter impredecible, excepcional y específico del panorama de la

---

10 Decisión n.º 1313/2013/UE del Parlamento Europeo y del Consejo, de 17 de diciembre de 2013, relativa a un Mecanismo de Protección Civil de la Unión (Texto pertinente a efectos del EEE).

11 Reglamento (UE) 2021/836 del Parlamento Europeo y del Consejo, de 20 de mayo de 2021, por el que se modifica la Decisión n.º 1313/2013/UE relativa a un Mecanismo de Protección Civil de la Unión (Texto pertinente a efectos del EEE).

12 Reglamento (UE, Euratom) 2018/1046 del Parlamento Europeo y del Consejo, de 18 de julio de 2018, sobre las normas financieras aplicables al presupuesto general de la Unión (DO L 193 de 30.7.2018, p. 1).

ciberseguridad y las ciberamenazas, el Mecanismo de Emergencia en materia de Ciberseguridad debe beneficiarse de un cierto grado de flexibilidad en relación con la gestión presupuestaria, permitiéndose, en particular, que los créditos de compromiso y de pago no utilizados para acciones que persigan los objetivos establecidos en el Reglamento se prorroguen automáticamente al ejercicio siguiente. Dado que esta nueva norma plantea problemas en relación con el Reglamento Financiero, esta cuestión podría abordarse en el contexto de las negociaciones en curso sobre la refundición del Reglamento Financiero.

- **Subsidiariedad (en el caso de competencia no exclusiva)**

El marcado carácter transfronterizo de las amenazas a la ciberseguridad y el creciente número de riesgos e incidentes, que tienen efectos expansivos que traspasan fronteras, sectores y productos, hacen que los objetivos de la intervención actual no puedan ser alcanzados eficazmente por los Estados miembros por sí solos y requieran la acción común y la solidaridad a escala de la Unión.

La experiencia de la lucha contra las ciberamenazas derivadas de la guerra contra Ucrania, junto con las conclusiones extraídas de un ejercicio de ciberseguridad realizado bajo la Presidencia francesa (EU CyCLES), puso de manifiesto que deben desarrollarse mecanismos concretos de apoyo mutuo, en particular la cooperación con el sector privado, para lograr la solidaridad a escala de la UE. En este contexto, en las Conclusiones del Consejo de 23 de mayo de 2022 sobre el afianzamiento de la posición de la Unión Europea en materia cibernética se insta a la Comisión a que presente una propuesta sobre un nuevo Fondo de Respuesta a Emergencias en materia de Ciberseguridad.

El apoyo y las acciones a escala de la Unión para detectar mejor las amenazas a la ciberseguridad y aumentar las capacidades de preparación y respuesta aportan valor añadido, ya que evitan la duplicación de esfuerzos en la Unión y los Estados miembros. Ello daría lugar a una mejor explotación de los activos existentes y a una mayor coordinación e intercambio de información sobre las conclusiones extraídas. El Mecanismo de Ciberemergencia también prevé prestar apoyo a terceros países asociados al programa Europa Digital a través de la Reserva de Ciberseguridad de la UE.

El apoyo prestado a través de las diversas iniciativas que se establezcan y financien a escala de la Unión complementará y no duplicará las capacidades nacionales en materia de detección, conciencia situacional, preparación y respuesta ante ciberamenazas y ciberincidentes.

- **Proporcionalidad**

Las acciones no van más allá de lo necesario para alcanzar los objetivos generales y específicos del Reglamento. Las acciones del presente Reglamento no afectan a la responsabilidad de los Estados miembros en materia de seguridad nacional y seguridad pública y de prevención, investigación, detección y enjuiciamiento de infracciones penales. Tampoco afectan a las obligaciones jurídicas de las entidades que operan en sectores críticos y muy críticos de adoptar medidas de ciberseguridad, de conformidad con la Directiva SRI 2.

Las acciones cubiertas por el presente Reglamento complementan dichos esfuerzos y medidas, ya que apoyan la creación de infraestructuras para mejorar la detección y el análisis de las amenazas y prestan apoyo a las acciones de preparación y respuesta en caso de incidentes significativos o a gran escala.

- **Elección del instrumento**

La propuesta adopta la forma de un Reglamento del Parlamento Europeo y del Consejo. Este es el instrumento jurídico más adecuado, ya que solo un Reglamento, con sus disposiciones jurídicas directamente aplicables, puede aportar el grado de uniformidad necesario para la creación y el funcionamiento de un Ciberescudo Europeo y de un Mecanismo de Ciberemergencia, al proporcionar el apoyo del programa Europa Digital para su establecimiento, así como condiciones claras para su utilización y dotación.

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

- **Consultas con las partes interesadas**

Las acciones del presente Reglamento contarán con el apoyo del programa Europa Digital, que fue objeto de una amplia consulta. Además, se basarán en los primeros pasos que se han preparado en estrecha cooperación con las principales partes interesadas. Por lo que se refiere a los COS, la Comisión ha elaborado un documento de reflexión sobre el desarrollo de plataformas de COS transfronterizos y una convocatoria de manifestaciones de interés en estrecha cooperación con los Estados miembros en el marco del Centro Europeo de Competencia en Ciberseguridad (ECCC, por sus siglas en inglés). En este contexto, se llevó a cabo una encuesta sobre las capacidades de los COS nacionales y se debatieron enfoques comunes y requisitos técnicos en el grupo de trabajo técnico del ECCC que reúne a representantes de los Estados miembros. Además, se mantuvieron intercambios con la industria, en particular a través del grupo de expertos sobre COS creado por la ENISA y la Organización Europea de Ciberseguridad (ECSO, por sus siglas en inglés).

En segundo lugar, por lo que se refiere a la preparación y la respuesta a los incidentes, la Comisión ha establecido un programa a corto plazo para apoyar a los Estados miembros mediante financiación adicional asignada a la ENISA con cargo al programa Europa Digital, con el fin de reforzar inmediatamente la preparación y las capacidades para responder a ciberincidentes graves. Las observaciones recabadas de los Estados miembros y la industria durante la ejecución de este programa a corto plazo ya están proporcionando información valiosa que se ha tenido en cuenta en la preparación de la propuesta de Reglamento para abordar las deficiencias detectadas. Se trata de un primer paso en consonancia con las Conclusiones del Consejo sobre la posición cibernética, en las que se pide a la Comisión que presente una propuesta relativa a un nuevo Fondo de Respuesta a Emergencias en materia de Ciberseguridad.

Además, el 16 de febrero de 2023 se celebró un taller con expertos de los Estados miembros sobre el Mecanismo de Ciberemergencia, sobre la base de un documento de reflexión. Todos los Estados miembros participaron en este taller y once de ellos aportaron contribuciones adicionales por escrito.

- **Evaluación de impacto**

Dada la urgencia de la propuesta, no se ha llevado a cabo ninguna evaluación de impacto. Las acciones del presente Reglamento contarán con el apoyo del programa Europa Digital y estarán en consonancia con las establecidas en dicho Reglamento, que fue objeto de una evaluación de impacto específica. El presente Reglamento no tendrá repercusiones administrativas o medioambientales significativas más allá de las ya evaluadas en la evaluación de impacto del Reglamento del programa Europa Digital.

Es más, la propuesta se basa en las primeras acciones desarrolladas en estrecha colaboración con las principales partes interesadas, como se ha indicado anteriormente, y responde a la petición de los Estados miembros de que la Comisión presente una propuesta sobre un nuevo Fondo de Respuesta de Emergencia para la Ciberseguridad antes de finales del segundo trimestre de 2022.

Concretamente, por lo que respecta a la conciencia situacional y la detección en el contexto del Ciberescudo Europeo, en el marco del programa de trabajo sobre ciberseguridad 2021-2022 del programa Europa Digital, se celebró una convocatoria de manifestaciones de interés para la adquisición conjunta de herramientas e infraestructuras con el fin de establecer COS transfronterizos, y una convocatoria de subvenciones para permitir el desarrollo de capacidades de los COS que están al servicio de organizaciones públicas y privadas.

En el ámbito de la preparación y la respuesta a los incidentes, como se ha mencionado anteriormente, la Comisión ha establecido un programa a corto plazo para apoyar a los Estados miembros del programa Europa Digital, que está siendo ejecutado por la ENISA. Los servicios cubiertos incluyen actividades de preparación, como pruebas de penetración de entidades críticas con el fin de detectar las vulnerabilidades. El programa también refuerza las posibilidades de asistir a los Estados miembros en caso de un incidente grave que afecte a entidades críticas. La ejecución de este programa a corto plazo por parte de la ENISA está en curso y ya ha proporcionado información pertinente que se ha tenido en cuenta en la preparación del presente Reglamento.

- **Derechos fundamentales**

Al contribuir a la seguridad de la información digital, la presente propuesta ayudará a proteger el derecho a la libertad y a la seguridad, de conformidad con el artículo 6 de la Carta de los Derechos Fundamentales de la UE, y el derecho al respeto de la vida privada y familiar, de conformidad con el artículo 7 de la Carta de los Derechos Fundamentales de la UE. Al proteger a las empresas de ciberataques económicamente perjudiciales, la propuesta contribuirá asimismo a la libertad de empresa, de conformidad con el artículo 16 de la Carta

de los Derechos Fundamentales de la UE, y al derecho a la propiedad, de conformidad con el artículo 17 de la Carta de los Derechos Fundamentales de la UE. Por último, al proteger la integridad de las infraestructuras críticas frente a los ciberataques, la propuesta contribuirá al derecho a la atención sanitaria, de conformidad con el artículo 35 de la Carta de los Derechos Fundamentales de la UE, y al derecho de acceso a los servicios de interés económico general, de conformidad con el artículo 36 de la Carta de los Derechos Fundamentales de la UE.

4. REPERCUSIONES PRESUPUESTARIAS

Las acciones del presente Reglamento recibirán apoyo financiero en el marco del objetivo estratégico «Ciberseguridad» del programa Europa Digital.

El presupuesto total contempla un incremento de 100 millones EUR que el presente Reglamento propone reasignar de otros objetivos estratégicos del programa Europa Digital. Esto elevará el nuevo importe total disponible para acciones de ciberseguridad en el marco del programa Europa Digital a 842,8 millones EUR.

Una parte de los 100 millones EUR adicionales reforzará el presupuesto gestionado por el ECCC para ejecutar acciones relacionadas con los COS y la preparación como parte de su programa o programas de trabajo. Además, la financiación adicional servirá para apoyar la creación de la Reserva de Ciberseguridad de la UE.

Complementa el presupuesto ya previsto para acciones similares en el programa de trabajo general del programa Europa Digital y en el programa de trabajo centrado en la ciberseguridad de Europa Digital para el período 2023-2027, lo que podría suponer un importe total de 551 millones para el período 2023-2027, si bien ya se dedicaron 115 millones a proyectos piloto para el período 2021-2022. Si se incluyen las contribuciones de los Estados miembros, el presupuesto total podría ascender a 1 109 millones EUR.

La ficha de financiación legislativa que acompaña a la presente propuesta ofrece un resumen de los costes que todo ello supone.

5. OTROS ELEMENTOS

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

La Comisión hará un seguimiento de la ejecución, la aplicación y el cumplimiento de estas nuevas disposiciones con el fin de evaluar su eficacia. La Comisión presentará un informe sobre la evaluación y examen del presente Reglamento al Parlamento Europeo y al Consejo a más tardar cuatro años después de su fecha de aplicación.

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

Objetivos generales, objeto y definiciones (capítulo I)

El capítulo I presenta los objetivos del Reglamento, a saber: reforzar la solidaridad a escala de la Unión con el fin de mejorar la detección de las amenazas e incidentes de ciberseguridad, la preparación frente a ellos y la respuesta a ellos y, en particular, reforzar la capacidad común de la Unión de detección y conciencia situacional de ciberamenazas y ciberincidentes, consolidar la preparación de las entidades que operan en sectores críticos y muy críticos en toda la Unión y afianzar la solidaridad mediante el desarrollo de capacidades comunes de respuesta frente a incidentes de ciberseguridad significativos o a gran escala, y mejorar la resiliencia de la Unión mediante la revisión y evaluación de los incidentes significativos o a gran escala. Este capítulo también expone las acciones a través de las cuales se alcanzarán estos objetivos: el despliegue de un Ciberescudo Europeo, la creación de un Mecanismo de Ciberemergencia y el establecimiento de un Mecanismo de Revisión de Incidentes de Ciberseguridad. Además, establece las definiciones utilizadas en todo el instrumento.

El Ciberescudo Europeo (capítulo II)

El capítulo II establece el Ciberescudo Europeo y expone sus diversos elementos y las condiciones de participación. En primer lugar, anuncia el objetivo general del Ciberescudo Europeo, a saber, desarrollar capacidades avanzadas para que la Unión detecte y analice las ciberamenazas y los ciberincidentes en la Unión y trate los datos relativos ellos, así como los objetivos operativos específicos. Especifica que la financiación de la Unión para el Ciberescudo Europeo debe ejecutarse de conformidad con el Reglamento sobre el programa Europa Digital.

Además, en este capítulo se describe el tipo de entidades que han de integrar el Ciberescudo Europeo. El escudo debe estar compuesto por todos los centros de operaciones de seguridad nacionales (COS nacionales) y los centros de operaciones de seguridad transfronterizos (COS transfronterizos). Cada Estado miembro participante debe designar un COS nacional, que actúe como punto de referencia y pasarela a otras organizaciones públicas y privadas a nivel nacional para recopilar y analizar información sobre amenazas e incidentes de ciberseguridad y contribuya a un COS transfronterizo. Tras una convocatoria de manifestaciones de interés, el ECCC podrá seleccionar un COS nacional que participe en una adquisición conjunta de herramientas e infraestructuras con el CECC y reciba una subvención para la gestión de las herramientas e infraestructuras. Si un COS nacional recibe apoyo de la Unión, debe comprometerse a solicitar su participación en un COS transfronterizo en un plazo de dos años.

Los COS transfronterizos deben estar compuestos por un consorcio de al menos tres Estados miembros, representados por COS nacionales, que se comprometan a colaborar para coordinar sus actividades de ciberdetección y seguimiento de amenazas. Tras una convocatoria inicial de manifestaciones de interés, el ECCC podrá seleccionar un consorcio anfitrión que participe en una adquisición conjunta de herramientas e infraestructuras con el ECCC y reciba una subvención a fin de gestionar las herramientas e infraestructuras. Los miembros del consorcio anfitrión deben celebrar un acuerdo de consorcio escrito en el que se establezcan sus disposiciones internas. A continuación, este capítulo detalla los requisitos del intercambio de información entre los participantes de un COS transfronterizo y entre un COS transfronterizo y otros COS transfronterizos, así como con las entidades pertinentes de la UE. Los COS

nacionales que participen en un COS transfronterizo deben intercambiar la información pertinente relacionada con las ciberamenazas, así como los detalles, y deben definirse en un acuerdo de consorcio el compromiso de intercambiar una cantidad significativa de datos y las condiciones de dicho intercambio. Los COS transfronterizos han de garantizar un alto nivel de interoperabilidad entre ellos. Los COS transfronterizos también deben celebrar acuerdos de cooperación con otros COS transfronterizos en los que se especifiquen los principios del intercambio de información. Cuando los COS transfronterizos obtengan información relativa a un incidente de ciberseguridad a gran escala potencial o en curso, han de facilitar la información pertinente a EU-CyCLONe, a la red de CSIRT y a la Comisión, teniendo en cuenta sus respectivas funciones de gestión de crisis de conformidad con la Directiva (UE) 2022/2555. El capítulo II concluye especificando las condiciones de seguridad para participar en el Ciberescudo Europeo.

Mecanismo de Emergencia en materia de Ciberseguridad (capítulo III)

El capítulo III establece el Mecanismo de Ciberemergencia para mejorar la resiliencia de la Unión frente a las principales amenazas para la ciberseguridad y prepararse y mitigar, en un espíritu de solidaridad, el impacto a corto plazo de los incidentes o crisis de ciberseguridad significativos y a gran escala. Las acciones de ejecución del Mecanismo de Ciberemergencia contarán con el apoyo financiero del programa Europa Digital. El Mecanismo organiza acciones destinadas a apoyar la preparación, incluidas pruebas coordinadas de entidades que operan en sectores muy críticos, la respuesta a incidentes de ciberseguridad significativos o a gran escala y la recuperación inmediata de ellos o a mitigar las ciberamenazas significativas, así como acciones de asistencia mutua.

Entre las acciones de preparación del Mecanismo de Ciberemergencia se incluyen las pruebas coordinadas de preparación de las entidades que operan en sectores muy críticos. La Comisión, previa consulta a la ENISA y al Grupo de Cooperación SRI, debe determinar periódicamente entre los sectores de alta criticidad enumerados en el anexo I de la Directiva (UE) 2022/2555 los sectores o subsectores pertinentes cuyas entidades puedan ser objeto de las pruebas coordinadas de preparación a escala de la UE.

A efectos de la ejecución de las acciones propuestas en respuesta a incidentes, el presente Reglamento establece una Reserva de Ciberseguridad de la UE, consistente en servicios de respuesta a incidentes prestados por proveedores de confianza, seleccionados de conformidad con los criterios establecidos en el presente Reglamento. Entre los usuarios de los servicios de la Reserva de Ciberseguridad de la UE han de incluirse las autoridades de gestión de cibercrisis de los Estados miembros, los CSIRT y las instituciones, órganos y organismos de la Unión. La Comisión tendrá la responsabilidad general de la ejecución de la Reserva de Ciberseguridad de la UE y podrá encomendar, total o parcialmente, a la ENISA su funcionamiento y administración.

Para recibir apoyo de la Reserva de Ciberseguridad de la UE, los usuarios deben tomar sus propias medidas para mitigar los efectos del incidente para el que se solicite el apoyo. Las solicitudes de apoyo de la Reserva de Ciberseguridad de la UE deben incluir la información

pertinente necesaria sobre el incidente y las medidas ya tomadas por los usuarios. El capítulo describe también las modalidades de aplicación, incluida la evaluación de las solicitudes presentadas a la Reserva de Ciberseguridad de la UE.

El Reglamento establece asimismo los principios de contratación pública y los criterios de selección relativos a los proveedores de confianza de la Reserva de Ciberseguridad de la UE.

Los terceros países podrán solicitar el apoyo de la Reserva de Ciberseguridad de la UE cuando así lo prevean los acuerdos de asociación celebrados en relación con su participación en el programa Europa Digital. En este capítulo se describen otras condiciones y modalidades de dicha participación.

Mecanismo de Revisión de Incidentes de Ciberseguridad (capítulo IV)

A petición de la Comisión, de EU-CyCLONe o de la red de CSIRT, la ENISA debe revisar y evaluar las amenazas, vulnerabilidades y medidas de mitigación con respecto a un incidente específico de ciberseguridad significativo o a gran escala. La ENISA debe presentar la revisión y evaluación en forma de informe de revisión del incidente a la red de CSIRT, a EU-CyCLONe y a la Comisión para ayudarlos en el desempeño de sus funciones. Cuando el incidente se refiera a un tercer país, la Comisión debe dar a conocer el informe al Alto Representante. El informe debe incluir las conclusiones extraídas y, cuando proceda, recomendaciones para mejorar la posición cibernética de la Unión.

Disposiciones finales (capítulo V)

El capítulo V recoge modificaciones del Reglamento sobre el programa Europa Digital y la obligación de la Comisión de elaborar informes periódicos para el Parlamento Europeo y el Consejo sobre la evaluación y revisión del Reglamento. La Comisión está facultada para adoptar tales actos de ejecución de conformidad con el procedimiento de examen a que se refiere el artículo 21, a fin de: especificar las condiciones de interoperabilidad entre los COS transfronterizos; determinar las disposiciones de procedimiento para el intercambio de información relacionada con un incidente de ciberseguridad a gran escala potencial o en curso entre los COS transfronterizos y las entidades de la Unión; establecer requisitos técnicos para garantizar un elevado nivel de seguridad de los datos y de seguridad física de las infraestructuras y proteger los intereses de seguridad de la Unión cuando se intercambie información con entidades que no sean organismos públicos de los Estados miembros; especificar los tipos y el número de servicios de respuesta necesarios para la Reserva de Ciberseguridad de la UE; y especificar en mayor medida las disposiciones detalladas para la asignación de los servicios de apoyo de la Reserva de Ciberseguridad de la UE.

2023/0109 (COD)

Propuesta de

REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO

por el que se establecen medidas destinadas a reforzar la solidaridad y las capacidades en la Unión a fin de detectar amenazas e incidentes de ciberseguridad, prepararse para ellos y responder a ellos

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular su artículo 173, apartado 3, y su artículo 322, apartado 1, letra a),

Vista la propuesta de la Comisión Europea,

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

Visto el dictamen del Tribunal de Cuentas[1],

Visto el dictamen del Comité Económico y Social Europeo[2],

Visto el dictamen del Comité de las Regiones[3],

De conformidad con el procedimiento legislativo ordinario,

Considerando lo siguiente:

1) La utilización y dependencia de las tecnologías de la información y la comunicación constituyen un elemento esencial en todos los sectores de actividad económica, ya que tanto nuestras administraciones públicas como nuestras empresas y ciudadanos están más interconectados y son más interdependientes que nunca, en todos los sectores y por encima de todas las fronteras.

2) La magnitud, la frecuencia y los efectos de los incidentes de ciberseguridad están aumentando, incluidos los ataques a la cadena de suministro con fines de ciberespionaje, secuestro de archivos o perturbación. Representan una grave amenaza para el funcionamiento de las redes y los sistemas de información. En vista de la rápida evolución del panorama de amenazas, la amenaza de un posible incidente a gran escala que provoque perturbaciones y daños significativos en las infraestructuras críticas exige una mayor preparación a todos los niveles del marco de ciberseguridad de la UE. Esa amenaza va más allá de la agresión militar de Rusia a Ucrania y probablemente persistirá, dada la multiplicidad de agentes estatales, criminales y *hacktivistas* implicados en las tensiones geopolíticas actuales. Tales incidentes pueden obstaculizar la prestación de servicios públicos y el desarrollo de actividades económicas, incluso en sectores críticos o muy críticos, generar pérdidas económicas sustanciales, socavar la confianza de los usuarios, causar graves daños a la economía de la Unión e incluso suponer una amenaza para la salud o la vida. Además, los incidentes de ciberseguridad son impredecibles, ya que a menudo surgen y

[1] DO C […] de […], p. […].
[2] DO C […] de […], p. […].
[3] DO C […] de […], p. […].

evolucionan en períodos de tiempo muy breves, no se limitan a ninguna zona geográfica específica y se producen simultáneamente o se propagan de forma instantánea por muchos países.

3) Es necesario afianzar la posición competitiva de los sectores de la industria y los servicios de la Unión en el conjunto de la economía digitalizada y apoyar su transformación digital reforzando el nivel de ciberseguridad en el mercado único digital. Tal como se recomendó en tres propuestas distintas de la Conferencia sobre el Futuro de Europa[4], es necesario aumentar la resiliencia de los ciudadanos, las empresas y las entidades que gestionan infraestructuras críticas frente a las crecientes amenazas a la ciberseguridad, que pueden tener repercusiones sociales y económicas devastadoras. Por lo tanto, es necesaria la inversión en infraestructuras y servicios que apoyen una detección de las amenazas e incidentes de ciberseguridad y una respuesta a ellos más rápidas, y los Estados miembros precisan de asistencia para prepararse mejor y responder a los incidentes de ciberseguridad significativos y a gran escala. La Unión también debe aumentar sus capacidades en estos ámbitos, en particular en lo que se refiere a la recopilación y el análisis de datos sobre amenazas e incidentes de ciberseguridad.

4) La Unión ya ha tomado una serie de medidas para reducir las vulnerabilidades y aumentar la resiliencia de las infraestructuras y entidades críticas frente a los riesgos de ciberseguridad, en particular la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo[5], la Recomendación (UE) 2017/1584 de la Comisión[6], la Directiva 2013/40/UE del Parlamento Europeo y del Consejo[7] y el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo[8]. Además, la Recomendación del Consejo sobre un enfoque coordinado a escala de la Unión para reforzar la resiliencia de las infraestructuras críticas invita a los Estados miembros a tomar medidas urgentes y eficaces y a cooperar de manera leal, eficiente, solidaria y coordinada entre sí, con la Comisión y otras autoridades públicas pertinentes, así como con las entidades afectadas, a fin de aumentar la resiliencia de las infraestructuras críticas utilizadas para prestar servicios esenciales en el mercado interior.

5) Los crecientes riesgos de ciberseguridad y un panorama general de amenazas complejo, con un claro riesgo de propagación rápida de ciberincidentes de un Estado miembro a otros y de un tercer país a la Unión, requieren una solidaridad reforzada a escala de la Unión para mejorar la detección de las amenazas e incidentes de ciberseguridad, la preparación frente a ellos y la respuesta a ellos. Los Estados miembros también han invitado a la Comisión a que presente una propuesta sobre un

---

4 https://futureu.europa.eu/es/

5 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 (DO L 333 de 27.12.2022).

6 Recomendación (UE) 2017/1584 de la Comisión, de 13 de septiembre de 2017, sobre la respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala (DO L 239 de 19.9.2017, p. 36).

7 Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo (DO L 218 de 14.8.2013, p. 8).

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).

nuevo Fondo de Respuesta de Emergencia para la Ciberseguridad en las Conclusiones del Consejo sobre la posición cibernética de la UE[9].

6) La Comunicación conjunta sobre la política de ciberdefensa de la UE[10], adoptada el 10 de noviembre de 2022, anunció una Iniciativa de Cibersolidaridad de la UE con los siguientes objetivos: refuerzo de las capacidades comunes de detección, conciencia situacional y respuesta de la UE mediante la promoción del despliegue de una infraestructura de la UE de centros de operaciones de seguridad («COS»), el apoyo a la creación gradual de una reserva de ciberseguridad a escala de la UE con servicios de proveedores privados de confianza y la realización de pruebas de entidades críticas para detectar posibles vulnerabilidades basadas en evaluaciones de riesgos de la UE.

7) Es necesario reforzar la capacidad de detección y conciencia situacional de las ciberamenazas y ciberincidentes en toda la Unión y afianzar la solidaridad mejorando la preparación y las capacidades de los Estados miembros y de la Unión para responder a incidentes de ciberseguridad significativos y a gran escala. Procede, por lo tanto, desplegar una infraestructura paneuropea de COS (el Ciberescudo Europeo) para desarrollar y mejorar las capacidades comunes de detección y conciencia situacional; debe crearse un Mecanismo de Ciberemergencia para ayudar a los Estados miembros a prepararse, responder a incidentes de ciberseguridad significativos y a gran escala y recuperarse inmediatamente de ellos; conviene establecer un Mecanismo de Revisión de Incidentes de Ciberseguridad para revisar y evaluar incidentes específicos significativos o a gran escala. Estas acciones deben entenderse sin perjuicio de lo dispuesto en los artículos 107 y 108 del Tratado de Funcionamiento de la Unión Europea (TFUE).

8) Para alcanzar estos objetivos, procede también modificar el Reglamento (UE) 2021/694 del Parlamento Europeo y del Consejo[11] en determinados ámbitos. En particular, el presente Reglamento debe modificar el Reglamento (UE) 2021/694 en lo que respecta a la adición de nuevos objetivos operativos relacionados con el Ciberescudo Europeo y el Mecanismo de Ciberemergencia en el marco del objetivo específico 3 del programa Europa Digital, cuya finalidad es garantizar la resiliencia, la integridad y la fiabilidad del mercado único digital, reforzar las capacidades para seguir los ciberataques y amenazas y responder a ellos, y reforzar la cooperación transfronteriza en materia de ciberseguridad. Esto ha de completarse con el establecimiento de las condiciones específicas en las que pueda concederse ayuda financiera para dichas acciones y la definición de los mecanismos de gobernanza y coordinación necesarios para alcanzar los objetivos previstos. Otras modificaciones del Reglamento (UE) 2021/694 deben incluir descripciones de las acciones propuestas en el marco de los nuevos objetivos operativos, así como indicadores mensurables para seguir la aplicación de estos nuevos objetivos operativos.

9) La financiación de las acciones en virtud del presente Reglamento debe estar prevista en el Reglamento (UE) 2021/694, que debe seguir siendo el acto de base pertinente para estas acciones, consagradas en el objetivo específico 3 del programa Europa

---

9 Conclusiones del Consejo en relación con el afianzamiento de una posición de la Unión Europea en materia cibernética, aprobadas por el Consejo en su sesión de 23 de mayo de 2022 (9364/22).

10 Comunicación conjunta al Parlamento Europeo y al Consejo, Política de ciberdefensa de la UE, JOIN(2022) 49 final.

11 Reglamento (UE) 2021/694 del Parlamento Europeo y del Consejo, de 29 de abril de 2021, por el que se establece el Programa Europa Digital y por el que se deroga la Decisión (UE) 2015/2240 (DO L 166 de 11.5.2021, p. 1).

Digital. Deben establecerse las condiciones específicas de participación en relación con cada acción, de conformidad con las disposiciones aplicables del Reglamento (UE) 2021/694.

10) Son de aplicación al presente Reglamento las normas financieras horizontales adoptadas por el Parlamento Europeo y el Consejo en virtud del artículo 322 del TFUE. Dichas normas se establecen en el Reglamento Financiero y determinan, en particular, el procedimiento de elaboración y ejecución del presupuesto de la Unión, y prevén el control de la responsabilidad de los agentes financieros. Las normas adoptadas sobre la base del artículo 322 del TFUE también incluyen un régimen general de condicionalidad para la protección del presupuesto de la Unión tal como establece el Reglamento (UE, Euratom) 2020/2092 del Parlamento Europeo y del Consejo.

11) A efectos de una buena gestión financiera, deben establecerse normas específicas para la prórroga de los créditos de compromiso y de pago no utilizados. Al tiempo que se respeta el principio de que el presupuesto de la Unión se establece anualmente, el presente Reglamento, debido al carácter impredecible, excepcional y específico del panorama de la ciberseguridad, debe prever la posibilidad de prorrogar los fondos no utilizados más allá de los establecidos en el Reglamento Financiero, maximizando así la capacidad del Mecanismo de Ciberemergencia para ayudar a los Estados miembros a hacer frente eficazmente a las ciberamenazas.

12) Para prevenir, evaluar y responder de manera más eficaz a las ciberamenazas y ciberincidentes, es necesario desarrollar conocimientos más completos sobre las amenazas para las infraestructuras y los activos críticos en el territorio de la Unión, incluida su distribución geográfica, su interconexión y los posibles efectos en caso de ciberataques que les afecten. Debe desplegarse una infraestructura de COS de la Unión a gran escala (el «Ciberescudo Europeo») que incluya varias plataformas transfronterizas interoperativas, cada una de ellas integrada por varios COS nacionales. Dicha infraestructura debe servir a los intereses y necesidades nacionales y de la Unión en materia de ciberseguridad, y debe aprovechar la tecnología más puntera para las herramientas avanzadas de recopilación y análisis de datos, mejorar las capacidades de ciberdetección y gestión y proporcionar conciencia situacional en tiempo real. Tal infraestructura debe servir para aumentar la detección de amenazas e incidentes de ciberseguridad y complementar y apoyar así a las entidades y redes de la Unión responsables de la gestión de crisis en la Unión, en particular la red europea de organizaciones de enlace para las crisis de ciberseguridad («EU-CyCLONe»), tal como se define en la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo[12].

13) Cada Estado miembro debe designar un organismo público a nivel nacional encargado de coordinar las actividades de detección de ciberamenazas en dicho Estado miembro. Estos COS nacionales deben actuar como punto de referencia y pasarela a nivel nacional para la participación en el Ciberescudo Europeo y deben garantizar que la información sobre ciberamenazas procedente de entidades públicas y privadas se comparta y recopile a nivel nacional de manera eficaz y racional.

[12] 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).

14) Como parte del Ciberescudo Europeo, debe crearse una serie de centros de operaciones de ciberseguridad transfronterizos («COS transfronterizos»). Estos deben reunir a los COS nacionales de al menos tres Estados miembros, de modo que puedan lograrse plenamente los beneficios de la detección transfronteriza de amenazas y del intercambio y la gestión de la información. El objetivo general de los COS transfronterizos debe ser reforzar las capacidades para analizar, prevenir y detectar las amenazas a la ciberseguridad y apoyar la producción de inteligencia de alta calidad sobre las amenazas a la ciberseguridad, en particular mediante el intercambio de datos procedentes de diversas fuentes, públicas o privadas, así como mediante el intercambio y el uso conjunto de herramientas de vanguardia, y el desarrollo conjunto de capacidades de detección, análisis y prevención en un entorno de confianza. Deben proporcionar nuevas capacidades adicionales, aprovechando y complementando los COS existentes y los equipos de respuesta a incidentes de seguridad informática («CSIRT») y otros agentes pertinentes.

15) A nivel nacional, el seguimiento, la detección y el análisis de las ciberamenazas suelen correr a cargo de los COS de las entidades públicas y privadas, en combinación con los CSIRT. Además, los CSIRT intercambian información en el contexto de la red de CSIRT, de conformidad con la Directiva (UE) 2022/2555. Los COS transfronterizos deben constituir una nueva capacidad que sea complementaria de la red de CSIRT, mediante la puesta en común y el intercambio de datos sobre las amenazas a la ciberseguridad de entidades públicas y privadas, aumentando el valor de dichos datos mediante el análisis de expertos y la adquisición conjunta de infraestructuras y herramientas punteras, y contribuyendo al desarrollo de las capacidades y la soberanía tecnológica de la Unión.

16) Los COS transfronterizos deben actuar como punto central que permita una amplia puesta en común de datos pertinentes y de inteligencia sobre ciberamenazas, y permitir la difusión de información sobre amenazas entre un amplio y diverso conjunto de agentes [por ejemplo, los equipos de respuesta a emergencias informáticas (CERT), la red de CSIRT, los centros de intercambio y análisis de información (ISAC) y los operadores de infraestructuras críticas]. La información intercambiada entre los participantes en un COS transfronterizo podría incluir datos de redes y sensores, fuentes de información sobre amenazas, indicadores de compromiso e información contextualizada sobre incidentes, amenazas y vulnerabilidades. Además, los COS transfronterizos también deben celebrar acuerdos de cooperación con otros COS transfronterizos.

17) Que las autoridades pertinentes compartan la conciencia situacional es un requisito indispensable para la preparación y la coordinación a escala de la Unión con respecto a los incidentes de ciberseguridad significativos y a gran escala. La Directiva (UE) 2022/2555 crea EU-CyCLONe a fin de respaldar la gestión coordinada de los incidentes y las crisis de ciberseguridad a gran escala en el ámbito operativo y de garantizar el intercambio periódico de información pertinente entre los Estados miembros y las instituciones, órganos y organismos de la Unión. La Recomendación (UE) 2017/1584 sobre la respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala aborda el papel de todos los agentes pertinentes. La Directiva (UE) 2022/2555 también recuerda las responsabilidades de la Comisión en el Mecanismo de Protección Civil de la Unión («UCPM») establecido por la Decisión 1313/2013/UE del Parlamento Europeo y del Consejo, así como en lo relativo a la presentación de informes analíticos para el Dispositivo de Respuesta Política Integrada a las Crisis («Dispositivo RPIC») en virtud de la Decisión de Ejecución (UE)

2018/1993. Por lo tanto, en situaciones en las que los COS transfronterizos obtengan información relacionada con un incidente de ciberseguridad a gran escala potencial o en curso, deben proporcionar la información pertinente a EU-CyCLONe, a la red de CSIRT y a la Comisión. En particular, dependiendo de la situación, la información que debe compartirse podría incluir información técnica, información sobre la naturaleza y los motivos del agresor o posible agresor, e información no técnica de nivel superior sobre un incidente de ciberseguridad a gran escala potencial o en curso. En este contexto, debe prestarse la debida atención al principio de la necesidad de conocer y al carácter potencialmente sensible de la información compartida.

18) Las entidades que participen en el Ciberescudo Europeo deben garantizar un alto nivel de interoperabilidad entre ellas, incluido, cuando proceda, en lo que respecta a los formatos de datos, la taxonomía, las herramientas de tratamiento y análisis de datos y los canales de comunicación seguros, así como un nivel mínimo de seguridad de la capa de aplicación, un cuadro de indicadores de conciencia situacional y los indicadores. La adopción de una taxonomía común y el desarrollo de una plantilla de informes de situación para describir la causa técnica y las repercusiones de los incidentes de ciberseguridad deben tener en cuenta el trabajo en curso sobre la notificación de incidentes en el contexto de la aplicación de la Directiva (UE) 2022/2555.

19) A fin de permitir el intercambio de datos sobre amenazas a la ciberseguridad procedentes de diversas fuentes, a gran escala, en un entorno de confianza, las entidades que participen en el Ciberescudo Europeo deben estar dotadas de herramientas, equipos e infraestructuras de última generación y de alta seguridad. Esto debería permitir mejorar las capacidades de detección colectiva y las alertas oportunas a las autoridades y entidades pertinentes, en particular mediante el uso de las últimas tecnologías de inteligencia artificial y análisis de datos.

20) Al recopilar, compartir e intercambiar datos, el Ciberescudo Europeo debe reforzar la soberanía tecnológica de la Unión. La puesta en común de datos gestionados de alta calidad también debería contribuir al desarrollo de tecnologías avanzadas de inteligencia artificial y análisis de datos. Debe facilitarse mediante la conexión del Ciberescudo Europeo con la infraestructura paneuropea de informática de alto rendimiento establecida por el Reglamento (UE) 2021/1173 del Consejo[13].

21) Si bien el Ciberescudo Europeo es un proyecto civil, la comunidad de ciberdefensa podría beneficiarse de unas capacidades civiles más sólidas de detección y conciencia situacional desarrolladas para la protección de las infraestructuras críticas. Los COS transfronterizos, con el apoyo de la Comisión y del Centro Europeo de Competencia en Ciberseguridad («ECCC»), y en cooperación con el Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad (el «Alto Representante»), deben desarrollar gradualmente protocolos y normas específicos que permitan la cooperación con la comunidad de ciberdefensa, incluidas las condiciones de habilitación y seguridad. El desarrollo del Ciberescudo Europeo debe ir acompañado de una reflexión que permita la futura colaboración con las redes y plataformas responsables del intercambio de información en la comunidad de ciberdefensa, en estrecha cooperación con el Alto Representante.

[13] Reglamento (UE) 2021/1173 del Consejo, de 13 de julio de 2021, por el que se crea la Empresa Común de Informática de Alto Rendimiento Europea y por el que se deroga el Reglamento (UE) 2018/1488 (DO L 256 de 19.7.2021, p. 3).

22) El intercambio de información entre los participantes del Ciberescudo Europeo debe cumplir los requisitos jurídicos vigentes y, en particular, la legislación nacional y de la Unión en materia de protección de datos, así como las normas de la Unión en materia de competencia que rigen el intercambio de información. El destinatario de la información debe aplicar, en la medida en que sea necesario el tratamiento de datos personales, medidas técnicas y organizativas que salvaguarden los derechos y libertades de los interesados, destruir los datos tan pronto como dejen de ser necesarios para la finalidad declarada e informar al organismo que los ponga a disposición de que se han destruido los datos.

23) Sin perjuicio de lo dispuesto en el artículo 346 del TFUE, el intercambio de información confidencial con arreglo a las normas de la Unión o nacionales debe limitarse a aquella que sea pertinente y proporcionada en cuanto a la finalidad de dicho intercambio. El intercambio de tal información debe preservar la confidencialidad de esta y proteger la seguridad y los intereses comerciales de las entidades afectadas, respetando plenamente los secretos comerciales.

24) En vista del aumento de los riesgos y del número de ciberincidentes que afectan a los Estados miembros, es necesario crear un instrumento de apoyo a las crisis para mejorar la resiliencia de la Unión frente a incidentes de ciberseguridad significativos y a gran escala y complementar las acciones de los Estados miembros a través del apoyo financiero de emergencia para la preparación, la respuesta y la recuperación inmediata de los servicios esenciales. Dicho instrumento debe permitir el despliegue rápido de la ayuda en circunstancias definidas y en condiciones claras y permitir un seguimiento y una evaluación minuciosos de la manera en que se utilizan los recursos. Si bien la responsabilidad principal de prevenir los incidentes y crisis de ciberseguridad, prepararse para ellos y responder a ellos recae en los Estados miembros, el Mecanismo de Ciberemergencia promueve la solidaridad entre los Estados miembros de conformidad con el artículo 3, apartado 3, del Tratado de la Unión Europea («TUE»).

25) El Mecanismo de Ciberemergencia debe prestar apoyo a los Estados miembros complementando sus propias medidas y recursos, así como otras opciones de apoyo existentes para la respuesta y recuperación inmediata de incidentes de ciberseguridad significativos y a gran escala, como los servicios prestados por la Agencia de la Unión Europea para la Ciberseguridad (la «ENISA») de conformidad con su mandato, la respuesta coordinada y la asistencia de la red de CSIRT, el apoyo a la mitigación de EU-CyCLONe, así como la asistencia mutua entre los Estados miembros, también en el contexto del artículo 42, apartado 7, del TUE, los equipos de respuesta telemática rápida de la CEP[14] y los equipos de respuesta rápida contra amenazas híbridas. Debe abordar la necesidad de garantizar la disponibilidad de medios especializados para apoyar la preparación y la respuesta a los incidentes de ciberseguridad en toda la Unión y en terceros países.

26) El presente instrumento se entiende sin perjuicio de los procedimientos y marcos para coordinar la respuesta a las crisis a escala de la Unión, en particular el UCPM[15], el

[14] Decisión (PESC) 2017/2315 del Consejo, de 11 de diciembre de 2017, por la que se establece una cooperación estructurada permanente y se fija la lista de los Estados miembros participantes.

[15] Decisión n.º 1313/2013/UE del Parlamento Europeo y del Consejo, de 17 de diciembre de 2013, relativa a un Mecanismo de Protección Civil de la Unión (DO L 347 de 20.12.2013, p. 924).

Dispositivo RPIC[16], y la Directiva (UE) 2022/2555. Puede contribuir o complementar acciones ejecutadas en el contexto del artículo 42, apartado 7, del TUE o en situaciones definidas en el artículo 222 del TFUE. El uso del presente instrumento también debe coordinarse con la aplicación de las medidas del conjunto de instrumentos de ciberdiplomacia, cuando proceda.

27) La asistencia prestada en virtud del presente Reglamento debe apoyar y complementar las medidas tomadas por los Estados miembros a nivel nacional. A tal fin, debe garantizarse una estrecha cooperación y consulta entre la Comisión y el Estado miembro afectado. Al solicitar apoyo en el marco del Mecanismo de Ciberemergencia, el Estado miembro debe facilitar información pertinente que justifique la necesidad de apoyo.

28) La Directiva (UE) 2022/2555 exige a los Estados miembros que designen o establezcan una o varias autoridades de gestión de crisis de ciberseguridad y velen por que estas dispongan de los recursos adecuados para llevar a cabo sus cometidos de manera eficaz y eficiente. También exige a los Estados miembros que determinen las capacidades, los activos y los procedimientos que se pueden desplegar en caso de crisis, así como que adopten un plan nacional de respuesta a incidentes y crisis de ciberseguridad a gran escala en el que se fijen los objetivos y las disposiciones de la gestión de los incidentes y las crisis de ciberseguridad a gran escala. Asimismo, los Estados miembros están obligados a establecer uno o varios CSIRT encargados de las responsabilidades de gestión de incidentes de conformidad con un proceso bien definido y que abarquen al menos los sectores, subsectores y tipos de entidades incluidos en el ámbito de aplicación de dicha Directiva, y a velar por que dispongan de los recursos adecuados para llevar a cabo eficazmente sus cometidos. El presente Reglamento se entiende sin perjuicio del papel de la Comisión a la hora de garantizar el cumplimiento por parte de los Estados miembros de las obligaciones que les impone la Directiva (UE) 2022/2555. El Mecanismo de Ciberemergencia debe proporcionar asistencia para las acciones destinadas a reforzar la preparación, así como las acciones de respuesta a incidentes para mitigar los efectos de incidentes de ciberseguridad significativos y a gran escala, apoyar la recuperación inmediata o restablecer el funcionamiento de los servicios esenciales.

29) Como parte de las acciones de preparación, a fin de promover un enfoque coherente y reforzar la seguridad en toda la Unión y su mercado interior, debe prestarse apoyo para la puesta a prueba y la evaluación de la ciberseguridad de las entidades que operan en los sectores muy críticos determinados de conformidad con la Directiva (UE) 2022/2555 de manera coordinada. A tal fin, la Comisión, con el apoyo de la ENISA y en cooperación con el Grupo de Cooperación SRI establecido por la Directiva (UE) 2022/2555, debe determinar periódicamente los sectores o subsectores pertinentes, los cuales deben poder optar a recibir ayuda financiera para la realización de pruebas coordinadas a escala de la Unión. Los sectores o subsectores deben seleccionarse del anexo I de la Directiva (UE) 2022/2555 («Sectores de alta criticidad»). Los ejercicios de pruebas coordinados deben basarse en metodologías y escenarios de riesgo comunes. La selección de sectores y el desarrollo de escenarios de riesgo deben tener en cuenta las evaluaciones de riesgos y los escenarios de riesgo pertinentes a escala de la Unión, incluida la necesidad de evitar duplicaciones, tales como la evaluación de

[16] El Dispositivo de Respuesta Política Integrada a las Crisis (Dispositivo RPIC) y de conformidad con la Recomendación (UE) 2017/1584 de la Comisión, de 13 de septiembre de 2017, sobre la respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala.

riesgos y los escenarios de riesgo requeridos en las Conclusiones del Consejo sobre el desarrollo de la posición cibernética de la Unión Europea que lleven a cabo la Comisión, el Alto Representante y el Grupo de Cooperación SRI, en coordinación con los organismos y agencias civiles y militares pertinentes y las redes establecidas, incluida la red EU CyCLONe, así como la evaluación de riesgos de las redes e infraestructuras de comunicaciones solicitada por el llamamiento ministerial conjunto de Nevers y llevada a cabo por el Grupo de Cooperación SRI, con el apoyo de la Comisión y la ENISA, y en cooperación con el Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE), las evaluaciones coordinadas de riesgos que se lleven a cabo en virtud del artículo 22 de la Directiva (UE) 2022/2555 y las pruebas de resiliencia operativa digital previstas en el Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo[17]. La selección de los sectores también debe tener en cuenta la Recomendación del Consejo relativa a un enfoque coordinado en toda la Unión para reforzar la resiliencia de las infraestructuras críticas.

30) Además, el Mecanismo de Ciberemergencia debe respaldar otras acciones de preparación y apoyo a la preparación en otros sectores no cubiertos por las pruebas coordinadas de entidades que operan en sectores muy críticos. Estas acciones podrían incluir diversos tipos de actividades nacionales de preparación.

31) El Mecanismo de Ciberemergencia también debe respaldar las acciones de respuesta a incidentes para mitigar los efectos de incidentes de ciberseguridad significativos y a gran escala, apoyar la recuperación inmediata o restablecer el funcionamiento de los servicios esenciales. Cuando proceda, debe complementar al UCPM para garantizar un enfoque global que responda a las repercusiones de los ciberincidentes en los ciudadanos.

32) El Mecanismo de Ciberemergencia debe apoyar la asistencia prestada por los Estados miembros a un Estado miembro afectado por un incidente de ciberseguridad significativo o a gran escala, incluida la red de CSIRT establecida en el artículo 15 de la Directiva (UE) 2022/2555. Los Estados miembros que presten asistencia deben poder presentar solicitudes para cubrir los costes relacionados con el envío de equipos de expertos en el marco de la asistencia mutua. Los costes subvencionables podrían incluir los gastos de viaje, alojamiento y dietas de los expertos en ciberseguridad.

33) Debe crearse gradualmente una reserva de ciberseguridad a escala de la Unión, compuesta por servicios de proveedores privados de servicios de seguridad gestionados para apoyar las acciones de respuesta y recuperación inmediata en caso de incidentes de ciberseguridad significativos o a gran escala. La Reserva de Ciberseguridad de la UE debe garantizar la disponibilidad y el estado de preparación de los servicios. Los servicios de la Reserva de Ciberseguridad de la UE deben servir para ayudar a las autoridades nacionales a prestar asistencia a las entidades afectadas que operen en sectores críticos o muy críticos como complemento de sus propias acciones a nivel nacional. Al solicitar el apoyo de la Reserva de Ciberseguridad de la UE, los Estados miembros deben especificar el apoyo prestado a la entidad afectada a nivel nacional, que debe tenerse en cuenta al evaluar la solicitud del Estado miembro. Los servicios de la Reserva de Ciberseguridad de la UE también pueden servir para

[17] Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 y (UE) 2016/1011 (Texto pertinente a efectos del EEE).

apoyar a las instituciones, órganos y organismos de la Unión, en condiciones similares.

34) A efectos de la selección de proveedores de servicios privados para prestar servicios en el contexto de la Reserva de Ciberseguridad de la UE, es necesario establecer un conjunto de criterios mínimos que deben incluirse en la licitación para seleccionar a estos proveedores, a fin de garantizar que se satisfagan las necesidades de las autoridades y entidades de los Estados miembros que operen en sectores críticos o muy críticos.

35) Para apoyar la creación de la Reserva de Ciberseguridad de la UE, la Comisión podría considerar la posibilidad de solicitar a la ENISA que prepare una propuesta de esquema de certificación de conformidad con el Reglamento (UE) 2019/881 para los servicios de seguridad gestionados en los ámbitos cubiertos por el Mecanismo de Ciberemergencia.

36) Con el fin de apoyar los objetivos del presente Reglamento de promover una conciencia situacional común, mejorar la resiliencia de la Unión y permitir una respuesta eficaz a incidentes de ciberseguridad significativos y a gran escala, EU-CyCLONe, la red de CSIRT o la Comisión deben poder solicitar a la ENISA que revise y evalúe las amenazas, las vulnerabilidades y las medidas de mitigación con respecto a un incidente de ciberseguridad significativo o a gran escala específico. Una vez finalizada la revisión y evaluación de un incidente, la ENISA debe elaborar un informe de revisión del incidente, en colaboración con las partes interesadas pertinentes, incluidos los representantes del sector privado, los Estados miembros, la Comisión y otras instituciones, órganos y organismos pertinentes de la UE. Por lo que se refiere al sector privado, la ENISA está desarrollando canales para el intercambio de información con proveedores especializados, incluidos los proveedores de soluciones de seguridad gestionadas y los vendedores, con el fin de contribuir a la misión de la ENISA de lograr un elevado nivel común de ciberseguridad en toda la Unión. Sobre la base de la colaboración con las partes interesadas, incluido el sector privado, el informe de revisión sobre incidentes específicos debe tener por objeto evaluar las causas, los efectos y las medidas de mitigación de un incidente, una vez que se haya producido. Debe prestarse especial atención a las aportaciones y conclusiones de los proveedores de servicios de seguridad gestionados que cumplan las condiciones de máxima integridad profesional, imparcialidad y conocimientos técnicos necesarios, tal como exige el presente Reglamento. El informe debe presentarse y contribuir al trabajo de EU-CyCLONe, la red de CSIRT y la Comisión. Cuando el incidente se refiera a un tercer país, la Comisión también debe dar a conocer el informe al Alto Representante.

37) Teniendo en cuenta el carácter impredecible de los ataques de ciberseguridad y el hecho de que a menudo no se limitan a una zona geográfica específica y plantean un alto riesgo de contagio, el refuerzo de la resiliencia de los países vecinos y de su capacidad de responder eficazmente a incidentes de ciberseguridad significativos y a gran escala contribuye a la protección de la Unión en su conjunto. Por consiguiente, los terceros países asociados al programa Europa Digital pueden recibir apoyo de la Reserva de Ciberseguridad de la UE, cuando así lo disponga el acuerdo de asociación correspondiente al programa Europa Digital. La financiación para los terceros países asociados debe contar con el apoyo de la Unión en el marco de las asociaciones e instrumentos de financiación pertinentes para dichos países. El apoyo debe abarcar servicios en el ámbito de la respuesta a incidentes de ciberseguridad significativos o a gran escala y de la recuperación inmediata de ellos. Las condiciones establecidas en el

presente Reglamento para la Reserva de Ciberseguridad de la UE y los proveedores de confianza deben aplicarse a la hora de prestar apoyo a los terceros países asociados al programa Europa Digital.

38) A fin de garantizar unas condiciones uniformes de aplicación del presente Reglamento, procede otorgar a la Comisión competencias de ejecución para: especificar las condiciones de interoperabilidad entre los COS transfronterizos; determinar las disposiciones de procedimiento para el intercambio de información relacionada con un incidente de ciberseguridad a gran escala potencial o en curso entre los COS transfronterizos y las entidades de la Unión; establecer los requisitos técnicos para garantizar la seguridad del Ciberescudo Europeo; especificar los tipos y el número de servicios de respuesta necesarios para la Reserva de Ciberseguridad de la UE; y especificar en mayor medida las disposiciones detalladas para la asignación de los servicios de apoyo de la Reserva de Ciberseguridad de la UE. Dichas competencias deben ejercerse de conformidad con el Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo.

39) El objetivo del presente Reglamento puede lograrse mejor a escala de la Unión que por los Estados miembros. Por tanto, la Unión puede adoptar medidas con arreglo a los principios de subsidiariedad y proporcionalidad establecidos en el artículo 5 del Tratado de la Unión Europea. El presente Reglamento no excede de lo necesario para alcanzar dicho objetivo.

HAN ADOPTADO EL PRESENTE REGLAMENTO:

Capítulo I

OBJETIVOS GENERALES, OBJETO Y DEFINICIONES

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 las siguientes acciones:

a) el despliegue de una infraestructura paneuropea de centros de operaciones de seguridad («Ciberescudo Europeo») para desarrollar y mejorar las capacidades comunes de detección y conciencia situacional;

b) la creación de un Mecanismo de Emergencia en materia de Ciberseguridad para ayudar a los Estados miembros a prepararse para incidentes de ciberseguridad significativos y a gran escala, responder a ellos y recuperarse inmediatamente de ellos;

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

2. El presente Reglamento persigue el objetivo de reforzar la solidaridad a escala de la Unión mediante los siguientes objetivos específicos:

a) afianzar la capacidad común de la Unión de detección y conciencia situacional de ciberamenazas y ciberincidentes, permitiendo así reforzar la posición competitiva de la industria y los sectores de servicios de la Unión en toda la economía digital y contribuir a la soberanía tecnológica de la Unión en el ámbito de la ciberseguridad;

b) consolidar la preparación de las entidades que operan en sectores críticos y muy críticos en toda la Unión y reforzar la solidaridad mediante el desarrollo de capacidades comunes de respuesta frente a incidentes de ciberseguridad significativos o a gran escala, en particular poniendo 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 mediante la revisión y evaluación de incidentes significativos o a gran escala, incluida la extracción de conclusiones y, en su caso, la formulación de recomendaciones.

3. El presente Reglamento se entiende sin perjuicio de la responsabilidad principal de los Estados miembros en materia de seguridad nacional y seguridad pública y de prevención, investigación, detección y enjuiciamiento de infracciones penales.

Artículo 2

Definiciones

A los efectos del presente Reglamento, se entenderá por:

1) **«centro de operaciones de seguridad transfronterizo» («COS transfronterizo»)**: una plataforma plurinacional que reúne en una estructura de red coordinada a los COS nacionales de al menos tres Estados miembros que forman un consorcio anfitrión, y que se ha concebido para prevenir ciberamenazas y ciberincidentes y apoyar la producción de inteligencia de alta calidad, en particular mediante el intercambio de datos procedentes de diversas fuentes, públicas y privadas, así como mediante el intercambio de herramientas de vanguardia y el desarrollo conjunto de capacidades de detección, análisis y prevención cibernéticos y de prevención y protección en un entorno de confianza;

2) **«organismo público»**: los organismos de Derecho público, según se definen en el artículo 2, apartado 1, punto 4, de la Directiva 2014/24/UE del Parlamento Europeo y del Consejo[18];

3) **«consorcio anfitrión»**: un consorcio compuesto por Estados participantes, representados por los COS nacionales, que han acordado establecer y contribuir a la adquisición de herramientas e infraestructuras para un COS transfronterizo y a su funcionamiento;

[18] 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).

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 críticos o muy críticos»**: el tipo de entidades enumeradas en los anexos I y II de la Directiva (UE) 2022/2555;

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

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

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

9) **«preparación»**: estado de preparación y capacidad para garantizar una respuesta rápida eficaz a un incidente de ciberseguridad significativo o a gran escala, obtenido como resultado de la evaluación de riesgos y de las medidas de seguimiento adoptadas con antelación;

10) **«respuesta»**: actuación en caso de incidente de ciberseguridad significativo o a gran escala, o durante o después de dicho incidente, para hacer frente a sus consecuencias adversas inmediatas y a corto plazo;

11) **«proveedores de confianza»**: los proveedores de servicios de seguridad gestionados, según se definen en el artículo 6, punto 40, de la Directiva (UE) 2022/2555, seleccionados de conformidad con el artículo 16 del presente Reglamento.

Capítulo II

EL CIBERESCUDO EUROPEO

Artículo 3

Creación del Ciberescudo Europeo

1. Se creará una infraestructura paneuropea interconectada de centros de operaciones de seguridad («Ciberescudo Europeo») a fin de desarrollar capacidades avanzadas para que la Unión pueda detectar, analizar y tratar datos sobre ciberamenazas y ciberincidentes en la Unión. Estará compuesta por todos los centros de operaciones de seguridad nacionales («COS nacionales») y los centros de operaciones de seguridad transfronterizos («COS transfronterizos»).

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

2. El Ciberescudo Europeo:

a) reunirá y pondrá en común datos sobre ciberamenazas y ciberincidentes procedentes de diversas fuentes a través de los COS transfronterizos;

b) producirá información de alta calidad y utilizable e inteligencia sobre ciberamenazas, mediante el uso de herramientas de vanguardia, en particular tecnologías de inteligencia artificial y análisis de datos;

c) contribuirá a mejorar la protección frente a las ciberamenazas y la respuesta a ellas;

d) contribuirá a una detección más rápida de las ciberamenazas y a la conciencia situacional en toda la Unión;

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 avanzadas de inteligencia artificial y análisis de datos.

Se desarrollará en cooperación con la infraestructura paneuropea de informática de alto rendimiento creada en virtud del Reglamento (UE) 2021/1173.

Artículo 4

Centros de operaciones de seguridad nacionales

1. A fin de participar en el Ciberescudo Europeo, cada Estado miembro designará, al menos, a un COS nacional. El COS nacional será un organismo público.

Tendrá la capacidad de actuar como punto de referencia y pasarela a otras organizaciones públicas y privadas a nivel nacional para recopilar y analizar información sobre amenazas e incidentes de ciberseguridad y contribuir a un COS transfronterizo. Estará equipado con tecnologías de vanguardia capaces de detectar, agregar y analizar datos pertinentes para las amenazas e incidentes de ciberseguridad.

2. Tras una convocatoria de manifestaciones de interés, el Centro Europeo de Competencia en Ciberseguridad («ECCC», por sus siglas en inglés) seleccionará a COS nacionales para que participen con él en una adquisición conjunta de herramientas e infraestructuras. El ECCC podrá conceder subvenciones a los COS nacionales seleccionados para financiar el funcionamiento de dichas herramientas e infraestructuras. La contribución financiera de la Unión sufragará hasta el 50 % de los costes de adquisición de las herramientas e infraestructuras y hasta el 50 % de los costes de funcionamiento, y los costes restantes correrán a cargo del Estado miembro. Antes de iniciar el procedimiento para la adquisición de las herramientas e infraestructuras, el ECCC y el COS nacional celebrarán un acuerdo de alojamiento y uso que regule el uso de las herramientas e infraestructuras.

3. Los COS nacionales seleccionados de conformidad con el apartado 2 se comprometerán a solicitar su participación en un COS transfronterizo en un plazo de dos años a partir de la fecha en la que se adquieran las herramientas e infraestructuras o en la que reciban financiación mediante subvenciones, si esta fecha se produce antes. Si los COS nacionales no participan para entonces en un COS transfronterizo, no podrán optar al apoyo adicional de la Unión en virtud del presente Reglamento.

Artículo 5

Centros de operaciones de seguridad transfronterizos

1. En las acciones destinadas a crear un COS transfronterizo podrá participar un consorcio anfitrión, compuesto por al menos tres Estados miembros, representados por COS nacionales, que se comprometan a colaborar para coordinar sus actividades de ciberdetección y seguimiento de amenazas.

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

3. Los miembros del consorcio anfitrión celebrarán un acuerdo de consorcio escrito en el que se establecerán sus disposiciones internas para la aplicación del acuerdo de alojamiento y uso.

4. Los COS transfronterizos estarán representados a efectos jurídicos por un COS nacional que actúe como COS coordinador, o por el consorcio anfitrión si este tiene personalidad jurídica. El COS coordinador será responsable del cumplimiento de los requisitos del acuerdo de alojamiento y uso y del presente Reglamento.

Artículo 6

Cooperación e intercambio de información dentro de los COS transfronterizos y entre ellos

1. Los miembros de un consorcio anfitrión intercambiarán entre sí la información pertinente dentro del COS transfronterizo, incluida 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 dicho intercambio de información:

a) se haga con el objetivo de prevenir, detectar o responder a incidentes, recuperarse de ellos o reducir su repercusión;

b) refuerce el nivel de ciberseguridad, en particular, 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 de mitigación o 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 una cantidad significativa de los datos a que se refiere el apartado 1 y las condiciones en las que se intercambiará dicha información;

b) un marco de gobernanza que incentive la puesta en común de información entre todos los participantes;

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

3. Para fomentar el intercambio de información entre los COS transfronterizos, estos deberán garantizar un alto nivel de interoperabilidad entre sí. Para facilitar la interoperabilidad entre los COS transfronterizos, la Comisión podrá, mediante actos de ejecución, previa consulta al ECCC, especificar las condiciones de dicha interoperabilidad. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 21, apartado 2.

4. Los COS transfronterizos celebrarán acuerdos de cooperación entre sí, especificando los principios de intercambio de información entre las plataformas transfronterizas.

Artículo 7

Cooperación e intercambio de información con entidades de la Unión

1. Cuando los COS transfronterizos obtengan información relativa a un incidente de ciberseguridad a gran escala potencial o en curso, facilitarán, sin demora indebida, la información pertinente a EU-CyCLONe, a la red de CSIRT y a la Comisión, teniendo en cuenta sus respectivas funciones de gestión de crisis de conformidad con la Directiva (UE) 2022/2555.

2. La Comisión podrá determinar, mediante actos de ejecución, las disposiciones de procedimiento para el intercambio de información previsto en el apartado 1. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 21, apartado 2.

Artículo 8

Seguridad

1. Los Estados miembros que participen en el Ciberescudo Europeo garantizarán un alto nivel de seguridad de los datos y de seguridad física de la infraestructura del Ciberescudo Europeo, y velarán por que la infraestructura se gestione y controle adecuadamente, de tal manera que se proteja de las amenazas y se garantice su seguridad y la de los sistemas, incluida la de los datos intercambiados a través de la infraestructura.

2. Los Estados miembros que participen en el Ciberescudo Europeo velarán por que el intercambio de información dentro del Ciberescudo Europeo con entidades que no sean organismos públicos de los Estados miembros no afecte negativamente a los intereses de seguridad de la Unión.

3. La Comisión podrá adoptar actos de ejecución que establezcan requisitos técnicos para que los Estados miembros cumplan las obligaciones que les imponen los apartados 1 y 2. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 21, apartado 2. Al hacerlo, la Comisión, con el apoyo del Alto

Representante, tendrá en cuenta las normas de seguridad pertinentes en materia de defensa, con el fin de facilitar la cooperación con los mandos militares.

Capítulo III

MECANISMO DE CIBEREMERGENCIA

Artículo 9

Creación del Mecanismo de Ciberemergencia

1. Se crea un Mecanismo de Ciberemergencia para mejorar la resiliencia de la Unión ante las principales amenazas para la ciberseguridad, prepararla para los efectos a corto plazo de los incidentes de ciberseguridad significativos y a gran escala, y mitigar dichos efectos, en un espíritu de solidaridad (el «Mecanismo»).

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

Artículo 10

Tipos de acciones

1. El Mecanismo apoyará los siguientes tipos de acciones:

a) acciones de preparación, incluida la realización de pruebas coordinadas de preparación de las entidades que operan en sectores muy críticos en toda la Unión;

b) acciones de respuesta, que apoyen la respuesta a incidentes de ciberseguridad significativos y a gran escala y la recuperación inmediata de ellos, de las que se ocuparán los proveedores de confianza que participen en la Reserva de Ciberseguridad de la UE establecida en virtud del artículo 12;

c) acciones de asistencia mutua consistentes en la prestación de asistencia por parte de las autoridades nacionales de un Estado miembro a otro, en particular conforme a lo dispuesto en el artículo 11, apartado 3, letra f), de la Directiva (UE) 2022/2555.

Artículo 11

Pruebas coordinadas de preparación de las entidades

1. Con el fin de apoyar las pruebas coordinadas de preparación de las entidades a que se refiere el artículo 10, apartado 1, letra a), en toda la Unión, la Comisión, previa consulta al Grupo de Cooperación SRI y a la 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 cuyas entidades podrán ser objeto de las pruebas coordinadas de preparación, teniendo en cuenta las evaluaciones de riesgos y las pruebas de resiliencia coordinadas existentes y previstas a escala de la Unión.

2. El Grupo de Cooperación SRI, en colaboración con la Comisión, la ENISA y el Alto Representante, elaborará escenarios de riesgo y metodologías comunes para los ejercicios de pruebas coordinadas.

Artículo 12

Creación de la Reserva de Ciberseguridad de la UE

1. Se creará una reserva de ciberseguridad de la UE para ayudar a los usuarios a que se refiere el apartado 3 a responder o a prestar apoyo para responder a incidentes de ciberseguridad significativos o a gran escala y para recuperarse inmediatamente de tales incidentes.

2. La Reserva de Ciberseguridad de la UE consistirá en servicios de respuesta a incidentes prestados por proveedores de confianza seleccionados de conformidad con los criterios establecidos en el artículo 16. La Reserva incluirá servicios comprometidos previamente. Los servicios deberán poder desplegarse en todos los Estados miembros.

3. Entre los usuarios de los servicios de la Reserva de Ciberseguridad de la UE se incluirán:

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

b) las instituciones, órganos y organismos de la Unión.

4. Los usuarios a que se refiere el apartado 3, letra a), utilizarán los servicios de la Reserva de Ciberseguridad de la UE para responder o apoyar la respuesta a incidentes significativos o a gran escala que afecten a entidades que operen en sectores críticos o muy críticos y la recuperación inmediata de tales incidentes.

5. La Comisión tendrá la responsabilidad general de la ejecución de la Reserva de Ciberseguridad de la UE. La Comisión 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 en virtud del presente Reglamento, así como con otras acciones y programas de la Unión.

6. La Comisión podrá encomendar el funcionamiento y la administración de la Reserva de Ciberseguridad de la UE, total o parcialmente, a la ENISA, mediante acuerdos de contribución.

7. Con el fin de apoyar a la Comisión en la creación de la Reserva de Ciberseguridad de la UE, la ENISA elaborará una cartografía de los servicios necesarios, previa consulta a los Estados miembros y a la Comisión. La ENISA elaborará una cartografía similar, previa consulta a la Comisión, para determinar las necesidades de los terceros países que puedan optar al apoyo de la Reserva de Ciberseguridad de la UE de conformidad con el artículo 17. La Comisión, cuando proceda, consultará al Alto Representante.

8. La Comisión podrá, mediante actos de ejecución, especificar los tipos y el número de servicios de respuesta necesarios para la Reserva de Ciberseguridad de la UE. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 21, apartado 2.

Artículo 13

Solicitudes de apoyo de la Reserva de Ciberseguridad de la UE

1. Los usuarios a que se refiere el artículo 12, apartado 3, podrán solicitar los servicios de la Reserva de Ciberseguridad de la UE para apoyar la respuesta a incidentes de ciberseguridad significativos o a gran escala y la recuperación inmediata de tales incidentes.

2. Para recibir el apoyo de la Reserva de Ciberseguridad de la UE, los usuarios a que se refiere el artículo 12, apartado 3, tomarán medidas para mitigar los efectos del incidente para el que se solicite el apoyo, incluida la prestación de asistencia técnica directa, y otros recursos para ayudar a la respuesta y a los esfuerzos inmediatos de recuperación.

3. Las solicitudes de apoyo de los usuarios a que se refiere el artículo 12, apartado 3, letra a), del presente Reglamento se transmitirán a la Comisión y a la ENISA a través del punto de contacto único designado o establecido por el Estado miembro de conformidad con el artículo 8, apartado 3, de la Directiva (UE) 2022/2555.

4. Los Estados miembros informarán a la red de CSIRT y, cuando proceda, a EU-CyCLONe, de sus solicitudes de apoyo para la respuesta a incidentes y la recuperación inmediata con arreglo al presente artículo.

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

a) información adecuada sobre la entidad afectada y las posibles repercusiones del incidente y sobre el uso previsto del apoyo solicitado, incluida una indicación de las necesidades estimadas;

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

c) información sobre otras formas de apoyo a disposición de la entidad afectada, incluidos los acuerdos contractuales vigentes para la respuesta a incidentes y los servicios de recuperación inmediata, así como los contratos de seguro que puedan cubrir este tipo de incidente.

6. La ENISA, en cooperación con la Comisión y el Grupo de Cooperación SRI, elaborará una plantilla para facilitar la presentación de solicitudes de apoyo de la Reserva de Ciberseguridad de la UE.

7. La Comisión podrá especificar, mediante actos de ejecución, las disposiciones detalladas para la asignación de los servicios de apoyo de la Reserva de Ciberseguridad de la UE. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 21, apartado 2.

Artículo 14

Ejecución del apoyo de la Reserva de Ciberseguridad de la UE

1. Las solicitudes de apoyo de la Reserva de Ciberseguridad de la UE serán evaluadas por la Comisión, con el apoyo de la ENISA o según se defina en los acuerdos de contribución con arreglo al artículo 12, apartado 6, y se transmitirá sin demora una respuesta a los usuarios a que se refiere el artículo 12, apartado 3.

2. Para establecer el orden de prioridad de las solicitudes, en caso de múltiples solicitudes concurrentes, se tendrán en cuenta, cuando proceda, los siguientes criterios:

a) la gravedad del incidente de ciberseguridad;

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

c) el impacto potencial en el Estado o Estados miembros o en los usuarios afectados;

d) el posible carácter transfronterizo del incidente y el riesgo de contagio a otros Estados miembros o usuarios;

e) las medidas tomadas por el usuario para ayudar a la respuesta y los esfuerzos inmediatos de recuperación a que se refieren el artículo 13, apartado 2, y el artículo 13, apartado 5, letra b).

3. Los servicios de la Reserva de Ciberseguridad de la UE se prestarán de conformidad con acuerdos específicos entre el proveedor de servicios y el usuario al que se preste el apoyo en el marco de la Reserva de Ciberseguridad de la UE. Dichos acuerdos incluirán condiciones de responsabilidad.

4. Los acuerdos a que se refiere el apartado 3 podrán basarse en plantillas preparadas por la ENISA, previa consulta a los Estados miembros.

5. La Comisión y la ENISA 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.

6. En el plazo de un mes a partir del fin de la acción de apoyo, los usuarios facilitarán a la Comisión y a la ENISA un informe resumido sobre el servicio prestado, los resultados obtenidos y las conclusiones extraídas. Cuando el usuario proceda de un tercer país, tal como se establece en el artículo 17, dicho informe se dará a conocer al Alto Representante.

7. La Comisión informará periódicamente al Grupo de cooperación SRI sobre el uso y los resultados del apoyo.

Artículo 15

Coordinación con los mecanismos de gestión de crisis

1. En los casos en que los incidentes de ciberseguridad significativos o a gran escala se produzcan a raíz de catástrofes o den lugar a catástrofes, tal como se definen en la Decisión 1313/2013/UE[19], el apoyo en virtud del presente Reglamento para responder a tales incidentes complementará las acciones previstas en la Decisión 1313/2013/UE y sin perjuicio de esta.

[19] Decisión n.º 1313/2013/UE del Parlamento Europeo y del Consejo, de 17 de diciembre de 2013, relativa a un Mecanismo de Protección Civil de la Unión (DO L 347 de 20.12.2013, p. 924).

2. En caso de incidente transfronterizo de ciberseguridad a gran escala en el que se active el Dispositivo de Respuesta Política Integrada a las Crisis (Dispositivo RPIC), 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 Dispositivo RPIC.

3. En consulta con el Alto Representante, el apoyo prestado en el marco del Mecanismo de Ciberemergencia podrá complementar la asistencia prestada en el contexto de la política exterior y de seguridad común y de la política común de seguridad y defensa, en particular a través de los Equipos de Respuesta Telemática Rápida. También podrá complementar o contribuir a la asistencia prestada por un Estado miembro a otro en el contexto del artículo 42, apartado 7, del Tratado de la Unión Europea.

4. El apoyo en el marco del Mecanismo de Ciberemergencia podrá formar parte de la respuesta conjunta de la Unión y los Estados miembros en las situaciones a que se refiere el artículo 222 del Tratado de Funcionamiento de la Unión Europea.

Artículo 16

Proveedores 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) 2018/1046 y con los siguientes principios:

a) garantizar que la Reserva de Ciberseguridad de la UE incluya servicios que puedan desplegarse en todos los Estados miembros, teniendo en cuenta, en particular, los requisitos nacionales para la prestación de tales servicios, incluida 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 UE, 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 UE.

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 de selección:

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, sus filiales y subcontratistas habrán establecido un marco para proteger la información sensible relacionada con el servicio y, en particular, las pruebas, conclusiones e informes, y cumplirán las normas de seguridad de la Unión sobre la protección de la información clasificada de la UE;

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 el despliegue de servicios;

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

f) el proveedor estará equipado con el equipo técnico de *hardware* y *software* necesario para prestar el servicio solicitado;

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

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

i) el proveedor deberá poder prestar el servicio en el idioma local del Estado o Estados miembros en los que pueda prestar el servicio;

j) una vez que se haya establecido un esquema de certificación de la UE para los servicios de seguridad gestionados, Reglamento (UE) 2019/881, el proveedor será certificado de conformidad con dicho esquema.

Artículo 17

Apoyo a terceros países

1. Los terceros países podrán solicitar el apoyo de la Reserva de Ciberseguridad de la UE cuando así lo contemplen los acuerdos de asociación celebrados en relación con su participación en el programa Europa Digital.

2. El apoyo de la Reserva de Ciberseguridad de la UE se ajustará a lo dispuesto en el presente Reglamento y cumplirá las condiciones específicas establecidas en los acuerdos de asociación a que se refiere el apartado 1.

3. Entre los usuarios de los terceros países asociados que puedan optar a recibir los servicios de la Reserva de Ciberseguridad de la UE figurarán las autoridades competentes, como los CSIRT y las autoridades de gestión de crisis de ciberseguridad.

4. Cada tercer país 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.

5. Antes de recibir el apoyo de la Reserva de Ciberseguridad de la UE, los terceros países facilitarán a la Comisión y al Alto Representante 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 a gran escala, así como información sobre las entidades nacionales responsables, incluidos los CSIRT o entidades equivalentes, sus capacidades y los recursos que tienen asignados. Cuando las disposiciones de los artículos 13 y 14 del presente Reglamento se refieran a los Estados miembros, se aplicarán a terceros países con arreglo a lo dispuesto en el apartado 1.

6. La Comisión 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.

Capítulo IV

MECANISMO DE REVISIÓN DE INCIDENTES DE CIBERSEGURIDAD

Artículo 18

Mecanismo de Revisión de Incidentes de Ciberseguridad

1. A petición de la Comisión, de EU-CyCLONe o de la red de CSIRT, la ENISA revisará y evaluará las amenazas, vulnerabilidades y medidas de mitigación con respecto a un incidente específico de ciberseguridad significativo o a gran escala. Una vez finalizada la revisión y evaluación de un incidente, la ENISA presentará un informe de revisión del incidente a la red de CSIRT, a EU-CyCLONe 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. Cuando proceda, la Comisión dará a conocer el informe al Alto Representante.

2. Para preparar el informe de revisión del incidente a que se refiere el apartado 1, la ENISA colaborará con todas las partes interesadas pertinentes, incluidos los representantes de los Estados miembros, la Comisión, otras instituciones, órganos y organismos pertinentes de la UE, los proveedores de servicios de seguridad gestionados y los usuarios de servicios de ciberseguridad. Cuando proceda, la ENISA también colaborará con las entidades afectadas por incidentes de ciberseguridad significativos o a gran escala. Para apoyar la revisión, la ENISA también podrá consultar a otros tipos de partes interesadas. Los representantes consultados revelarán cualquier posible conflicto de intereses.

3. El informe incluirá una revisión y un análisis del incidente específico de ciberseguridad significativo o a gran escala, incluidas las principales causas, vulnerabilidades y conclusiones extraídas. Protegerá la información confidencial, de conformidad con la legislación nacional o de la Unión relativa a la protección de la información sensible o clasificada.

4. Cuando proceda, el informe formulará recomendaciones para mejorar la posición de la Unión en materia de ciberseguridad.

5. En la medida de lo posible, se pondrá a disposición del público una versión del informe. Esta versión solo incluirá información pública.

Capítulo V

DISPOSICIONES FINALES

Artículo 19

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:

1) se añade la letra a *bis*) siguiente:

«a *bis*) apoyar el desarrollo de un Ciberescudo de la UE, incluido el desarrollo, despliegue y funcionamiento de plataformas nacionales y transfronterizas de COS que contribuyan a la conciencia situacional en la Unión y a la mejora de las capacidades de inteligencia sobre amenazas para la ciberseguridad de la Unión;»;

2) se añade la letra g) siguiente:

«g) establecer y gestionar un Mecanismo de Ciberemergencia para ayudar a los Estados miembros a prepararse ante incidentes significativos de ciberseguridad y darles respuesta, como complemento de los recursos y capacidades nacionales y otras formas de apoyo disponibles a escala de la Unión, incluida la creación de una Reserva de Ciberseguridad de la UE;»;

a) 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[20], con excepción de las acciones de ejecución de la Reserva de Ciberseguridad de la UE, que serán ejecutadas por la Comisión y la ENISA.»;

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) 1 776 956 000 EUR para el objetivo específico 2 – Inteligencia artificial;

c) 1 629 566 000 EUR para el objetivo específico 3 – Ciberseguridad y confianza;

d) 482 347 000 EUR para el objetivo específico 4 – Capacidades digitales avanzadas;»;

b) se añade el apartado 8 siguiente:

«8. No obstante lo dispuesto en el artículo 12, apartado 4, del Reglamento (UE, Euratom) 2018/1046, los créditos de compromiso y de pago no utilizados para acciones 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.»;

[20] 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).

3) 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 contratos públicos principalmente, así como subvenciones y premios.

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[27] y 2014/25/UE[28] 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 pública para la Reserva de Ciberseguridad de la UE establecida por el artículo 12 del Reglamento (UE) 2023/XX, la Comisión y la ENISA podrán actuar como central de compras para la contratación en nombre o por cuenta de terceros países asociados al Programa, de conformidad con el artículo 10. La Comisión y la 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 169, apartado 3 del Reglamento (UE) XXX/XXXX [RF refundido], la solicitud de un único tercer país es suficiente para otorgar un mandato a la Comisión o a la ENISA para que actúen.

Al ejecutar los procedimientos de contratación pública para la Reserva de Ciberseguridad de la UE establecida por el artículo 12 del Reglamento (UE) 2023/XX, la Comisión y la ENISA podrán actuar como central de compras para la contratación en nombre o por cuenta de las instituciones, órganos y organismos de la UE. La Comisión y la ENISA también podrán actuar como mayoristas, comprando, almacenando, revendiendo o donando suministros y servicios, incluidos los alquileres, a las instituciones, órganos y organismos de la Unión. Como excepción a lo dispuesto en el artículo 169, apartado 3, del Reglamento (UE) n.º XXX/XXXX [RF refundido], la solicitud de una única institución, organismo o agencia de la Unión es suficiente para otorgar un mandato a la Comisión o a la ENISA para que actúen.

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

4) se añade el artículo 16 *bis* siguiente:

«En el caso de las acciones de ejecución del Ciberescudo Europeo establecido por el artículo 3 del Reglamento (UE) 2023/XX, las normas aplicables serán las establecidas en los artículos 4 y 5 del Reglamento (UE) 2023/XX. En caso de conflicto entre las disposiciones del presente Reglamento y los artículos 4 y 5 del Reglamento (UE) 2023/XX, este último prevalecerá y se aplicará a dichas acciones específicas.»;

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

«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 COS nacionales a que se refiere el artículo 4 del Reglamento XXXX y al consorcio anfitrión a que se refiere el artículo 5 del Reglamento XXXX, de conformidad con el artículo 195, apartado 1, letra d), del Reglamento Financiero.

El apoyo en forma de subvenciones para el Mecanismo de Ciberemergencia, tal como se establece en el artículo 10 del Reglamento XXXX, 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.

En el caso de las acciones especificadas en el artículo 10, apartado 1, letra c), del Reglamento 202X/XXXX, el ECCC informará a la Comisión y a la ENISA sobre las solicitudes de subvenciones directas de los Estados miembros sin convocatoria de propuestas.

Para el apoyo a la asistencia mutua en respuesta a un incidente de ciberseguridad significativo o a gran escala, tal como se define en el artículo 10, letra c), del Reglamento XXXX, 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.»;

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

Artículo 20

Evaluación

A más tardar [cuatro años después de la fecha de aplicación del presente Reglamento], la Comisión presentará al Parlamento Europeo y al Consejo un informe sobre la evaluación y revisión del presente Reglamento.

Artículo 21

Procedimiento de comité

1. La Comisión estará asistida por el Comité de Coordinación del programa Europa Digital establecido por el 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.

Artículo 22

Entrada en vigor

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

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

Hecho en Estrasburgo, el

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

FICHA DE FINANCIACIÓN LEGISLATIVA

1. MARCO DE LA PROPUESTA/INICIATIVA

1.1. Denominación de la propuesta/iniciativa

1.2. Política(s) afectada(s)

1.3. La propuesta/iniciativa se refiere a:

1.4. Objetivo(s)

1.4.1. Objetivo(s) general(es)

1.4.2. Objetivo(s) específico(s)

1.4.3. Resultado(s) e incidencia esperados

1.4.4. Indicadores de rendimiento

1.5. Justificación de la propuesta/iniciativa

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

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

1.5.3. Principales conclusiones extraídas de experiencias similares anteriores

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

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

1.6. Duración e incidencia financiera de la propuesta/iniciativa

1.7. Método(s) de ejecución presupuestaria previsto(s)

2. MEDIDAS DE GESTIÓN

2.1. Normas en materia de seguimiento e informes

2.2. Sistema(s) de gestión y de control

2.2.1. Justificación del / de los modo(s) de gestión, del / de los mecanismo(s) de aplicación de la financiación, de las modalidades de pago y de la estrategia de control propuestos

2.2.2. Información relativa a los riesgos identificados y al / a los sistema(s) de control interno establecidos para atenuarlos

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

2.3. Medidas de prevención del fraude y de las irregularidades

3. INCIDENCIA FINANCIERA ESTIMADA DE LA PROPUESTA/INICIATIVA

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

3.2. Incidencia financiera estimada de la propuesta en los créditos

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

3.2.2. Resultados estimados financiados con créditos de operaciones

3.2.3. Resumen de la incidencia estimada en los créditos administrativos

3.2.3.1. Necesidades estimadas de recursos humanos

3.2.4. Compatibilidad con el marco financiero plurianual vigente

3.2.5. Contribución de terceros

3.3. Incidencia estimada en los ingresos

1. MARCO DE LA PROPUESTA/INICIATIVA

1.1. Denominación de la propuesta/iniciativa

Reglamento del Parlamento Europeo y del Consejo por el que se establecen medidas destinadas a reforzar la solidaridad y las capacidades en la Unión a fin de detectar amenazas e incidentes de ciberseguridad, prepararse para ellos y responder a ellos

1.2. Política(s) afectada(s)

Una Europa Adaptada a la Era Digital

Inversiones estratégicas europeas

Actividad: Configurar el futuro digital de Europa.

1.3. La propuesta/iniciativa se refiere a:

☒ **una acción nueva**

☐ **una acción nueva a raíz de un proyecto piloto / una acción preparatoria**[33]

☐ **la prolongación de una acción existente**

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

1.4. Objetivo(s)

1.4.1. Objetivo(s) general(es)

La Ley de Cibersolidaridad reforzará la solidaridad a escala de la Unión para mejorar la detección de amenazas e incidentes de ciberseguridad, la preparación frente a ellos y la respuesta a ellos. Sus objetivos son los siguientes:

a) reforzar la capacidad común de la UE de detección y conciencia situacional de ciberamenazas y ciberincidentes;

b) afianzar la preparación de las entidades críticas en toda la UE y reforzar la solidaridad mediante el desarrollo de capacidades comunes de respuesta frente a incidentes de ciberseguridad significativos o a gran escala, en particular poniendo el apoyo a la respuesta a incidentes de ciberseguridad a disposición de terceros países asociados al programa Europa Digital;

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

1.4.2. Objetivo(s) específico(s)

La Ley de Cibersolidaridad alcanzará el conjunto de objetivos a través de:

a) El despliegue de una infraestructura paneuropea de centros de operaciones de seguridad (Ciberescudo Europeo) para desarrollar y mejorar las capacidades comunes de detección y conciencia situacional.

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

b) La creación de un Mecanismo de Emergencia en materia de Ciberseguridad para ayudar a los Estados miembros a prepararse para incidentes de ciberseguridad significativos y a gran escala, responder a ellos y recuperarse inmediatamente de ellos. El apoyo a la respuesta a incidentes también se pondrá a disposición de las instituciones, órganos y organismos de la Unión.

Estas acciones recibirán financiación del programa Europa Digital, que el presente instrumento legislativo modificará para establecer las acciones mencionadas, proporcionar apoyo financiero para su ejecución y aclarar las condiciones necesarias para recibir la ayuda financiera.

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

1.4.3. Resultado(s) e incidencia esperados

Especificar los efectos que la propuesta/iniciativa debería tener sobre los beneficiarios / los grupos destinatarios.

La propuesta beneficiaría considerablemente a las distintas partes interesadas. El Ciberescudo Europeo mejorará las capacidades de detección de ciberamenazas de los Estados miembros. El Mecanismo de Ciberemergencia complementará las acciones de los Estados miembros a través del apoyo de emergencia para la preparación, la respuesta y la recuperación inmediata o el restablecimiento del funcionamiento de los servicios esenciales.

Estas acciones afianzarán la posición competitiva de la industria y la empresa en Europa en el conjunto de la economía digitalizada y apoyarán su transformación digital reforzando el nivel de ciberseguridad en el mercado único digital. Se pretende, en particular, aumentar la resiliencia de los ciudadanos, las empresas y las entidades que operan en sectores críticos y muy críticos frente a las crecientes amenazas a la ciberseguridad, que pueden tener repercusiones sociales y económicas devastadoras. Ello se logrará invirtiendo en herramientas en apoyo de una detección de las amenazas e incidentes de ciberseguridad y una respuesta a ellos más rápidas, y ayudará a los Estados miembros a prepararse mejor para los incidentes de ciberseguridad significativos y a gran escala y a responder mejor a ellos. Esto debería contribuir también a que Europa se dotase de capacidades más sólidas en estos ámbitos, en particular en lo que se refiere a la recopilación y el análisis de datos sobre amenazas e incidentes de ciberseguridad.

1.4.4. Indicadores de rendimiento

Precisar los indicadores para hacer un seguimiento de los avances y logros.

Con el fin de promover la solidaridad a escala de la Unión, podrían tenerse en cuenta varios indicadores:

1) Número de infraestructuras o herramientas de ciberseguridad contratadas conjuntamente

2) Número de acciones de apoyo a la preparación y la respuesta ante incidentes de ciberseguridad en el marco del Mecanismo de Ciberemergencia.

1.5. Justificación de la propuesta/iniciativa

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

El Reglamento debería ser de plena aplicación tras su adopción, es decir, a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

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

El marcado carácter transfronterizo de las amenazas a la ciberseguridad en general y el creciente número de riesgos e incidentes con efectos expansivos que traspasan fronteras, sectores y productos hacen que los objetivos de la intervención actual no puedan ser alcanzados eficazmente por los Estados miembros por sí solos y requieran la acción común y la solidaridad a escala de la Unión. La experiencia de la lucha contra las ciberamenazas derivadas de la guerra contra Ucrania, junto con las conclusiones extraídas de un ejercicio de ciberseguridad realizado bajo la Presidencia francesa (EU CyCLES), puso de manifiesto que deben desarrollarse mecanismos concretos de apoyo mutuo, en particular la cooperación con el sector privado, para lograr la solidaridad a escala de la UE. En este contexto, en las Conclusiones del Consejo de 23 de mayo de 2022 sobre el afianzamiento de la posición de la Unión Europea en materia cibernética se insta a la Comisión a que presente una propuesta sobre un nuevo Fondo de Respuesta a Emergencias en materia de Ciberseguridad. El apoyo y las acciones a escala de la Unión para detectar mejor las amenazas a la ciberseguridad y aumentar las capacidades de preparación y respuesta aportan valor añadido, ya que evitan la duplicación de esfuerzos en la Unión y los Estados miembros. Ello daría lugar a una mejor explotación de los activos existentes y a una mayor coordinación e intercambio de información sobre las conclusiones extraídas.

1.5.3. Principales conclusiones extraídas de experiencias similares anteriores

Por lo que respecta a la conciencia situacional y la detección en el contexto del Ciberescudo Europeo, en el marco del programa de trabajo sobre ciberseguridad 2021-2022 del programa Europa Digital, se celebró una convocatoria de manifestaciones de interés para la adquisición conjunta de herramientas e infraestructuras con el fin de establecer COS transfronterizos, y una convocatoria de subvenciones para permitir el desarrollo de capacidades de los COS que están al servicio de organizaciones públicas y privadas.

Por lo que se refiere a la preparación y la respuesta a los incidentes, la Comisión ha establecido un programa a corto plazo para apoyar a los Estados miembros, mediante financiación adicional asignada a la ENISA, con el fin de reforzar inmediatamente la preparación y las capacidades para responder a ciberincidentes graves. Los servicios cubiertos incluyen actividades de preparación, como pruebas de penetración de entidades críticas con el fin de detectar las vulnerabilidades. El programa también refuerza las posibilidades de asistir a los Estados miembros en caso de un incidente grave que afecte a entidades críticas. La ejecución de este programa a corto plazo por parte de la ENISA está en curso y ya ha proporcionado valiosa información pertinente que se ha tenido en cuenta en la preparación del presente Reglamento.

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

La Ley de Cibersolidaridad se basará en las acciones actualmente apoyadas por la Unión y los Estados miembros para mejorar la conciencia situacional y la detección de ciberamenazas, así como para responder a incidentes de ciberseguridad a gran escala y transfronterizos. Además, el instrumento es coherente con otros marcos de gestión de crisis, como el Dispositivo RPIC, la política común de seguridad y defensa, incluidos los equipos de respuesta telemática rápida, y la asistencia prestada por un Estado miembro a otro en el contexto del artículo 42, apartado 7, del Tratado de la Unión Europea. La nueva propuesta también complementaría y apoyaría las estructuras desarrolladas en el marco de otros instrumentos de ciberseguridad, como la Directiva (UE) 2022/2555 (Directiva SRI 2) o el Reglamento 2019/881 (Reglamento sobre la Ciberseguridad).

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

La gestión de los ámbitos de actuación asignados a la ENISA se ajusta a su actual mandato y funciones generales. Estos ámbitos de actuación pueden requerir perfiles específicos o nuevas asignaciones, pero estos no podrían ser absorbidos por los recursos existentes de la ENISA y resolverse mediante la reasignación o la vinculación de varias asignaciones. La ENISA está ejecutando actualmente un programa a corto plazo que fue creado en 2022 por la Comisión para reforzar inmediatamente la preparación y las capacidades de respuesta ante ciberincidentes graves. Los servicios cubiertos incluyen la posibilidad de asistir a los Estados miembros en caso de un incidente grave que afecte a entidades críticas. La ejecución de este programa a corto plazo por parte de la ENISA está en curso y ya ha proporcionado valiosa información pertinente que se ha tenido en cuenta en la preparación del presente Reglamento. Los recursos asignados al programa a corto plazo podrían utilizarse también en el contexto del presente Reglamento.

1.6. Duración e incidencia financiera de la propuesta/iniciativa

☒ **Duración limitada**

– ☒ en vigor desde la fecha de adopción de la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo al refuerzo de la solidaridad y las capacidades en la Unión a fin de detectar amenazas e incidentes de ciberseguridad, prepararse para ellos y responder a ellos («Ley de Cibersolidaridad»)

– ☒ incidencia financiera desde 2023 hasta 2027 para los créditos de compromiso y desde 2023 hasta 2031 para los créditos de pago[34].

☐ **Duración ilimitada**

– Ejecución: fase de puesta en marcha desde AAAA hasta AAAA

– y pleno funcionamiento a partir de la última fecha.

1.7. Método(s) de ejecución presupuestaria previsto(s)[35]

☒ **Gestión directa** por la Comisión

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

– ☐ por las agencias ejecutivas.

☐ **Gestión compartida** con los Estados miembros

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

– ☐ terceros países o los organismos que estos hayan designado;

– ☐ organizaciones internacionales y sus agencias (especificar);

– ☐ el BEI y el Fondo Europeo de Inversiones;

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

– ☐ organismos de Derecho público;

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

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

– ☐ organismos o personas a quienes se haya encomendado la ejecución de acciones específicas en el marco de la PESC, de conformidad con el título V del TUE, y que estén identificadas en el acto de base correspondiente.

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

Observaciones

---

34 Las acciones recogidas en la Ley deben contar con el apoyo del próximo marco financiero plurianual.

35 Los detalles sobre los métodos de ejecución presupuestaria y las referencias al Reglamento Financiero pueden consultarse en el sitio BUDGpedia: https://myintracomm.ec.europa.eu/corp/budget/financial-rules/budget-implementation/Pages/implementation-methods.aspx.

Las acciones relacionadas con el Ciberescudo Europeo serán ejecutadas por el ECCC. Hasta que el ECCC tenga capacidad para ejecutar su propio presupuesto, la Comisión Europea ejecutará las acciones en régimen de gestión directa en nombre del ECCC. El ECCC podrá seleccionar entidades sobre la base de convocatorias de manifestaciones de interés para participar en la adquisición conjunta de herramientas. El ECCC podrá conceder subvenciones para el funcionamiento de estas herramientas.

Además, el ECCC podrá conceder subvenciones para acciones de preparación en el marco del Mecanismo de Emergencia en materia de Ciberseguridad.

La Comisión tendrá la responsabilidad general de la ejecución de la Reserva de Ciberseguridad de la UE. La Comisión podrá encomendar, total o parcialmente, mediante acuerdos de contribución, el funcionamiento y la administración de la Reserva de Ciberseguridad de la UE a la ENISA. Los cometidos asignados en virtud del presente Reglamento a la ENISA están en consonancia con su mandato actual. Entre ellos se incluyen: i) apoyar al Grupo de Cooperación SRI en el desarrollo de las acciones de preparación con arreglo a las evaluaciones de riesgos; ii) apoyar a la Comisión en el establecimiento y la supervisión de la ejecución de la Reserva de Ciberseguridad de la UE, incluida la recepción y la tramitación de las solicitudes de apoyo; iii) elaborar plantillas para facilitar la presentación de las solicitudes de apoyo y los acuerdos específicos que deben celebrarse entre el proveedor de servicios y el usuario al que se preste el apoyo en el marco de la Reserva de Ciberseguridad de la UE; iv) revisar y evaluar las amenazas, vulnerabilidades y medidas de mitigación con respecto a incidentes de ciberseguridad significativos o a gran escala específicos y preparar los informes al respecto.

Se calcula que el desempeño de todos estos cometidos requiere unos siete ETC de los recursos existentes de la ENISA, sobre la base de los conocimientos especializados y del trabajo preparatorio que realiza actualmente la ENISA en el marco del proyecto piloto de apoyo de emergencia para la preparación y la respuesta a incidentes.

2. MEDIDAS DE GESTIÓN

2.1. Normas en materia de seguimiento e informes

Especificar la frecuencia y las condiciones de dichas medidas.

La Comisión hará un seguimiento de la ejecución, la aplicación y el cumplimiento de estas nuevas disposiciones con el fin de evaluar su eficacia. La Comisión presentará un informe sobre la evaluación y examen del presente Reglamento al Parlamento Europeo y al Consejo a más tardar cuatro años después de su fecha de aplicación.

2.2. Sistema(s) de gestión y de control

2.2.1. Justificación del / de los modo(s) de gestión, del / de los mecanismo(s) de aplicación de la financiación, de las modalidades de pago y de la estrategia de control propuestos

El Reglamento introduce un marco para ejecutar la financiación de la UE con vistas a aumentar la resiliencia en materia de ciberseguridad a través de acciones que mejoren las capacidades de detección, respuesta y recuperación en caso de incidentes de ciberseguridad significativos y a gran escala. Las unidades de la DG CNECT encargadas del ámbito político gestionarán la aplicación de la Directiva.

Para que puedan hacer frente a las nuevas tareas, es necesario dotar adecuadamente a los servicios de la Comisión. Se calcula que la aplicación del nuevo Reglamento requiere seis ETC (tres AD y tres AC) para desempeñar las siguientes tareas:

- determinar las acciones de preparación en función de las evaluaciones de riesgos;
- garantizar la interoperabilidad entre las plataformas de COS transfronterizos;
- elaborar los posibles actos de ejecución (dos para los COS y dos para el Mecanismo de Emergencia en materia de Ciberseguridad);
- gestionar los acuerdos de alojamiento y uso para los COS;
- establecer y gestionar la Reserva de Ciberseguridad de la UE, directamente o a través de un acuerdo de contribución a la ENISA. En caso de acuerdo de contribución a la ENISA, elaborar el acuerdo de contribución para las tareas asignadas a la ENISA y supervisar su aplicación;
- participar en los grupos de consulta convocados por la ENISA para revisar y evaluar los incidentes de ciberseguridad significativos y a gran escala y preparar los informes.

2.2.2. Información relativa a los riesgos identificados y al /a los sistema(s) de control interno establecidos para atenuarlos

Por lo que respecta al Ciberescudo Europeo, uno de los riesgos detectados es que los Estados miembros no compartan una cantidad suficiente de información pertinente sobre ciberamenazas ni dentro de las plataformas de COS transfronterizos, ni entre las plataformas transfronterizas y otras entidades pertinentes a escala de la UE. Con el fin de mitigar estos riesgos, la asignación de fondos irá precedida de una convocatoria de manifestaciones de interés en la que los Estados miembros se comprometan a compartir una determinada cantidad de información con el nivel de la UE. Este compromiso se formalizará, entonces, a través de un acuerdo de

alojamiento y uso, que otorgará al ECCC la facultad de llevar a cabo auditorías para garantizar que las herramientas e infraestructuras adquiridas conjuntamente se utilicen de conformidad con el acuerdo. Los compromisos relativos a un alto nivel de intercambio de información dentro de los COS transfronterizos se formalizarán en un acuerdo de consorcio.

Por lo que respecta al Mecanismo de Ciberemergencia, uno de los riesgos detectados es que los usuarios que participan en el mecanismo no tomen medidas suficientes para garantizar la preparación frente a los ciberataques. Por este motivo, para poder recibir apoyo de la Reserva de Ciberseguridad de la UE, los usuarios están obligados a tomar tales medidas de preparación. Al presentar las solicitudes de apoyo a la Reserva de Ciberseguridad de la UE, los usuarios deben explicar qué medidas se han tomado ya para responder al incidente, las cuales se tendrán en cuenta durante la evaluación de las solicitudes presentadas a la Reserva de Ciberseguridad de la UE.

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

Dado que las normas de participación en el programa Europa Digital aplicables al apoyo en virtud de la Ley de Cibersolidaridad son similares a las que utilizará la Comisión en sus programas de trabajo, y que el perfil de riesgo de los beneficiarios es similar al de los beneficiarios de programas en régimen de gestión directa, cabe esperar que el margen de error sea similar al previsto por la Comisión para el programa Europa Digital, es decir, que es razonable asegurar que el riesgo de error a lo largo del período de gasto plurianual irá del 2 al 5 % anual, con el objetivo último de alcanzar un porcentaje de error residual lo más cercano posible al 2 % al cierre de los programas plurianuales, una vez que se hayan tenido en cuenta el impacto económico de todas las auditorías y las medidas de corrección y recuperación.

2.3. Medidas de prevención del fraude y de las irregularidades

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

En el caso del Ciberescudo Europeo, el ECCC estará facultado para auditar, sobre la base del acceso a la información y de los controles sobre el terreno, las herramientas e infraestructuras contratadas conjuntamente, de conformidad con el acuerdo de alojamiento y uso que deberán firmar el consorcio anfitrión y el ECCC.

Las medidas existentes de prevención del fraude aplicables a las instituciones, órganos y organismos de la Unión cubrirán los créditos adicionales necesarios para el presente Reglamento.

3. INCIDENCIA FINANCIERA ESTIMADA DE LA PROPUESTA/INICIATIVA

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

- Líneas presupuestarias existentes

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

Rúbrica del marco financiero plurianual	Línea presupuestaria	Tipo de gasto	Contribución			
	Número	CD/CND[36].	de países de la AELC[37]	de países candidatos y candidatos potenciales [38]	de otros terceros países	otros ingresos afectados
1	02 04 01 10 – programa Europa Digital – Ciberseguridad	CD	SÍ	SÍ	NO	NO
1	02 04 01 11 – programa Europa Digital – Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad	CD	SÍ	SÍ	NO	NO
1	02 04 03 – Programa Europa Digital – Inteligencia artificial	CD	SÍ	SÍ	NO	NO
1	02 04 04 – programa Europa Digital – Capacidades	CD	SÍ	SÍ	NO	NO
1	02 01 30 – Gasto de apoyo para el programa Europa Digital	CND	SÍ	SÍ	NO	NO

[36] CD = créditos disociados / CND = créditos no disociados.
[37] AELC: Asociación Europea de Libre Comercio.
[38] Países candidatos y, en su caso, países candidatos potenciales.

3.2. Incidencia financiera estimada de la propuesta en los créditos

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

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

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

En millones EUR (al tercer decimal)

Rúbrica del marco financiero plurianual	Número	1 **Mercado único, innovación y economía digital**

La propuesta no aumentará el nivel total de créditos de compromiso en el marco del programa Europa Digital. De hecho, la contribución a esta iniciativa es una redistribución de los créditos de compromiso procedentes del OE2 y del OE4 para reforzar el presupuesto del OE3 y del ECCC. Cualquier aumento de los créditos de compromiso en el marco del programa Europa Digital derivado de una revisión del MFP podría utilizarse a efectos de esta iniciativa.

DG CONNECT			Año **2025**	Año **2026**	Año **2027**	Año **2028+**	Insertar tantos años como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6)			**TOTAL**
○ Créditos de operaciones										
Línea presupuestaria[39] 02.040110 (redistribución de 02.0403 y 02.0404)	Créditos de compromiso	(1a)	15,000	15,000	6,000	p.m.				**36,000**
	Créditos de pago	(2a)	15,000	15,000	6,000					**36,000**
Línea presupuestaria 02.040111.02 (redistribución de 02.0403 y 02.0404)	Créditos de compromiso	(1b)	13,000	23,000	28,000	p.m.				**64,000**
	Créditos de pago	(2b)	8,450	18,200	25,250	12,100				**64,000**
Créditos de carácter administrativo financiados mediante la dotación de programas específicos[40]										

[39] Según la nomenclatura presupuestaria oficial.

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

Línea presupuestaria 02.0130		(3)	0,150	0,150	0,150	p.m.				0,450
TOTAL de los créditos para la DG CONNECT	Créditos de compromiso	=1a+1b +3	**28,150**	**38,150**	**34,150**	**p.m.**				**100,450**
	Créditos de pago	=2a+2b +3	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

○ TOTAL de los créditos de operaciones	Créditos de compromiso	(4)	28,000	38,000	34,000	p.m.				**100,000**
	Créditos de pago	(5)	23,450	33,200	31,250	12,100				**100,000**
○ TOTAL de los créditos de carácter administrativo financiados mediante la dotación de programas específicos		(6)	0,150	0,150	0,150	p.m.				**0,450**
TOTAL de los créditos correspondientes a la RÚBRICA 1 del marco financiero plurianual	Créditos de compromiso	=4+ 6	**28,150**	**38,150**	**34,150**	**p.m.**				**100,450**
	Créditos de pago	=5+ 6	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

Si la propuesta/iniciativa afecta a más de una línea operativa, repetir la sección anterior:

○ TOTAL de los créditos de operaciones (todas las líneas operativas)	Créditos de compromiso	(4)	28,000	38,000	34,000	p.m.				**100,000**
	Créditos de pago	(5)	23,450	33,200	31,250	12,100				**100,000**
TOTAL de los créditos de carácter administrativo financiados mediante la dotación de programas específicos (todas las líneas operativas)		(6)	0,150	0,150	0,150					**0,450**
TOTAL de los créditos correspondientes a las RÚBRICAS 1 a 6 del marco financiero plurianual	Créditos de compromiso	=4+ 6	**28,150**	**38,150**	**34,150**	**p.m.**				**100,450**
	Créditos de pago	=5+ 6	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

(Importe de referencia)										

Rúbrica del marco financiero plurianual	7	«Gastos administrativos»

Esta sección debe rellenarse mediante «los datos presupuestarios de carácter administrativo» introducidos primeramente en el anexo de la Ficha de Financiación Legislativa (anexo 5 de la Decisión de la Comisión sobre las normas internas de ejecución de la sección de la Comisión del presupuesto general de la Unión Europea), que se carga en DECIDE a efectos de consulta entre servicios.

En millones EUR (al tercer decimal)

		Año **2025**	Año **2026**	Año **2027**	Año **2028+**	Insertar tantos años como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6)			**TOTAL**
DG: CONNECT									
○ Recursos humanos		0,786	0,786	0,786	p.m.				**2,358**
○ Otros gastos administrativos		0,035	0,035	0,035	p.m.				**0,105**
TOTAL PARA LA DG CONNECT	Créditos	**0,821**	**0,821**	**0,821**					**2,463**

TOTAL de los créditos correspondientes a la RÚBRICA 7 del marco financiero plurianual	(Total de los créditos de compromiso = total de los créditos de pago)	**0,821**	**0,821**	**0,821**					**2,463**

En millones EUR (al tercer decimal)

		Año **2025**	Año **2026**	Año **2027**	Año **2028+**	Insertar tantos años como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6)			**TOTAL**
TOTAL de los créditos correspondientes a las RÚBRICAS 1 a 7 del marco financiero plurianual	Créditos de compromiso	**28,971**	**38,971**	**34,971**	**p.m.**				**102,913**
	Créditos de pago	**24,421**	**34,171**	**32,221**	**12,100**				**102,913**

3.2.2. Resultados estimados financiados con créditos de operaciones

Créditos de compromiso en millones EUR (al tercer decimal)

Indicar los objetivos y los resultados ⇩			Año **N**		Año **N+1**		Año **N+2**		Año **N+3**		Insertar tantos años como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6)						**TOTAL**	
	RESULTADOS																	
	Tipo[41]	Coste medio	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	N.º	Coste	Número total	Coste total
OBJETIVO ESPECÍFICO N.º 1[42]…																		
- Resultado																		
- Resultado																		
- Resultado																		
Subtotal del objetivo específico n.º 1																		
OBJETIVO ESPECÍFICO N.º 2 ...																		
- Resultado																		
Subtotal del objetivo específico n.º 2																		
TOTALES																		

41 Los resultados son los productos y servicios que van a suministrarse (por ejemplo, número de intercambios de estudiantes financiados, número de kilómetros de carreteras construidos, etc.).

42 Según se describe en el punto 1.4.2. «Objetivo(s) específico(s)…».

3.2.3. Resumen de la incidencia estimada en los créditos administrativos

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

– ☒ La propuesta/iniciativa exige la utilización de créditos administrativos, tal como se explica a continuación:

En millones EUR (al tercer decimal)

	Año 2025	Año 2026	Año 2027	Año N+3	Insertar tantos años como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6)			**TOTAL**
RÚBRICA 7 del marco financiero plurianual								
Recursos humanos	0,786	0,786	0,786					**2,358**
Otros gastos administrativos	0,035	0,035	0,035					**0,105**
Subtotal de la RÚBRICA 7 del marco financiero plurianual	**0,821**	**0,821**	**0,821**					**2,463**
Al margen de la RÚBRICA 7[43] del marco financiero plurianual								
Recursos humanos								
Otros gastos administrativos	0,150	0,150	0,150					**0,450**
Subtotal al margen de la RÚBRICA 7 del marco financiero plurianual	**0,150**	**0,150**	**0,150**					**0,450**
TOTAL	**0,971**	**0,971**	**0,971**					**2,913**

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

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

3.2.3.1. Necesidades estimadas de recursos humanos

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

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

Estimación que debe expresarse en unidades de equivalente a jornada completa

		Año **2025**	Año **2026**	Año 2027	Año **N+3**	Insertar tantos años como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6)		
o Empleos de plantilla (funcionarios y personal temporal)								
20 01 02 01 (Sede y Oficinas de Representación de la Comisión)		3	3	3				
20 01 02 03 (Delegaciones)								
01 01 01 01 (Investigación indirecta)								
01 01 01 11 (Investigación directa)								
Otras líneas presupuestarias (especificar)								
o Personal externo (en unidades de equivalente a jornada completa: EJC)[44]								
20 02 01 (AC, ENCS, INT de la «dotación global»)		3	3	3				
20 02 03 (AC, AL, ENCS, INT y JPD en las Delegaciones)								
XX 01 xx **yy zz** [45]	- en la sede							
	- en las Delegaciones							
01 01 01 02 (AC, ENCS, INT - investigación indirecta)								
01 01 01 12 (AC, INT, ENCS - investigación directa)								
Otras líneas presupuestarias (especificar)								
TOTAL		**6**	**6**	**6**				

XX es la política o título presupuestario en cuestión.

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

Descripción de las tareas que deben llevarse a cabo:

Funcionarios y agentes temporales	- determinar las acciones de preparación en función de las evaluaciones de riesgos (artículo 11); - elaborar los posibles actos de ejecución (dos para los COS y dos para el Mecanismo de Emergencia en materia de Ciberseguridad); - gestionar los acuerdos de alojamiento y uso para los COS; - establecer y gestionar la Reserva de Ciberseguridad de la UE, directamente o a través de un acuerdo de contribución a la ENISA.

44 AC = agente contractual; AL = agente local; ENCS = experto nacional en comisión de servicios; INT = personal de empresas de trabajo temporal («intérimaires»); JPD = joven profesional en delegación.

45 Subtecho para el personal externo con cargo a créditos de operaciones (antiguas líneas «BA»).

Personal externo	Bajo la supervisión de un funcionario, - determinar las acciones de preparación en función de las evaluaciones de riesgos (artículo 11); - elaborar los posibles actos de ejecución (dos para los COS y dos para el Mecanismo de Emergencia en materia de Ciberseguridad); - gestionar los acuerdos de alojamiento y uso para los COS; - establecer y gestionar la Reserva de Ciberseguridad de la UE, directamente o a través de un acuerdo de contribución a la ENISA.

3.2.4. *Compatibilidad con el marco financiero plurianual vigente*

La propuesta/iniciativa:

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

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

	2023	2024	2025	2026	2027	total
SO1	16.232.897	20.528.765	17.406.899	16.223.464	10.022.366	80.414.391
SO2 initial	226.316.819	295.067.000	195.649.000	221.809.000	246.608.000	1.185.449.819
To CYBER initiative			18.000.000	28.000.000	19.000.000	65.000.000
NEW SO2	**226.316.819**	**295.067.000**	**177.649.000**	**193.809.000**	**227.608.000**	**1.120.449.819**
SO3 DB 24	24.361.553	35.596.172	3.638.000	3.638.000	11.175.000	78.408.725
Fom SO2-SO4			15.000.000	15.000.000	6.000.000	36.000.000
New SO3	**24.361.553**	**35.596.172**	**18.638.000**	**18.638.000**	**17.175.000**	**114.408.725**
ECCC initial	176.222.303	208.374.879	104.228.130	90.704.986	84.851.497	664.381.795
From SO2-SO4			13.000.000	23.000.000	28.000.000	64.000.000
New ECCC	**176.222.303**	**208.374.879**	**117.228.130**	**113.704.986**	**112.851.497**	**728.381.795**
SO4 initial	66.902.708	64.892.032	56.577.977	70.477.245	72.107.201	330.957.163
To CYBER initiative			10.000.000	10.000.000	15.000.000	35.000.000
NEW SO4	**66.902.708**	**64.892.032**	**46.577.977**	**60.477.245**	**57.107.201**	**295.957.163**

– [ ] requiere el uso de los márgenes no asignados con cargo a la rúbrica correspondiente del MFP o el uso de instrumentos especiales tal como se define en el Reglamento del MFP.

Explicar qué es lo que se requiere, precisando las rúbricas y líneas presupuestarias afectadas, los importes correspondientes y los instrumentos propuestos que van a usarse.

– [ ] requiere una revisión del MFP.

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

3.2.5. *Contribución de terceros*

La propuesta/iniciativa:

– [X] no prevé la cofinanciación por terceros

– [ ] prevé la cofinanciación por terceros que se estima a continuación:

Créditos en millones EUR (al tercer decimal)

	Año **N**[46]	Año **N+1**	Año **N+2**	Año **N+3**	Insertar tantos años como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6)	Total

[46] El año N es el año de comienzo de la ejecución de la propuesta/iniciativa. Sustitúyase «N» por el primer año de aplicación prevista (por ejemplo: 2021). Lo mismo para los años siguientes.

Especificar el organismo de cofinanciación								
TOTAL de los créditos cofinanciados								

3.3. Incidencia estimada en los ingresos

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

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

– ☐ en los recursos propios

– ☐ en otros ingresos

– indicar si los ingresos se asignan a líneas de gasto ☐

En millones EUR (al tercer decimal)

Línea presupuestaria de ingresos:	Créditos disponibles para el ejercicio presupuestario en curso	Incidencia de la propuesta/iniciativa[47]						
		Año **N**	Año **N+1**	Año **N+2**	Año **N+3**	Insertar tantos años como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6)		
Artículo …….								

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

[…]

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

[…]

[47] Por lo que se refiere a los recursos propios tradicionales (derechos de aduana, cotizaciones sobre el azúcar), los importes indicados deben ser importes netos, es decir, importes brutos tras la deducción del 20 % de los gastos de recaudación.