EUROPEO
COMISIÓN

Estrasburgo, 18.4.2023
COM(2023) 209 final

2023/0109 (COD)

Propuesta para un

REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO

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

MEMORANDO EXPLICATIVO

1. CONTEXTO DE LA PROPUESTA

• Razones y objetivos de la propuesta

Esta exposición de motivos acompaña a la propuesta de Ley de Cibersolidaridad. El uso y la dependencia de las tecnologías de la información y la comunicación se han convertido en aspectos fundamentales en todos los sectores de la actividad económica, ya que nuestras administraciones públicas, empresas y ciudadanos están más interconectados e interdependientes entre sectores y fronteras que nunca. Esta mayor adopción de tecnologías digitales aumenta la exposición a incidentes de seguridad cibernética y sus impactos potenciales. Al mismo tiempo, los Estados miembros se enfrentan a riesgos de ciberseguridad cada vez mayores y a un panorama general de amenazas complejo, con un claro riesgo de que los ciberincidentes se propaguen rápidamente de un Estado miembro a otros.

Además, las operaciones cibernéticas están cada vez más integradas en estrategias híbridas y de guerra, con efectos significativos en el objetivo. En particular, la agresión militar de Rusia contra Ucrania estuvo precedida y está acompañada por una estrategia de operaciones cibernéticas hostiles, que es un cambio de juego para la percepción y evaluación de la preparación colectiva de la gestión de crisis de ciberseguridad de la UE y un llamado a la acción urgente. La amenaza de un posible incidente a gran escala que provoque trastornos y daños significativos en infraestructuras críticas exige una mayor preparación en todos los niveles del ecosistema de ciberseguridad de la UE. Esa amenaza va más allá de la agresión militar de Rusia contra Ucrania e incluye amenazas cibernéticas continuas de actores estatales y no estatales, que probablemente persistan, dada la multiplicidad de actores criminales y hacktivistas alineados con el estado involucrados en las tensiones geopolíticas actuales. En los últimos años, la cantidad de ciberataques ha aumentado drásticamente, incluidos los ataques a la cadena de suministro con el objetivo de ciberespionaje, ransomware o interrupción. En 2020, el ataque a la cadena de suministro de SolarWinds afectó a más de 18 000 organizaciones en todo el mundo, incluidas agencias gubernamentales y empresas importantes. Los incidentes significativos de ciberseguridad pueden ser demasiado perjudiciales para que uno o varios Estados miembros afectados los aborden solos. Por ese motivo, se requiere una solidaridad reforzada a nivel de la Unión para detectar, prepararse y responder mejor a las amenazas e incidentes de ciberseguridad.

En cuanto a la detección de ciberamenazas e incidentes, existe una necesidad urgente de incrementar el intercambio de información y mejorar nuestras capacidades colectivas para reducir drásticamente el tiempo necesario para detectar las ciberamenazas, antes de que puedan causar daños y costes a gran escala[1] .
Si bien muchas amenazas e incidentes de ciberseguridad tienen una dimensión transfronteriza potencial, debido a la interconexión de las infraestructuras digitales, el intercambio de información relevante entre los Estados miembros sigue siendo limitado. La creación de una red de Centros de Operaciones de Seguridad (SOC) transfronterizos para mejorar las capacidades de detección y respuesta tiene como objetivo ayudar a abordar este problema.

[1] Según un informe del Ponemon Institute e IBM Security, el tiempo promedio para identificar una brecha en 2022 fue de 207 días, con 70 días adicionales para contenerla. Al mismo tiempo, en 2022, las brechas de datos con un ciclo de vida superior a 200 días tuvieron un coste medio de 4,86 millones de euros, frente a los 3,74 millones de euros de menos de 200 días. ('Costo de una violación de datos 2022", https://www.ibm.com/reports/data-breach)

En lo que respecta a la preparación y respuesta a incidentes de ciberseguridad, actualmente existe un apoyo limitado a nivel de la Unión y solidaridad entre los Estados miembros. Las Conclusiones del Consejo de octubre de 2021 destacaron la necesidad de abordar estas lagunas, al pedir a la Comisión que presente una propuesta sobre un nuevo Fondo de Respuesta de Emergencia para la Ciberseguridad2 .

Este Reglamento también implementa la Estrategia de Ciberseguridad de la UE adoptada en diciembre de 20203 que anunció la creación de un Escudo Cibernético Europeo, reforzando las capacidades de detección de ciberamenazas e intercambio de información en la Unión Europea a través de una federación de SOC nacionales y transfronterizos.

Este Reglamento se basa en los primeros pasos ya desarrollados en estrecha colaboración con las principales partes interesadas y apoyado por el Programa Europa Digital (DEP). En particular, sobre los SOC, se realizó una convocatoria de expresión de interés para adquirir conjuntamente herramientas e infraestructura para establecer SOC transfronterizos, y una convocatoria de subvenciones para permitir el desarrollo de capacidades de los SOC que prestan servicios a organizaciones públicas y privadas, bajo el programa de trabajo de seguridad cibernética 2021 del DEP. -2022. En lo que respecta a la preparación y respuesta a incidentes, la Comisión ha establecido un programa a corto plazo para apoyar a los Estados miembros, mediante financiación adicional asignada a la Agencia de Ciberseguridad de la Unión Europea (ENISA), con el fin de reforzar inmediatamente la preparación y las capacidades para responder a los principales ciberataques. incidentes Ambas acciones se han preparado en estrecha coordinación con los Estados miembros. Este Reglamento aborda las deficiencias e integra los conocimientos de esas acciones.

Por último, esta propuesta cumple el compromiso, en consonancia con la Comunicación conjunta sobre ciberdefensa4 adoptada el 10 de noviembre, de preparar una propuesta de Iniciativa de solidaridad cibernética de la UE con los siguientes objetivos: reforzar las capacidades comunes de detección, conciencia situacional y respuesta de la UE, para construir una reserva de ciberseguridad a nivel de la UE con servicios de proveedores privados confiables y para respaldar las pruebas de entidades críticas.

En este contexto, la Comisión propone la presente Ley de cibersolidaridad para reforzar la solidaridad a nivel de la Unión con el fin de detectar, prepararse y responder mejor a las amenazas e incidentes de ciberseguridad a través de los siguientes objetivos específicos:

- reforzar la detección común de la UE y la conciencia situacional de las ciberamenazas e incidentes, y así contribuir a la soberanía tecnológica europea en el ámbito de la ciberseguridad;

- reforzar la preparación de las entidades críticas en toda la UE y fortalecer la solidaridad mediante el desarrollo de capacidades de respuesta comunes frente a incidentes de ciberseguridad significativos o a gran escala, incluso poniendo a disposición de terceros países apoyo de respuesta a incidentes. asociado a DEP; –

2 Conclusiones del Consejo sobre el desarrollo de la postura cibernética de la Unión Europea aprobadas por el Consejo en su reunión del 23 de mayo de
3 2022 (9364/22 Comunicación conjunta al Parlamento Europeo y al Consejo, The EU's Cybersecurity Strategy for the Digital Decade, JOIN202018 final.
4 Comunicación conjunta al Parlamento Europeo y al Consejo, Política de la UE en materia de ciberdefensa, JOIN(2022) 49 final.

- mejorar la resiliencia de la Unión y contribuir a una respuesta eficaz mediante la revisión y evaluación de incidentes significativos o de gran escala, incluida la extracción de lecciones aprendidas y, en su caso, recomendaciones.

Estos objetivos se implementarán a través de las siguientes acciones:

- El despliegue de una infraestructura paneuropea de SOC (European Cyber Shield) para construir y mejorar las capacidades comunes de detección y conciencia situacional.
- La creación de un Mecanismo de emergencia cibernética para ayudar a los Estados miembros a prepararse, responder y recuperarse inmediatamente de incidentes de ciberseguridad significativos y de gran escala. El apoyo para la respuesta a incidentes también se pondrá a disposición de las instituciones, organismos, oficinas y agencias europeas de la Unión (EUIBA).
- El establecimiento de un Mecanismo Europeo de Revisión de Incidentes de Ciberseguridad para revisar y evaluar incidentes específicos significativos o de gran escala.

El Escudo Cibernético Europeo y el Mecanismo de Emergencia Cibernética contarán con el apoyo financiero del DEP, que este instrumento legislativo modificará para establecer las acciones mencionadas, proporcionar apoyo financiero para su desarrollo y aclarar las condiciones para beneficiarse de la financiación. apoyo.

- Coherencia con las disposiciones de política existentes en el área de política

El marco de la UE comprende varias legislaciones ya en vigor o propuestas a nivel 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 incidentes y crisis de ciberseguridad a gran escala, en particular la Directiva sobre medidas para un alto nivel de protección común. nivel de seguridad de las redes y los sistemas de información en toda la Unión (NIS2)[5] , la Ley de ciberseguridad[6], la Directiva sobre ataques contra los sistemas de información[7], la Recomendación de la Comisión (UE) 2017/1584 sobre la respuesta coordinada a incidentes y crisis de ciberseguridad a gran escala[8] .

Las acciones propuestas bajo la Ley de Solidaridad Cibernética cubren la conciencia situacional, el intercambio de información, así como el apoyo para la preparación y respuesta a incidentes cibernéticos. Estas acciones son coherentes con los objetivos del marco normativo vigente a nivel de la Unión y los respaldan, en particular en virtud de la Directiva (UE) 2022/2555 («la Directiva NIS2»). La Ley de Solidaridad Cibernética se basará y apoyará especialmente la cooperación operativa existente en materia de ciberseguridad

[5] Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, sobre medidas para un alto 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 NIS 2).

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

[7] Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, sobre 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 sobre requisitos de ciberseguridad horizontal para productos con elementos digitales y por el que se modifica el Reglamento (UE) 2019/1020, COM/2022/454 final.

y marcos de gestión de crisis, en particular, la red europea de organizaciones de enlace de cibercrisis (EU-CYCLONe) y la red de equipos de respuesta a incidentes de seguridad informática (CSIRT).

Las plataformas transfronterizas de SOC deben constituir una nueva capacidad que sea complementaria a la red de CSIRT, al agrupar y compartir datos sobre amenazas a la seguridad cibernética de entidades públicas y privadas, mejorando el valor de dichos datos a través de análisis de expertos y herramientas de última generación, y contribuir al desarrollo de las capacidades y la soberanía tecnológica de la Unión.

Por último, esta propuesta es coherente con la Recomendación del Consejo sobre un enfoque coordinado a escala de la Unión para reforzar la resiliencia de las infraestructuras críticas9 que invita a los Estados miembros a adoptar medidas urgentes y eficaces y a cooperar leal, eficiente, solidaria y coordinadamente con entre sí, la Comisión y otras autoridades públicas pertinentes, así como las entidades interesadas, para mejorar la resiliencia de las infraestructuras críticas utilizadas para prestar servicios esenciales en el mercado interior.

- Coherencia con otras políticas de la Unión

La propuesta es consistente con otros mecanismos y protocolos de emergencia de crisis, como el Mecanismo Político Integrado de Respuesta a Crisis (IPCR). La Ley de Solidaridad Cibernética complementará estos marcos y protocolos de gestión de crisis al brindar apoyo dedicado para la preparación y respuesta a incidentes de ciberseguridad. 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), incluso a través de la Caja de herramientas de ciberdiplomacia de la UE. La propuesta complementará las acciones implementadas en el contexto del artículo 42, apartado 7, del Tratado de la Unión Europea o en 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)10establecido en diciembre de 2013 y completado con una nueva legislación adoptada en mayo de 202111, que refuerza los pilares de prevención, preparación y respuesta del UCPM y dota a la UE de capacidades adicionales para responder a nuevos riesgos en Europa y el mundo e impulsa la reserva rescEU.

---

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

10 Decisión nº 1313/2013/UE del Parlamento Europeo y del Consejo de 17 de diciembre de 2013 sobre 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).

2. BASE JURÍDICA, SUBSIDIARIEDAD Y PROPORCIONALIDAD

- Base legal

La base jurídica de esta propuesta es 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 TFUE establece que la Unión y los Estados miembros velarán por que se den las condiciones necesarias para la competitividad de la industria de la Unión. Este Reglamento tiene como objetivo fortalecer la posición competitiva de la industria y los sectores de servicios en Europa en la economía digitalizada y apoyar su transformación digital, reforzando el nivel de ciberseguridad en el Mercado Único Digital.
En particular, tiene como objetivo aumentar la resiliencia de los ciudadanos, empresas y entidades que operan en sectores críticos y altamente críticos frente a las crecientes amenazas a la ciberseguridad, que pueden tener impactos sociales y económicos devastadores.

La propuesta también se basa en el artículo 322, apartado 1, letra a), del TFUE porque contiene normas de prórroga específicas 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 la naturaleza impredecible, excepcional y específica del panorama de la ciberseguridad y las ciberamenazas, el Mecanismo de Emergencia para la Ciberseguridad debe beneficiarse de un cierto grado de flexibilidad en relación con la gestión presupuestaria y, en particular, permitiendo compromisos no utilizados y los créditos de pago para acciones que persigan los objetivos establecidos en el Reglamento se prorroguen automáticamente al ejercicio siguiente. Dado que esta nueva regla plantea problemas con el Reglamento Financiero, este asunto podría abordarse en el contexto de las negociaciones actuales de la refundición del Reglamento Financiero.

- Subsidiariedad (por competencia no exclusiva)

La fuerte naturaleza transfronteriza de las amenazas a la ciberseguridad y el creciente número de riesgos e incidentes, que tienen efectos indirectos a través de fronteras, sectores y productos, significan que los objetivos de la presente intervención no pueden ser alcanzados de manera efectiva por los Estados miembros por sí solos y requieren acción común y solidaridad a nivel de la Unión.

La experiencia de contrarrestar las ciberamenazas derivadas de la guerra contra Ucrania, junto con las lecciones aprendidas de un ejercicio de ciberseguridad realizado bajo la Presidencia francesa (EU CyCLES), mostró que deben desarrollarse mecanismos concretos de apoyo mutuo, en particular la cooperación con el sector privado. lograr la solidaridad a nivel de la UE. En este contexto, las Conclusiones del Consejo de 23 de mayo de 2022 sobre el desarrollo de la postura cibernética de la Unión Europea piden a la Comisión que presente una propuesta sobre un nuevo Fondo de Respuesta de Emergencia para la Ciberseguridad.

El apoyo y las acciones a nivel de la Unión para detectar mejor las amenazas a la ciberseguridad y aumentar las capacidades de preparación y respuesta proporcionan valor añadido porque evita la duplicación de esfuerzos en la Unión y los Estados miembros. Conduciría a una mejor explotación de los

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).

activos y a una mayor coordinación e intercambio de información sobre las lecciones aprendidas. El Mecanismo de Ciberemergencia también contempla brindar apoyo a terceros países asociados a DEP desde la Reserva de Ciberseguridad de la UE.

El apoyo proporcionado a través de las diversas iniciativas que se establecerán y financiarán a nivel de la Unión complementará y no duplicará las capacidades nacionales en lo que respecta a la detección, el conocimiento de la situación, la preparación y la respuesta a las ciberamenazas e incidentes.

- 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 las responsabilidades de los Estados miembros en materia de seguridad nacional, seguridad pública, prevención, investigación, detección y enjuiciamiento de infracciones penales. Tampoco afectan a las obligaciones legales de las entidades que operan en sectores críticos y altamente críticos de adoptar medidas de ciberseguridad, de acuerdo con la Directiva NIS 2.

Las acciones cubiertas por este Reglamento son complementarias a tales esfuerzos y medidas, al apoyar la creación de infraestructuras para una mejor detección y análisis de amenazas y brindar apoyo para las acciones de preparación y respuesta en caso de incidentes significativos o de gran escala.

- Elección del instrumento

La propuesta adopta la forma de un Reglamento del Parlamento Europeo y del Consejo.
Este es el instrumento legal más adecuado, ya que solo un Reglamento, con sus disposiciones legales directamente aplicables, puede proporcionar el grado de uniformidad necesario para el establecimiento y funcionamiento de un Mecanismo Europeo de Ciberescudo y Ciberemergencia, proporcionando el apoyo de DEP para su establecimiento, así como condiciones claras para el uso y la asignación de este apoyo.

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

- Consultas de partes interesadas

Las acciones de este Reglamento serán apoyadas por el DEP, 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. En lo que respecta a los SOC, la Comisión ha elaborado un documento conceptual sobre el desarrollo de plataformas transfronterizas de SOC y una convocatoria de manifestación de interés en estrecha cooperación con los Estados miembros en el marco del Centro Europeo de Competencia en Ciberseguridad (ECCC). En este contexto, se llevó a cabo una encuesta sobre las capacidades de los SOC nacionales y se discutieron enfoques comunes y requisitos técnicos dentro del grupo de trabajo técnico de la ECCC que reúne a representantes de

Estados miembros. Además, se produjeron intercambios con la industria, en particular a través del grupo de expertos en SOC creado por ENISA y la Organización Europea de Seguridad Cibernética (ECSO).

En segundo lugar, en lo que respecta a la preparación y la respuesta a incidentes, la Comisión ha establecido un programa a corto plazo para apoyar a los Estados miembros, a través de fondos adicionales asignados a ENISA por parte del DEP, para reforzar inmediatamente la preparación y las capacidades para responder a incidentes cibernéticos importantes. Los comentarios de los Estados miembros y de la industria recopilados durante la implementación de este programa a corto plazo ya están proporcionando información valiosa que se ha incorporado a la preparación de la propuesta de Reglamento para abordar las deficiencias identificadas. Este fue un primer paso en línea con las conclusiones del Consejo sobre la postura cibernética que solicita a la Comisión que presente una propuesta para un nuevo Fondo de Respuesta de Emergencia para la Ciberseguridad.

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

- Evaluación de impacto

Debido al carácter urgente de la propuesta, no se llevó a cabo ninguna evaluación de impacto. Las acciones de este Reglamento serán respaldadas por el DEP y están en línea con las establecidas en el Reglamento DEP, que fue objeto de una evaluación de impacto específica. El presente Reglamento no supondrá impactos administrativos o ambientales significativos más allá de los ya evaluados en la evaluación de impacto del Reglamento DEP.

Además, se basa en las primeras acciones desarrolladas en estrecha colaboración con las principales partes interesadas, como se establece anteriormente, y da seguimiento al llamamiento de los Estados miembros para que la Comisión presente una propuesta sobre un nuevo Fondo de Respuesta de Emergencia para la Ciberseguridad para fines del tercer trimestre de 2022. .

Específicamente, con respecto a la conciencia situacional y la detección bajo el Escudo Cibernético Europeo, se realizó una Convocatoria de expresión de interés para adquirir conjuntamente herramientas e infraestructura para establecer SOC transfronterizos, y una convocatoria de subvenciones para permitir el desarrollo de capacidades de SOC al servicio de organizaciones públicas y privadas. bajo el programa de trabajo de ciberseguridad DEP 2021-2022.

En el área de preparación y respuesta a incidentes, como se mencionó anteriormente, la Comisión ha establecido un programa a corto plazo para apoyar a los Estados miembros desde DEP, siendo implementado por ENISA. Los servicios cubiertos incluyen acciones de preparación, como pruebas de penetración de entidades críticas para identificar vulnerabilidades. También fortalece las posibilidades de ayudar a los Estados miembros en caso de un incidente importante que afecte a entidades críticas. La implementación por parte de ENISA de este programa a corto plazo está en marcha y ya ha proporcionado información relevante que se ha tenido en cuenta en la preparación de este Reglamento.

- Derechos fundamentales

Al contribuir a la seguridad de la información digital, esta propuesta contribuirá a proteger el derecho a la libertad y 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 la Carta de los Derechos Fundamentales de la UE. Al proteger a las empresas de los ciberataques económicamente perjudiciales, la propuesta también contribuirá a la libertad de empresa de conformidad con el artículo 16 de la Carta de los Derechos Fundamentales de la UE y al derecho de 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 asistencia 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 con el artículo 36 de la Carta de los Derechos Fundamentales de la UE.

4. IMPLICACIONES PRESUPUESTARIAS

Las acciones de este Reglamento serán apoyadas por fondos bajo el Objetivo Estratégico 'Ciberseguridad' de DEP.

El presupuesto total incluye un incremento de 100 millones de euros que este Reglamento propone reasignar de otros Objetivos Estratégicos de DEP. Esto elevará la nueva cantidad total disponible para acciones de Ciberseguridad bajo DEP a 842,8 millones EUR.

Parte de los 100 millones EUR adicionales reforzarán el presupuesto gestionado por el ECCC para implementar acciones sobre los SOC y la preparación como parte de su(s) programa(s) de trabajo. Además, la financiación adicional servirá para apoyar el establecimiento de la Reserva de Ciberseguridad de la UE.

Complementa el presupuesto ya previsto para acciones similares en los principales DEP y DEP de Ciberseguridad WP del periodo 2023-2027 que podría llevar la cantidad total a 551 millones para 2023-2027, mientras que 115 millones ya se dedicaron en forma de pilotos para 2021 -2022. Incluyendo las contribuciones de los Estados miembros, el presupuesto global podría ascender a 1 109 millones de euros.

En la «Ficha financiera legislativa» que acompaña a esta propuesta se incluye una descripción general de los costes implicados.

5. OTROS ELEMENTOS

- Planes de implementación y arreglos de seguimiento, evaluación y presentación de informes

La Comisión supervisará la implementación, 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 revisión del presente Reglamento al Parlamento Europeo y al Consejo en un plazo de cuatro años a partir de la fecha de su aplicación.

- Explicación detallada de las disposiciones específicas de la propuesta

Objetivos generales, tema y definiciones (Capítulo I)

El capítulo I establece los objetivos del Reglamento para reforzar la solidaridad a nivel de la Unión a fin de detectar, prepararse y responder mejor a las amenazas e incidentes de ciberseguridad y, en particular, reforzar la detección común de la Unión y la conciencia situacional de las amenazas e incidentes cibernéticos, para reforzar la preparación de 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 de gran escala y mejorar la resiliencia de la Unión mediante el examen y la evaluación de incidentes significativos o de gran escala. Este Capítulo también establece las acciones a través de las cuales se lograrán estos objetivos: el despliegue de un Escudo Cibernético Europeo, la creación de un Mecanismo de Emergencia Cibernética y el establecimiento de un Mecanismo de Revisión de Incidentes de Ciberseguridad. También establece las definiciones utilizadas en todo el instrumento.

El Ciberescudo Europeo (Capítulo II)

El Capítulo II establece el Ciberescudo Europeo y expone sus distintos elementos y las condiciones de participación. En primer lugar, anuncia el objetivo general del European Cyber Shield, que es desarrollar capacidades avanzadas para que la Unión detecte, analice y procese datos sobre ciberamenazas e incidentes en la Unión, así como los objetivos operativos específicos.
Especifica que la financiación de la Unión para el Escudo Cibernético Europeo se ejecutará de conformidad con el Reglamento DEP.

Además, el capítulo describe el tipo de entidades que formarán el Escudo Cibernético Europeo.
El escudo consistirá en Centros de Operaciones de Seguridad Nacional ('SOC Nacionales') y Centros de Operaciones de Seguridad Transfronterizos ('SOC Transfronterizos'). Cada Estado miembro participante designará un SOC nacional. Este actuará como punto de referencia y puerta de entrada a otras organizaciones públicas y privadas a nivel nacional para recopilar y analizar información sobre amenazas e incidentes de ciberseguridad y contribuir a un SOC transfronterizo.
Después de una convocatoria de expresión de interés, el ECCC puede seleccionar un SOC nacional para participar en una adquisición conjunta de herramientas e infraestructuras con el ECCC y recibir una subvención para operar las herramientas e infraestructuras. Si un SOC nacional se beneficia del apoyo de la Unión, se comprometerá a solicitar su participación en un SOC transfronterizo en un plazo de dos años.

Los SOC transfronterizos estarán formados por un consorcio de al menos tres Estados miembros, representados por SOC nacionales, que se comprometen a trabajar juntos para coordinar sus actividades de supervisión de ciberdetección y amenazas. Después de una convocatoria inicial de expresión de interés, el ECCC puede seleccionar un consorcio de alojamiento para participar en una adquisición conjunta de herramientas e infraestructuras con el ECCC y recibir una subvención para ejecutar las herramientas e infraestructuras. Los miembros del Consorcio de alojamiento deberán celebrar un acuerdo de consorcio por escrito que establezca sus arreglos internos. Luego, este capítulo detalla los requisitos para compartir información entre los participantes en un SOC transfronterizo, y para compartir información

entre un SOC transfronterizo y otros SOC transfronterizos, así como con las entidades pertinentes de la UE. Los SOC nacionales que participen en un SOC transfronterizo compartirán entre sí información relevante relacionada con las amenazas cibernéticas, y los detalles, incluido el compromiso de compartir una cantidad significativa de datos y las condiciones del mismo, deben definirse en un acuerdo de consorcio. Los SOC transfronterizos garantizarán un alto nivel de interoperabilidad entre ellos. Los SOC transfronterizos también deben celebrar acuerdos de cooperación con otros SOC transfronterizos, especificando los principios de intercambio de información. Cuando los SOC transfronterizos obtengan información relacionada con un incidente de ciberseguridad a gran escala potencial o en curso, proporcionarán la información pertinente a EU CyCLONe, la red de CSIRT y la Comisión, en vista de 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 de Ciberseguridad (Capítulo III)

El Capítulo III establece el Mecanismo de Emergencia Cibernética para mejorar la resiliencia de la Unión ante las principales amenazas de ciberseguridad y prepararse y mitigar, con espíritu de solidaridad, el impacto a corto plazo de incidentes o crisis de ciberseguridad significativos y de gran escala. Las acciones que implementen el Mecanismo de Emergencia Cibernética serán apoyadas con financiamiento de la DEP. El Mecanismo prevé acciones para apoyar la preparación, incluidas pruebas coordinadas de entidades que operan en sectores altamente críticos, respuesta y recuperación inmediata de incidentes de seguridad cibernética significativos o a gran escala o mitigar amenazas cibernéticas significativas y acciones de asistencia mutua.

Las acciones de preparación del Mecanismo de Emergencia Cibernética incluyen pruebas de preparación coordinadas de entidades que operan en sectores altamente críticos. La Comisión, previa consulta a ENISA y al Grupo de Cooperación NIS, debe identificar periódicamente los sectores o subsectores pertinentes de los Sectores de alta criticidad enumerados en el anexo I de la Directiva (UE) n.º 2022/2555, a partir de los cuales las entidades pueden estar sujetas a las pruebas de preparación coordinadas a nivel de la UE.

Con el fin de implementar las acciones de respuesta a incidentes propuestas, el presente Reglamento establece una Reserva de Ciberseguridad de la UE, compuesta por servicios de respuesta a incidentes de proveedores de confianza, seleccionados de acuerdo con los criterios establecidos en este Reglamento. Entre los usuarios de los servicios de la Reserva de Ciberseguridad de la UE se incluirán las autoridades de gestión de cibercrisis de los Estados miembros y los CSIRT y las instituciones, organismos y agencias de la Unión. La Comisión tendrá la responsabilidad general de la aplicación de la Reserva de Ciberseguridad de la UE y podrá confiar, total o parcialmente, a ENISA el funcionamiento y la administración de la Reserva de Ciberseguridad de la UE.

Para recibir apoyo de la Reserva de Ciberseguridad de la UE, los usuarios deberán tomar sus propias medidas para mitigar los efectos del incidente por el cual se solicita el apoyo. Las solicitudes de apoyo de la Reserva de Ciberseguridad de la UE deben incluir la información relevante necesaria sobre el incidente y las medidas ya tomadas por los usuarios. El capítulo

describe también las modalidades de implementación, incluida la evaluación de las solicitudes a la Reserva de Ciberseguridad de la UE.

El Reglamento también establece los principios de contratación y los criterios de selección de los proveedores de confianza de la Reserva de Ciberseguridad de la UE.

Los terceros países pueden solicitar el apoyo de la Reserva de Ciberseguridad de la UE cuando los Acuerdos de Asociación celebrados en relación con su participación en DEP así lo dispongan. Este Capítulo describe otras condiciones y modalidades de dicha participación.

Mecanismo de Revisión de Incidentes de Ciberseguridad (Capítulo IV)

A petición de la Comisión, EU-CYCLONe o la red de CSIRT, ENISA debe revisar y evaluar las amenazas, las vulnerabilidades y las acciones de mitigación con respecto a un incidente de ciberseguridad específico significativo o de gran escala. La revisión y la evaluación deben ser entregadas por ENISA en forma de un informe de revisión de incidentes a la red de CSIRT, EU CyclONe y la Comisión para apoyarlos en el desempeño de sus tareas. Cuando el incidente se refiera a un tercer país, la Comisión debe compartir el informe con el Alto Representante. El informe debe incluir lecciones aprendidas y, cuando corresponda, recomendaciones para mejorar la postura cibernética de la Unión.

Disposiciones Finales (Capítulo V)

El Capítulo V contiene modificaciones al Reglamento DEP y la obligación de que la Comisión prepare informes periódicos para la evaluación y revisión del Reglamento al Parlamento Europeo y al Consejo. La Comisión estará facultada para adoptar actos de ejecución de conformidad con el procedimiento de examen a que se refiere el artículo 21 para: especificar las condiciones de esta interoperabilidad entre los SOC 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 SOC transfronterizos y las entidades de la Unión; establecer requisitos técnicos para garantizar un alto nivel de seguridad física y de los datos de la infraestructura y para proteger los intereses de seguridad de la Unión al compartir 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 más las disposiciones detalladas para la asignación de los servicios de apoyo de la Reserva de Ciberseguridad de la UE.

2023/0109 (COD)

Propuesta para un

REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO

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

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,

Tras la transmisión del proyecto de acto legislativo a los parlamentos nacionales,

Visto el dictamen del Tribunal de Cuentas1

Visto el dictamen del Comité Económico y Social Europeo2 ,

Visto el dictamen del Comité de las Regiones3 ,

Actuando de conformidad con el procedimiento legislativo ordinario,

Mientras que:

(1) El uso y la dependencia de las tecnologías de la información y la comunicación se han convertido en aspectos fundamentales en todos los sectores de la actividad económica, ya que nuestras administraciones públicas, empresas y ciudadanos están más interconectados e interdependientes entre sectores y fronteras que nunca.

(2) La magnitud, la frecuencia y el impacto de los incidentes de ciberseguridad están aumentando, incluidos los ataques a la cadena de suministro con el objetivo de ciberespionaje, ransomware o interrupción. Representan una gran amenaza para el funcionamiento de las redes y los sistemas de información. En vista del panorama de amenazas en rápida evolución, la amenaza de posibles incidentes a gran escala que provoquen perturbaciones o daños significativos en infraestructuras críticas exige una mayor preparación en todos los niveles del marco de ciberseguridad de la Unión. Esa amenaza va más allá de la agresión militar de Rusia contra Ucrania, y es probable que persista dada la multiplicidad de actores criminales y hacktivistas alineados con el estado involucrados en las tensiones geopolíticas actuales. Dichos incidentes pueden impedir la prestación de servicios públicos y el desarrollo de actividades económicas, incluso en sectores críticos o muy críticos, generar pérdidas financieras sustanciales, socavar la confianza de los usuarios, causar daños importantes a la economía de la Unión e incluso podrían afectar la salud o la vida. -Consecuencias amenazantes. Además, los incidentes de ciberseguridad son impredecibles, ya que a menudo surgen y evolucionan en períodos de tiempo muy cortos, no están contenidos en un área geográfica específica y ocurren simultáneamente o se propagan instantáneamente en muchos países.

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

(3) Es necesario reforzar la posición competitiva de los sectores de la industria y los servicios de la Unión en la economía digitalizada y apoyar su transformación digital reforzando el nivel de ciberseguridad en el mercado único digital. Como se recomienda en tres propuestas diferentes de la Conferencia sobre el Futuro de Europa4 , es necesario aumentar la resiliencia de los ciudadanos, las empresas y las entidades que operan infraestructuras críticas frente a las crecientes amenazas a la ciberseguridad, que pueden tener efectos sociales y económicos devastadores. Por lo tanto, se necesita invertir en infraestructuras y servicios que permitan una detección y una respuesta más rápidas a las amenazas e incidentes de ciberseguridad, y los Estados miembros necesitan asistencia para prepararse mejor y responder a incidentes de ciberseguridad significativos y a gran escala. La Unión también debe aumentar sus capacidades en estas áreas, en particular en lo que respecta a la recopilación y el análisis de datos sobre amenazas e incidentes de ciberseguridad.

(4) La Unión ya ha adoptado 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 Consejo5 Recomendación (UE) de la Comisión 2017/15846 Directiva 2013/40/UE del Parlamento Europeo y del Consejo7 y Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo8 . 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 adoptar medidas urgentes y eficaces y a cooperar entre sí de manera leal, eficiente, solidaria y coordinada, la Comisión y otras autoridades públicas pertinentes, así como las entidades interesadas, para mejorar la resiliencia de las infraestructuras críticas utilizadas para prestar servicios esenciales en el mercado interior.

(5) Los crecientes riesgos para la ciberseguridad y un panorama general de amenazas complejo, con un claro riesgo de contagio rápido de ciberincidentes de un Estado miembro a otros y de un tercer país a la Unión, requiere una mayor solidaridad a nivel de la Unión para detectar mejor, prepararse y responder a las amenazas e incidentes de ciberseguridad. Los Estados miembros también han invitado a la Comisión a presentar una propuesta sobre un nuevo Fondo de Respuesta de Emergencia para la Ciberseguridad en las Conclusiones del Consejo sobre una Postura Cibernética de la UE9 .

---

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

5 Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, sobre medidas para un alto nivel común de ciberseguridad en toda la Unión, por la que se modifica el Reglamento (UE) n. 910/2014 y 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 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 del Consejo 2005/222/JAI (JL 218, 14.8.2013, p. 8).

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

9 Conclusiones del Consejo sobre el desarrollo de la postura cibernética de la Unión Europea aprobadas por el Consejo en su reunión del 23 de mayo de 2022 (9364/22)

(6) La Comunicación conjunta sobre la política de la UE en materia de ciberdefensa10, adoptada el 10 de noviembre de 2022, anunció una Iniciativa de solidaridad cibernética de la UE con los siguientes objetivos: reforzar las capacidades comunes de detección, conocimiento de la situación y respuesta de la UE mediante la promoción del despliegue de una infraestructura de seguridad de la UE Centros de operaciones ('SOC'), que respaldan la construcción gradual de una reserva de ciberseguridad a nivel de la UE con servicios de proveedores privados confiables y pruebas de entidades críticas para detectar posibles vulnerabilidades basadas en evaluaciones de riesgo de la UE.

(7) Es necesario reforzar la detección y el conocimiento de la situación de las ciberamenazas e incidentes en toda la Unión y reforzar 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. Por lo tanto, debe desplegarse una infraestructura paneuropea de SOC (European Cyber Shield) para construir y mejorar las capacidades comunes de detección y conocimiento de la situación; debe establecerse un mecanismo de emergencia de ciberseguridad para ayudar a los Estados miembros a prepararse, responder y recuperarse inmediatamente de incidentes de ciberseguridad significativos y de gran escala; Se debe establecer un Mecanismo de Revisión de Incidentes de Ciberseguridad para revisar y evaluar incidentes específicos significativos o de gran escala. Estas acciones se entenderán sin perjuicio de los artículos 107 y 108 del Tratado de Funcionamiento de la Unión Europea ('TFUE').

(8) Para lograr estos objetivos, también es necesario modificar el Reglamento (UE) 2021/694 del Parlamento Europeo y del Consejo11 en determinadas áreas. 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 Escudo Cibernético Europeo y el Mecanismo de Emergencia Cibernética en el marco del Objetivo Específico 3 de DEP, cuyo objetivo es garantizar la resiliencia, integridad y confiabilidad de los Mercado Único Digital, en el fortalecimiento de las capacidades para monitorear los ciberataques y amenazas y para responder a ellos, y en el refuerzo de la cooperación transfronteriza en materia de ciberseguridad. Esto se complementará con las condiciones específicas en las que se podrá conceder apoyo financiero a dichas actuaciones, debiendo definirse los mecanismos de gobernanza y coordinación necesarios para alcanzar los objetivos previstos. Otras enmiendas al Reglamento (UE) 2021/694 deben incluir descripciones de las acciones propuestas en el marco de los nuevos objetivos operativos, así como indicadores medibles para monitorear la implementación 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 consagrado en el objetivo específico 3 del DEP. Las condiciones específicas de participación relativas a cada acción se establecerán en los programas de trabajo correspondientes, de conformidad con la disposición aplicable del Reglamento (UE) 2021/694.

(10) Se aplican al presente Reglamento las normas financieras horizontales adoptadas por el Parlamento Europeo y el Consejo sobre la base del artículo 322 del TFUE. Esas normas se establecen en el Reglamento financiero y determinan, en particular, el procedimiento para establecer y ejecutar el presupuesto de la Unión, y prevén controles sobre la responsabilidad de los agentes financieros. Las normas adoptadas sobre la base del artículo 322 TFUE también incluyen una

---

10 Join Comunicación al Parlamento Europeo y al Consejo Política de la UE en materia de Ciberdefensa 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 se deroga la Decisión (UE) 2015/2240 (DO L 166 de 11.5.2021, p. 1).

régimen general de condicionalidad para la protección del presupuesto de la Unión según lo establecido en 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. Sin dejar de respetar el principio de que el presupuesto de la Unión se establece anualmente, el presente Reglamento debe, debido a la naturaleza impredecible, excepcional y específica del panorama de la ciberseguridad, 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 Emergencia de Ciberseguridad para ayudar a los Estados miembros a contrarrestar eficazmente las ciberamenazas.

(12) Para prevenir, evaluar y responder de manera más eficaz a las amenazas e incidentes cibernéticos, es necesario desarrollar un conocimiento más completo sobre las amenazas a los activos e infraestructuras críticos en el territorio de la Unión, incluida su distribución geográfica, interconexión y efectos potenciales en caso de ciberataques que afecten a dichas infraestructuras. Debe desplegarse una infraestructura de SOC de la Unión a gran escala («el escudo cibernético europeo»), compuesta por varias plataformas transfronterizas interoperativas, cada una de las cuales agrupe varios SOC nacionales. Esa infraestructura debe servir a los intereses y necesidades de ciberseguridad nacionales y de la Unión, aprovechando la tecnología más avanzada para herramientas avanzadas de recopilación y análisis de datos, mejorando las capacidades de gestión y detección cibernética y proporcionando conocimiento de la situación en tiempo real. Esa infraestructura debe servir para aumentar la detección de amenazas e incidentes de ciberseguridad y, por lo tanto, complementar y apoyar a las entidades y redes de la Unión responsables de la gestión de crisis en la Unión, en particular, la Red de organizaciones de enlace de cibercrisis de la UE («EU-CYCLONe»), tal como se define en la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo12 .

(13) Cada Estado miembro debe designar un organismo público a nivel nacional encargado de coordinar las actividades de detección de ciberamenazas en ese Estado miembro. Estos SOC nacionales deben actuar como punto de referencia y puerta de entrada a nivel nacional para la participación en el Escudo Cibernético Europeo y deben garantizar que la información sobre amenazas cibernéticas de entidades públicas y privadas se comparta y recopile a nivel nacional de manera eficaz y simplificada.

(14) Como parte del Escudo Cibernético Europeo, deben establecerse varios Centros de Operaciones de Ciberseguridad Transfronterizos («SOC transfronterizos»). Estos deben reunir a los SOC nacionales de al menos tres Estados miembros, de modo que se puedan lograr plenamente los beneficios de la detección de amenazas transfronterizas y el intercambio y la gestión de la información. El objetivo general de los SOC transfronterizos debe ser fortalecer las capacidades para analizar, prevenir y detectar amenazas a la ciberseguridad y apoyar la producción de inteligencia de alta calidad sobre amenazas a la ciberseguridad, en particular mediante el intercambio de datos de diversas fuentes, públicas o privadas, según corresponda. así como mediante el intercambio y uso conjunto de herramientas de última generación, y el desarrollo conjunto de capacidades de detección, análisis y prevención en un entorno de confianza. Deben proporcionar nueva capacidad adicional, aprovechando y complementando los SOC existentes y los equipos de respuesta a incidentes informáticos ('CSIRT') y otros actores relevantes.

---

12 Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, sobre medidas para un alto nivel común de ciberseguridad en toda la Unión, por la que se modifica el Reglamento (UE) n.º 910/2014 y Directiva (UE) 2018/1972, y por la que se deroga la Directiva (UE) 2016/1148 (Directiva NIS 2) (DO L 333 de 27.12.2022, p. 80).

(15) A escala nacional, el seguimiento, la detección y el análisis de las ciberamenazas suelen estar a cargo de los SOC de entidades públicas y privadas, en combinación con los CSIRT. Además, los CSIRT intercambian información en el contexto de la red CSIRT, de conformidad con la Directiva (UE) 2022/2555. Los SOC transfronterizos deberían constituir una nueva capacidad que sea complementaria a la red de CSIRT, al agrupar y compartir datos sobre amenazas a la seguridad cibernética de entidades públicas y privadas, mejorando el valor de dichos datos a través de análisis de expertos e infraestructuras adquiridas conjuntamente y estado del arte. herramientas, y contribuyendo al desarrollo de las capacidades y la soberanía tecnológica de la Unión.

(16) Los SOC transfronterizos deben actuar como un punto central que permita una amplia puesta en común de datos relevantes e inteligencia sobre amenazas cibernéticas, permitir la difusión de información sobre amenazas entre un conjunto grande y diverso de actores (por ejemplo, Equipos de Respuesta a Emergencias Informáticas (' CERT'), CSIRT, Centros de análisis e intercambio de información ('ISAC'), operadores de infraestructuras críticas). La información intercambiada entre los participantes en un SOC transfronterizo podría incluir datos de redes y sensores, fuentes de inteligencia de amenazas, indicadores de compromiso e información contextualizada sobre incidentes, amenazas y vulnerabilidades. Además, los SOC transfronterizos también deben celebrar acuerdos de cooperación con otros SOC transfronterizos.

(17) El conocimiento de la situación compartido entre las autoridades pertinentes es un requisito previo indispensable para la preparación y la coordinación en toda la Unión con respecto a incidentes de ciberseguridad significativos y de gran escala. La Directiva (UE) 2022/2555 establece EU-CYCLONe para apoyar la gestión coordinada de incidentes y crisis de ciberseguridad a gran escala a nivel operativo y para garantizar el intercambio regular de información relevante entre los Estados miembros y las instituciones, organismos y agencias de la Unión.
La Recomendación (UE) 2017/1584 sobre la respuesta coordinada a incidentes y crisis de ciberseguridad a gran escala aborda el papel de todos los actores relevantes. 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 de proporcionar informes analíticos para el Sistema Integrado Acuerdos del Mecanismo Político de Respuesta a Crisis ('IPCR') en virtud de la Decisión de Ejecución (UE) 2018/1993. Por lo tanto, en situaciones en las que los SOC transfronterizos obtengan información relacionada con un incidente de ciberseguridad a gran escala potencial o en curso, deben proporcionar información relevante a EU-CyCLONe, la red de CSIRT y la Comisión. En particular, según la situación, la información que se compartirá podría incluir información técnica, información sobre la naturaleza y los motivos del atacante o posible atacante, e información no técnica de nivel superior sobre un incidente de ciberseguridad a gran escala potencial o en curso. En este contexto, se debe prestar la debida atención al principio de necesidad de saber y a la naturaleza potencialmente sensible de la información compartida.

(18) Las entidades que participen en el Escudo cibernético europeo deben garantizar un alto nivel de interoperabilidad entre ellas, incluido, según 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, un nivel mínimo de capa de aplicación seguridad, panel de control de la situación e indicadores. La adopción de una taxonomía común y el desarrollo de una plantilla para informes de situación para describir la causa técnica y los impactos de los incidentes de ciberseguridad deben tener en cuenta el trabajo en curso sobre notificación de incidentes en el contexto de la implementación de la Directiva (UE) 2022/2555.

(19) A fin de permitir el intercambio de datos sobre amenazas a la ciberseguridad de varias fuentes, a gran escala, en un entorno de confianza, las entidades que participan en la Unión Europea

Cyber Shield debe estar equipado con 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 análisis de datos e inteligencia artificial.

(20) Al recopilar, compartir e intercambiar datos, el Ciberescudo europeo debe mejorar la soberanía tecnológica de la Unión. La puesta en común de datos seleccionados de alta calidad también debería contribuir al desarrollo de tecnologías avanzadas de análisis de datos e inteligencia artificial. Debería facilitarse mediante la conexión del Escudo cibernético europeo con la infraestructura informática paneuropea de alto rendimiento establecida por el Reglamento (UE) 2021/117313 del Consejo .

(21) Si bien el Escudo Cibernético Europeo es un proyecto civil, la comunidad de defensa cibernética podría beneficiarse de capacidades más fuertes de detección civil y conciencia situacional desarrolladas para la protección de infraestructuras críticas. Los SOC transfronterizos, con el apoyo de la Comisión y el 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»), deberían desarrollarse gradualmente protocolos y estándares dedicados para permitir la cooperación con la comunidad de defensa cibernética, incluidas las condiciones de investigación y seguridad. El desarrollo del Escudo cibernético europeo debe ir acompañado de una reflexión que permita la futura colaboración con redes y plataformas responsables del intercambio de información en la comunidad de ciberdefensa, en estrecha cooperación con el Alto Representante.

(22) El intercambio de información entre los participantes del Escudo Cibernético Europeo debe cumplir los requisitos legales existentes y, en particular, la legislación nacional y de la Unión en materia de protección de datos, así como las normas de la Unión sobre 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, y destruir los datos tan pronto como ya no sean necesarios para la finalidad declarada e informar el organismo que pone a disposición los datos que los datos han sido destruidos.

(23) Sin perjuicio de lo dispuesto en el artículo 346 del TFUE, el intercambio de información que sea confidencial con arreglo a las normas nacionales o de la Unión debe limitarse a la que sea pertinente y proporcionada al objeto de dicho intercambio. El intercambio de dicha información debe preservar la confidencialidad de la información y proteger la seguridad y los intereses comerciales de las entidades involucradas, con pleno respeto de los secretos comerciales y comerciales.

(24) En vista del aumento de los riesgos y del número de ciberincidentes que afectan a los Estados miembros, es necesario establecer 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 mediante medidas financieras de emergencia. apoyo para la preparación, respuesta y recuperación inmediata de los servicios esenciales. Ese instrumento debe permitir el despliegue rápido de la asistencia en circunstancias definidas y en condiciones claras y permitir un seguimiento y una evaluación cuidadosos de cómo se han utilizado los recursos. Si bien la responsabilidad principal de prevenir, prepararse y responder a incidentes y crisis de ciberseguridad recae en los Estados miembros, la emergencia cibernética

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

El mecanismo 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 proporcionar apoyo a los Estados miembros complementando sus propias medidas y recursos, y otras opciones de apoyo existentes en caso de respuesta y recuperación inmediata de incidentes de ciberseguridad significativos y de gran escala, como los servicios prestados por la Unión Europea. Agencia de la Unión para la Ciberseguridad («ENISA») de conformidad con su mandato, la respuesta coordinada y la asistencia de la red de CSIRT, el apoyo de mitigación de EU CyCLONe, así como la asistencia mutua entre los Estados miembros, incluso en el contexto del artículo 42(7) de TEU, los Equipos de Respuesta Rápida Cibernética PESCO14 y los Equipos de Respuesta Rápida Híbridos. Debe abordar la necesidad de garantizar la disponibilidad de medios especializados para respaldar 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 UCPM15, el IPCR16 y la Directiva (UE) 2022/2555. Puede contribuir o complementar acciones implementadas en el contexto del artículo 42, apartado 7, del TUE o en situaciones definidas en el artículo 222 del TFUE. El uso de este instrumento también debe coordinarse con la implementación de las medidas de Cyber Diplomacy Toolbox, cuando corresponda.

(27) La asistencia proporcionada en virtud del presente Reglamento debe apoyar y complementar las acciones emprendidas por los Estados miembros a nivel nacional. Con este fin, debe garantizarse una estrecha cooperación y consulta entre la Comisión y el Estado miembro afectado. Al solicitar apoyo bajo el Mecanismo de Emergencia Cibernética, el Estado miembro debe proporcionar información relevante que justifique la necesidad de apoyo.

(28) La Directiva (UE) 2022/2555 exige a los Estados miembros que designen o establezcan una o más autoridades de gestión de cibercrisis y garanticen que cuentan con los recursos adecuados para llevar a cabo sus tareas de manera eficaz y eficiente. También requiere que los Estados miembros identifiquen las capacidades, los activos y los procedimientos que pueden implementarse en caso de una crisis, así como que adopten un plan nacional de respuesta a incidentes y crisis de ciberseguridad a gran escala donde los objetivos y las disposiciones para la gestión de incidentes a gran escala Se exponen los incidentes y crisis de ciberseguridad. Los Estados miembros también están obligados a establecer uno o más CSIRT encargados de las responsabilidades de gestión de incidentes de acuerdo con un proceso bien definido y que abarque al menos los sectores, subsectores y tipos de entidades bajo el ámbito de aplicación de dicha Directiva, y garantizar que cuenten con los recursos adecuados. para llevar a cabo con eficacia sus tareas. El presente Reglamento se entiende sin perjuicio de la función de la Comisión de garantizar el cumplimiento por parte de los Estados miembros de las obligaciones de la Directiva (UE) 2022/2555. El Mecanismo de Emergencia Cibernética debe brindar asistencia para acciones destinadas a reforzar la preparación, así como acciones de respuesta a incidentes para mitigar el impacto de incidentes de ciberseguridad significativos y de gran escala, para apoyar la recuperación inmediata y/o restablecer el funcionamiento de los servicios esenciales.

---

14 DECISIÓN DEL CONSEJO (PESC) 2017/ 2315 - de 11 de diciembre de 2017 - por la que se establece una cooperación estructurada permanente (PESCO) y se determina la lista de 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).

16 Acuerdos de respuesta política integrada a las crisis (IPCR) y de acuerdo con la Recomendación de la Comisión (UE) 2017/1584, de 13 de septiembre de 2017, sobre la respuesta coordinada a incidentes y crisis de ciberseguridad a gran escala.

(29) Como parte de las acciones de preparación, para promover un enfoque coherente y reforzar la seguridad en toda la Unión y su mercado interior, debe prestarse apoyo para probar y evaluar la ciberseguridad de las entidades que operan en sectores muy críticos identificados con arreglo a la Directiva (UE) 2022 /2555 de manera coordinada. A tal fin, la Comisión, con el apoyo de ENISA y en cooperación con el Grupo de Cooperación NIS establecido por la Directiva (UE) 2022/2555, debe identificar periódicamente los sectores o subsectores pertinentes, que deben ser elegibles para recibir apoyo financiero para pruebas coordinadas en nivel sindical. Los sectores o subsectores deben seleccionarse del Anexo I de la Directiva (UE) 2022/2555 ('Sectores de alta criticidad'). Los ejercicios de prueba coordinados deben basarse en escenarios de riesgo y metodologías comunes. La selección de sectores y el desarrollo de escenarios de riesgo deben tener en cuenta las evaluaciones de riesgo y los escenarios de riesgo pertinentes a escala de la Unión, incluida la necesidad de evitar la duplicación, como la evaluación del riesgo y los escenarios de riesgo solicitados en las Conclusiones del Consejo sobre el desarrollo de la Unión Europea. La postura cibernética de la Unión será llevada a cabo por la Comisión, el Alto Representante y el Grupo de Cooperación NIS, en coordinación con los organismos y agencias civiles y militares pertinentes y las redes establecidas, incluido EU CyCLONe, así como la evaluación de riesgos de las redes e infraestructuras de comunicaciones solicitadas. por la Convocatoria Ministerial Conjunta de Nevers y realizada por el Grupo de Cooperación NIS, con el apoyo de la Comisión y ENISA, y en cooperación con el Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE), las evaluaciones de riesgo coordinadas que se llevarán a cabo de conformidad con el artículo 22 de la Directiva (UE) 2022/2555 y pruebas de resiliencia operativa digital según lo dispuesto en el Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo17. La selección de sectores también debe tener en cuenta la Recomendación del Consejo sobre un enfoque coordinado a escala de la Unión para reforzar la resiliencia de las infraestructuras críticas.

(30) Además, el Mecanismo de Emergencia Cibernética debe ofrecer apoyo para otras acciones de preparación y apoyo a la preparación en otros sectores, no cubiertos por las pruebas coordinadas de entidades que operan en sectores altamente críticos. Esas acciones podrían incluir varios tipos de actividades nacionales de preparación.

(31) El Mecanismo de Emergencia Cibernética también debe brindar apoyo a las acciones de respuesta a incidentes para mitigar el impacto de incidentes de ciberseguridad significativos y a gran escala, para respaldar la recuperación inmediata o restablecer el funcionamiento de los servicios esenciales. Cuando corresponda, debe complementar el UCPM para garantizar un enfoque integral para responder a los impactos de los incidentes cibernéticos en los ciudadanos.

(32) El Mecanismo de Ciberemergencia debe respaldar la asistencia proporcionada 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. Debe permitirse a los Estados miembros que presten asistencia 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 nivel de la Unión, compuesta por servicios de proveedores privados de servicios de seguridad gestionados para apoyar la respuesta y

17 Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativo a la resiliencia operativa digital del sector financiero y por el que se modifica el Reglamento (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 y (UE) n.º 2016/1011

acciones de recuperación inmediata en casos de incidentes de ciberseguridad significativos o de gran magnitud. La Reserva de Ciberseguridad de la UE debe garantizar la disponibilidad y preparación de los servicios. Los servicios de la Reserva de Ciberseguridad de la UE deben servir para apoyar a las autoridades nacionales en la prestación de asistencia a las entidades afectadas que operan en sectores críticos o altamente críticos como complemento a sus propias acciones a nivel nacional. Al solicitar apoyo a la Reserva de Ciberseguridad de la UE, los Estados miembros deben especificar el apoyo proporcionado 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 apoyar a las instituciones, organismos y agencias de la Unión, en condiciones similares.

(34) A efectos de seleccionar 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 las licitaciones para seleccionar estos proveedores, a fin de velar por que se satisfagan las necesidades de las autoridades y entidades de los Estados miembros que operan en sectores críticos o muy críticos.

(35) Para apoyar el establecimiento de la Reserva de Ciberseguridad de la UE, la Comisión podría considerar solicitar a ENISA que prepare un plan de certificación candidato de conformidad con el Reglamento (UE) 2019/881 para los servicios de seguridad gestionados en las áreas cubiertas por el Mecanismo de Emergencia Cibernética.

(36) A fin de apoyar los objetivos del presente Reglamento de promover una concienciación compartida de la situación, 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 ENISA para revisar y evaluar amenazas, vulnerabilidades y acciones de mitigación con respecto a un incidente específico de ciberseguridad significativo o de gran escala. Después de completar una revisión y evaluación de un incidente, ENISA debe preparar un informe de revisión de incidentes, en colaboración con las partes interesadas relevantes, incluidos representantes del sector privado, los Estados miembros, la Comisión y otras instituciones, organismos y agencias de la UE relevantes. En lo que respecta al sector privado, ENISA está desarrollando canales para intercambiar información con proveedores especializados, incluidos proveedores de soluciones de seguridad gestionada y proveedores, con el fin de contribuir a la misión de ENISA de lograr un alto 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 apuntar a evaluar las causas, los impactos y las mitigaciones de un incidente, después de que haya ocurrido.

Debe prestarse especial atención a las aportaciones y lecciones compartidas por los proveedores de servicios de seguridad gestionados que cumplan las condiciones de máxima integridad profesional, imparcialidad y experiencia técnica requeridas por el presente Reglamento. El informe debe entregarse y alimentar el trabajo de EU=CYCLONe, la red de CSIRT y la Comisión. Cuando el incidente se refiera a un tercer país, la Comisión también lo comunicará al Alto Representante.

(37) Teniendo en cuenta la naturaleza impredecible de los ataques a la ciberseguridad y el hecho de que a menudo no están contenidos en un área geográfica específica y presentan un alto riesgo de contagio, el fortalecimiento de la resiliencia de los países vecinos y su capacidad para responder de manera efectiva a ataques significativos y incidentes de ciberseguridad a gran escala contribuye a la protección de la Unión en su conjunto. Por lo tanto, los terceros países asociados a la DEP podrán recibir apoyo de la Reserva de Ciberseguridad de la UE, cuando así esté previsto en el respectivo acuerdo de asociación a la DEP. La Unión debe apoyar la financiación de terceros países asociados en el marco de asociaciones e instrumentos de financiación pertinentes para dichos países. El apoyo debe cubrir los servicios en el

área de respuesta y recuperación inmediata de incidentes de ciberseguridad significativos o de gran escala. Las condiciones establecidas para la Reserva de Ciberseguridad de la UE y los proveedores de confianza en este Reglamento deben aplicarse al brindar apoyo a los terceros países asociados a DEP.

(38) A fin de garantizar condiciones uniformes para la aplicación del presente Reglamento, deben conferirse a la Comisión competencias de ejecución para especificar las condiciones de interoperabilidad entre los SOC 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 SOC transfronterizos y las entidades de la Unión; establecer requisitos técnicos para garantizar la seguridad del Escudo Cibernético Europeo; especificar los tipos y el número de servicios de respuesta necesarios para la Reserva de Ciberseguridad de la UE; y, especificar más las disposiciones detalladas para la asignación de los servicios de apoyo de la Reserva de Ciberseguridad de la UE. Dichos poderes 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 a nivel de los Estados miembros. Por tanto, la Unión puede adoptar medidas, de conformidad con 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 ese objetivo.

HAN ADOPTADO ESTE REGLAMENTO:

Capítulo I

OBJETIVOS GENERALES, TEMÁTICA Y DEFINICIONES

Articulo 1

Objeto y objetivos

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

a) el despliegue de una infraestructura paneuropea de centros de operaciones de seguridad («escudo cibernético europeo») para construir y mejorar las capacidades comunes de detección y conocimiento de la
situación; (b) la creación de un Mecanismo de emergencia de ciberseguridad para ayudar a los Estados miembros a prepararse, responder y recuperarse inmediatamente de incidentes de ciberseguridad significativos y de
gran escala; c) el establecimiento de un Mecanismo Europeo de Revisión de Incidentes de Ciberseguridad para revisar y evaluar incidentes significativos o de gran escala.

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

reforzar la detección común de la Unión y el conocimiento de la situación de las amenazas e incidentes cibernéticos, lo que permite reforzar la posición competitiva de los sectores de la industria y los servicios en la Unión en toda la economía digital y contribuir a la soberanía tecnológica de la Unión en el ámbito de la ciberseguridad;

(b) reforzar la preparación de las entidades que operan en sectores críticos y altamente críticos en toda la Unión y fortalecer la solidaridad mediante el desarrollo de capacidades de respuesta comunes frente a incidentes de ciberseguridad significativos o de gran escala, incluso poniendo a disposición de terceros países asociados al Programa Europa Digital el apoyo de respuesta a incidentes de ciberseguridad de la Unión ('DEP');

(C) mejorar la resiliencia de la Unión y contribuir a una respuesta eficaz mediante la revisión y evaluación de incidentes significativos o de gran escala, incluida la extracción de lecciones aprendidas y, en su caso, recomendaciones.

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

Artículo 2

Definiciones

A los efectos del presente Reglamento, se aplican las siguientes definiciones:

(1) 'Centro de operaciones de seguridad transfronterizo' ("SOC transfronterizo") significa una plataforma multinacional, que reúne en una estructura de red coordinada SOC nacionales de al menos tres Estados miembros que forman un Consorcio de alojamiento, y que está diseñado para prevenir ciberamenazas e incidentes y apoyar la producción de inteligencia de alta calidad, en particular mediante el intercambio de datos de diversas fuentes, públicas y privadas, así como mediante el intercambio de herramientas de última generación y el desarrollo conjunto de ciberdetección , análisis y capacidades de prevención y protección en un entorno de confianza;

(2) «organismo público» : un organismo de derecho público tal como se define en el artículo 2, apartado 1, punto 4, de la Directiva 2014/24/UE del Parlamento Europeo y del Consejo18;

(3) 'Consorcio de alojamiento' se refiere a un consorcio compuesto por estados participantes, representados por SOC nacionales, que han acordado establecer y contribuir a la adquisición de herramientas e infraestructura para el funcionamiento de un SOC transfronterizo;

(4) «entidad» : una entidad tal como 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;

---

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).

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

(7) «incidente significativo de ciberseguridad» : 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 tal como 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 y eficaz a un incidente de ciberseguridad significativo o de gran escala, obtenido como resultado de la evaluación de riesgos y las acciones de seguimiento realizadas con antelación;

(10) «respuesta» : acción en caso de un incidente de ciberseguridad importante o de gran escala, o durante o después de dicho incidente, para abordar sus consecuencias adversas inmediatas y a corto plazo; «proveedores de

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

Capitulo dos

EL ESCUDO CIBERNÉTICO EUROPEO

Artículo 3

Establecimiento del Escudo Cibernético Europeo

1. Se establecerá una infraestructura paneuropea interconectada de centros de operaciones de seguridad («European Cyber Shield») para desarrollar capacidades avanzadas para que la Unión detecte, analice y procese datos sobre ciberamenazas e incidentes en la Unión. Estará integrado por todos los Centros de Operaciones de Seguridad Nacional ('SOC Nacionales') y los Centros de Operaciones de Seguridad Transfronterizos ('SOC Transfronterizos').

Las acciones que implementen el Escudo Cibernético Europeo contarán con el apoyo financiero del Programa Europa Digital y se implementarán de conformidad con el Reglamento (UE) 2021/694 y, en particular, el Objetivo Específico 3 del mismo.

2. El Ciberescudo Europeo deberá:

(a) reunir y compartir datos sobre ciberamenazas e incidentes de varias fuentes a través de SOC transfronterizos;

(b) producir información procesable de alta calidad e inteligencia sobre amenazas cibernéticas, mediante el uso de herramientas de última generación, en particular, inteligencia artificial y tecnologías de análisis de datos;

(c) contribuir a una mejor protección y respuesta a las ciberamenazas;

(d) contribuir a una detección más rápida de amenazas cibernéticas y conciencia situacional en todo el Unión;

e) prestar servicios y actividades para la comunidad de la ciberseguridad en la Unión, incluida la contribución al desarrollo de herramientas avanzadas de análisis de datos e inteligencia artificial.

Se desarrollará en cooperación con la infraestructura informática paneuropea de alto rendimiento establecida de conformidad con el Reglamento (UE) 2021/1173.

Artículo 4

Centros de Operaciones de Seguridad Nacional

1. Para participar en el Escudo cibernético europeo, cada Estado miembro designará al menos un SOC nacional. El SOC Nacional será un organismo público.

Tendrá capacidad para actuar como punto de referencia y puerta de entrada a otras organizaciones públicas y privadas a nivel nacional para recopilar y analizar información sobre amenazas e incidentes de ciberseguridad y contribuir a un SOC transfronterizo. Estará equipado con tecnologías de punta capaces de detectar, agregar y analizar datos relevantes para amenazas e incidentes de seguridad cibernética.

2. Tras una convocatoria de manifestaciones de interés, los SOC nacionales serán seleccionados por el Centro Europeo de Competencia en Ciberseguridad («ECCC») para participar en una adquisición conjunta de herramientas e infraestructuras con el ECCC. El ECCC puede otorgar subvenciones a los SOC nacionales seleccionados para financiar el funcionamiento de esas herramientas e infraestructuras. La contribución financiera de la Unión cubrirá hasta el 50 % de los costes de adquisición de las herramientas y las 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, la ECCC y el SOC Nacional deberán celebrar un acuerdo de alojamiento y uso que regule el uso de las herramientas e infraestructuras.

3. Un SOC nacional seleccionado de conformidad con el apartado 2 se comprometerá a solicitar su participación en un SOC transfronterizo en un plazo de dos años a partir de la fecha en que se adquieran las herramientas e infraestructuras o en la que reciba la subvención, lo que ocurra antes. Si un SOC nacional no participa en un SOC transfronterizo en ese momento, no podrá optar a ayuda adicional de la Unión en virtud del presente Reglamento.

Artículo 5

Centros de Operaciones de Seguridad Transfronteriza

1. Un consorcio de alojamiento formado por al menos tres Estados miembros, representados por SOC nacionales, comprometidos a trabajar juntos para coordinar sus actividades de detección cibernética y seguimiento de amenazas, podrá participar en acciones para establecer un SOC transfronterizo.

2. Tras una convocatoria de manifestaciones de interés, el ECCC seleccionará un Consorcio de alojamiento para participar en una adquisición conjunta de herramientas e infraestructuras con el ECCC. El

ECCC podrá otorgar al Consorcio de Alojamiento una subvención para financiar el funcionamiento de las herramientas e infraestructuras. La contribución financiera de la Unión cubrirá hasta el 75 % de los costes de adquisición de las herramientas e infraestructuras, y hasta el 50 % de los costes de funcionamiento, siendo los costes restantes cubiertos por el Consorcio de acogida. Antes de iniciar el procedimiento para la adquisición de las herramientas e infraestructuras, la ECCC y el Consorcio de Alojamiento deberán celebrar un acuerdo de alojamiento y uso que regule el uso de las herramientas e infraestructuras.

3. Los miembros del Consorcio de alojamiento celebrarán un acuerdo de consorcio por escrito que establezca sus acuerdos internos para implementar el Acuerdo de uso y alojamiento.

4. Un SOC Transfronterizo estará representado a efectos legales por un SOC Nacional que actúe como SOC coordinador, o por el Consorcio de Vivienda si tuviera personalidad jurídica. El SOC 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 y entre los SOC transfronterizos

1. Los miembros de un consorcio de hospedaje intercambiarán información relevante entre ellos dentro del SOC transfronterizo, incluida información relacionada con amenazas cibernéticas, cuasi accidentes, vulnerabilidades, técnicas y procedimientos, indicadores de compromiso, tácticas antagónicas, información específica del actor de amenazas, ciberseguridad alertas y recomendaciones relativas a la configuración de herramientas de ciberseguridad para detectar ciberataques, cuando dicho intercambio de información:

(a) tiene como objetivo prevenir, detectar, responder o recuperarse de incidentes o mitigar su impacto;

(b) mejora el nivel de ciberseguridad, en particular mediante la sensibilización en relación con las ciberamenazas, limitando o impidiendo la capacidad de propagación de dichas amenazas, apoyando una gama de capacidades defensivas, remediación y divulgación de vulnerabilidades, técnicas de detección, contención y prevención de amenazas, estrategias de mitigación , o etapas de respuesta y recuperación o promover la investigación colaborativa de amenazas entre entidades públicas y privadas.

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

(a) un compromiso de compartir una cantidad significativa de datos mencionados en el párrafo 1, y las condiciones bajo las cuales se intercambiará esa información;

(b) un marco de gobernanza que incentiva el intercambio de información entre todos los participantes;

(C) objetivos de contribución al desarrollo de herramientas avanzadas de inteligencia artificial y análisis de datos.

3. Para fomentar el intercambio de información entre SOC transfronterizos, los SOC transfronterizos garantizarán un alto nivel de interoperabilidad entre ellos. Para facilitar la interoperabilidad entre los SOC transfronterizos, la Comisión podrá, mediante actos de ejecución, previa consulta al ECCC, especificar las condiciones para esta interoperabilidad.
Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 21, apartado 2, del presente Reglamento.

4. Los SOC 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 SOC transfronterizos obtengan información relativa a un incidente de ciberseguridad a gran escala potencial o en curso, proporcionarán la información pertinente a EU=CYCLONe, a la red de CSIRT y a la Comisión, en vista de sus respectivas funciones de gestión de crisis de conformidad con la Directiva (UE) 2022/2555 sin demora indebida.

2. La Comisión podrá, mediante actos de ejecución, determinar las modalidades 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, del presente Reglamento.

Artículo 8

Seguridad

1. Los Estados miembros que participen en el Escudo Cibernético Europeo garantizarán un alto nivel de seguridad de los datos y la seguridad física de la infraestructura del Escudo Cibernético Europeo y garantizarán que la infraestructura se gestione y controle adecuadamente de forma que quede protegida de las amenazas. y para garantizar 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 Escudo cibernético europeo garantizarán que el intercambio de información dentro del Escudo cibernético 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 su obligación en virtud de 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, del presente Reglamento. Al hacerlo, la Comisión, con el apoyo del Alto Representante, tendrá en cuenta las normas de seguridad aplicables al nivel de defensa, a fin de facilitar la cooperación con los actores militares.

Capítulo III

MECANISMO DE EMERGENCIA CIBERNÉTICA

Artículo 9

Establecimiento del Mecanismo de Emergencia Cibernética

1. Se establece un Mecanismo de Ciberemergencia para mejorar la resiliencia de la Unión frente a las principales amenazas a la ciberseguridad y preparar y mitigar, con un espíritu de solidaridad, el impacto a corto plazo de incidentes de ciberseguridad significativos y a gran escala (el «Mecanismo»).

2. Las acciones que implementen el Mecanismo de Ciberemergencia serán financiadas por DEP y ejecutadas de conformidad con el Reglamento (UE) 2021/694 y, en particular, el Objetivo Específico 3 del mismo.

Artículo 10

Tipo de acciones

1. El Mecanismo apoyará los siguientes tipos de acciones: (a)

acciones de preparación, incluidas las pruebas coordinadas de preparación de entidades que operan en sectores muy críticos en toda la Unión;

(b) acciones de respuesta, que respaldan la respuesta y la recuperación inmediata de incidentes de ciberseguridad significativos y a gran escala, a cargo de proveedores de confianza que participan 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 de las autoridades nacionales de un Estado miembro a otro Estado miembro, en particular según lo dispuesto en el artículo 11, apartado 3, letra f), de la Directiva (UE) 2022/2555.

Artículo 11

Pruebas coordinadas de preparación de entidades

1. Con el fin de apoyar las pruebas de preparación coordinadas 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 NIS y ENISA, identificará los sectores o sub -sectores, en cuestión, de los sectores de alta criticidad enumerados en el anexo I de la Directiva (UE) 2022/2555 de los cuales las entidades pueden estar sujetas a las pruebas de preparación coordinadas, teniendo en cuenta las evaluaciones de riesgos coordinadas existentes y previstas y las pruebas de resiliencia a nivel de la Unión .

2. El Grupo de Cooperación NIS, en cooperación con la Comisión, ENISA y el Alto Representante, desarrollará escenarios de riesgo y metodologías comunes para los ejercicios de ensayo coordinados.

Artículo 12

Establecimiento de la Reserva de Ciberseguridad de la UE

1. Se establecerá una Reserva de Ciberseguridad de la UE para ayudar a los usuarios a que se refiere el apartado 3 a responder o proporcionar apoyo para responder a incidentes de ciberseguridad significativos o de gran escala, y a la recuperación inmediata de tales incidentes.

2. La Reserva de Ciberseguridad de la UE estará formada por servicios de respuesta a incidentes de proveedores de confianza seleccionados de acuerdo con los criterios establecidos en el artículo 16. La Reserva incluirá servicios comprometidos previamente. Los servicios serán desplegables en todos los Estados miembros.

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

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

b) Instituciones, órganos y organismos de la Unión.

4. Los usuarios a los 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 y la recuperación inmediata de incidentes significativos o de gran escala que afecten a entidades que operan en sectores críticos o muy críticos. .

5. La Comisión tendrá la responsabilidad general de la aplicación 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, y 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 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 ENISA, mediante acuerdos de contribución.

7. Con el fin de ayudar a la Comisión a establecer la Reserva de Ciberseguridad de la UE, ENISA preparará un mapeo de los servicios necesarios, previa consulta a los Estados miembros y la Comisión. ENISA preparará un mapeo similar, previa consulta a la Comisión, para identificar las necesidades de los terceros países elegibles para el apoyo de la Reserva de Ciberseguridad de la UE de conformidad con el artículo 17. La Comisión, cuando corresponda, 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 los que se refiere el artículo 12, apartado 3, podrán solicitar servicios de la Reserva de Ciberseguridad de la UE para respaldar la respuesta y la recuperación inmediata de incidentes de ciberseguridad significativos o de gran escala.

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

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 ENISA a través del punto único de contacto 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, en su caso, a EU-CYCLONe, sobre sus solicitudes de respuesta a incidentes y apoyo para la recuperación inmediata de conformidad con el presente artículo.

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

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

(b) información sobre las medidas adoptadas para mitigar el incidente para el que se solicita el apoyo, a que se refiere el apartado 2;

(C) información sobre otras formas de apoyo disponibles para la entidad afectada, incluidos los arreglos contractuales vigentes para la respuesta a incidentes y los servicios de recuperación inmediata, así como los contratos de seguros que podrían cubrir este tipo de incidente.

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

7. La Comisión podrá, mediante actos de ejecución, especificar más 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

Implementación 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 ENISA o según lo definido en los acuerdos de contribución en virtud del artículo 12, apartado 6, y se transmitirá una respuesta a los usuarios a que se refiere el artículo 12. (3) sin demora.

2. Para la priorización de las solicitudes, en el caso de múltiples solicitudes concurrentes, se tendrán en cuenta, en su caso, 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 tal como se definen en el artículo 3, apartado 1, de la Directiva (UE) 2022/2555;

(C) el impacto potencial en los Estados miembros o usuarios afectados;

(d) la posible naturaleza transfronteriza del incidente y el riesgo de contagio a otros Estados miembros o usuarios;

(mi) las medidas adoptadas por el usuario para ayudar en la respuesta y los esfuerzos de recuperación inmediata, tal como se contemplan en 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 presta 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 modelos elaborados por ENISA, previa consulta a los Estados miembros.

5. La Comisión y ENISA no asumirán ninguna responsabilidad contractual por los daños causados a terceros por los servicios prestados en el marco de la implementación de la Reserva de Ciberseguridad de la UE.

6. En el plazo de un mes desde el final de la acción de apoyo, los usuarios proporcionarán a la Comisión ya ENISA un informe resumido sobre el servicio prestado, los resultados obtenidos y las lecciones aprendidas. Cuando el usuario sea de un tercer país según lo establecido en el artículo 17, dicho informe se compartirá con el Alto Representante.

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

Artículo 15

Coordinación con mecanismos de gestión de crisis

1. En los casos en que incidentes de ciberseguridad significativos o a gran escala se originen 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 se complementará con arreglo a la Decisión 1313/2013/UE y sin perjuicio de ella. .

2. En el caso de un incidente de ciberseguridad transfronterizo a gran escala en el que se activen los acuerdos de respuesta política integrada a las crisis (IPCR), el apoyo en virtud del presente Reglamento para responder a dicho incidente se gestionará de conformidad con los protocolos y procedimientos pertinentes en virtud del IPCR. .

3. En consulta con el Alto Representante, el apoyo en el marco del Mecanismo de Ciberemergencia podrá complementar la asistencia proporcionada en el contexto de la Política Exterior y de Seguridad Común y la Política Común de Seguridad y Defensa, incluso a través de los Equipos de Respuesta Cibernética Rápida. También puede complementar o contribuir a la asistencia proporcionada por un Estado miembro a otro Estado miembro en el contexto del artículo 42, apartado 7, del Tratado de la Unión Europea.

4. El apoyo en virtud del Mecanismo de Ciberemergencia podrá formar parte de la respuesta conjunta entre 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 a efectos de constituir 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 de conformidad con los siguientes principios:

[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).

(a) garantizar que la Reserva de Ciberseguridad de la UE incluya servicios que puedan desplegarse en todos Estados miembros, teniendo en cuenta, en particular, los requisitos nacionales para la prestación de dichos servicios, incluida la certificación o acreditación;

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

(C) garantizar que la Reserva de Ciberseguridad de la UE aporte valor añadido a la UE, contribuyendo a los objetivos establecidos en el artículo 3 del Reglamento (UE) 2021/694, incluida la promoción del desarrollo de capacidades en ciberseguridad en la UE.

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

(a) el proveedor deberá demostrar que su personal tiene el más alto grado de integridad profesional, independencia, responsabilidad y la competencia técnica requerida para realizar las actividades en su campo específico, y asegura la permanencia/continuidad de la experiencia, así como los recursos técnicos requeridos;

(b) el proveedor, sus filiales y subcontratistas dispondrán de un marco para proteger la información sensible relacionada con el servicio y, en particular, las pruebas, los resultados y los informes, y cumplirán las normas de seguridad de la Unión sobre la protección de información clasificada de la UE;

(C) el proveedor deberá proporcionar prueba suficiente de que su estructura de gobierno es transparente, no susceptible de comprometer su imparcialidad y la calidad de sus servicios o de causar conflictos de interés;

(d) el proveedor deberá tener la habilitación de seguridad adecuada, al menos para el personal destinado al despliegue del servicio;

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

(F) el prestador deberá contar con los equipos técnicos de hardware y software necesarios para soportar el servicio solicitado;

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

(h) el proveedor deberá poder prestar el servicio en un plazo breve en el Estado(s) miembro(s) donde puede prestar el servicio;

(i) el proveedor deberá poder prestar el servicio en el idioma local del miembro Estado(s) donde puede prestar el servicio;

(j) una vez que esté en vigor un sistema de certificación de la UE para el Reglamento (UE) 2019/881 de servicios de seguridad gestionados, el proveedor deberá estar certificado de conformidad con dicho sistema.

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 dispongan los Acuerdos de Asociación celebrados en relación con su participación en DEP.

2. El apoyo de la Reserva de Ciberseguridad de la UE se realizará de conformidad con el presente Reglamento y cumplirá las condiciones específicas establecidas en los Acuerdos de Asociación mencionados en el apartado 1.

3. Los usuarios de terceros países asociados que puedan recibir servicios de la Reserva de Ciberseguridad de la UE incluirán autoridades competentes como los CSIRT y las autoridades de gestión de cibercrisis.

4. Cada tercer país elegible para recibir apoyo de la Reserva de Ciberseguridad de la UE designará una autoridad para que actúe como punto de contacto único a efectos del presente Reglamento.

5. Antes de recibir cualquier apoyo de la Reserva de Ciberseguridad de la UE, los terceros países proporcionarán a la Comisión y al Alto Representante información sobre su ciberresiliencia y capacidades de gestión de riesgos, incluida al menos información sobre las medidas nacionales adoptadas para prepararse para riesgos significativos o a gran escala. incidentes de ciberseguridad, así como información sobre las entidades nacionales responsables, incluidos los CSIRT o entidades equivalentes, sus capacidades y los recursos que se les asignan. Cuando las disposiciones de los artículos 13 y 14 del presente Reglamento se refieran a Estados miembros, se aplicarán a terceros países tal como se establece en el apartado 1.

6. La Comisión se coordinará con el Alto Representante sobre las solicitudes recibidas y la implementación del apoyo otorgado a terceros países desde la Reserva de Ciberseguridad de la UE.

Capítulo IV

MECANISMO DE REVISIÓN DE INCIDENTES DE CIBERSEGURIDAD

Artículo 18

Mecanismo de revisión de incidentes de ciberseguridad

1. A petición de la Comisión, la red EU-CYCLONe o los CSIRT, ENISA revisará y evaluará las amenazas, las vulnerabilidades y las medidas de mitigación con respecto a un incidente de ciberseguridad específico significativo o de gran escala. Tras la finalización de una revisión y evaluación de un incidente, ENISA entregará un informe de revisión de incidentes a la red de CSIRT, EU-CYCLONe y la Comisión para ayudarlos en el desempeño de sus funciones, en particular en vista de las establecidas en los artículos 15 y 16 de la Directiva (UE) 2022/2555.

Cuando proceda, la Comisión compartirá el informe con el Alto Representante.

2. Para preparar el informe de revisión de incidentes a que se refiere el apartado 1, ENISA colaborará con todas las partes interesadas pertinentes, incluidos los representantes de los Estados miembros, la Comisión, otras instituciones, organismos y agencias de la UE pertinentes, proveedores de servicios de seguridad gestionada y usuarios de servicios de ciberseguridad. En su caso, ENISA también colaborará con las entidades afectadas por incidentes de ciberseguridad significativos o de gran magnitud. Para respaldar la revisión, ENISA también puede consultar a otros tipos de partes interesadas. Los representantes consultados deberán revelar cualquier posible conflicto de interés.

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

4. Cuando proceda, el informe formulará recomendaciones para mejorar la postura cibernética de la Unión.

5. Siempre que sea posible, se pondrá a disposición del público una versión del informe. Esta versión sólo incluirá información pública.

Capítulo V

PROVISIONES FINALES

Artículo 19

Modificaciones del Reglamento (UE) 2021/694

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

(1) Se modifica el artículo 6 como sigue:

(a) el apartado 1 se modifica como sigue:

(1) se inserta el punto (aa) siguiente:

«a bis) apoyar el desarrollo de un Cyber Shield de la UE, incluidos el desarrollo, el despliegue y el funcionamiento de plataformas SOC nacionales y transfronterizas que contribuyan a la concienciación de la situación en la Unión y a la mejora de las capacidades de inteligencia frente a amenazas cibernéticas de la Unión»;

(2) se añade la letra g) siguiente:

«g) establecer y operar un mecanismo de emergencia cibernética para ayudar a los Estados miembros a prepararse y responder a incidentes de ciberseguridad significativos, como complemento de los recursos y capacidades nacionales y otras formas de apoyo disponibles a nivel de la Unión, incluido el establecimiento de una reserva de ciberseguridad de la UE». ;

(a) El apartado 2 se sustituye por el siguiente:

'2. Las acciones del Objetivo Específico 3 se implementarán 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 Consejo20 con la excepción de acciones

---

20 Reglamento (UE) 2021/887 del Parlamento Europeo y del Consejo, de 20 de mayo de 2021, por el que se crea 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). -31).

implementar la Reserva de Ciberseguridad de la UE, que será implementada por la Comisión y ENISA.».

(2) El artículo 9 se modifica como sigue:

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

«b), 1 776 956 000 EUR para el objetivo específico n° 2: inteligencia artificial;

c), 1 629 566 000 EUR para el objetivo específico n.º 3: Ciberseguridad y confianza;

d), 482 347 000 EUR para el objetivo específico n.º 4 «Habilidades 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 ejecutarán automáticamente y podrá comprometerse y pagarse hasta el 31 de diciembre del ejercicio siguiente.».

(3) En el artículo 14, el apartado 2 se sustituye por el siguiente:

“2. El Programa podrá proporcionar financiación en cualquiera de las formas previstas en el Reglamento Financiero, incluso en particular mediante la contratación como forma primaria, o subvenciones y premios.

Cuando la consecución del objetivo de una acción requiera la adquisición de bienes y servicios innovadores, las subvenciones solo podrán concederse a beneficiarios que sean poderes adjudicadores o entidades adjudicadoras tal 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 comercialmente a gran escala sea necesario para lograr los objetivos de una acción, el poder adjudicador o la entidad adjudicadora podrán autorizar la adjudicación de múltiples contratos dentro del mismo procedimiento de contratación.

Por razones de seguridad pública debidamente justificadas, el poder adjudicador o la entidad adjudicadora podrán exigir que el lugar de ejecución del contrato esté situado en el territorio de la Unión.

Al implementar los procedimientos de contratación para la Reserva de Ciberseguridad de la UE establecidos por el artículo 12 del Reglamento (UE) 2023/XX, la Comisión y ENISA pueden actuar como organismo central de compras para contratar en nombre o en nombre de terceros países asociados al Programa en en consonancia con el artículo 10. La Comisión y ENISA también podrán actuar como mayoristas, comprando, almacenando y revendiendo o donando suministros y servicios, incluidos los alquileres, a esos terceros países. No obstante lo dispuesto en el artículo 169, apartado 3, del Reglamento (UE). XXX/XXXX [Refundición FR], la solicitud de un solo tercer país es suficiente para obligar a la Comisión o ENISA a actuar.

Al implementar los procedimientos de contratación para la Reserva de Ciberseguridad de la UE establecidos por el artículo 12 del Reglamento (UE) 2023/XX, la Comisión y ENISA pueden actuar como organismo central de compras para contratar en nombre de instituciones, organismos y agencias de la Unión. La Comisión y ENISA también pueden actuar como mayoristas, comprando, almacenando y revendiendo o donando suministros y servicios, incluidos los alquileres, a instituciones, organismos y agencias de la Unión. No obstante lo dispuesto en el artículo 169, apartado 3, del Reglamento (UE) XXX/XXXX [Refundición FR], la solicitud de una sola institución, organismo u organismo de la Unión es suficiente para autorizar a la Comisión o a ENISA
actuar.

El Programa también podrá proporcionar financiamiento en forma de instrumentos financieros dentro de las operaciones de combinación."

(4) Se añade el siguiente artículo 16 bis:

En el caso de acciones que implementen el Ciberescudo Europeo establecido por el artículo 3 del Reglamento (UE) 2023/XX, las reglas aplicables serán las establecidas en los artículos 4 y 5 del Reglamento (UE) 2023/XX. En caso de conflicto entre lo dispuesto en el presente Reglamento y los artículos 4 y 5 del Reglamento (UE) 2023/XX, prevalecerán estos últimos y se aplicarán a dichas actuaciones concretas.

(5) El artículo 19 se sustituye por el siguiente:

«Las subvenciones del Programa se concederán y gestionarán de conformidad con el título VIII del Reglamento financiero y podrán cubrir hasta el 100 % de los costes subvencionables, sin perjuicio del principio de cofinanciación establecido en el artículo 190 del Reglamento financiero. Dichas ayudas se concederán y gestionarán según se especifique para cada objetivo específico.

El ECCC puede otorgar apoyo en forma de subvenciones directamente sin una convocatoria de propuestas a los SOC nacionales mencionados en el artículo 4 del Reglamento XXXX y al Consorcio de acogida mencionado en el artículo 5 del Reglamento XXXX, de conformidad con el artículo 195(1).), letra d) del Reglamento financiero.

El ECCC puede otorgar apoyo en forma de subvenciones para el Mecanismo de Emergencia Cibernética como se establece en el Artículo 10 del Reglamento XXXX directamente a los Estados miembros sin una convocatoria de propuestas, de conformidad con el Artículo 195(1), letra (d) de el Reglamento Financiero.

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

Para el apoyo de la asistencia mutua para la respuesta a un incidente de ciberseguridad significativo o de 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 Reglamento Financiero, en casos debidamente justificados, los costes podrán considerarse subvencionables incluso si se han incurrido antes de la presentación de la solicitud de subvención.»;

(6) Los anexos I y II se modifican de conformidad con 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 un informe sobre la evaluación y revisión del presente Reglamento al Parlamento Europeo y al Consejo.

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) 182/2011.

2. Cuando se haga referencia al presente apartado, el artículo 5 del Reglamento (UE) 182/2011 se aplicarán.

Artículo 22

Entrada en vigor

El presente Reglamento entrará en vigor el vigésimo día siguiente al 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,

Por el Parlamento Europeo
El presidente

para el Consejo
El presidente

ESTADO FINANCIERO LEGISLATIVO

1. MARCO DE LA PROPUESTA/INICIATIVA

1.1. Título de la propuesta/iniciativa

1.2. Área(s) política(s) en cuestión

1.3. La propuesta/iniciativa se refiere a:

1.4. Objetivo(s)

1.4.1. Objetivos generales)

1.4.2. Objetivos específicos)

1.4.3. Resultado(s) esperado(s) e impacto

1.4.4. Indicadores de desempeño

1.5. Motivos de la propuesta/iniciativa

1.5.1. Requisitos que deben cumplirse a corto o largo plazo, incluido un cronograma detallado para despliegue de la implementación de la iniciativa

1.5.2. Valor añadido de la participación de la Unión (puede deberse a diferentes factores, por ejemplo, ganancias de coordinación, seguridad jurídica, mayor eficacia o complementariedades). A los efectos de este punto, el «valor añadido de la participación de la Unión» es el valor resultante de la intervención de la Unión, que es adicional al valor que de otro modo habrían creado los Estados miembros por sí solos.

1.5.3. Lecciones aprendidas de experiencias similares en el pasado

1.5.4. Compatibilidad con el Marco Financiero Plurianual y posibles sinergias con otros instrumentos apropiados

1.5.5. Evaluación de las diferentes opciones de financiación disponibles, incluido el alcance de la redistribución

1.6. Duración e impacto financiero de la propuesta/iniciativa

1.7. Método(s) de ejecución del presupuesto planificado

2. MEDIDAS DE GESTIÓN

2.1. Normas de seguimiento y presentación de informes

2.2. Sistema(s) de gestión y control

2.2.1. Justificación de los modos de gestión, los mecanismos de ejecución de la financiación, las modalidades de pago y la estrategia de control propuesta

2.2.2. Información sobre los riesgos identificados y el o los sistemas de control interno implantados para mitigarlos

2.2.3. Estimación y justificación de la rentabilidad de los controles (proporción de "costos de control ÷ valor de los fondos relacionados gestionados") y evaluación de los niveles esperados de riesgo de error (al momento del pago y al cierre)

2.3. Medidas para prevenir el fraude y las irregularidades

3. IMPACTO FINANCIERO ESTIMADO DE LA PROPUESTA/INICIATIVA

1. MARCO DE LA PROPUESTA/INICIATIVA

1.1. Título de la propuesta/iniciativa

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

1.2. Área(s) política(s) en cuestión

Una Europa apta para la era digital

Inversiones Estratégicas Europeas

Actividad: Dando forma al futuro digital de Europa.

1.3. La propuesta/iniciativa se refiere a:

una nueva acción

una nueva acción después de un proyecto piloto/acción preparatoria33

la extensión de una acción existente

una fusión o redirección de una o más acciones hacia otra/una nueva acción

1.4. Objetivo(s)

1.4.1. Objetivos generales)

La Ley de cibersolidaridad reforzará la solidaridad a nivel de la Unión para detectar, prepararse y responder mejor a las amenazas e incidentes de ciberseguridad. Esto me pertenece:

a) reforzar la detección común de la UE y la conciencia situacional de las ciberamenazas e incidentes;

b) reforzar la preparación de las entidades críticas en toda la UE y fortalecer la solidaridad mediante el desarrollo de capacidades de respuesta comunes frente a incidentes de ciberseguridad significativos o de gran escala, incluso poniendo a disposición de terceros países apoyo para la respuesta a incidentes. asociado a DEP;

c) mejorar la resiliencia de la Unión y contribuir a una respuesta eficaz mediante el examen y la evaluación de incidentes significativos o de gran escala, incluida la extracción de lecciones aprendidas y, en su caso, recomendaciones.

1.4.2. Objetivos específicos)

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

(a) El despliegue de una infraestructura paneuropea de Centros de Operaciones de Seguridad (European Cyber Shield) para construir y mejorar las capacidades comunes de detección y conocimiento de la situación.

(b) La creación de un Mecanismo de Emergencia de Ciberseguridad para apoyar a los Miembros Estados en la preparación, respuesta y recuperación inmediata de importantes

33 A que se refiere el artículo 58, apartado 2, letras a) o b), del Reglamento financiero.

e incidentes de ciberseguridad a gran escala. El apoyo para la respuesta a incidentes también se pondrá a disposición de las instituciones, organismos, oficinas y agencias europeas de la Unión (EUIBA).

Estas acciones contarán con el apoyo financiero del DEP, que este instrumento legislativo modificará para establecer las acciones antes mencionadas, prever el apoyo financiero para su desarrollo y aclarar las condiciones para beneficiarse del apoyo financiero.

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

1.4.3. Resultado(s) esperado(s) e impacto

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

La propuesta traería beneficios significativos a las diversas partes interesadas. El Escudo cibernético europeo mejorará las capacidades de detección de ciberamenazas de los Estados miembros. El Mecanismo de emergencia cibernética complementará las acciones de los Estados miembros a través del apoyo de emergencia para la preparación, la respuesta y la recuperación/restauración inmediata del funcionamiento de los servicios esenciales.

Estas acciones fortalecerán la posición competitiva de la industria y las empresas en Europa en la economía digitalizada y respaldarán su transformación digital, al reforzar el nivel de ciberseguridad en el Mercado Único Digital. En particular, tiene como objetivo aumentar la resiliencia de los ciudadanos, empresas y entidades que operan en sectores críticos o altamente críticos frente a las crecientes amenazas a la ciberseguridad, que pueden tener impactos sociales y económicos devastadores. Lo hará invirtiendo en herramientas que permitan una detección y una respuesta más rápidas a las amenazas e incidentes de ciberseguridad, y ayudará a los Estados miembros a prepararse mejor para responder a incidentes de ciberseguridad significativos y a gran escala. Esto también debería ayudar a dotar a Europa de capacidades más sólidas en estas áreas, especialmente en lo que respecta a la recopilación y el análisis de datos sobre amenazas e incidentes de ciberseguridad.

1.4.4. Indicadores de desempeño Especificar

los indicadores para monitorear el progreso y los logros.

Para promover la solidaridad a nivel de la Unión, podrían tenerse en cuenta varios indicadores:

(1) La cantidad de infraestructura o herramientas de ciberseguridad, o ambas, adquiridas conjuntamente

(2) Número de acciones de apoyo a la preparación y respuesta a incidentes de ciberseguridad en el marco del Mecanismo de Emergencia Cibernética.

1.5. Justificación de la propuesta/iniciativa 1.5.1. Requisitos

que deben cumplirse a corto o largo plazo, incluido un cronograma detallado para despliegue de la implementación de la iniciativa

El Reglamento debe ser plenamente aplicable poco después de su adopción, es decir, el vigésimo día siguiente al de su publicación en el Diario Oficial de la Unión Europea.

1.5.2. Valor añadido de la participación de la Unión (puede deberse a diferentes factores, por ejemplo, ganancias de coordinación, seguridad jurídica, mayor eficacia o complementariedades). A los efectos de este punto, el «valor añadido de la participación de la Unión» es el valor resultante

de la intervención de la Unión, que es adicional al valor que, de otro modo, habrían creado los Estados miembros por sí solos.

La fuerte naturaleza transfronteriza de las amenazas a la ciberseguridad en general y el creciente número de riesgos e incidentes, que tienen efectos indirectos a través de fronteras, sectores y productos, significan que los objetivos de la presente intervención no pueden ser alcanzados de manera efectiva por los Estados miembros por sí solos. y requieren una acción común y solidaridad a nivel de la Unión. La experiencia de contrarrestar las ciberamenazas derivadas de la guerra contra Ucrania, junto con las lecciones aprendidas de un ejercicio de ciberseguridad realizado bajo la Presidencia francesa (EU CyCLES), mostró que deben desarrollarse mecanismos concretos de apoyo mutuo, en particular la cooperación con el sector privado. lograr la solidaridad a nivel de la UE. En este contexto, las Conclusiones del Consejo de 23 de mayo de 2022 sobre el desarrollo de la postura cibernética de la Unión Europea piden a la Comisión que presente una propuesta sobre un nuevo Fondo de Respuesta de Emergencia para la Ciberseguridad. El apoyo y las acciones a nivel de la Unión para detectar mejor las amenazas a la ciberseguridad y aumentar las capacidades de preparación y respuesta proporcionan valor añadido porque evita la duplicación de esfuerzos en la Unión y los Estados miembros. Conduciría a una mejor explotación de los activos existentes ya una mayor coordinación e intercambio de información sobre las lecciones aprendidas.

1.5.3. Lecciones aprendidas de experiencias similares en el pasado

Con respecto a la conciencia situacional y la detección bajo el Escudo Cibernético Europeo, se realizó una convocatoria de expresión de interés para adquirir conjuntamente herramientas e infraestructura para establecer SOC transfronterizos, y una convocatoria de subvenciones para permitir el desarrollo de capacidades de SOC al servicio de organizaciones públicas y privadas, bajo Programa de trabajo de ciberseguridad DEP 2021-2022.

En lo que respecta a la preparación y respuesta a incidentes, la Comisión ha establecido un programa a corto plazo para apoyar a los Estados miembros, mediante financiación adicional asignada a ENISA, con el fin de reforzar inmediatamente la preparación y las capacidades para responder a ciberincidentes graves. Los servicios cubiertos incluyen acciones de preparación, como pruebas de penetración de entidades críticas para identificar vulnerabilidades. También fortalece las posibilidades de ayudar a los Estados miembros en caso de un incidente importante que afecte a entidades críticas. La implementación por parte de ENISA de este programa a corto plazo está en marcha y ya ha proporcionado información valiosa relevante que se ha tenido en cuenta en la preparación de este Reglamento.

1.5.4. Compatibilidad con el Marco Financiero Plurianual y posibles sinergias con otros instrumentos apropiados

La Ley de Solidaridad Cibernética se basará en las acciones actualmente respaldadas por la Unión y los Estados miembros para mejorar la conciencia situacional y la detección de amenazas cibernéticas, y para responder a incidentes de ciberseguridad a gran escala y transfronterizos. Además, el instrumento es coherente con otros marcos de gestión de crisis, incluido el IPCR, la Política Común de Seguridad y Defensa, incluidos los Equipos de respuesta cibernética rápida, y la asistencia proporcionada por un Estado miembro a otro Estado miembro en el contexto del artículo 42 (7) del Tratado de la Unión Europea. La nueva propuesta también complementaría y respaldaría las estructuras desarrolladas en el marco de otros instrumentos de ciberseguridad, como la Directiva (UE) 2022/2555 (Directiva NIS2) o el Reglamento 2019/881 (Ley de ciberseguridad).

1.5.5. Evaluación de las diferentes opciones de financiación disponibles, incluido el alcance de la redistribución

La gestión de las áreas de acción asignadas a ENISA se ajusta a su mandato actual y tareas generales. Estas áreas de actuación pueden requerir perfiles específicos o nuevas asignaciones, pero estas pueden ser absorbidas por los recursos existentes de ENISA y resueltas mediante la reasignación o vinculación de varias asignaciones. ENISA está implementando actualmente un programa a corto plazo que fue establecido en 2022 por la Comisión para reforzar inmediatamente la preparación y las capacidades para responder a incidentes cibernéticos importantes. Los servicios cubiertos incluyen posibilidades de ayudar a los Estados miembros en caso de un incidente importante que afecte a entidades críticas. La implementación por parte de ENISA de este programa a corto plazo está en marcha y ya ha proporcionado información valiosa relevante que se ha tenido en cuenta en la preparación de este Reglamento. Los recursos asignados para el programa a corto plazo también podrían utilizarse en el contexto de este Reglamento. .

1.6. Duración e impacto financiero de la propuesta/iniciativa

duración limitada

– en vigor a partir de la fecha de adopción de la propuesta de Reglamento de la Parlamento Europeo y del Consejo sobre el refuerzo de la solidaridad y las capacidades en la Unión para detectar, prepararse y responder a las amenazas e incidentes de ciberseguridad ('la Ley de Solidaridad Cibernética') – Impacto financiero de 2023 a

2027 para los créditos de compromiso y de 2023 a 2031 para los créditos de pago34 .

duración ilimitada

– Implementación con un período de puesta en marcha de AAAA a AAAA,

– seguido de funcionamiento a gran escala.

1.7. Método(s) de ejecución del presupuesto previsto35 Gestión

directa por parte de la Comisión

– por sus departamentos, incluido su personal en las delegaciones de la Unión; – por

las agencias ejecutivas Gestión

compartida con los Estados miembros Gestión indirecta al

encomendar tareas de ejecución presupuestaria a:

– terceros países o los organismos que estos hayan designado;

– organizaciones internacionales y sus agencias (por especificar); – el BEI y el

Fondo Europeo de Inversiones; – organismos a que se

refieren los artículos 70 y 71 del Reglamento Financiero; – organismos de derecho público;

– organismos de derecho privado con misión de servicio público en la medida en que estén provistos de garantías financieras adecuadas; – organismos de derecho

privado de un Estado miembro encargados de la ejecución de una asociación público-privada y provistos de garantías financieras adecuadas;

– órganos o personas encargadas de la ejecución de acciones específicas de la PESC en virtud del Título V del TUE, e identificadas en el acto de base correspondiente.

– Si se indica más de un modo de gestión, proporcione detalles en la sección 'Comentarios'.

Comentarios

Las acciones relacionadas con el Escudo Cibernético Europeo serán implementadas por el ECCC. Hasta que el ECCC tenga la capacidad de implementar su propio presupuesto, la Comisión Europea implementará las acciones en gestión directa en nombre del ECCC. La ECCC puede seleccionar

34 Las acciones de la Ley deberían estar respaldadas por el próximo marco financiero plurianual.

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

entidades en base a convocatorias de manifestación de interés para participar en la adquisición conjunta de herramientas. El ECCC puede otorgar subvenciones para el funcionamiento de estas herramientas.

Además, el ECCC puede otorgar subvenciones para acciones de preparación en el marco del Mecanismo de Emergencia de Ciberseguridad.

La Comisión tendrá la responsabilidad general de la implementación 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 ENISA. Las acciones asignadas por este Reglamento a ENISA están en línea con su mandato actual. Esas acciones incluyen: (i) Apoyar al Grupo de Cooperación NIS en el desarrollo de las acciones de preparación de acuerdo con las evaluaciones de riesgo; (ii) ayudar a la Comisión a establecer y supervisar la implementación de la Reserva de Ciberseguridad de la UE, incluida la recepción y el procesamiento de las solicitudes de apoyo; (iii) desarrollar plantillas para facilitar la presentación de solicitudes de apoyo y acuerdos específicos que se celebren entre el proveedor de servicios y el usuario al que se proporciona el apoyo bajo la Reserva de Ciberseguridad de la UE; (iv) revisar y evaluar amenazas, vulnerabilidades y acciones de mitigación con respecto a incidentes de ciberseguridad significativos o de gran escala específicos y preparar informes de los mismos.

Todas estas asignaciones se estiman en aproximadamente 7 FTE de los recursos existentes de ENISA, basándose en la experiencia y el trabajo preparatorio que ENISA realiza actualmente dentro del piloto del apoyo de emergencia para la preparación y respuesta a incidentes.

2. MEDIDAS DE GESTIÓN

2.1. Normas de seguimiento y presentación de informes

Especificar frecuencia y condiciones.

La Comisión supervisará la implementación, 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 revisión del presente Reglamento al Parlamento Europeo y al Consejo en un plazo de cuatro años a partir de la fecha de su aplicación.

2.2. Sistema(s) de gestión y control

2.2.1. Justificación de los modos de gestión, los mecanismos de ejecución de la financiación, las modalidades de pago y la estrategia de control propuesta

El Reglamento introduce un marco para la ejecución de la financiación de la UE con vistas a aumentar la resiliencia de la ciberseguridad mediante acciones que mejoren las capacidades de detección, respuesta y recuperación en caso de incidentes de ciberseguridad significativos y a gran escala. Las unidades dentro de la DG CNECT a cargo del campo de la política gestionarán la implementación de la Directiva.

Para hacer frente a las nuevas tareas, es necesario dotar adecuadamente los servicios de la Comisión. Se estima que la aplicación del nuevo Reglamento requerirá 6 FTE (3 AD y 3 CA) para cubrir las siguientes tareas:

- Determinar las acciones de preparación de acuerdo con las evaluaciones de riesgo;
- Garantizar la interoperabilidad entre las plataformas SOC transfronterizas;
- Elaborar posibles Actos de Ejecución (dos para los SOC y dos para el Mecanismo de Emergencia de Ciberseguridad);
- Administrar los Acuerdos de Hosting y Uso para los SOC;
- Constitución y gestión de la Reserva de Ciberseguridad de la UE, directamente o mediante un acuerdo de contribución a ENISA. En caso de convenio de contribución a ENISA, elaborar y supervisar la ejecución del convenio de contribución para las tareas encomendadas a ENISA;
- Participar en los grupos de consulta convocados por ENISA para revisar y evaluar incidentes de ciberseguridad significativos y de gran magnitud y elaborar los informes.

2.2.2. Información sobre los riesgos identificados y el o los sistemas de control interno implantados para mitigarlos

Un riesgo identificado para el Escudo Cibernético Europeo es que los Estados miembros no comparten una cantidad suficiente de información relevante sobre amenazas cibernéticas dentro de las plataformas SOC transfronterizas o entre plataformas transfronterizas y otras entidades relevantes a nivel de la UE. Para mitigar estos riesgos, la asignación de fondos seguirá una convocatoria de manifestación de interés en la que los Estados miembros se comprometan a compartir una cierta cantidad de información con el nivel de la UE. Este compromiso luego se formalizará en un acuerdo de alojamiento y uso, que otorgará a la ECCC los poderes para realizar auditorías para garantizar que las herramientas y la infraestructura adquiridas conjuntamente se utilicen de acuerdo

el acuerdo. Los compromisos de un alto nivel de intercambio de información dentro de los SOC transfronterizos se formalizarán en un acuerdo de consorcio.

Un riesgo identificado para el Mecanismo de Emergencia Cibernética es que los usuarios que participan en el mecanismo no toman las medidas suficientes para garantizar la preparación frente a los ataques cibernéticos. Por ese motivo, para poder recibir apoyo de la Reserva de Ciberseguridad de la UE, los usuarios están obligados a tomar dichas medidas de preparación. Al enviar 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, que se tendrán en cuenta durante la evaluación de las solicitudes a la Reserva de Ciberseguridad de la UE.

2.2.3. Estimación y justificación de la rentabilidad de los controles (proporción de "costos de control ÷ valor de los fondos relacionados gestionados") y evaluación de los niveles esperados de riesgo de error (al momento del pago y al cierre)

Dado que las normas de participación en el programa Europa Digital aplicables a las ayudas en virtud de la Ley de Solidaridad Cibernética son similares a las que utilizará la Comisión en sus programas de trabajo, y con una población de beneficiarios con un perfil de riesgo similar al de los programas bajo directa gestión, se puede esperar que el margen de error sea similar al previsto por la Comisión para el programa Europa Digital, es decir, para dar una garantía razonable de que el riesgo de error en el transcurso del período de gasto plurianual es, sobre una base anual, dentro de un rango de 2-5 %, con el objetivo final de lograr una tasa de error residual lo más cercana posible al 2 % al cierre de los programas plurianuales, una vez que se haya determinado el impacto financiero de todas las auditorías, medidas de corrección y recuperación tenido en cuenta.

2.3. Medidas para prevenir el fraude y las irregularidades

Especificar las medidas de prevención y protección existentes o previstas, por ejemplo, de la Estrategia Antifraude.

En el caso del Escudo Cibernético Europeo, las ECCC tendrán la facultad de auditar, sobre la base del acceso a la información y controles sobre el terreno, de las herramientas e infraestructuras adquiridas conjuntamente, de conformidad con el acuerdo de alojamiento y uso a ser firmado entre el consorcio anfitrión y el ECCC.

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

3. IMPACTO FINANCIERO ESTIMADO DE LA PROPUESTA/INICIATIVA

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

• Líneas presupuestarias existentes

Por orden de rúbricas del marco financiero plurianual y líneas presupuestarias.

Rúbrica del marco financiero plurianual	Línea presupuestaria	tipo de gasto	Contribución			
	Número	Dif./No dif.[36]	de Países de la AELC[37]	de países candidatos y candidatos potenciales[38]	de otros terceros países	otro asignado ganancia
1	02 04 01 10 - Programa Europa Digital - La seguridad cibernética	Dif.	SÍ	SÍ	NO	NO
1	02 04 01 11 - Programa Europa Digital - Ciberseguridad Europea Industrial, Competencia tecnológica y de investigación Centro	diferencia	SÍ	SÍ	NO	NO
1	02 04 03 - Programa Europa Digital - Inteligencia artificial	diferencia	SÍ	SÍ	NO	NO
1	02 04 04 - Programa Europa Digital – Habilidades	diferencia	SÍ	SÍ	NO	NO
1	02 01 30 - Gastos de apoyo para la Programa Europa Digital	No Dif	SÍ	SÍ	NO	NO

[36] Dif. = Créditos diferenciados / Non-dif. = Créditos no disociados.

[37] EFTA: 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 del impacto estimado en las consignaciones operativas

– La propuesta/iniciativa no requiere el uso de créditos operativos

– X La propuesta/iniciativa requiere el uso de créditos operativos, como se explica a continuación:

millones de euros (al tercer decimal)

Rúbrica del marco financiero plurianual	Número 1	Mercado Único, Innovación y Digital

La propuesta no aumentará el nivel total de compromisos en el marco del Programa Europa Digital. De hecho, la contribución a esta iniciativa es una redistribución de los compromisos provenientes de SO2 y SO4 para reforzar el presupuesto de SO3 y ECCC. Cualquier aumento de los compromisos en el marco del Programa Europa Digital derivado de una revisión del MFP podría utilizarse a efectos de esta iniciativa.

DG CONECTAR			Año 2025	Año 2026	Año 2027	Año 2028+	Ingrese tantos años como sea necesario para mostrar la duración del impacto (ver punto 1.6)			TOTAL
Créditos operativos										
Línea presupuestaria 39 02.040110 (redistribución de 02.0403 y 02.0404)	compromisos	(1a)	15,000	15,000	6,000	pm				36,000
	Pagos	(2a)	15,000	15,000	6,000					36,000
Línea presupuestaria 02.040111.02 (redistribución de 02.0403 y 02.0404)	compromisos	(1b)	13.000	23.000	28.000	pm				64.000
	Pagos	(2b)	8.450	18.200	25.250	12.100				64.000
Créditos de carácter administrativo financiados con cargo a la dotación de programas específicos40 Línea										
presupuestaria 02.0130		(3)	0,150	0,150	0,150	pm				0,450
Apropiaciones TOTALES	compromisos	=1a+1b	28,150	38,150	34,150	pm				100.450

39 Según la nomenclatura presupuestaria oficial.

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

para DG CONECTAR		+3								
	Pagos	=2a+2b +3	23.600	33.350	31.400	12.100				100.450

TOTAL créditos operativos	compromisos	(4)	28.000	38.000	34.000		pm			100,000
	Pagos	(5)	23.450	33.200	31.250	12.100				100,000
TOTAL créditos de carácter administrativo financiados con cargo a la dotación para programas específicos		(6)	0,150	0,150	0,150		pm			0,450
TOTAL créditos de la RÚBRICA 1 del marco financiero plurianual	compromisos	=4+ 6	28.150	38.150	34.150		pm			100.450
	Pagos	=5+ 6	23.600	33.350	31.400	12.100				100.450

Si más de un encabezado operativo se ve afectado por la propuesta/iniciativa, repita la sección anterior:

TOTAL de créditos operativos (todas las rúbricas operativas)	compromisos	(4)	28.000	38.000	34.000		pm			100,000
	Pagos	(5)	23.450	33.200	31.250	12.100				100,000
TOTAL créditos de carácter administrativo financiados con cargo a la dotación para programas específicos (todas las rúbricas operativas)		(6)	0,150	0,150	0,150					0,450
TOTAL créditos de las RÚBRICAS 1 a 6 del marco financiero plurianual (Cantidad de referencia)	compromisos	=4+ 6	28.150	38.150	34.150		pm			100.450
	Pagos	=5+ 6	23.600	33.350	31.400	12.100				100.450

Rúbrica del marco financiero plurianual	7	'Gastos administrativos'

Esta sección debe rellenarse utilizando los «datos presupuestarios de carácter administrativo» que se introducirán en primer lugar en el anexo de la ficha financiera legislativa (anexo 5 de la decisión de la Comisión sobre las normas internas para la ejecución de la sección de la Comisión del presupuesto general de la Unión Europea), que se carga en DECIDE con fines de consulta interservicios.

millones de euros (al tercer decimal)

		Año 2025	Año 2026	Año 2027	Año 2028+	Ingrese tantos años como sea necesario para mostrar la duración del impacto (ver punto 1.6)			TOTAL
DG: CONECTAR									
Recursos humanos		0,786	0,786	0,786	pm				2,358
Otros gastos administrativos		0,035	0,035	0,035	pm				0,105
CONEXIÓN DG TOTAL	Asignaciones	0,821	0,821	0,821					2,463

TOTAL créditos de la RÚBRICA 7 del marco financiero plurianual	(Compromisos totales = Pagos totales)	0,821	0,821	0,821					2,463

millones de euros (al tercer decimal)

		Año 2025	Año 2026	Año 2027	Año 2028+	Ingrese tantos años como sea necesario para mostrar la duración del impacto (ver punto 1.6)			TOTAL
TOTAL créditos de las RÚBRICAS 1 a 7 del marco financiero plurianual	compromisos	28.971	38.971	34.971	pm				102,913
	Pagos	24.421	34.171	32.221	12,100				102,913

3.2.2. Producto estimado financiado con consignaciones operativas

Créditos de compromiso en millones EUR (al tercer decimal)

Indicar objetivos y productos			Año norte		Año N+1		Año N+2		Año N+3		Ingrese tantos años como sea necesario para mostrar la duración del impacto (ver punto 1.6)						TOTAL	
	SALIDAS																	
	Tipo41	promedio costo de ge	ºN	Costo	ºN	Costo	ºN	Costo	ºN	Costo	ºN	Costo	ºN	Costo	ºN	Costo	Total No	Total costo
OBJETIVO ESPECÍFICO nº 142…																		
- Producción																		
- Producción																		
- Producción																		
Subtotal del objetivo específico nº 1																		
OBJETIVO ESPECÍFICO nº 2 ...																		
- Producción																		
Subtotal del objetivo específico nº 2																		
TOTALES																		

41 Los productos son productos y servicios a suministrar (por ejemplo: número de intercambios de estudiantes financiados, número de kilómetros de caminos construidos, etc.).

42 Como se describe en el punto 1.4.2. 'Objetivos específicos)…'

3.2.3. Resumen del impacto estimado en las asignaciones administrativas

– La propuesta/iniciativa no requiere el uso de créditos de un naturaleza administrativa

– X La propuesta/iniciativa exige el uso de créditos de carácter administrativo naturaleza, como se explica a continuación:

millones de euros (al tercer decimal)

	Año 2025	Año r 2026	Año 2027	Año N+3	Ingrese tantos años como sea necesario para mostrar la duración del impacto (ver 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 RÚBRICA 7 del marco financiero plurianual	0,821	0,821	0,821					2,463
Fuera de PARTIDA 743 del plurianual marco financiero								
Recursos humanos								
Otros gastos de carácter administrativo naturaleza	0,150	0,150	0,150					0,450
Total parcial fuera de la PARTE 7 del plurianual marco financiero	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 con los créditos de la DG que ya estén asignados a la gestión de la acción y/o hayan sido reasignados dentro de la DG, junto con, si es necesario, cualquier asignación adicional que pueda ser concedidas a la DG gestora con arreglo al procedimiento de asignación anual y teniendo en cuenta las restricciones presupuestarias.

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

3.2.3.1. Requerimientos estimados de recursos humanos

– La propuesta/iniciativa no requiere el uso de recursos humanos.

– X La propuesta/iniciativa requiere el uso de recursos humanos, como se explica abajo:

Estimación que se expresará en unidades equivalentes a tiempo completo

		Año 2025	Año 2026	Año 2027	Año N+3	Ingrese tantos años como sea necesario para mostrar la duración del impacto (ver punto 1.6)		
Puestos de plantilla (funcionarios y temporales)								
20 01 02 01 (Sede y Representación de la Comisión Oficinas)		3	3	3				
20 01 02 03 (Delegaciones)								
01 01 01 01 (Investigación indirecta)								
01 01 01 11 (Investigación directa)								
Otras líneas presupuestarias (especificar)								
Personal externo (en unidad equivalente a tiempo completo: FTE)[44]								
20 02 01 (AC, END, INT del 'sobre global')		3	3	3				
20 02 03 (AC, AL, END, INT y JPD en las delegaciones)								
XX 01 xx yy zz [45]	- en la Sede							
	- en Delegaciones							
01 01 01 02 (AC, END, INT - Investigación indirecta)								
01 01 01 12 (AC, END, INT - Investigación directa)								
Otras líneas presupuestarias (especificar)								
TOTAL		6	6	6				

XX es el área política o el título del presupuesto en cuestión.

Los recursos humanos necesarios serán proporcionados por el personal de la DG que ya esté asignado a la gestión de la acción y/o haya sido reasignado dentro de la DG, junto con cualquier asignación adicional que pueda otorgarse a la DG gestora en virtud de la asignación anual, si fuera necesario. procedimiento y teniendo en cuenta las restricciones presupuestarias.

Descripción de las tareas a realizar:

Funcionarios y personal temporal	- determinar las acciones de preparación de acuerdo con las evaluaciones de riesgo (art. 11) - Elaborar posibles Actos de Ejecución (dos para los SOC y dos para el Mecanismo de Emergencia de Ciberseguridad) - Gestionar los Contratos de Hosting y Uso de los SOCs; - Establecer y gestionar la Reserva de Ciberseguridad de la UE, directamente o mediante un acuerdo de contribución a ENISA.
Personal externo	Bajo la supervisión de un funcionario, - determinar las acciones de preparación de acuerdo con las evaluaciones de riesgo (art. 11) - Elaborar posibles Actos de Ejecución (dos para los SOC y dos para el Mecanismo de Emergencia de Ciberseguridad) - Gestionar los Contratos de Hosting y Uso de los SOCs; - Establecer y gestionar la Reserva de Ciberseguridad de la UE, directamente o mediante un acuerdo de contribución a ENISA.

[44] AC= Personal Contratado; AL = Personal local; END= Experto Nacional Adscrito; INT = personal de la agencia; JPD= Profesionales Junior en Delegaciones.

[45] Sublímite para personal externo cubierto por créditos operativos (antiguas líneas 'BA').

3.2.4. Compatibilidad con el actual marco financiero plurianual

La propuesta/iniciativa:

– X puede financiarse íntegramente mediante redistribución dentro de la rúbrica correspondiente de la Marco Financiero Plurianual (MFP).

Explique qué reprogramación se requiere, especificando las líneas presupuestarias correspondientes y los montos correspondientes. Proporcione una tabla de Excel en el caso de una reprogramación importante.

	2023	2024	2025	2026	total 2027	
SO1	16.232.897	20.528.765	17.406.899	16.223.464	10.022.366	80.414.391
SO2 inicial	226.316.819	295.067.000	195.649.000	221.809.000	246.608.000	1.185.449.819
A la iniciativa CYBER			18.000.000	28.000.000	19.000.000	65.000.000
NUEVO 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
De SO2-SO4			15.000.000	15.000.000	6.000.000	36.000.000
nuevo SO3	24.361.553	35.596.172	18.638.000	18.638.000	17.175.000	114.408.725
Inicial ECCC	176.222.303	208.374.879	104.228.130	90.704.986	84.851.497	664.381.795
De SO2-SO4			13.000.000	23.000.000	28.000.000	64.000.000
Nuevo ECCC	176.222.303	208.374.879	117.228.130	113.704.986	112.851.497	728.381.795
SO4 inicial	66.902.708	64.892.032	56.577.977	70.477.245	72.107.201	330.957.163
A la iniciativa CYBER			10.000.000	10.000.000	15.000.000	35.000.000
NUEVO SO4	66.902.708	64.892.032	46.577.977	60.477.245	57.107.201	295.957.163

– requiere el uso del margen no asignado bajo la rúbrica correspondiente del MFP y/o el uso de los instrumentos especiales tal como se definen en el Reglamento MFP.

Explique lo que se requiere, especificando las rúbricas y líneas presupuestarias correspondientes, los importes correspondientes y los instrumentos que se propone utilizar.

– exige una revisión del MFP.

Explique lo que se requiere, especificando las rúbricas y líneas presupuestarias correspondientes y los importes correspondientes.

3.2.5. Contribuciones de terceros

La propuesta/iniciativa:

– X no contempla la cofinanciación por terceros

– prevé la cofinanciación por terceros estimada a continuación:

Créditos en millones EUR (al tercer decimal)

	Año N46	Año N+1	Año N+2	Año N+3	Ingrese tantos años como sea necesario para mostrar la duración del impacto (ver punto 1.6)			Total
Especificar el organismo cofinanciador								

46 El año N es el año en que comienza la implementación de la propuesta/iniciativa. Reemplace "N" por el primer año de implementación esperado (por ejemplo: 2021). Lo mismo para los años siguientes.

TOTAL créditos cofinanciados								

3.3. Impacto estimado en los ingresos

– X La propuesta/iniciativa no tiene impacto financiero en los ingresos.

– La propuesta/iniciativa tiene el siguiente impacto financiero:

  – sobre recursos propios

  – sobre otros ingresos

  – por favor indique, si los ingresos están asignados a líneas de gastos

millones de euros (al tercer decimal)

Línea de ingresos presupuestarios:	Asignaciones disponibles para el actual año financiero	Impacto de la propuesta/iniciativa47						
		Año norte	Año N+1	Año N+2	Año N+3	Ingrese tantos años como sea necesario para mostrar la duración del impacto (ver punto 1.6)		
Artículo								

Para los ingresos afectados, especifique las líneas de gasto presupuestario afectadas.

[…]

Otras observaciones (por ejemplo, método/fórmula utilizada para calcular el impacto en los ingresos o cualquier otra información).

[…]

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