Consejo de la Unión Europea

Bruselas, 18 de noviembre de 2024
(OR. en)

15644/24

Expediente interinstitucional: 2023/0109(COD)

CODEC 2118
CYBER 326
TELECOM 335
CADREFIN 188
FIN 1009
BUDGET 63
IND 514
JAI 1656
MI 926
DATAPROTECT 318
RELEX 1429
PE 252

NOTA INFORMATIVA

De:	Secretaría General del Consejo
A:	Comité de Representantes Permanentes/Consejo
Asunto:	Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO por el que se establecen medidas destinadas a reforzar la solidaridad y las capacidades en la Unión a fin de detectar amenazas e incidentes de ciberseguridad, prepararse para ellos y responder a ellos – Resultado de la primera lectura del Parlamento Europeo y procedimiento de corrección de errores (Estrasburgo, 24 de abril de 2024, y Bruselas, 14 de noviembre de 2024)

I. INTRODUCCIÓN

De conformidad con lo dispuesto en el artículo 294 del TFUE y en la Declaración común sobre las modalidades prácticas del procedimiento de codecisión[1], el Consejo, el Parlamento Europeo y la Comisión han mantenido una serie de contactos informales con vistas a alcanzar un acuerdo en primera lectura sobre este expediente legislativo.

[1] DO C 145 de 30.6.2007, p. 5.

Estaba previsto que el expediente[2] fuese objeto de un procedimiento de corrección de errores[3] en el Parlamento Europeo tras la aprobación por el Parlamento saliente de su posición en primera lectura.

II. VOTACIÓN

En su sesión del 24 de abril de 2024, el Parlamento Europeo aprobó la enmienda 2 (sin revisión jurídico-lingüística) a la propuesta de la Comisión, la enmienda 3, que contiene una declaración de la Comisión, y una resolución legislativa, que constituye la posición del Parlamento Europeo en primera lectura. Dicha posición recoge lo acordado provisionalmente entre las instituciones.

El 14 de noviembre de 2024, tras la formalización jurídico- lingüística del texto aprobado, el Parlamento Europeo aprobó una corrección de errores de la posición aprobada en primera lectura.

Merced a dicha corrección de errores, el Consejo debería poder aprobar la posición del Parlamento Europeo que figura en el anexo[4], poniendo fin así a la primera lectura en ambas instituciones.

El acto se adoptaría entonces con la redacción correspondiente a la posición del Parlamento Europeo.

---

2 10819/24 + COR 1.

3 Reglamento Interno del Parlamento Europeo, artículo 251.

4 El texto de la corrección de errores figura en el anexo. Se presenta en forma de texto consolidado en el que los cambios respecto de la propuesta de la Comisión se señalan mediante negrita y cursiva. El símbolo « ▌ » indica la supresión de texto.

P9_TA(2024)0355

Reglamento de Cibersolidaridad

Resolución legislativa del Parlamento Europeo, de 24 de abril de 2024, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen medidas destinadas a reforzar la solidaridad y las capacidades en la Unión a fin de detectar amenazas e incidentes de ciberseguridad, prepararse para ellos y responder a ellos (COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

(Procedimiento legislativo ordinario: primera lectura)

El Parlamento Europeo,

– Vista la propuesta de la Comisión al Parlamento Europeo y al Consejo (COM(2023)0209),

– Vistos el artículo 294, apartado 2, y los artículos 173, apartado 3, y 322, apartado 1, letra a), del Tratado de Funcionamiento de la Unión Europea, conforme a los cuales la Comisión le ha presentado su propuesta (C9-0136/2023),

– Visto el artículo 294, apartado 3, del Tratado de Funcionamiento de la Unión Europea,

– Vista la opinión del Tribunal de Cuentas de 18 de abril de 2023[1],

– Vista la opinión del Comité Económico y Social Europeo de 13 de julio de 2023[2],

– Visto el dictamen del Comité de las Regiones de 30 de noviembre de 2023[3],

– Vistos el acuerdo provisional aprobado por la comisión competente con arreglo al artículo 74, apartado 4, de su Reglamento interno y el compromiso asumido por el representante del Consejo, mediante carta de 21 de marzo de 2024, de aprobar la Posición del Parlamento Europeo, de conformidad con el artículo 294, apartado 4, del Tratado de Funcionamiento de la Unión Europea,

– Visto el artículo 59 de su Reglamento interno,

– Vistas las opiniones de la Comisión de Asuntos Exteriores y de la Comisión de Transportes y Turismo,

– Visto el informe de la Comisión de Industria, Investigación y Energía (A9-0426/2023),

---

1 Pendiente de publicación en el Diario Oficial.
2 DO C 349 de 29.9.2023, p. 167.
3 DO C, C/2024/1049, 9.2.2024, ELI: http://data.europa.eu/eli/C/2024/1049/oj.

1. Aprueba la Posición en primera lectura que figura a continuación;

2. Toma nota de la declaración de la Comisión adjunta a la presente Resolución, que se publicará en la serie C del *Diario Oficial de la Unión Europea*;

3. Pide a la Comisión que le consulte de nuevo si sustituye su propuesta, la modifica sustancialmente o se propone modificarla sustancialmente;

4. Encarga a su presidenta que transmita la Posición del Parlamento al Consejo y a la Comisión, así como a los Parlamentos nacionales.

P9_TC1-COD(2023)0109

Posición del Parlamento Europeo aprobada en primera lectura el 24 de abril de 2024 con vistas a la adopción del Reglamento (UE) 2024/... del Parlamento Europeo y del Consejo por el que se establecen medidas destinadas a reforzar la solidaridad y las capacidades en la Unión a fin de detectar ciberamenazas e incidentes, prepararse y responder a ellos *y por el que se modifica el Reglamento (UE) 2021/694 (Reglamento de Cibersolidaridad)*

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

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

Vista la propuesta de la Comisión Europea,

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

Visto el dictamen del Tribunal de Cuentas[1],

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

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

De conformidad con el procedimiento legislativo ordinario[4],

---

1 ***Dictamen de 18 de abril de 2023 (pendiente de publicación en el Diario Oficial).***
2 ***DO C 349 de 29.9.2023, p. 167.***
3 ***DO C, C/2024/1049, 9.2.2024, ELI: http://data.europa.eu/eli/C/2024/1049/oj.***
4 ***Posición del Parlamento Europeo de 24 de abril de 2024.***

Considerando lo siguiente:

(1) La utilización y dependencia de las tecnologías de la información y la comunicación constituyen un elemento esencial en todos los sectores de la actividad económica ***y de la sociedad en vista de la creciente interconectividad e interdependencia de*** las administraciones públicas de los Estados miembros, las empresas y los ciudadanos en todos los sectores y por encima de todas las fronteras***, lo que genera posibles vulnerabilidades de manera simultánea***.

(2) La magnitud, la frecuencia y los efectos de los incidentes de ciberseguridad, incluidos los ataques a la cadena de suministro con fines de ciberespionaje, programas de secuestro («ransomware») o perturbación, están aumentando ***en la Unión y en todo el mundo***. Representan una grave amenaza para el funcionamiento de las redes y los sistemas de información. En vista de la rápida evolución del panorama de amenazas, la amenaza de posibles incidentes de ciberseguridad a gran escala que provoque perturbaciones o daños significativos en las infraestructuras críticas exige una mayor preparación ▌ del marco de ciberseguridad de la Unión. Esa amenaza va más allá de la ***guerra de*** agresión de Rusia a Ucrania y probablemente persistirá, dada la multiplicidad de agentes ▌ implicados en las tensiones geopolíticas actuales. Tales incidentes pueden obstaculizar la prestación de servicios públicos, ***ya que los ciberataques se dirigen con frecuencia a servicios e infraestructuras públicos locales, regionales o nacionales, y las autoridades locales son especialmente vulnerables, en particular debido a sus limitados recursos***. ***Pueden impedir asimismo*** el desarrollo de actividades económicas, incluso en ***sectores de alta criticidad u otros*** sectores críticos, generar pérdidas económicas sustanciales, socavar la confianza de los usuarios, causar graves daños a las economías y ***a los sistemas democráticos*** de la Unión e incluso suponer una amenaza para la salud o la vida.

Además, los incidentes de ciberseguridad son impredecibles, ya que a menudo surgen y evolucionan rápidamente, no se limitan a ninguna zona geográfica específica y se producen simultáneamente o se propagan de forma instantánea por muchos países. ***Es importante que exista una estrecha cooperación entre el sector público, el sector privado, el mundo académico, la sociedad civil y los medios de comunicación.***

(3) Es necesario afianzar la posición competitiva de la industria y los servicios de la Unión en el conjunto de la economía digitalizada y apoyar su transformación digital reforzando el nivel de ciberseguridad en el mercado único digital ▌, tal y como se recomendó en tres propuestas distintas de la Conferencia sobre el Futuro de Europa***.*** Es necesario aumentar la resiliencia de los ciudadanos, las empresas, ***incluidas las microempresas, las pequeñas y medianas empresas y las empresas emergentes***, y las entidades que gestionan infraestructuras críticas, frente a las crecientes amenazas de ciberseguridad, que pueden tener unas repercusiones sociales y económicas devastadoras. Por lo tanto, es necesaria la inversión en infraestructuras y servicios ***y la adquisición de competencias para desarrollar capacidades en materia de ciberseguridad*** que apoyen una detección y una respuesta más rápidas a las ciberamenazas e incidentes. Adicionalmente, los Estados miembros precisan de asistencia para prepararse mejor y responder a los incidentes de ciberseguridad significativos y a gran escala, ***así como apoyo en la recuperación inicial de ellos***. ***Basándose en las estructuras existentes y en estrecha colaboración con ellas,*** la Unión también debe aumentar sus capacidades en dichos ámbitos, en particular en lo que se refiere a la recopilación y el análisis de datos sobre amenazas e incidentes de ciberseguridad.

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

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

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

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

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

(5) Los crecientes riesgos de ciberseguridad y un panorama general de amenazas complejo, con un claro riesgo de propagación rápida de incidentes de un Estado miembro a otros y de un tercer país a la Unión, requieren el ***refuerzo de la*** solidaridad a escala de la Unión para mejorar la detección, preparación, respuesta y recuperación con respecto de las ciberamenazas e incidentes***, en especial mediante el refuerzo de las capacidades de las estructuras existentes***. Además, las Conclusiones del Consejo de 23 de mayo de 2022 sobre el desarrollo de la posición de la Unión en materia cibernética han invitado a la Comisión a que presente una propuesta sobre un nuevo Fondo de Respuesta de Emergencia para la Ciberseguridad.

(6) La Comunicación conjunta de la Comisión y el Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad al Parlamento Europeo y al Consejo sobre la política de ciberdefensa de la UE de 10 de noviembre de 2022, anunció una Iniciativa de Cibersolidaridad de la UE con los objetivos de reforzar las capacidades comunes de detección, la conciencia situacional y la respuesta de la Unión mediante la promoción de la implantación de una infraestructura de la Unión de centros de operaciones de seguridad (COS), el apoyo a la creación gradual de una ciberreserva a escala de la Unión con servicios de proveedores privados de confianza y la realización de pruebas de entidades críticas para detectar posibles vulnerabilidades basadas en evaluaciones de riesgos de la Unión.

(7) Es necesario reforzar la capacidad de detección y la conciencia situacional de las ciberamenazas y los incidentes en toda la Unión y afianzar la solidaridad mejorando la preparación y las capacidades de los Estados miembros y de la Unión para ***prevenir y*** responder a incidentes de ciberseguridad significativos ***y a gran escala***. Procede, por lo tanto, crear una ***red de centros cibernéticos*** paneuropea (en lo sucesivo, «***Sistema*** Europeo ***de Alerta de Ciberseguridad***») para desarrollar ***capacidades coordinadas de detección y conciencia situacional, reforzando las*** capacidades ***de la Unión*** de detección ***de amenazas y puesta en común de información***; debe crearse un Mecanismo de Emergencia en materia de Ciberseguridad para ayudar a los Estados miembros***, previa solicitud de estos,*** a prepararse, responder a incidentes de ciberseguridad significativos y a gran escala, atenuar sus repercusiones e ***iniciar la recuperación*** de los incidentes de ciberseguridad significativos y a gran escala, y apoyar a otros usuarios en su respuesta a incidentes de ciberseguridad significativos y a incidentes de ciberseguridad equivalentes a gran escala; y debe crearse un Mecanismo Europeo de Revisión de Incidentes de Ciberseguridad para revisar y evaluar incidentes de ciberseguridad significativos o a gran escala específicos**.** ***Las acciones en virtud del presente Reglamento deben llevarse a cabo respetando debidamente las competencias de los Estados miembros y deben complementar, sin duplicar, las actividades que llevan a cabo la red de CSIRT, la Red europea de organizaciones de enlace para la gestión de cibercrisis (EU-CyCLONe, por sus siglas en inglés) o el Grupo de Cooperación establecido en virtud de la Directiva (UE) 2022/2555***. Estas acciones se entienden sin perjuicio de lo dispuesto en los artículos 107 y 108 del Tratado de Funcionamiento de la Unión Europea (TFUE).

(8) Para alcanzar estos objetivos, procede modificar el Reglamento (UE) 2021/694 del Parlamento Europeo y del Consejo[9] en determinados ámbitos. En particular, el presente Reglamento debe modificar el Reglamento (UE) 2021/694 en lo que respecta a la adición de nuevos objetivos operativos relacionados con el ***Sistema*** Europeo ***de Alerta de Ciberseguridad*** y el Mecanismo de Emergencia en materia de Ciberseguridad en el marco del objetivo específico 3 del ***Programa Europa Digital,*** cuya finalidad es garantizar la resiliencia, la integridad y la fiabilidad del mercado único digital, reforzar las capacidades para seguir los ciberataques y ciberamenazas y responder a ellos, y reforzar la cooperación y ***la coordinación*** transfronterizas en materia de ciberseguridad. ***El Sistema Europeo de Alerta de Ciberseguridad podría representar un importante apoyo para los Estados miembros a la hora de anticiparse y protegerse frente a las ciberamenazas, y la Reserva de Ciberseguridad de la UE podría ofrecer una considerable ayuda a los Estados miembros, a las instituciones, órganos y organismos de la Unión y a los terceros países asociados al Programa Europa Digital a la hora de responder y atenuar las repercusiones de incidentes de ciberseguridad significativos, incidentes de ciberseguridad a gran escala e incidentes de ciberseguridad equivalentes a gran escala.***

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

Dichas repercusiones podrían incluir daños materiales o inmateriales considerables y riesgos graves para la seguridad y el orden públicos. A la luz de las funciones específicas que podrían desempeñar el Sistema Europeo de Alerta de Ciberseguridad y la Reserva de Ciberseguridad de la UE, el presente Reglamento debe modificar el Reglamento (UE) 2021/694 en lo que respecta a la participación de entidades jurídicas establecidas en la Unión, pero controladas desde terceros países, en los casos en que exista un riesgo real de que las herramientas, infraestructuras y servicios necesarios y suficientes, o la tecnología, los conocimientos especializados y la capacidad, no estén disponibles en la Unión y los beneficios de la inclusión de dichas entidades compensen el riesgo para la seguridad. Esto ha de completarse con el establecimiento de las condiciones específicas en las que pueda concederse ayuda financiera para ***las acciones de ejecución del Sistema Europeo de Alerta de Ciberseguridad y de la Reserva de Ciberseguridad de la UE*** y mediante la definición de los mecanismos de gobernanza y coordinación necesarios para alcanzar los objetivos previstos. Otras modificaciones del Reglamento (UE) 2021/694 deben incluir descripciones de las acciones propuestas en el marco de los nuevos objetivos operativos, así como indicadores mensurables para seguir la aplicación de estos nuevos objetivos operativos.

(9) Para reforzar la respuesta de la Unión frente a las ciberamenazas y los incidentes es esencial la cooperación con las organizaciones internacionales, así como con los socios internacionales afines y de confianza. En este contexto, debe entenderse por socios internacionales afines y de confianza aquellos países que comparten los principios que han inspirado la creación de la Unión, a saber la democracia, el Estado de Derecho, la universalidad e indivisibilidad de los derechos humanos y las libertades fundamentales, el respeto de la dignidad humana, así como los principios de igualdad y solidaridad y el respeto de los principios de la Carta de las Naciones Unidas y del Derecho internacional, y que no socavan los intereses esenciales de seguridad de la Unión o de sus Estados miembros.

Dicha cooperación también podría ser beneficiosa en relación con las acciones adoptadas en virtud del presente Reglamento, en particular con el Sistema Europeo de Alerta de Ciberseguridad y la Reserva de Ciberseguridad de la UE. El Reglamento (UE) 2021/694 debe establecer que, si se cumplen determinadas condiciones de disponibilidad y seguridad, las licitaciones para el Sistema Europeo de Alerta de Ciberseguridad y la Reserva de Ciberseguridad de la UE se abran a entidades jurídicas controladas por terceros países, cuando se cumplan los requisitos de seguridad. Al evaluar el riesgo para la seguridad de abrir de ese modo la contratación pública, es importante tener en cuenta los principios y valores que la Unión comparte con socios internacionales de confianza y afines, cuando dichos principios estén relacionados con intereses y valores esenciales de seguridad de la Unión. Además, cuando dichos requisitos de seguridad estén siendo considerados con arreglo al Reglamento (UE) 2021/694, podrían tenerse en cuenta varios elementos, como la estructura corporativa y el proceso de toma de decisiones de las entidades, la seguridad de los datos y la información clasificada o sensible, y garantizar que los resultados de la acción no estén controlados o restringidos por parte de terceros países no admisibles.

(10) 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 las acciones contempladas en el objetivo específico 3 del Programa Europa Digital. En los programas de trabajo pertinentes, han de establecerse las condiciones específicas de participación en relación con cada acción, de conformidad con el Reglamento (UE) 2021/694.

(11) Son de aplicación al presente Reglamento las normas financieras horizontales adoptadas por el Parlamento Europeo y el Consejo en virtud del artículo 322 del TFUE. Dichas normas se establecen en el ***Reglamento (UE, Euratom) 2024/2509 del Parlamento Europeo y del Consejo***[10] y determinan, en particular, el procedimiento de elaboración y ejecución del presupuesto de la Unión, y prevén el control de la responsabilidad de los agentes financieros. Las normas adoptadas sobre la base del artículo 322 del TFUE también incluyen un régimen general de condicionalidad para la protección del presupuesto de la Unión tal como establece el Reglamento (UE, Euratom) 2020/2092 del Parlamento Europeo y del Consejo[11].

---

10 ***Reglamento (UE, Euratom) 2024/2509 del Parlamento Europeo y del Consejo, de 23 de septiembre de 2024, sobre las normas financieras aplicables al presupuesto general de la Unión (DO L, 2024/2509, 23.9.2024, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).***

11 ***Reglamento (UE, Euratom) 2020/2092 del Parlamento Europeo y del Consejo de 16 de diciembre de 2020 sobre un régimen general de condicionalidad para la protección del presupuesto de la Unión (DO L 433I de 22.12.2020, p. 1, ELI: http://data.europa.eu/eli/reg/2020/2092/oj).***

(12) ***Si bien las medidas de prevención y preparación son esenciales para aumentar la resiliencia de la Unión frente a incidentes de ciberseguridad significativos, incidentes de ciberseguridad a gran escala e incidentes de ciberseguridad equivalentes a gran escala, la frecuencia, el momento de aparición y la magnitud de dichos incidentes son, por su propia naturaleza, impredecibles. Los recursos financieros necesarios para garantizar una respuesta adecuada pueden variar considerablemente de un año a otro y*** deben ***poder ponerse a disposición inmediatamente. Conciliar el principio presupuestario de predictibilidad con la necesidad de actuar con rapidez ante las nuevas necesidades exige la adaptación, por tanto, de la ejecución financiera de los programas de trabajo. Por consiguiente, procede autorizar la prórroga de créditos*** no utilizados, ***si bien solo hasta el año siguiente y únicamente para la Reserva de Ciberseguridad de la UE y las acciones que apoyen la asistencia mutua, además de la prórroga de créditos autorizados en virtud del artículo 12, apartado 4, del Reglamento (UE, Euratom) 2024/2509***.

(13) Para prevenir, evaluar, responder y recuperarse de las ciberamenazas y los incidentes de manera más eficaz***,*** es necesario desarrollar conocimientos más completos sobre las amenazas para las infraestructuras y los activos críticos en el territorio de la Unión, incluida su distribución geográfica, su interconexión y los posibles efectos en caso de ciberataques que afecten dichas infraestructuras. ***Un enfoque proactivo para detectar, atenuar y prevenir ciberamenazas comprende una mayor capacidad en competencias de detección avanzada.*** El ***Sistema*** Europeo ***de Alerta de Ciberseguridad debe constar*** de varios ***centros cibernéticos transfronterizos interoperativos***, cada uno integrado por ***tres o más centros cibernéticos*** nacionales. Dicha infraestructura debe servir a los intereses y necesidades nacionales y de la Unión en materia de ciberseguridad, y debe aprovechar ***la tecnología de vanguardia para la recogida de datos e información pertinentes, en su caso, anonimizados,*** y los instrumentos analíticos, mejorar las capacidades ***coordinadas*** de ciberdetección y gestión y proporcionar conciencia situacional en tiempo real. Tal infraestructura debe servir para ***mejorar la posición en materia cibernética, aumentando la*** detección, ***la agregación y el análisis de datos e información con el fin de prevenir*** amenazas e incidentes de ciberseguridad y complementar y apoyar así a las entidades y redes de la Unión responsables de la gestión de crisis en la Unión, en particular la EU-CyCLONe ▌**.**

(14) ***La participación en el Sistema Europeo de Alerta de Ciberseguridad es voluntaria para los Estados miembros.*** Cada Estado miembro debe designar una ***única entidad*** a nivel nacional encargada de coordinar las actividades de detección de ciberamenazas en dicho Estado miembro. Esos ***centros cibernéticos*** nacionales deben actuar como punto de referencia y pasarela a nivel nacional para la participación en el ***Sistema*** Europeo ***de Alerta de Ciberseguridad*** y deben garantizar que la información sobre ciberamenazas procedente de entidades públicas y privadas se ponga en común y recopile a nivel nacional de manera eficaz y racional. ***Los centros cibernéticos nacionales podrían reforzar la cooperación y la puesta en común de información entre entidades públicas y privadas y también podrían respaldar el intercambio de datos e información pertinentes con las comunidades sectoriales e intersectoriales pertinentes, incluidos los centros de puesta en común y análisis de información pertinentes (ISAC, por sus siglas en inglés). Para reforzar la ciberresiliencia de la Unión es esencial una cooperación estrecha y coordinada entre las entidades públicas y privadas. Dicha cooperación es especialmente valiosa en el contexto de la puesta en común de inteligencia sobre ciberamenazas con vistas a mejorar la ciberprotección activa. Como parte de tal cooperación y puesta en común de información, los centros cibernéticos nacionales podrían solicitar y recibir información específica.***

Dichos centros no tienen la obligación ni la potestad en virtud del presente Reglamento de hacer cumplir dichas solicitudes. Cuando proceda y de conformidad con el Derecho de la Unión y nacional, la información solicitada o recibida podría incluir datos de telemetría, sensores y registro procedente de entidades, como los proveedores de servicios de seguridad gestionados, que operen en sectores de alta criticidad u otros sectores críticos dentro del Estado miembro, con el fin de mejorar la rápida detección de posibles ciberamenazas e incidentes en una fase más temprana, aumentando así la conciencia situacional. Si el centro cibernético nacional no es la autoridad competente designada o establecida por el Estado miembro de que se trate en virtud del artículo 8, apartado 1, de la Directiva (UE) 2022/2555, es esencial que se coordine con dicha autoridad competente en lo que respecta a solicitudes de tales datos y a su recepción.

(15) Como parte del ***Sistema*** Europeo ***de Alerta de Ciberseguridad***, debe crearse una serie de ***centros cibernéticos transfronterizos***. Dichos centros cibernéticos transfronterizos deben reunir a los ***centros cibernéticos*** nacionales de al menos tres Estados miembros, a fin de garantizar que puedan lograrse plenamente los beneficios de la detección transfronteriza de amenazas y de la puesta en común y la gestión de la información. El objetivo general de los ***centros cibernéticos transfronterizos*** debe ser reforzar las capacidades para analizar, prevenir y detectar las ciberamenazas y apoyar la producción de inteligencia de alta calidad sobre las ciberamenazas, en particular mediante la puesta en común de ***información pertinente, en su caso anonimizada, en un entorno de confianza y seguro,*** procedente de diversas fuentes, públicas o privadas, así como mediante la puesta en común y el uso conjunto de herramientas de vanguardia, y el desarrollo conjunto de capacidades de detección, análisis y prevención en un entorno de confianza ***y seguro***. Los ***centros cibernéticos transfronterizos*** deben proporcionar nuevas capacidades adicionales, aprovechando y complementando los ***COS*** existentes y los ▌«CSIRT»▌ y otros agentes pertinentes***, incluida la red de CSIRT***.

(16) El ***Estado miembro seleccionado por el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad (ECCC, por sus siglas en inglés), creado por el Reglamento (UE) 2021/887 del Parlamento y del Consejo[12] tras una convocatoria de manifestaciones de interés para crear un centro cibernético nacional o mejorar las capacidades de uno existente debe adquirir las herramientas, infraestructuras o servicios pertinentes conjuntamente con el ECCC. Tal Estado miembro debe poder optar a una subvención para explotar las herramientas, infraestructuras o servicios. El ECCC debe poder seleccionar un consorcio anfitrión compuesto por al menos tres Estados miembros, tras una convocatoria de manifestaciones de interés para crear un centro cibernético transfronterizo o mejorar las capacidades de uno existente, debe adquirir las herramientas, infraestructuras o servicios pertinentes conjuntamente con el ECCC. El consorcio anfitrión debe poder optar a una subvención para explotar las herramientas, infraestructuras o servicios. El procedimiento de contratación pública para adquirir las herramientas, infraestructuras o servicios pertinentes debe llevarse a cabo conjuntamente por el ECCC y los órganos de contratación pertinentes de los Estados miembros seleccionados a raíz de tal convocatoria de manifestaciones de interés.***

---

[12] ***Reglamento (UE) 2021/887 del Parlamento Europeo y del Consejo, de 20 de mayo de 2021, por el que se establecen el Centro Europeo de Competencia Industrial Tecnológica y de Investigación en Ciberseguridad y la Red de Centros Nacionales de Coordinación (DO L 202 de 8.6.2021, p. 1, ELI: http://data.europa.eu/eli/reg/2021/887/oj).***

Tal contratación pública debe ajustarse a lo dispuesto en el artículo 168, apartado 2, del Reglamento (UE, Euratom) 2024/2509 y en las normas financieras del ECCC. Por tanto, las entidades privadas no deben poder participar en las convocatorias de manifestaciones de interés para adquirir conjuntamente herramientas, infraestructuras o servicios con el ECCC, ni para recibir subvenciones para explotar dichas herramientas, infraestructuras o servicios. No obstante, los Estados miembros deben tener la posibilidad de hacer participar a las entidades privadas en la creación, la mejora y el funcionamiento de sus centros cibernéticos nacionales y centros cibernéticos transfronterizos por otras vías que consideren adecuadas, de conformidad con el Derecho de la Unión y nacional. Las entidades privadas también podrían optar a recibir financiación de la Unión en virtud del Reglamento (UE) 2021/887 a fin de dar apoyo a los centros cibernéticos nacionales.

(17) Con vistas a mejorar la detección de las ciberamenazas y la conciencia situacional en la Unión, el Estado miembro seleccionado tras una convocatoria de manifestaciones de interés para crear un centro cibernético nacional o mejorar las capacidades de uno existente debe comprometerse a solicitar participar en un centro cibernético transfronterizo. Si el Estado miembro no participa en un centro cibernético transfronterizo en el plazo de dos años a partir de la fecha en que se adquieran las herramientas, infraestructuras o servicios, o de la fecha en que reciba la financiación mediante subvenciones, si dicha fecha fuera anterior, no debe poder participar en otras acciones de apoyo de la Unión en el marco del Sistema Europeo de Alerta de Ciberseguridad para mejorar las capacidades de su centro cibernético nacional. En tales casos, las entidades de los Estados miembros podrían seguir participando en convocatorias de propuestas sobre otros temas en el marco del Programa Europa Digital o de otros programas de financiación de la Unión, incluidas las convocatorias de capacidades para la detección cibernética y la puesta en común de información, siempre que dichas entidades cumplan los criterios de admisibilidad establecidos en dichos programas.

(18) ▌ Los CSIRT intercambian información dentro de la red de CSIRT, de conformidad con la Directiva (UE) 2022/2555. El ***Sistema*** Europeo de ***Alerta de Ciberseguridad*** debe constituir una nueva capacidad que sea complementaria de la red de CSIRT, ***contribuyendo a crear conciencia situacional de la Unión que permita reforzar las capacidades de la red de CSIRT***. ***Los centros cibernéticos transfronterizos deben coordinarse y cooperar estrechamente con la red de CSIRT. Deben proceder a*** la agrupación y puesta en común ***de datos, así como la puesta en común de información pertinente, en su caso anonimizada,*** sobre las ciberamenazas procedentes de entidades públicas y privadas, aumentando el valor de dichos datos e información mediante el análisis de expertos y la adquisición conjunta de infraestructuras y ***herramientas de vanguardia, y contribuyendo a la soberanía tecnológica de la Unión, su autonomía estratégica abierta, su competitividad y resiliencia y al*** ▌ desarrollo de las capacidades de la Unión ▌ .

(19) Los ***centros cibernéticos transfronterizos*** deben actuar como puntos centrales que permitan una amplia agrupación y puesta en común de datos pertinentes y de inteligencia sobre ciberamenazas, y permitir la difusión de información sobre amenazas entre un amplio y diverso conjunto de ***partes interesadas, tales como*** los equipos de respuesta a emergencias informáticas (CERT, por sus siglas en inglés), los CSIRT, los ISAC y los operadores de infraestructuras críticas. ***Los miembros del consorcio anfitrión deben especificar en el acuerdo de consorcio la información pertinente que se ha de poner en común entre los participantes del centro cibernético transfronterizo de que se trate.*** La información intercambiada entre los participantes en un ***centro cibernético transfronterizo*** podría incluir***, por ejemplo,*** datos procedentes de redes y sensores, fuentes de información sobre amenazas, indicadores de compromiso e información contextualizada sobre incidentes, ciberamenazas***, cuasiincidentes, vulnerabilidades y, técnicas y procedimientos, tácticas de los adversarios, información específica de los agentes de amenazas, alertas de ciberseguridad y recomendaciones relativas a la configuración de las herramientas de ciberseguridad para detectar ciberataques.*** Además, los ***centros cibernéticos transfronterizos*** también deben celebrar acuerdos de cooperación entre sí***.***

Tales acuerdos de cooperación deben especificar, en particular, los principios de puesta en común de información y la interoperabilidad. Sus cláusulas relativas a la interoperabilidad, en particular los formatos y protocolos de puesta en común de información, deben guiarse por las directrices de interoperabilidad publicadas por la Agencia de la Unión Europea para la Ciberseguridad establecida por el Reglamento (UE) 2019/881 (ENISA) y, por tanto, tomarlas como punto de partida. Dichas directrices deben emitirse rápidamente para garantizar que los centros cibernéticos transfronterizos puedan tenerlas en cuenta en una fase temprana. Deben tomar en consideración las normas internacionales y las mejores prácticas y el funcionamiento de los centros cibernéticos transfronterizos establecidos.

(20) Los centros cibernéticos transfronterizos y la red de CSIRT deben cooperar estrechamente para garantizar las sinergias y la complementariedad de su actividad. A tal fin, deben acordar el procedimiento a seguir en materia de cooperación y puesta en común de la información pertinente. Esto podría incluir la puesta en común de información pertinente sobre ciberamenazas e incidentes de ciberseguridad significativos y la garantía de que se pongan en común experiencia con las herramientas de vanguardia, en particular, la inteligencia artificial y la tecnología de análisis de datos, utilizadas en los centros cibernéticos transfronterizos, con la red de CSIRT .

(21) Que las autoridades pertinentes compartan la conciencia situacional es un requisito indispensable para la preparación y la coordinación a escala de la Unión con respecto a los incidentes de ciberseguridad significativos y a gran escala. La Directiva (UE) 2022/2555 creó la EU-CyCLONe a fin de respaldar la gestión coordinada de los incidentes y crisis de ciberseguridad a gran escala en el ámbito operativo y de garantizar el intercambio periódico de información pertinente entre los Estados miembros y las instituciones, órganos y organismos de la Unión. ***La Directiva (UE) 2022/2555 también constituyó la red de CSIRT, para promover una cooperación operativa ágil y eficaz entre los Estados miembros. Para garantizar la conciencia situacional y reforzar la solidaridad, en situaciones en las que los centros cibernéticos transfronterizos obtengan información relacionada con un incidente de ciberseguridad a gran escala, potencial o en curso, deben proporcionar la información pertinente a la red de CSIRT, e informar, como alerta temprana, a la EU-CyCLONe. En particular, dependiendo de la situación, la información que ha de ponerse en común podría incluir información técnica, información sobre la naturaleza y los motivos del agresor o posible agresor, e información no técnica de nivel superior sobre un incidente de ciberseguridad a gran escala, ya sea potencial o en curso. En este contexto, debe prestarse la debida atención al principio de la necesidad de conocer y al carácter potencialmente sensible de la información puesta en común.***

La Directiva (UE) 2022/2555 también reitera las responsabilidades de la Comisión en el Mecanismo de Protección Civil de la Unión (UCPM, por sus siglas en inglés) establecido por la Decisión 1313/2013/UE del Parlamento Europeo y del Consejo[13], así como en lo relativo a la presentación de informes analíticos para el dispositivo de la UE de respuesta política integrada a las crisis (en lo sucesivo, « DIRPC») en virtud de la Decisión de Ejecución (UE) 2018/1993 del Consejo[14]. ***Cuando los centros cibernéticos transfronterizos pongan en común*** información ***pertinente y alertas tempranas*** relacionadas con un incidente de ciberseguridad a gran escala, potencial o en curso, ***con la EU-CyCLONe y la red de CSIRT, es imprescindible que dicha*** información ***se ponga en común a través de esas redes con las autoridades de los Estados miembros, así como con*** la Comisión. ***A este respecto, la Directiva (UE) 2022/2555 dispone que el objetivo de la EU-CyCLONe es respaldar la gestión coordinada de los incidentes y crisis de ciberseguridad a gran escala en el ámbito operativo y de garantizar el intercambio periódico de información relevante entre los Estados miembros y las instituciones, los órganos y los organismos de la Unión. Las funciones de la EU-CyCLONe comprenden el desarrollo de conciencia situacional compartida en relación con tales incidentes y crisis. Es de vital importancia que la EU-CyCLONe garantice, en consonancia con su objetivo y funciones, que tal información se transmita de forma inmediata a los representantes de los Estados miembros pertinentes y a la Comisión. A tal fin, es fundamental que el reglamento interno de la EU-CyCLONe recoja las disposiciones adecuadas.***

---

13 ***Decisión n ° 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, ELI: http://data.europa.eu/eli/dec/2013/1313/oj).***

14 ***Decisión de Ejecución (UE) 2018/1993 del Consejo, de 11 de diciembre de 2018, sobre el dispositivo de la UE de respuesta política integrada a las crisis (DO L 320 de 17.12.2018, p. 28, ELI: http://data.europa.eu/eli/dec_impl/2018/1993/oj).***

(22) Las entidades que participen en el ***Sistema*** Europeo ***de Alerta de Ciberseguridad*** deben garantizar un alto nivel de interoperabilidad entre ellas, incluido, cuando proceda, en lo que respecta a los formatos de datos, la taxonomía, las herramientas de tratamiento herramientas analíticas de datos. Asimismo, deben garantizar canales de comunicación seguros, así como un nivel mínimo de seguridad de la capa de aplicación, un cuadro de mandos de conciencia situacional y los indicadores. La adopción de una taxonomía común y el desarrollo de una plantilla de informes de situación para describir las ***causas de las ciberamenazas detectadas y los riesgos*** deben tener en cuenta ***el trabajo existente realizado*** en el contexto de la aplicación de la Directiva (UE) 2022/2555.

(23) A fin de permitir el intercambio ***de datos e información pertinentes*** sobre ciberamenazas procedentes de diversas fuentes, a gran escala, en un entorno de confianza ***y seguro***, las entidades que participen en el ***Sistema*** Europeo ***de Alerta de Ciberseguridad*** deben estar dotadas de herramientas, equipos e infraestructuras de vanguardia y de alta seguridad***, así como de personal cualificado***. Ello debería permitir mejorar las capacidades de detección colectiva y las alertas oportunas a las autoridades y entidades pertinentes, en particular mediante el uso de las últimas tecnologías de inteligencia artificial y análisis de datos.

(24) Al recopilar, ***analizar,*** poner en común e intercambiar ***datos e información pertinentes***, el ***Sistema*** Europeo ***de Alerta de Ciberseguridad*** debe reforzar la soberanía tecnológica de la Unión ***y su autonomía estratégica abierta en el ámbito de la ciberseguridad, su competitividad y su resiliencia.*** La agrupación y puesta en común de datos seleccionados de alta calidad también ***podría*** contribuir al desarrollo de tecnologías avanzadas de inteligencia artificial y análisis de datos. ***La supervisión humana y, a tal efecto, una mano de obra cualificada siguen siendo esenciales para la agrupación y puesta en común eficaz de datos de alta calidad.***

(25) Si bien el ***Sistema*** Europeo de ***Alerta de Ciberseguridad*** es un proyecto civil, la comunidad de ciberdefensa podría beneficiarse de unas capacidades civiles más sólidas de detección y conciencia situacional desarrolladas para la protección de las infraestructuras críticas. ▌

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

(27) ***Es de vital importancia preservar la confidencialidad y la seguridad de la información a los efectos de los tres pilares del presente Reglamento, ya sea para fomentar la puesta en común o el intercambio de información en el contexto del Sistema Europeo de Alerta de Ciberseguridad, preservar los intereses de las entidades que solicitan apoyo en el marco del Mecanismo de Emergencia en materia de Ciberseguridad, o garantizar que los informes en el marco del Mecanismo Europeo de Revisión de Incidentes de Ciberseguridad puedan aportar conclusiones útiles extraídas sin causar un efecto negativo en las entidades afectadas por los incidentes. La participación de los Estados miembros y las entidades en dichos mecanismos depende de las relaciones de confianza entre sus componentes. Cuando la información, en virtud de las normas de la Unión o nacionales, sea confidencial, su puesta en común o intercambio con arreglo al presente Reglamento debe limitarse a lo que sea pertinente y proporcionado para la finalidad de la puesta en común o el intercambio. Dicha puesta en común o intercambio debe preservar la confidencialidad de la información y proteger los intereses comerciales y de seguridad de las entidades afectadas. La puesta en común o el intercambio de información en virtud del presente Reglamento podría llevarse a cabo utilizando acuerdos de no divulgación o directrices sobre la distribución de la información, como el protocolo del semáforo o TLP (del inglés, «traffic light protocol»). El TLP debe entenderse como un medio para facilitar información sobre las limitaciones respecto de la difusión ulterior de la información. Se utiliza en casi todos los CSIRT y en algunos ISAC. Además de esos requisitos generales, en lo que respecta al Sistema Europeo de Alerta de Ciberseguridad, los acuerdos de los consorcios anfitriones deben establecer normas específicas relativas a las condiciones para la puesta en común de información en el seno del centro cibernético transfronterizo pertinente. Los acuerdos podrían, en particular, exigir que solo se proceda a poner en común la información de conformidad con el Derecho de la Unión y nacional.***

(28) Con respecto a la implantación de la Reserva de Ciberseguridad de la UE, se requieren normas de confidencialidad específicas. La ayuda se solicitará, evaluará y prestará en un contexto de crisis y respecto a las entidades que operen en sectores sensibles. Para que la Reserva de Ciberseguridad de la UE funcione eficazmente, es esencial que los usuarios y las entidades puedan poner en común y dar acceso, sin demora, a toda la información necesaria para que cada entidad desempeñe su función en la evaluación de las solicitudes y la prestación de la ayuda. En consecuencia, el presente Reglamento debe establecer que toda esa información solo se utilice o ponga en común cuando sea necesario para el funcionamiento de la Reserva de Ciberseguridad de la UE, y que la información confidencial o clasificada en virtud del Derecho de la Unión y nacional ha de utilizarse y ponerse en común únicamente de conformidad con dicho Derecho. Además, los usuarios siempre deben poder, cuando proceda, utilizar protocolos de puesta en común de información, como el TLP, para especificar mejor las limitaciones. Si bien los usuarios tienen discrecionalidad a este respecto, es importante que, al aplicar las limitaciones, tengan en cuenta las posibles consecuencias, en particular por lo que se refiere al retraso en la evaluación o la prestación de los servicios solicitados. Para disponer de una Reserva de Ciberseguridad de la UE eficiente, es importante que el órgano de contratación aclare estas consecuencias al usuario antes de que este proceda a la presentación de una solicitud. Esas salvaguardias se limitan a la solicitud y la prestación de los servicios de la Reserva de Ciberseguridad de la UE y no afectan al intercambio de información en otros contextos, como en la contratación pública de la Reserva de Ciberseguridad de la UE.

I

(29) En vista del aumento de los riesgos y del número de incidentes que afectan a los Estados miembros, es necesario crear un instrumento de apoyo a las crisis***, a saber, el Mecanismo de Emergencia en materia de Ciberseguridad***, para mejorar la resiliencia de la Unión frente a incidentes de ciberseguridad significativos, a gran escala y equivalentes a gran escala y complementar las acciones de los Estados miembros a través del apoyo financiero de emergencia para la preparación, la respuesta a los incidentes y la recuperación ***inicial*** de los servicios esenciales. ***Dado que la plena recuperación de un incidente es un proceso global de restablecimiento del funcionamiento de la entidad afectada por el incidente al estado previo a que este se produjera y podría ser un proceso largo que acarree costes significativos, el apoyo de la Reserva de Ciberseguridad de la UE debe limitarse a la fase inicial del proceso de recuperación, que conduzca al restablecimiento de las funcionalidades básicas de los sistemas.*** El Mecanismo de Emergencia en materia de Ciberseguridad debe permitir la prestación rápida ***y eficaz*** de la ayuda en circunstancias definidas y en condiciones claras y permitir un seguimiento y una evaluación minuciosos de la manera en que se utilizan los recursos. Si bien la responsabilidad principal de prevenir los incidentes y crisis, prepararse para ellos y responder a ellos recae en los Estados miembros, el Mecanismo de ***Emergencia en materia de Ciberseguridad*** promueve la solidaridad entre los Estados miembros de conformidad con el artículo 3, apartado 3, del Tratado de la Unión Europea (TUE).

(30) El Mecanismo ***de Emergencia en materia de Ciberseguridad*** debe prestar apoyo a los Estados miembros complementando sus propias medidas y recursos, así como otras opciones de apoyo existentes para la respuesta y recuperación ***inicial*** de incidentes de ciberseguridad significativos y a gran escala, como los servicios prestados por ENISA de conformidad con su mandato, la respuesta coordinada y la asistencia de la red de CSIRT, el apoyo a la atenuación por parte de la EU-CyCLONe, así como la asistencia mutua entre los Estados miembros, también en el contexto del artículo 42, apartado 7, del TUE, y los equipos de respuesta telemática rápida de la Cooperación Estructurada Permanente (CEP) creados en virtud de la Decisión (PESC) 2017/2315 del Consejo[15] ▌. Debe abordar la necesidad de garantizar la disponibilidad de medios especializados para apoyar la preparación, ***la respuesta y la recuperación respecto*** a los incidentes de ciberseguridad en toda la Unión y terceros países ***asociados al Programa Europa Digital***.

---

15 Decisión (PESC) 2017/2315 del Consejo, de 11 de diciembre de 2017, por la que se establece una cooperación estructurada permanente y se fija la lista de los Estados miembros participantes. (DO L 331 de 14.12.2017, p. 57, ELI: http://data.europa.eu/eli/dec/2017/2315/2023-05-23).

(31) El presente Reglamento se entiende sin perjuicio de los procedimientos y marcos para coordinar la respuesta a las crisis a escala de la Unión, en particular la Directiva (UE) 2022/2555, ***el Mecanismo de Protección Civil de la Unión establecido por la Decisión 1313/2013/UE del Parlamento Europeo y del Consejo[16], el DIRPC, la Recomendación (UE) 2017/1584 de la Comisión[17]***. ***El apoyo prestado en el marco del Mecanismo de Emergencia en materia de Ciberseguridad podrá complementar la asistencia prestada en el contexto de la política exterior y de seguridad común y de la política común de seguridad y defensa, en particular a través de los Equipos de Respuesta Telemática Rápida, habida cuenta del carácter civil del Mecanismo de Emergencia en materia de Ciberseguridad. El apoyo prestado en el marco del Mecanismo de Emergencia en materia de Ciberseguridad*** puede complementar las acciones ejecutadas en el contexto del artículo 42, apartado 7, ***del TUE, incluida la asistencia prestada por un Estado miembro a otro Estado miembro, o formar parte de la respuesta conjunta entre la Unión y los Estados miembros o*** en las situaciones ***a que se refiere*** el artículo 222 del ***TFUE***. ***La aplicación*** del presente ***Reglamento*** también debe coordinarse con la aplicación ***de las medidas con arreglo al*** conjunto de instrumentos de ciberdiplomacia ▌, cuando proceda.

---

16 ***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)***.

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

(32) La asistencia prestada en virtud del presente Reglamento debe apoyar y complementar las medidas tomadas por los Estados miembros a nivel nacional. A tal fin, debe garantizarse una estrecha cooperación y consulta entre la Comisión***, ENISA los Estados miembros, y, en su caso, el ECCC***. Al solicitar apoyo en el marco del Mecanismo de ***Emergencia en materia de Ciberseguridad***, el Estado miembro debe facilitar información pertinente que justifique la necesidad de apoyo.

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

(34) Como parte de las acciones de preparación, a fin de promover un enfoque coherente y reforzar la seguridad en toda la Unión y su mercado interior, debe prestarse apoyo para la puesta a prueba y la evaluación de la ciberseguridad de las entidades que operan en los ***sectores de alta criticidad*** determinados de conformidad con la Directiva (UE) 2022/2555 de manera coordinada, ***también a través de ejercicios y formación***. A tal fin, la Comisión, ***tras consultar con*** ENISA ▌, el Grupo de Cooperación ***y la EU-CyCLONe***, debe determinar periódicamente los sectores o subsectores pertinentes, los cuales deben poder optar a recibir ayuda financiera para la realización de pruebas coordinadas de preparación a escala de la Unión. Los sectores o subsectores deben seleccionarse de los sectores de alta criticidad enumerados en el anexo I de la Directiva (UE) 2022/2555. Las pruebas coordinadas de preparación deben basarse en metodologías y escenarios de riesgo comunes. La selección de sectores y el desarrollo de escenarios de riesgo deben tener en cuenta las evaluaciones de riesgos y los escenarios de riesgo pertinentes a escala de la Unión, incluida la necesidad de evitar duplicaciones, tales como la evaluación de riesgos y los escenarios de riesgo requeridos en las Conclusiones del Consejo sobre el desarrollo de la posición en materia cibernética de la Unión Europea ▌ que lleven a cabo la Comisión, el Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad (en lo sucesivo, «Alto Representante») y el Grupo de Cooperación, en coordinación con los organismos y agencias civiles y militares pertinentes y las redes establecidas, incluida la red ***EU-CyCLONe***, así como la evaluación de riesgos de las redes e infraestructuras de comunicaciones solicitada por el llamamiento ministerial conjunto de Nevers y llevada a cabo por el Grupo de Cooperación, con el apoyo de la Comisión y ENISA, y en cooperación con el Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE), establecido por el Reglamento (UE) 2018/1971 del Parlamento Europeo y del Consejo[18], las evaluaciones coordinadas de los riesgos de seguridad de las cadenas de suministro críticas a escala de la Unión que se lleven a cabo en virtud del artículo 22 de la Directiva (UE) 2022/2555 y las pruebas de resiliencia operativa digital previstas en el Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo[19]. La selección de los sectores también debe tener en cuenta la Recomendación del Consejo relativa a un enfoque coordinado en toda la Unión para reforzar la resiliencia de las infraestructuras críticas.

---

18 Reglamento (UE) 2018/1971 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por el que se establecen el Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE) y la Agencia de apoyo al ORECE (Oficina del ORECE), por el que se modifica el Reglamento (UE) 2015/2120 y por el que se deroga el Reglamento (CE) n.° 1211/2009 (DO L 321 de 17.12.2018, p.1).

19 Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 y (UE) 2016/1011. **(D***O L 333, 27.12.2022, p. 1)***.**

(35) Además, el Mecanismo ***de Emergencia en materia de Ciberseguridad*** debe respaldar otras acciones de preparación y apoyo a la preparación en otros sectores no incluidos en las pruebas coordinadas de preparación de entidades que operan en ***sectores de alta criticidad o entidades que operen en otros*** sectores críticos. Estas acciones podrían incluir diversos tipos de actividades nacionales de preparación.

(36) Cuando los Estados miembros reciban subvenciones para apoyar acciones de preparación, las entidades de sectores de alta criticidad tienen la posibilidad de participar en dichas acciones de forma voluntaria. Es una buena práctica que, tras esas acciones, las entidades participantes elaboren un plan corrector para aplicar las recomendaciones resultantes de medidas específicas a fin de obtener el mayor beneficio posible de la acción de preparación. Si bien es importante que los Estados miembros soliciten, como parte de las acciones, que las entidades participantes elaboren y apliquen dichos planes correctores, los Estados miembros no están obligados ni facultados por el presente Reglamento para hacer cumplir dichas solicitudes. Dichas solicitudes se entienden sin perjuicio de los requisitos aplicables a las entidades y de las facultades de supervisión de las autoridades competentes, de conformidad con la Directiva (UE) 2022/2555.

(37) El Mecanismo de ***Emergencia en materia de Ciberseguridad*** también debe respaldar las acciones de respuesta a incidentes para atenuar los efectos de incidentes de ciberseguridad significativos, a gran escala y equivalentes a gran escala, apoyar la recuperación ***inicial*** o restablecer el funcionamiento de los servicios esenciales. Cuando proceda, debe complementar el UCPM para garantizar un enfoque global que responda a las repercusiones de los incidentes en los ciudadanos.

(38) El Mecanismo ***de Emergencia en materia de Ciberseguridad*** debe apoyar la asistencia ***técnica*** prestada por ***un*** Estado miembro ***a otro*** que esté afectado por un incidente de ciberseguridad significativo o a gran escala, incluidos ▌ los CSIRT ***a que se refiere el*** artículo ***11, apartado 3, letra f),*** de la Directiva (UE) 2022/2555. Los Estados miembros que presten ***la*** asistencia deben poder presentar solicitudes para cubrir los costes relacionados con el envío de equipos de expertos en el marco de la asistencia mutua. Los costes subvencionables podrían incluir los gastos de viaje, alojamiento y dietas de los expertos en ciberseguridad.

(39) Dada la importancia esencial de las empresas privadas en la detección de incidentes de ciberseguridad a gran escala y equivalentes a gran escala, y en la preparación y respuesta frente a ellos, es crucial reconocer el valor de la cooperación voluntaria y gratuita con dichas empresas, en virtud de la cual ofrezcan servicios sin remuneración en caso de incidentes y crisis de ciberseguridad a gran escala y equivalentes a gran escala. ENISA, en cooperación con la EU-CyCLONe, podría realizar un seguimiento de la evolución de dichas iniciativas gratuitas y promover el cumplimiento por parte de estas de los criterios aplicables a los proveedores de confianza de servicios de seguridad gestionados con arreglo al presente Reglamento, también en relación con la fiabilidad de las empresas, su experiencia y la capacidad para tratar información delicada de manera segura.

(40) ***Como parte del Mecanismo de Emergencia en materia de Ciberseguridad***, debe crearse gradualmente una Reserva de Ciberseguridad de la UE, compuesta por servicios de proveedores ***de servicios de seguridad gestionados de confianza*** ▌ para apoyar la respuesta e ***iniciar*** acciones de recuperación en caso de incidentes de ciberseguridad significativos***, a gran escala o equivalentes a gran escala que afecten a los Estados miembros, a las instituciones, órganos y organismos de la Unión o a terceros países asociados al Programa Europa Digital.*** La Reserva de Ciberseguridad de la UE debe garantizar la disponibilidad y el estado de preparación de los servicios***. Debe incluir, por tanto, servicios comprometidos con antelación, también, por ejemplo, capacidades que están en reserva y son desplegables a corto plazo.*** Los servicios de la Reserva de Ciberseguridad de la UE deben servir para ayudar a las autoridades nacionales a prestar asistencia a entidades afectadas que operen en ***sectores de alta criticidad o a entidades afectadas que operen en otros*** sectores críticos como complemento de sus propias acciones a nivel nacional. ***Los servicios de la Reserva de Ciberseguridad de la UE también pueden servir para apoyar a las instituciones, órganos y organismos de la Unión, en condiciones similares. La Reserva de Ciberseguridad de la UE también podría contribuir a reforzar la posición competitiva de la industria y los servicios en la Unión en toda la economía digital, incluidas las microempresas y las pequeñas y medianas empresas, así como las empresas emergentes, entre otras cosas, incentivando la inversión en investigación e innovación. Es importante tener en cuenta el marco europeo de capacidades en ciberseguridad de ENISA a la hora de contratar los servicios para la Reserva de Ciberseguridad de la UE.*** Al solicitar el apoyo de la Reserva de Ciberseguridad de la UE, ***los usuarios deben incluir en su solicitud la información oportuna sobre la entidad afectada y las posibles repercusiones, información sobre el servicio solicitado de la Reserva de Ciberseguridad de la UE,*** el apoyo prestado a la entidad afectada a nivel nacional, que debe tenerse en cuenta al evaluar ***la petición del solicitante***. ***Para garantizar la complementariedad con otras formas de apoyo de las que dispone la entidad afectada, la solicitud debe incluir también, cuando proceda, información sobre los acuerdos contractuales vigentes para la respuesta a incidentes y los servicios de recuperación iniciales, así como los contratos de seguro que puedan cubrir este tipo de incidente.***

(41) ***A fin de garantizar el uso eficaz de la financiación de la Unión, los servicios objeto de compromiso previo con arreglo a la Reserva de Ciberseguridad deben poder convertirse, de conformidad con el contrato pertinente, en servicios de preparación relacionados con la prevención y respuesta a incidentes, en caso de que dichos servicios objeto de compromiso previo no se utilicen para dar respuesta a incidentes durante el período en el que hayan sido objeto de compromiso previo. Esos servicios deben ser complementarios y no duplicar las acciones de preparación que debe gestionar el ECCC.***

(42) ***Las solicitudes de apoyo en el marco de la Reserva de Ciberseguridad de la UE de las autoridades de gestión de crisis de ciberseguridad de los Estados miembros y de los CSIRT, o del CERT-EU, en nombre de instituciones, órganos y organismos de la Unión, deben ser evaluadas por el órgano de contratación. Cuando se haya encomendado a ENISA la administración y el funcionamiento de la Reserva de Ciberseguridad de la UE, se considera a ENISA como dicho órgano de contratación. Las solicitudes de apoyo de terceros países asociados al Programa Europa Digital deben ser evaluadas por la Comisión. Para facilitar la presentación y evaluación de las solicitudes de apoyo, ENISA podría crear una plataforma segura.***

(43) Cuando se reciban múltiples solicitudes concurrentes, debe establecerse el orden de prioridad de las solicitudes de conformidad con los criterios establecidos en el presente Reglamento. A la luz de los objetivos generales del presente Reglamento, esos criterios deben incluir la dimensión y gravedad del incidente, el tipo de entidad afectada, la posible repercusión del incidente en los Estados miembros y usuarios afectados, el posible carácter transfronterizo del incidente y el riesgo de contagio, y las medidas ya adoptadas por el usuario para asistir en la respuesta y la recuperación inicial. A la luz de esos objetivos y dado que las solicitudes de los usuarios de los Estados miembros están destinadas exclusivamente a ayudar, en toda la Unión, a entidades activas en sectores de alta criticidad o entidades activas en otros sectores críticos, las solicitudes de los usuarios de los Estados miembros deben recibir mayor prioridad cuando dos o más solicitudes se consideren iguales con arreglo a los criterios de evaluación. Todo ello se entiende sin perjuicio de las obligaciones que los Estados miembros puedan tener con arreglo a los acuerdos de alojamiento pertinentes de adoptar medidas para proteger y asistir a las instituciones, órganos y organismos de la Unión.

(44) La Comisión tendrá la responsabilidad general de la ejecución de la Reserva de Ciberseguridad de la UE. Dada la amplia experiencia adquirida por ENISA con la acción de apoyo a la ciberseguridad, esta es la agencia más adecuada para ejecutar la Reserva de Ciberseguridad de la UE, por lo que la Comisión debe encomendarle, parcialmente o, si la Comisión lo considera oportuno, en su totalidad, el funcionamiento y la administración de la Reserva de Ciberseguridad de la UE. La encomienda debe realizarse de conformidad con las normas aplicables con arreglo al Reglamento (UE, Euratom) 2024/2509 y, en particular, debe cumplir las condiciones pertinentes para la firma de un acuerdo de contribución. Los aspectos del funcionamiento y la administración de la Reserva de Ciberseguridad de la UE no encomendados a ENISA deben ser objeto de gestión directa por parte de la Comisión, incluso antes de la firma del acuerdo de contribución.

(45) Los Estados miembros deben desempeñar un papel central en la constitución, la implantación y la fase posterior a la implantación de la Reserva de Ciberseguridad de la UE. Dado que el Reglamento (UE) 2021/694 es el acto de base pertinente para las acciones de ejecución de la Reserva de Ciberseguridad de la UE, las acciones en el marco de dicha Reserva deben estar previstas en los programas de trabajo a que se refiere el artículo 24 del Reglamento (UE) 2021/694. En virtud del apartado 6 de dicho artículo, esos programas de trabajo han de adoptarse por la Comisión mediante actos de ejecución de conformidad con el procedimiento de examen. Además, la Comisión, en coordinación con el Grupo de Cooperación, debe determinar las prioridades y la evolución de la Reserva de Ciberseguridad de la UE.

(46) Los contratos que se establezcan en el marco de la Reserva de Ciberseguridad de la UE no deben afectar a la relación entre empresas ni a las obligaciones existentes entre la entidad afectada o los usuarios y el proveedor de servicios.

(47) A efectos de la selección de proveedores de servicios privados para prestar servicios en el contexto de la Reserva de Ciberseguridad de la UE, es necesario establecer un conjunto de criterios y requisitos mínimos que deben incluirse en la licitación para seleccionar a dichos proveedores, a fin de garantizar que se satisfagan las necesidades de las autoridades, entidades de los Estados miembros que operen en sectores de ***alta criticidad y entidades que operen en otros*** sectores críticos. ***Con el fin de atender las necesidades específicas de los Estados miembros, al contratar servicios para la Reserva de Ciberseguridad de la UE, el órgano de contratación debe, cuando proceda, desarrollar criterios de selección y requisitos complementarios a los establecidos en el presente Reglamento. Es importante fomentar la participación de los proveedores más pequeños, activos a nivel regional y local.***

(48) Al seleccionar a los proveedores para su inclusión en la Reserva de Ciberseguridad de la UE, el órgano de contratación debe procurar garantizar que la Reserva de Ciberseguridad de la UE, considerada en su conjunto, contenga proveedores capaces de satisfacer los requisitos lingüísticos de los usuarios. A tal fin, antes de preparar el pliego de condiciones, el órgano de contratación debe preguntarse si los usuarios potenciales de la Reserva de Ciberseguridad de la UE tienen requisitos lingüísticos específicos, de modo que los servicios de apoyo de la Reserva de Ciberseguridad de la UE puedan prestarse en una lengua de entre las lenguas oficiales de las instituciones de la Unión o de los Estados miembros, que pueda ser comprendida por el usuario o la entidad afectada. En caso de que un usuario requiera más de una lengua para la prestación de los servicios de apoyo de la Reserva de Ciberseguridad de la UE y dichos servicios se hayan contratado en esas lenguas para dicho usuario, este debe poder especificar, en la solicitud de apoyo de la Reserva de Ciberseguridad de la UE, en cuál de esas lenguas deben prestarse los servicios en relación con el incidente específico que dé lugar a la solicitud.

(49) Para apoyar la creación de la Reserva de Ciberseguridad de la UE, ***es importante que*** la Comisión ***solicite*** a ENISA que prepare una propuesta de esquema de certificación de ***la ciberseguridad*** para los servicios de seguridad gestionados en virtud del Reglamento (UE) 2019/881 en los ámbitos a los que se aplique el Mecanismo de ***Emergencia en materia de Ciberseguridad***.

(50) Con el fin de apoyar los objetivos del presente Reglamento de promover una conciencia situacional común, mejorar la resiliencia de la Unión y permitir una respuesta eficaz a incidentes de ciberseguridad significativos y a gran escala, ***la Comisión o la red EU-CyCLONe,*** deben poder solicitar a ENISA, ***con el apoyo de la red de CSIRT y con la autorización de los Estados miembros afectados,*** que revise y evalúe las ciberamenazas, las vulnerabilidades ***aprovechables conocidas*** y las medidas paliativas con respecto a un incidente de ciberseguridad significativo o a gran escala específico. Una vez finalizada la revisión y evaluación de un incidente, ENISA debe elaborar un informe de revisión del incidente, en colaboración con ***el Estado miembro afectado,*** las partes interesadas pertinentes, incluidos los representantes del sector privado, ▌ la Comisión y otras instituciones, órganos ***y organismos*** pertinentes de la Unión. Sobre la base de la colaboración con las partes interesadas, incluidas las provenientes del sector privado, el informe de revisión sobre incidentes específicos debe tener por objeto evaluar las causas, los efectos y las medidas paliativas de un incidente, una vez que se haya producido. Debe prestarse especial atención a las aportaciones y conclusiones de los proveedores de servicios de seguridad gestionados que cumplan las condiciones de máxima integridad profesional, imparcialidad y conocimientos técnicos necesarios, tal como exige el presente Reglamento. El informe debe presentarse ***a la EU-CyCLONe, a la red de CSIRT y a la Comisión y debe*** emplearse para informar ***sus respectivas actividades, así como a las de ENISA.*** Cuando el incidente se refiera a un tercer país ***asociado al Programa Europa Digital,*** la Comisión también ***debe*** dar a conocer el informe al Alto Representante.

(51) Teniendo en cuenta el carácter impredecible de los ciberataques y el hecho de que a menudo no se limitan a una zona geográfica específica y plantean un alto riesgo de contagio, el refuerzo de la resiliencia de los países vecinos y de su capacidad de responder eficazmente a incidentes de ciberseguridad significativos y equivalentes a gran escala contribuye a la protección de la Unión en su conjunto, ***y especialmente de su mercado interior y su industria. Esas actividades podrían contribuir más a la ciberdiplomacia de la Unión. Así, los terceros países asociados al Programa Europa Digital*** deben poder solicitar apoyo de la Reserva de Ciberseguridad de la UE, ***en la totalidad o en parte de sus territorios,*** cuando así esté previsto en el ***acuerdo a través del cual el tercer país se haya asociado al*** Programa Europa Digital. La financiación para los terceros países ***asociados al Programa Europa Digital*** debe contar con el apoyo de la Unión en el marco de las asociaciones e instrumentos de financiación pertinentes para dichos países. El apoyo debe abarcar servicios en el ámbito de la respuesta a incidentes de ciberseguridad significativos o a equivalentes a gran escala y de la recuperación ***inicial*** de ellos.

(52) Las condiciones establecidas en el presente Reglamento para la Reserva de Ciberseguridad de la UE y los proveedores de servicios de seguridad gestionados de confianza deben aplicarse a la hora de prestar apoyo a los terceros países asociados al Programa Europa Digital. Los terceros países asociados al Programa Europa Digital deben poder solicitar el apoyo de la Reserva de Ciberseguridad de la UE cuando las entidades destinatarias y para las que soliciten apoyo de la Reserva de Ciberseguridad de la UE sean entidades que operen en sectores de alta criticidad o entidades que operen en otros sectores críticos y cuando los incidentes detectados den lugar a perturbaciones operativas significativas o puedan tener efectos de contagio en la Unión. Los terceros países asociados al Programa Europa Digital solo deben poder optar a recibir ayuda cuando el acuerdo a través del cual estén asociados al Programa Europa Digital prevea específicamente dicho apoyo. Además, estos terceros países solo deben mantener el derecho a recibir la ayuda mientras se cumplan tres criterios. En primer lugar, el tercer país debe cumplir plenamente con las condiciones pertinentes de dicho acuerdo. En segundo lugar, dado el carácter complementario de la Reserva de Ciberseguridad de la UE, el tercer país debe haber adoptado medidas adecuadas para prepararse ante incidentes de ciberseguridad significativos o equivalentes a gran escala. En tercer lugar, la prestación de apoyo de la Reserva de Ciberseguridad de la UE debe ser coherente con la política de la Unión hacia ese país y sus relaciones generales con él, así como con otras políticas de la Unión en el ámbito de la seguridad. En el contexto de la evaluación del cumplimiento de dicho tercer criterio, la Comisión debe consultar al Alto Representante para la adaptación de la concesión de dicho apoyo a la política exterior y de seguridad común.

(53) La prestación de apoyo a los terceros países asociados al Programa Europa Digital puede afectar a las relaciones con terceros países y a la política de seguridad de la Unión, también en el contexto de la política exterior y de seguridad común y de la política común de seguridad y defensa. Por consiguiente, procede otorgar al Consejo competencias de ejecución para autorizar y especificar el período durante el cual puede prestarse dicho apoyo. El Consejo debe actuar sobre la base de una propuesta de la Comisión, teniendo debidamente en cuenta la evaluación de la Comisión de los tres criterios. Lo mismo es aplicable a las renovaciones y a las propuestas de modificación o derogación de tales actos. El Consejo, en caso de que, en circunstancias excepcionales, considere que se ha producido un cambio significativo de circunstancias en relación con el tercer criterio, debe poder actuar por iniciativa propia para modificar o derogar un acto de ejecución, sin esperar a una propuesta de la Comisión. Es probable que esos cambios significativos requieran medidas urgentes, tengan implicaciones especialmente importantes para las relaciones con terceros países y no requieran una evaluación detallada de antemano por parte de la Comisión. Además, la Comisión debe cooperar con el Alto Representante en relación con solicitudes de apoyo de terceros países asociados al Programa Europa Digital y la ejecución del apoyo concedido a dichos terceros países. La Comisión también debe tener en cuenta los puntos de vista facilitados por ENISA respecto a tales solicitudes y apoyo. La Comisión debe informar al Consejo del resultado de la evaluación de las solicitudes, también de las consideraciones pertinentes realizadas a este respecto, y de los servicios prestados.

(54) La Comunicación de la Comisión de 18 de abril de 2023 sobre la Academia de Cibercapacidades reconocía la escasez de profesionales cualificados. Tales cualificaciones son necesarias para cumplir los objetivos del presente Reglamento. La Unión necesita urgentemente profesionales con las capacidades y competencias adecuadas para prevenir, detectar y disuadir de ataques cibernéticos y defender a la Unión, incluidas sus infraestructuras más críticas, frente a tales ataques, así como para garantizar su resiliencia. A tal fin, es importante fomentar la cooperación entre las partes interesadas, incluidas las provenientes del sector privado, el mundo académico y el sector público. Es asimismo importante crear sinergias, en todos los territorios de la Unión, para la inversión en educación y formación a fin de promover la creación de salvaguardias para evitar la fuga de talentos y que el déficit de capacidades no se agrave más en algunas regiones que en otras. Es urgente solucionar el déficit de capacidades en materia de ciberseguridad, prestando especial atención a la reducción de la brecha de género en la mano de obra en ciberseguridad a fin de promover la presencia y la participación de las mujeres en el diseño de la gobernanza digital.

(55) Con vistas a impulsar la innovación en el mercado único digital, es importante reforzar la investigación y la innovación en materia de ciberseguridad, con vistas a contribuir a aumentar la resiliencia de los Estados miembros y la autonomía estratégica abierta de la Unión, ambos objetivos del presente Reglamento. Las sinergias son esenciales para reforzar la cooperación y la coordinación entre las distintas partes interesadas, incluidas las provenientes del sector privado, la sociedad civil y el mundo académico.

(56) El presente Reglamento debe tener en cuenta el compromiso, formulado en la Declaración Conjunta de 26 de enero de 2022 del Parlamento Europeo, el Consejo y la Comisión titulada «Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital», de proteger los intereses de las democracias, personas, empresas e instituciones públicas de la Unión frente a los riesgos de ciberseguridad y la ciberdelincuencia, incluidas las violaciones de la seguridad de los datos y la usurpación o manipulación de identidad.

(57) ***A fin de complementar determinados elementos no esenciales del presente Reglamento, deben delegarse en la Comisión los poderes para adoptar actos con arreglo al artículo 290 del TFUE, por lo que respecta a la especificación de los tipos y número de servicios de respuesta necesarios para la Reserva de Ciberseguridad de la UE. Reviste especial importancia que la Comisión lleve a cabo las consultas oportunas durante la fase preparatoria, en particular con expertos, y que esas consultas se realicen de conformidad con los principios establecidos en el Acuerdo interinstitucional de 13 de abril de 2016 sobre la mejora de la legislación[20]. En particular, a fin de garantizar una participación equitativa en la preparación de los actos delegados, el Parlamento Europeo y el Consejo reciben toda la documentación al mismo tiempo que los expertos de los Estados miembros, y sus expertos tienen acceso sistemáticamente a las reuniones de los grupos de expertos de la Comisión que se ocupen de la preparación de actos delegados.***

(58) A fin de garantizar condiciones uniformes de ejecución del presente Reglamento, deben conferirse a la Comisión competencias de ejecución para especificar ***de forma más detallada*** los procedimientos de ***asignación de los servicios de apoyo de la Reserva*** de Ciberseguridad ***de la UE. Dichas competencias deben ejercerse de conformidad con el Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo[21]***.

---

20 *DO L 123 de 12.5.2016, p. 1, ELI: http://data.europa.eu/eli/agree_interinstit/2016/512/oj.*

21 ***Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión (DO L 55 de 28.2.2011, p. 13, ELI: http://data.europa.eu/eli/reg/2011/182/oj).***

(59) Sin perjuicio de las normas relativas al presupuesto anual de la Unión con arreglo a los Tratados, la Comisión debe tener en cuenta las obligaciones derivadas del presente Reglamento al evaluar las necesidades presupuestarias y de personal de ENISA.

(60) La Comisión debe evaluar regularmente las medidas establecidas en el presente Reglamento. La primera de tales evaluaciones debe realizarse en los dos primeros años a partir de la fecha de entrada en vigor del presente Reglamento y, posteriormente, al menos cada cuatro años, teniendo en cuenta el calendario de revisión del marco financiero plurianual establecido en virtud del artículo 312 TFUE. La Comisión debe presentar un informe sobre los avances realizados al Parlamento Europeo y al Consejo. Con el fin de evaluar los diferentes elementos necesarios, incluido el alcance de la información puesta en común en el Sistema Europeo de Alerta de Ciberseguridad, la Comisión debe basarse exclusivamente en información que esté fácilmente disponible o que se facilite voluntariamente. Habida cuenta de la evolución geopolítica y con el fin de garantizar la continuidad y el ulterior desarrollo de las medidas establecidas en el presente Reglamento más allá de 2027, es importante que la Comisión evalúe la necesidad de asignar un presupuesto adecuado en el marco financiero plurianual para el período 2028-2034.

(61) Dado que los objetivos del presente Reglamento, a saber, reforzar la posición competitiva de la industria y los servicios en la Unión en toda la economía digital y contribuir a la soberanía tecnológica de la Unión y su autonomía estratégica abierta en el ámbito de la ciberseguridad, no pueden ser alcanzados de manera suficiente por los Estados miembros, sino que, debido a las dimensiones o los efectos de la acción, pueden lograrse mejor a escala de la Unión, esta puede adoptar medidas de acuerdo con el principio de subsidiariedad establecido en el artículo 5 del TUE. De conformidad con el principio de proporcionalidad establecido en el mismo artículo, el presente Reglamento no excede de lo necesario para alcanzar dichos objetivos**.**

HAN ADOPTADO EL PRESENTE REGLAMENTO:

Capítulo I
DISPOSICIONES GENERALES

Artículo 1
Objeto y objetivos

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

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

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

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

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

3. Los objetivos generales a que se refiere el apartado2 se alcanzarán mediante los siguientes objetivos específicos:

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

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

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

▌

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

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

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

Artículo 2
Definiciones

A los efectos del presente Reglamento, se entenderá por:

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

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

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

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

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

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

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

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

▌

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

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

11) «incidente grave»: un incidente grave según se define en el artículo 3, punto 8, del Reglamento (UE, Euratom) 2023/2841 ***del Parlamento Europeo y del Consejo***[22];

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

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

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

---

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

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

▌

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

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

Capítulo II

SISTEMA EUROPEO ***DE ALERTA DE CIBERSEGURIDAD***

Artículo 3

Establecimiento del ***Sistema*** Europeo ***de Alerta de Ciberseguridad***

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

2. El ***Sistema*** Europeo ***de Alerta de Ciberseguridad***:

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

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

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

▌

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

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

▌

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

Artículo 4

Centros cibernéticos nacionales

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

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

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

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

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

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

Artículo 5

Centros cibernéticos transfronterizos

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

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

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

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

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

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

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

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

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

Artículo 6

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

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

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

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

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

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

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

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

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

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

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

Artículo 7

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

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

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

Artículo 8
Seguridad

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

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

Artículo 9

Financiación del Sistema Europeo de Alerta de Ciberseguridad

1. Tras una convocatoria de manifestaciones de interés, el ECCC seleccionará de entre los Estados miembros que tengan la intención de participar en el Sistema Europeo de Alerta de Ciberseguridad a aquellos que participarán con el ECCC en una contratación conjunta de herramientas, infraestructuras o servicios, con el fin de crear, o mejorar las capacidades de los centros cibernéticos nacionales designados o establecidos en virtud del artículo 4, apartado 1. El ECCC podrá conceder subvenciones a los Estados miembros seleccionados para financiar el funcionamiento de tales herramientas, infraestructuras y servicios. La contribución financiera de la Unión sufragará hasta el 50 % de los costes de adquisición de las herramientas, infraestructuras o servicios, y hasta el 50 % de los costes de funcionamiento. Los Estados miembros seleccionados sufragarán los costes restantes. Antes de iniciar el procedimiento para la adquisición de las herramientas, infraestructuras o servicios, el ECCC y los Estados miembros seleccionados celebrarán un acuerdo de alojamiento y uso que regule el uso de las herramientas, infraestructuras o servicios.

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

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

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

Capítulo III

MECANISMO DE EMERGENCIA EN MATERIA DE CIBERSEGURIDAD

Artículo 10

Creación del Mecanismo de Emergencia en materia de Ciberseguridad

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

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

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

4. Las acciones en el marco del Mecanismo de Emergencia en materia de Ciberseguridad se ejecutarán principalmente a través del ECCC de conformidad con el Reglamento (UE) 2021/887. Sin embargo las acciones de ejecución de la Reserva de Ciberseguridad de la UE, a que se refiere el artículo 11, apartado 1, letra b), del presente Reglamento que se ejecutarán por la Comisión y ENISA.

Artículo 11

Tipos de acciones

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

a) acciones de preparación, ***a saber:***

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

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

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

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

Artículo 12

Pruebas coordinadas de preparación de las entidades

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

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

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

4. Con el fin de apoyar las pruebas coordinadas de preparación de las entidades a que se refiere el artículo 11, apartado 1, letra a)***, inciso i)***, del presente Reglamento en toda la Unión, la Comisión, previa consulta al Grupo de Cooperación***, a la EU-CyCLONe*** y a ENISA, determinará, a partir de los sectores de alta criticidad enumerados en el anexo I de la Directiva (UE) 2022/2555, los sectores o subsectores afectados ***para los que se pueda publicar una convocatoria de propuestas para la concesión de subvenciones***. ***La participación de los Estados miembros en dichas convocatorias de propuestas es voluntaria.***

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

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

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

Artículo 13

Otras acciones de preparación

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

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

Artículo 14

Creación de la Reserva de Ciberseguridad de la UE

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

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

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

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

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

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

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

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

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

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

Artículo 15

Solicitudes de apoyo de la Reserva de Ciberseguridad de la UE

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Artículo 16

Ejecución del apoyo de la Reserva de Ciberseguridad de la UE

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

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

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

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

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

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

a) la ***magnitud y la*** gravedad del incidente;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

I

Artículo 17

Proveedores de servicios de seguridad gestionados de confianza

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

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

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

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

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

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

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

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

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

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

f) el proveedor estará equipado con el ▌ *hardware* y *software* ***necesarios*** para prestar el servicio solicitado***, sin vulnerabilidades aprovechables conocidas, que incluirán las últimas actualizaciones de seguridad y cumplirán, en todo caso, toda disposición aplicable del Reglamento (UE) 2024../... del Parlamento Europeo y del Consejo***[23+];

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

---

[23] ***Reglamento (UE) .../... Reglamento (UE) …/… del Parlamento Europeo y del Consejo, de … sobre … (DO L, …, ELI: …).***

[+] ***DO: insértese en el texto el número de orden del Reglamento que figura en el documento PE-CONS 100/23*** [***2022/0272(COD)***] ***e insértese en la nota a pie de página el número de orden, la fecha, el título, la referencia de publicación en el DO y la referencia ELI de dicho Reglamento.***

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

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

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

▌

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

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

Artículo 18

Acciones de apoyo para la asistencia mutua

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

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

Artículo 19

Apoyo a terceros países ***asociados al Programa Europa Digital***

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Artículo 20

Coordinación con los mecanismos de gestión de crisis de la Unión

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

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

Capítulo IV

MECANISMO EUROPEO DE REVISIÓN DE INCIDENTES DE CIBERSEGURIDAD

Artículo 21

Mecanismo Europeo de Revisión de Incidentes de Ciberseguridad

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

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

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

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

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

Capítulo V
DISPOSICIONES FINALES

Artículo 22
Modificaciones del Reglamento (UE) 2021/694

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

1) el artículo 6 se modifica como sigue:

a) el apartado 1 se modifica como sigue:

i) se inserta la letra siguiente:

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

---

* ***Reglamento (UE) .../... del Parlamento Europeo y del Consejo, por el que se establecen medidas destinadas a reforzar la solidaridad y las capacidades en la Unión a fin de detectar ciberamenazas e incidentes, prepararse y responder a ellos y por el que se modifica el Reglamento (UE) 2021/694 (Reglamento de Cibersolidaridad) (DO L, …, ELI: …)***;

[+] ***DO: insértese en el texto el número de orden del Reglamento que figura en el documento PE-CONS 94/24*** [***2023/0109(COD)***] ***e insértese en la nota a pie de página el número de orden, la fecha, la referencia de publicación en el DO y la referencia ELI de dicho Reglamento.***

ii) se añade la letra siguiente:

«g) establecer y gestionar el Mecanismo de ***Emergencia en materia de Ciberseguridad,*** establecido por el artículo 10 del Reglamento (UE) …/…[+] incluida la Reserva de Ciberseguridad de la UE, ***establecida por el artículo 14, apartado 6, del Reglamento (UE) .../...[+] (en lo sucesivo, 'Reserva de Ciberseguridad de la UE')*** para ayudar a los Estados miembros a prepararse ante incidentes de ciberseguridad significativos y a gran escala, y darles respuesta, como complemento de los recursos y capacidades nacionales y otras formas de apoyo disponibles a escala de la Unión, y dar apoyo a otros usuarios en su respuesta a incidentes de ciberseguridad significativos y equivalentes a gran escala;»;

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

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

---

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

[+] **DO: insértese en el texto el número de orden del Reglamento que figura en el documento PE-CONS 94/24 (2023/0109(COD)).**

2) el artículo 9 se modifica como sigue:

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

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

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

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

b) se añade el apartado siguiente:

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

[+] **DO: insértese en el texto el número de orden del Reglamento que figura en el documento PE-CONS 94/24 (2023/0109(COD)).**

3) el artículo 12 se modifica como sigue:

a) se insertan los apartados siguientes***:***

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

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

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

[+] **DO: insértese en el texto el número de orden del Reglamento que figura en el documento PE-CONS 94/24 (2023/0109(COD)).**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

*** Reglamento (UE, Euratom) 2024/2509 del Parlamento Europeo y del Consejo, de 23 de septiembre de 2024, sobre las normas financieras aplicables al presupuesto general de la Unión, (versión refundida) (DO L, 2024/2509, 23.9.2024, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).

5) se inserta el artículo siguiente:

«Artículo 16 bis
Conflicto de normas

En el caso de las acciones de ejecución del ***Sistema Europeo de Alerta de Ciberseguridad***, las normas aplicables serán las establecidas en los artículos 4, 5 y 9 del Reglamento ***UE) .../...***[+24]. En caso de conflicto entre las disposiciones del presente Reglamento y los artículos 4, 5 y 9 de dicho Reglamento[+], estos últimos prevalecerán y se aplicarán a dichas acciones específicas.

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

[+] **DO: insértese en el texto el número de orden del Reglamento que figura en el documento PE-CONS 94/24 [2023/0109(COD)].**

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

«Artículo 19
Subvenciones

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

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

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

+

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

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

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

[+] ***DO: insértese en el texto el número de orden del Reglamento que figura en el documento PE-CONS 94/24 (2023/0109(COD)).***

Artículo 23

Ejercicio de la delegación

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

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

3. La delegación de poderes mencionada en el artículo 14, apartado 8, podrá ser revocada en cualquier momento por el Parlamento Europeo o por el Consejo. La decisión de revocación pondrá término a la delegación de los poderes que en ella se especifiquen. La decisión surtirá efecto el día siguiente al de su publicación en el Diario Oficial de la Unión Europea o en una fecha posterior indicada en ella. No afectará a la validez de los actos delegados que ya estén en vigor.

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

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

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

Artículo 24
Procedimiento de comité

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

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

Artículo 25

Evaluación ***y revisión***

1. A más tardar [***dos*** años ***a partir*** de la fecha de entrada en vigor del presente Reglamento] ***y, posteriormente, al menos cada cuatro años***, la Comisión ***evaluará el funcionamiento de las medidas establecidas en*** el presente Reglamento ***y presentará un informe*** al Parlamento Europeo y al Consejo.

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

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

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

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

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

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

Artículo 26

Entrada en vigor

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

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

Hecho en , el

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

Anexo

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

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

«Objetivo específico 3 – Ciberseguridad y confianza

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

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

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

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

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

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

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

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

«Objetivo específico 3 – Ciberseguridad y confianza

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

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

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

▌

Se ha realizado una declaración con respecto a este acto y se puede encontrar en [completado por la oficina del DO: DO C XXX de XX.XX.2024, p. XX] y en el siguiente enlace: [Oficina del DO: insértese el enlace a la declaración].

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

(Reglamento de Cibersolidaridad) [*]

1. La ficha de financiación legislativa de la Comisión que acompaña a la propuesta de Ley de Cibersolidaridad se publicó en abril de 2023. Desde entonces, las cifras estimadas pertinentes han cambiado debido a la adopción o la adopción prevista de otros actos legislativos.

2. El 5 de marzo de 2024, los colegisladores alcanzaron un acuerdo político preliminar para limitar a 22 millones EUR la reasignación del objetivo específico 4 «Capacidades digitales avanzadas» al objetivo específico 3 «Ciberseguridad y confianza» del programa Europa Digital prevista en la ficha de financiación legislativa.

3. Para reflejar los términos del acuerdo político preliminar, la Comisión actualizó la ficha de financiación legislativa de la Ley de Cibersolidaridad con respecto a las dotaciones financieras para los objetivos específicos 2 «Inteligencia artificial», 3 «Ciberseguridad y confianza» y 4 «Capacidades digitales avanzadas», teniendo en cuenta las reasignaciones acordadas por los colegisladores.

4. En consonancia, las dotaciones financieras para el período 2025-2027 presentadas en la ficha de financiación legislativa actualizada, sin perjuicio de las competencias de la Comisión en el contexto del procedimiento presupuestario anual, son las siguientes:

   - [544 726 000 EUR] para el objetivo específico 2 «Inteligencia artificial», teniendo en cuenta 65 millones EUR reasignados al objetivo específico 3 «Ciberseguridad y confianza»;
   - [44 451 000 EUR] para el objetivo específico 3 «Ciberseguridad y confianza», parte en régimen de gestión directa de la Comisión, incluidos 26 millones EUR reasignados de los objetivos específicos 2 y 4.
   - [353 190 613 EUR] para el objetivo específico 3 «Ciberseguridad y confianza», parte gestionada por el Centro Europeo de Competencia en Ciberseguridad, incluida la reasignación de 61 millones EUR de los objetivos específicos 2 y 4.
   - [167 162 423 EUR] para el objetivo específico 4 «Capacidades digitales avanzadas», teniendo en cuenta la reasignación de 22 millones EUR al objetivo específico 3 «Ciberseguridad y confianza».

---

[*] En el marco del acuerdo político provisional se decidió que la presente declaración de la Comisión Europea se publicaría en la serie C del Diario Oficial y que habría una referencia y un enlace a esta en la serie L, junto con el acto legislativo.

5. La Reserva de Ciberseguridad de la UE se financiará con cargo a la dotación financiera del objetivo específico 3 «Ciberseguridad y confianza», parte en régimen de gestión directa de la Comisión (que, según la ficha de financiación legislativa actualizada, se estima en [44 451 000] EUR).