ENMIENDAS 001-001
presentadas por la Comisión de Industria, Investigación y Energía

Informe
Lina Gálvez Muñoz **A9-0426/2023**
Reglamento de solidaridad cibernética

Propuesta de Reglamento (COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

Enmienda 1

ENMIENDAS DEL PARLAMENTO EUROPEO*

a la propuesta de la Comisión

2023/0109 (COD)

Propuesta de

REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO

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

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),

---

* Enmiendas: el texto nuevo o modificado se señala en negrita y cursiva; las supresiones se indican mediante el símbolo ▌.

Vista la propuesta de la Comisión Europea,

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

Visto el dictamen del Tribunal de Cuentas[1],

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

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

De conformidad con el procedimiento legislativo ordinario,

Considerando lo siguiente:

(1) La utilización y dependencia de las tecnologías de la información y la comunicación constituyen un elemento esencial, ***pero, al mismo tiempo, han introducido posibles vulnerabilidades,*** en todos los sectores de actividad económica ***y en la democracia,*** ya que tanto nuestras administraciones públicas como nuestras empresas y ciudadanos están más interconectados y son más interdependientes que nunca, en todos los sectores y por encima de todas las fronteras.

(2) La magnitud, la frecuencia y los efectos de los incidentes de ciberseguridad están aumentando ***en toda la Unión y en el mundo en términos del método y su repercusión***, incluidos los ataques a la cadena de suministro con fines de ciberespionaje, secuestro de archivos o perturbación. Representan una grave amenaza para el funcionamiento de las redes y los sistemas de información. En vista de la rápida evolución del panorama de amenazas, la amenaza de un posible incidente a gran escala que provoque perturbaciones y daños significativos en ***las economías y democracias, así como en*** las infraestructuras críticas ***de toda la Unión*** exige una mayor preparación a todos los niveles del marco de ciberseguridad de la UE. Esa amenaza va más allá de la agresión militar de Rusia a Ucrania y probablemente persistirá, dada la multiplicidad de agentes estatales ***y*** criminales ▌ implicados en las tensiones geopolíticas actuales. Tales incidentes pueden obstaculizar la prestación de servicios públicos y el desarrollo de actividades económicas, incluso en sectores críticos o muy críticos, generar pérdidas económicas sustanciales, socavar la confianza de los usuarios, causar graves daños a la economía de la Unión e incluso suponer una amenaza para la salud o la vida. Además, los incidentes de ciberseguridad son impredecibles, ya que a menudo surgen y evolucionan en períodos de tiempo muy breves, no se limitan a ninguna zona geográfica específica y se producen simultáneamente o se propagan de forma instantánea por muchos países. ***Por lo tanto, es necesaria una cooperación estrecha y coordinada entre el sector público, el sector privado, el mundo académico, la sociedad civil y los medios de comunicación. Además, la respuesta de la Unión debe coordinarse con las instituciones internacionales, así como con los socios internacionales de confianza y afines. Socios internacionales de confianza y afines son aquellos países que comparten los valores de la Unión de democracia, compromiso con los derechos humanos, multilateralismo efectivo y orden basado en normas, en consonancia con los marcos y acuerdos de cooperación internacional. A fin de garantizar la cooperación con socios internacionales fiables y afines y la protección contra rivales sistémicos, las entidades establecidas en terceros países que no sean partes en el ACP no deben***

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

estar autorizadas a participar en la contratación pública en virtud del presente Reglamento.

(3) Es necesario afianzar la posición competitiva de los sectores de la industria y los servicios de la Unión en el conjunto de la economía digitalizada y apoyar su transformación digital reforzando el nivel de ciberseguridad en el mercado único digital. Tal como se recomendó en tres propuestas distintas de la Conferencia sobre el Futuro de Europa[1], es necesario aumentar la resiliencia de los ciudadanos, las empresas, ***en particular, las microempresas, las pequeñas y medianas empresas (pymes), también las empresas emergentes,*** y las entidades que gestionan infraestructuras críticas***, incluidas las autoridades locales o regionales***, frente a las crecientes amenazas a la ciberseguridad, que pueden tener repercusiones sociales y económicas devastadoras. Por lo tanto, es necesaria la inversión en infraestructuras y servicios ***y la creación de capacidades para desarrollar competencias en ciberseguridad*** que apoyen una detección de las amenazas e incidentes de ciberseguridad y una respuesta a ellos más rápidas, y los Estados miembros precisan de asistencia para prepararse mejor y responder a los incidentes de ciberseguridad significativos y a gran escala. La Unión también debe aumentar sus capacidades en estos ámbitos, en particular en lo que se refiere a la recopilación y el análisis de datos sobre amenazas e incidentes de ciberseguridad.

(3 bis) Los ciberataques suelen dirigirse contra servicios e infraestructuras públicos locales, regionales o nacionales. Los entes locales se encuentran entre los objetivos más vulnerables de los ciberataques debido a su falta de recursos financieros y humanos. Por lo tanto, es especialmente importante que los poderes de decisión locales sean conscientes de la necesidad de fortalecer la resiliencia digital, aumentar su capacidad para reducir el impacto de los ciberataques y aprovechar las oportunidades que ofrece el presente Reglamento.

(4) La Unión ya ha tomado una serie de medidas para reducir las vulnerabilidades y aumentar la resiliencia de las infraestructuras y entidades críticas frente a los riesgos de ciberseguridad, en particular la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo[2], la Recomendación (UE) 2017/1584 de la Comisión[3], la Directiva 2013/40/UE del Parlamento Europeo y del Consejo[4] y el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo[5]. Además, la Recomendación del Consejo

---

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

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

3 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).

4 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).

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

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

(5) Los crecientes riesgos de ciberseguridad y un panorama general de amenazas complejo, con un claro riesgo de propagación rápida de ciberincidentes de un Estado miembro a otros y de un tercer país a la Unión, requieren una solidaridad reforzada a escala de la Unión para mejorar la detección de las amenazas e incidentes de ciberseguridad, la preparación frente a ellos, ▌ la respuesta a ellos ***y la recuperación de ellos***. Los Estados miembros también han invitado a la Comisión a que presente una propuesta sobre un nuevo Fondo de Respuesta de Emergencia para la Ciberseguridad en las Conclusiones del Consejo sobre la posición cibernética de la UE[1].

(6) La Comunicación conjunta sobre la política de ciberdefensa de la UE[2], adoptada el 10 de noviembre de 2022, anunció una Iniciativa de Cibersolidaridad de la UE con los siguientes objetivos: refuerzo de las capacidades comunes de detección, conciencia situacional y respuesta de la UE mediante la promoción del despliegue de una ***red*** de la UE de centros de operaciones de seguridad («COS»), el apoyo a la creación gradual de una reserva de ciberseguridad a escala de la UE con servicios de proveedores privados de confianza y la realización de pruebas de entidades críticas para detectar posibles vulnerabilidades basadas en evaluaciones de riesgos de la UE.

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

(8) Para alcanzar estos objetivos, procede también modificar el Reglamento (UE)

---

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).

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

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

2021/694 del Parlamento Europeo y del Consejo[1] en determinados ámbitos. En particular, el presente Reglamento debe modificar el Reglamento (UE) 2021/694 en lo que respecta a la adición de nuevos objetivos operativos relacionados con el Ciberescudo Europeo y el Mecanismo de ***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 amenazas y responder a ellos, y reforzar la cooperación transfronteriza en materia de ciberseguridad. Esto ha de completarse con el establecimiento de las condiciones específicas en las que pueda concederse ayuda financiera para dichas acciones y la definición de los mecanismos de gobernanza y coordinación necesarios para alcanzar los objetivos previstos. Otras modificaciones del Reglamento (UE) 2021/694 deben incluir descripciones de las acciones propuestas en el marco de los nuevos objetivos operativos, así como indicadores mensurables para seguir la aplicación de estos nuevos objetivos operativos.

(9) La financiación de las acciones en virtud del presente Reglamento debe estar prevista en el Reglamento (UE) 2021/694, que debe seguir siendo el acto de base pertinente para estas acciones, consagradas en el objetivo específico 3 del programa Europa Digital. Deben establecerse las condiciones específicas de participación en relación con cada acción, de conformidad con las disposiciones aplicables del Reglamento (UE) 2021/694.

(9 bis) A la luz de la evolución geopolítica y de la intensificación de las ciberamenazas (PPE 52), y con el fin de garantizar la continuidad y el ulterior desarrollo de las medidas establecidas en el presente Reglamento después de 2027, en particular el Ciberescudo Europeo y el Mecanismo de Emergencia en materia de Ciberseguridad, es necesario garantizar una línea presupuestaria específica en el marco financiero plurianual para el período 2028-2034. Los Estados miembros deben comprometerse a apoyar todas las medidas necesarias para reducir las ciberamenazas e incidentes en toda la Unión y a reforzar la solidaridad.

(10) Son de aplicación al presente Reglamento las normas financieras horizontales adoptadas por el Parlamento Europeo y el Consejo en virtud del artículo 322 del TFUE. Dichas normas se establecen en el Reglamento ***(UE, Euratom) 2018/1046 del Parlamento Europeo y del Consejo[2]*** 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,

---

1 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).

2 ***Reglamento (UE, Euratom) 2018/1046 del Parlamento Europeo y del Consejo, de 18 de julio de 2018, sobre las normas financieras aplicables al presupuesto general de la Unión, por el que se modifican los Reglamentos (UE) n.º 1296/2013, (UE) n.º 1301/2013, (UE) n.º 1303/2013, (UE) n.º 1304/2013, (UE) n.º 1309/2013, (UE) n.º 1316/2013, (UE) n.º 223/2014 y (UE) n.º 283/2014 y la Decisión n.º 541/2014/UE y por el que se deroga el Reglamento (UE, Euratom) n.º 966/2012 (DO L 193 de 30.7.2018, p. 1, ELI: http://data.europa.eu/eli/reg/2018/1046/oj).***

Euratom) 2020/2092 del Parlamento Europeo y del Consejo[1].

(11) A efectos de una buena gestión financiera, deben establecerse normas específicas para la prórroga de los créditos de compromiso y de pago no utilizados. Al tiempo que se respeta el principio de que el presupuesto de la Unión se establece anualmente, el presente Reglamento, debido al carácter impredecible, excepcional y específico del panorama de la ciberseguridad, debe prever la posibilidad de prorrogar los fondos no utilizados más allá de los establecidos en el ***Reglamento (UE, Euratom) 2018/1046***, maximizando así la capacidad del Mecanismo de Ciberemergencia para ayudar a los Estados miembros a hacer frente eficazmente a las ciberamenazas.

(11 bis) El Mecanismo de Emergencia en materia de Ciberseguridad y la Reserva de Ciberseguridad de la UE establecidos en el presente Reglamento son iniciativas nuevas que no se previeron en la elaboración del marco financiero plurianual para el período 2021-2027, y la financiación de dichas iniciativas tiene por objeto limitar en la medida de lo posible la reducción de la financiación para otras prioridades del programa Europa Digital. Por ello, el importe de los recursos financieros destinados a la Reserva de Ciberseguridad de la UE debe reducirse y debe extraerse principalmente de los márgenes no asignados dentro de los límites máximos del marco financiero plurianual o movilizarse a través de los instrumentos especiales del marco financiero plurianual no temáticos. Toda asignación o reasignación de fondos de los programas existentes debe reducirse al mínimo absoluto, con el fin de proteger los programas existentes, en particular Erasmus+, frente a los efectos negativos y garantizar que dichos programas puedan alcanzar los objetivos fijados.

(12) Para prevenir, evaluar, responder ***y recuperarse*** de manera más eficaz frente a las ciberamenazas y ciberincidentes, es necesario desarrollar conocimientos más completos sobre las amenazas para las infraestructuras y los activos críticos en el territorio de la Unión, incluida su distribución geográfica, su interconexión y los posibles efectos en caso de ciberataques que les afecten. ***Un enfoque proactivo para detectar, mitigar y prevenir posibles ciberamenazas comprende una mayor capacidad de detección avanzada, capacidad necesaria para detener las amenazas persistentes avanzadas. La inteligencia en materia de amenazas abarca la información recogida, analizada e interpretada para comprender posibles amenazas y riesgos. A través del análisis y el establecimiento de correlaciones de grandes cantidades de datos, desvela patrones, tendencias e indicadores de compromiso que pueden revelar actividades malintencionadas o vulnerabilidades***. Debe desplegarse una ***red*** de COS de la Unión a gran escala (el «Ciberescudo Europeo») que incluya varias plataformas transfronterizas interoperativas, cada una de ellas integrada por varios COS nacionales. Dicha infraestructura debe servir a los intereses y necesidades nacionales y de la Unión en materia de ciberseguridad, y debe aprovechar la tecnología más puntera para las herramientas avanzadas de recopilación y análisis de datos, mejorar las capacidades de ciberdetección y gestión y proporcionar conciencia situacional en tiempo real. ***Un COS nacional es una capacidad centralizada responsable de recopilar de manera continua información de inteligencia sobre amenazas y de mejorar la posición en materia de ciberseguridad de las entidades***

[1] ***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).***

bajo jurisdicción nacional mediante la prevención, la detección y el análisis de las amenazas a la ciberseguridad. Tal infraestructura debe servir para aumentar la detección de amenazas e incidentes de ciberseguridad y complementar y apoyar así a las entidades y redes de la Unión responsables de la gestión de crisis en la Unión, en particular la red europea de organizaciones de enlace para las crisis de ciberseguridad («EU-CyCLONe»), tal como se define en la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo[1].

(13) ***A fin de participar en el Ciberescudo, cada*** Estado miembro debe designar un organismo público a nivel nacional encargado de coordinar las actividades de detección de ciberamenazas en dicho Estado miembro. ***Se anima a los Estados miembros a que incorporen la capacidad del COS nacional a su estructura y gobernanza cibernéticas existentes para evitar la creación de nuevos niveles de gobernanza, así como a armonizar el presente Reglamento con los actos legislativos existentes, en particular con la Directiva (UE) 2022/2555.*** Estos COS nacionales deben actuar como punto de referencia y pasarela a nivel nacional para la participación ***de entidades privadas y públicas, en particular sus COS nacionales,*** en el Ciberescudo Europeo y deben garantizar que la información sobre ciberamenazas procedente de entidades públicas y privadas se comparta y recopile a nivel nacional de manera eficaz y racional. ***Los COS nacionales deben reforzar la cooperación y el intercambio de información entre entidades públicas y privadas para acabar con los compartimentos estancos de comunicación existentes. De este modo, pueden apoyar la creación de modelos de intercambio de datos y deben facilitar y fomentar el intercambio de información en un entorno de confianza y seguro. Para reforzar la resiliencia de la Unión en el ámbito de la ciberseguridad es esencial una cooperación estrecha y coordinada entre las entidades públicas y privadas.***

(14) Como parte del Ciberescudo Europeo, debe crearse una serie de centros de operaciones de ciberseguridad transfronterizos («COS transfronterizos»). Estos deben reunir a los COS nacionales de al menos tres Estados miembros, de modo que puedan lograrse plenamente los beneficios de la detección transfronteriza de amenazas y del intercambio y la gestión de la información. El objetivo general de los COS transfronterizos debe ser reforzar las capacidades para analizar, prevenir y detectar las amenazas a la ciberseguridad y apoyar la producción de inteligencia de alta calidad***, también mediante la recogida y el intercambio de datos e información sobre posibles actos de piratería maliciosa, amenazas maliciosas de nueva creación y programas intrusos que aún no se hayan desplegado en un ciberincidente, y esfuerzos de análisis***, sobre las amenazas a la ciberseguridad, en particular mediante el intercambio de datos procedentes de diversas fuentes, públicas o privadas, así como mediante el intercambio y el uso conjunto de herramientas de vanguardia, y el desarrollo conjunto de capacidades de detección, análisis y prevención en un entorno de confianza ***y seguro, con el respaldo de la ENISA, en asuntos relacionados con la cooperación operativa entre los Estados miembros***. ***Los COS transfronterizos deben facilitar y fomentar el intercambio de información en un entorno de confianza y seguro y*** proporcionar nuevas capacidades adicionales, aprovechando y complementando los

[1] 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).

COS existentes y los equipos de respuesta a incidentes de seguridad informática («CSIRT») y otros agentes pertinentes.

(15) A nivel nacional, el seguimiento, la detección y el análisis de las ciberamenazas suelen correr a cargo de los COS de las entidades públicas y privadas, en combinación con los CSIRT. Además, los CSIRT intercambian información en el contexto de la red de CSIRT, de conformidad con la Directiva (UE) 2022/2555. Los COS transfronterizos deben constituir una nueva capacidad que se ***incorpore a la infraestructura de ciberseguridad existente, especialmente*** la red de CSIRT, mediante la puesta en común y el intercambio de datos sobre las amenazas a la ciberseguridad de entidades públicas y privadas***, y en particular sus COS***, aumentando el valor de dichos datos mediante el análisis de expertos y la adquisición conjunta de infraestructuras y herramientas punteras, y contribuyendo ***a la soberanía tecnológica de la Unión, a su autonomía estratégica abierta, a su competitividad y resiliencia y al desarrollo de un ecosistema de ciberseguridad significativo, también en cooperación con socios internacionales de confianza y afines.***

(16) Los COS transfronterizos deben actuar como punto central que permita una amplia puesta en común de datos pertinentes y de inteligencia sobre ciberamenazas, y permitir la difusión de información sobre amenazas entre un amplio y diverso conjunto de agentes [por ejemplo, los equipos de respuesta a emergencias informáticas (CERT), la red de CSIRT, los centros de intercambio y análisis de información (ISAC) y los operadores de infraestructuras críticas] ***con vistas a facilitar el fin de los compartimentos estancos de comunicación existentes. De este modo, los COS transfronterizos también podrían apoyar la creación de modelos de intercambio de datos en toda la Unión.*** La información intercambiada entre los participantes en un COS transfronterizo podría incluir datos de redes y sensores, fuentes de información sobre amenazas, indicadores de compromiso e información contextualizada sobre incidentes, amenazas y vulnerabilidades***, también la recogida y el intercambio de datos e información sobre posibles actos de piratería maliciosa, amenazas maliciosas de nueva creación y programas intrusos que aún no se hayan desplegado en un ciberincidente, y esfuerzos de análisis***. Además, los COS transfronterizos también deben celebrar acuerdos de cooperación con otros COS transfronterizos.

(17) Que las autoridades pertinentes compartan la conciencia situacional es un requisito indispensable para la preparación y la coordinación a escala de la Unión con respecto a los incidentes de ciberseguridad significativos y a gran escala. La Directiva (UE) 2022/2555 crea EU-CyCLONe a fin de respaldar la gestión coordinada de los incidentes y las crisis de ciberseguridad a gran escala en el ámbito operativo y de garantizar el intercambio periódico de información pertinente entre los Estados miembros y las instituciones, órganos y organismos de la Unión. La Recomendación (UE) 2017/1584 sobre la respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala aborda el papel de todos los agentes pertinentes. La Directiva (UE) 2022/2555 también recuerda las responsabilidades de la Comisión en el Mecanismo de Protección Civil de la Unión («UCPM») establecido por la Decisión 1313/2013/UE del Parlamento Europeo y del Consejo[1], así como en lo

[1] ***Decisión n.º 1313/2013/UE del Parlamento Europeo y del Consejo, de 17 de diciembre de 2013, relativa a un Mecanismo de Protección Civil de la Unión (Texto pertinente a efectos del EEE) (***DO L 347 de 20.12.2013, p. 924, ***ELI:*** http://data.europa.eu/eli/dec/2013/1313/oj***).***

relativo a la presentación de informes analíticos para el Dispositivo de Respuesta Política Integrada a las Crisis («Dispositivo RPIC») en virtud de la Decisión de Ejecución (UE) 2018/1993 ***del Consejo***[1]. Por lo tanto, en situaciones en las que los COS transfronterizos obtengan información relacionada con un incidente de ciberseguridad a gran escala potencial o en curso, deben proporcionar la información pertinente a EU-CyCLONe, a la red de CSIRT y a la Comisión, de ***conformidad con la Directiva (UE) 2022/2555***. En particular, dependiendo de la situación, la información que debe compartirse podría incluir información técnica, información sobre la naturaleza y los motivos del agresor o posible agresor, e información no técnica de nivel superior sobre un incidente de ciberseguridad a gran escala potencial o en curso. En este contexto, debe prestarse la debida atención al principio de la necesidad de conocer y al carácter potencialmente sensible de la información compartida.

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

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

(20) Al recopilar, compartir e intercambiar datos, el Ciberescudo Europeo debe reforzar la soberanía tecnológica de la Unión***, su autonomía estratégica abierta, su competitividad y resiliencia y un ecosistema de ciberseguridad de la Unión significativo***. La puesta en común de datos gestionados de alta calidad también debería contribuir al desarrollo de tecnologías avanzadas de inteligencia artificial y análisis de datos. ***La inteligencia artificial es lo más eficaz cuando se combina con el análisis humano. Por lo tanto, una mano de obra cualificada sigue siendo esencial para la puesta en común de datos de alta calidad.*** Debe facilitarse mediante la conexión del Ciberescudo Europeo con la infraestructura paneuropea de informática de alto rendimiento establecida por el Reglamento (UE) 2021/1173 del Consejo[2].

---

1 ***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).***

2 Reglamento (UE) 2021/1173 del Consejo, de 13 de julio de 2021, por el que se crea la Empresa Común de Informática de Alto Rendimiento Europea y por el que se deroga el

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

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

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

(24) En vista del aumento de los riesgos y del número de ciberincidentes que afectan a los Estados miembros, es necesario crear un instrumento de apoyo a las crisis para mejorar la resiliencia de la Unión frente a incidentes de ciberseguridad significativos y a gran escala y complementar las acciones de los Estados miembros a través del apoyo financiero de emergencia para la preparación, la respuesta y la recuperación inmediata de los servicios esenciales. Dicho instrumento debe permitir el despliegue rápido ***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 de ciberseguridad, 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»).

(25) El Mecanismo ***de Emergencia en materia de Ciberseguridad*** debe prestar apoyo a los Estados miembros complementando sus propias medidas y recursos, así como otras

---

Reglamento (UE) 2018/1488 (DO L 256 de 19.7.2021, p. 3, ***ELI: http://data.europa.eu/eli/reg/2021/1173/oj***).

opciones de apoyo existentes para la respuesta y recuperación inmediata de incidentes de ciberseguridad significativos y a gran escala, como los servicios prestados por la Agencia de la Unión Europea para la Ciberseguridad (la «ENISA») de conformidad con su mandato, la respuesta coordinada y la asistencia de la red de CSIRT, el apoyo a la mitigación de EU-CyCLONe, así como la asistencia mutua entre los Estados miembros, también en el contexto del artículo 42, apartado 7, del TUE, los equipos de respuesta telemática rápida de la CEP[1] y los equipos de respuesta rápida contra amenazas híbridas. Debe abordar la necesidad de garantizar la disponibilidad de medios especializados para apoyar la preparación y la respuesta a los incidentes de ciberseguridad en toda la Unión y en terceros países.

(26) El presente instrumento se entiende sin perjuicio de los procedimientos y marcos para coordinar la respuesta a las crisis a escala de la Unión, en particular el UCPM[2], el Dispositivo RPIC[3], y la Directiva (UE) 2022/2555. Puede contribuir o complementar acciones ejecutadas en el contexto del artículo 42, apartado 7, del TUE o en situaciones definidas en el artículo 222 del TFUE. El uso del presente instrumento también debe coordinarse con la aplicación de las medidas del conjunto de instrumentos de ciberdiplomacia, cuando proceda.

(27) La asistencia prestada en virtud del presente Reglamento debe apoyar y complementar las medidas tomadas por los Estados miembros a nivel nacional. A tal fin, debe garantizarse una estrecha cooperación y consulta entre la Comisión***, la ENISA*** y el Estado miembro afectado. 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.

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

---

1 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.

2 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).

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

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 mitigar los efectos de incidentes de ciberseguridad significativos y a gran escala, apoyar la recuperación inmediata o restablecer el funcionamiento de los servicios esenciales.

(29) Como parte de las acciones de preparación, a fin de promover un enfoque coherente y reforzar la seguridad en toda la Unión y su mercado interior, debe prestarse apoyo para la puesta a prueba y la evaluación de la ciberseguridad de las entidades que operan en los sectores muy críticos determinados de conformidad con la Directiva (UE) 2022/2555 de manera coordinada. A tal fin, la Comisión, con el apoyo de la ENISA y en cooperación con el Grupo de Cooperación SRI establecido por la Directiva (UE) 2022/2555, debe determinar periódicamente los sectores o subsectores pertinentes, los cuales deben poder optar a recibir ayuda financiera para la realización de pruebas coordinadas a escala de la Unión. Los sectores o subsectores deben seleccionarse del anexo I de la Directiva (UE) 2022/2555 («Sectores de alta criticidad»). Los ejercicios de pruebas coordinados deben basarse en metodologías y escenarios de riesgo comunes. La selección de sectores y el desarrollo de escenarios de riesgo deben tener en cuenta las evaluaciones de riesgos y los escenarios de riesgo pertinentes a escala de la Unión, incluida la necesidad de evitar duplicaciones, tales como la evaluación de riesgos y los escenarios de riesgo requeridos en las Conclusiones del Consejo sobre el desarrollo de la posición cibernética de la Unión Europea que lleven a cabo la Comisión, el Alto Representante y el Grupo de Cooperación SRI, en coordinación con los organismos y agencias civiles y militares pertinentes y las redes establecidas, incluida la red EU CyCLONe, así como la evaluación de riesgos de las redes e infraestructuras de comunicaciones solicitada por el llamamiento ministerial conjunto de Nevers y llevada a cabo por el Grupo de Cooperación SRI, con el apoyo de la Comisión y la ENISA, y en cooperación con el Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE), las evaluaciones coordinadas de riesgos que se lleven a cabo en virtud del artículo 22 de la Directiva (UE) 2022/2555 y las pruebas de resiliencia operativa digital previstas en el Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo[1]. La selección de los sectores también debe tener en cuenta la Recomendación del Consejo relativa a un enfoque coordinado en toda la Unión para reforzar la resiliencia de las infraestructuras críticas.

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

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

---

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

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

(33) Debe crearse gradualmente una reserva de ciberseguridad a escala de la Unión, compuesta por servicios de proveedores privados de servicios de seguridad gestionados para apoyar las acciones de respuesta y recuperación inmediata en caso de incidentes de ciberseguridad significativos o a gran escala. La Reserva de Ciberseguridad de la UE debe garantizar la disponibilidad y el estado de preparación de los servicios, ***reforzando al mismo tiempo la resiliencia de la Unión, incluida la participación de proveedores europeos de servicios de seguridad gestionados que sean pymes y garantizando la creación de un ecosistema de ciberseguridad, en particular microempresas, pymes, incluidas las empresas emergentes, con inversiones en investigación e innovación (I+i) para desarrollar tecnologías punteras, como las relacionadas con la nube y la inteligencia artificial***. ***Los proveedores de confianza, incluidas las pymes, deben poder cooperar entre sí para cumplir los criterios anteriores.*** Los servicios de la Reserva de Ciberseguridad de la UE deben servir para ayudar a las autoridades nacionales a prestar asistencia a las entidades afectadas que operen en sectores críticos o muy críticos como complemento de sus propias acciones a nivel nacional. ***Por lo tanto, la Reserva de Ciberseguridad debe incentivar la inversión en investigación e innovación para impulsar el desarrollo de estas tecnologías. Cuando proceda, podrían llevarse a cabo ejercicios comunes con los proveedores de confianza y los usuarios potenciales de la Reserva de Ciberseguridad para garantizar un funcionamiento eficiente de la Reserva en caso necesario.*** Al solicitar el apoyo de la Reserva de Ciberseguridad de la UE, los Estados miembros deben especificar el apoyo prestado a la entidad afectada a nivel nacional, que debe tenerse en cuenta al evaluar la solicitud del Estado miembro. Los servicios de la Reserva de Ciberseguridad de la UE también pueden servir para apoyar a las instituciones, órganos y organismos de la Unión, en condiciones similares. ***La Comisión debe garantizar la participación y amplios intercambios con los Estados miembros a fin de evitar la duplicación de iniciativas similares, también dentro de la Organización del Tratado del Atlántico Norte (OTAN).***

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

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

derivadas de esta disposición, la ENISA debe recibir una financiación adicional adecuada.

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

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

(37 bis) Los terceros países podrían acceder a recursos y apoyo en virtud del presente Reglamento, utilizando el apoyo a la respuesta a incidentes de la Reserva de Ciberseguridad de la Unión. Además, los proveedores de servicios de respuesta a incidentes de terceros países, incluidos los terceros países asociados al programa Europa Digital u otros países socios internacionales, y países miembros de la OTAN, pueden ser necesarios para la prestación de servicios específicos en la Reserva de Ciberseguridad de la UE. No obstante lo dispuesto en el Reglamento (UE, Euratom)

2018/1046, a fin de reforzar la soberanía tecnológica de la Unión, su autonomía estratégica abierta, su competitividad y resiliencia, y salvaguardar los activos estratégicos, los intereses o la seguridad de la Unión, no debe permitirse la participación de entidades establecidas en terceros países que no sean parte en el ACP y que no hayan sido objeto de control en el sentido del Reglamento (UE) 2019/452 del Parlamento Europeo y del Consejo[1] y, en caso necesario, de medidas de mitigación, teniendo en cuenta los objetivos establecidos en el presente Reglamento. La dimensión exterior del presente Reglamento debe estar en consonancia con las disposiciones establecidas en el acuerdo de asociación en el marco del programa Europa Digital. La participación de terceros países debe estar sujeta a control público, con la participación de los poderes legislativos, para garantizar que los ciudadanos puedan participar en el proceso.

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

---

* ***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).***

(38 bis) Para la aplicación eficaz del Ciberescudo Europeo y del Mecanismo de Emergencia en materia de Ciberseguridad es imprescindible contar con un personal cualificado, capaz de prestar de forma fiable los servicios de ciberseguridad pertinentes al más alto nivel. Por lo tanto, es preocupante que la Unión se enfrente a una brecha de talento, que se caracteriza por la escasez de profesionales cualificados, al tiempo que debe hacer frente a un panorama de amenazas en rápida evolución, como se reconoce en la Comunicación de la Comisión, de 18 de abril de 2023, sobre la Academia de Cibercapacidades. Es importante superar ese déficit de talento reforzando la cooperación y la coordinación entre las distintas partes interesadas, incluido el sector privado, el mundo académico, los Estados miembros, la Comisión y la ENISA, a fin de aumentar y crear sinergias, en todos los territorios, para la inversión en educación y formación, el desarrollo de colaboraciones público-privadas, el apoyo a las iniciativas de investigación e innovación, el desarrollo y el reconocimiento mutuo de normas comunes y la certificación de capacidades en

---

1 Reglamento (UE) 2019/452 del Parlamento Europeo y del Consejo, de 19 de marzo de 2019, para el control de las inversiones extranjeras directas en la Unión (DO L 79I de 21.3.2019, p. 1), ELI: http://data.europa.eu/eli/reg/2019/452/oj.

materia de ciberseguridad, también a través del Marco Europeo de Capacidades en Ciberseguridad. Esto también debe facilitar la movilidad de los profesionales de la ciberseguridad dentro de la Unión. El presente Reglamento debe tener por objeto promover una mano de obra en materia de ciberseguridad más diversa. Todas las medidas destinadas a aumentar las capacidades en materia de ciberseguridad requieren salvaguardias para evitar la «fuga de cerebros» y los riesgos para la movilidad laboral.

(38 ter) Es necesario reforzar las capacidades y competencias especializadas, interdisciplinarias y generales en toda la Unión, prestando especial atención a las mujeres, ya que en el ámbito de la ciberseguridad persiste la brecha de género, dado que la presencia media de mujeres a escala mundial equivale al 20 %. Las mujeres deben estar presentes en el diseño del futuro digital y de su gobernanza y formar parte de este.

(38 quater) La finalidad de reforzar la investigación e innovación (I+i) en materia de ciberseguridad es aumentar la resiliencia y la autonomía estratégica abierta de la Unión. Asimismo, es importante crear sinergias con los programas de I + i y con los instrumentos e instituciones existentes, y reforzar la cooperación y la coordinación entre las distintas partes interesadas, incluidos el sector privado, la sociedad civil, el mundo académico, los Estados miembros, la Comisión y la ENISA;

(38 quinquies) El presente Reglamento debe contribuir al cumplimiento del compromiso, formulado en la Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital, de proteger los intereses de nuestras democracias, personas, empresas e instituciones públicas contra los riesgos de ciberseguridad y la ciberdelincuencia, incluidas las violaciones de la seguridad de los datos y la usurpación o manipulación de identidad. La aplicación del presente Reglamento también debe contribuir a mejorar la aplicación de otros actos legislativos, por ejemplo, en materia de inteligencia artificial, privacidad de datos y regulación de datos en términos de ciberseguridad y ciberresiliencia.

(38 sexies) Para la buena aplicación del presente Reglamento es esencial aumentar la cultura de ciberseguridad, conforme a la cual la seguridad, en particular la del entorno digital, se concibe como un bien público. Por lo tanto, el desarrollo de medidas para incluir y aumentar la sensibilización de los ciudadanos debe ser otro medio para garantizar la salvaguardia de nuestras democracias y valores fundamentales.

(38 septies) 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 con el fin de especificar las condiciones de interoperabilidad entre los COS transfronterizos, establecer las disposiciones de procedimiento para el intercambio de información entre los COS transfronterizos, por una parte, y EU-CyCLONe, la red de CSIRT y la Comisión, por otra, especificar los tipos y el número de servicios de respuesta necesarios para la Reserva de Ciberseguridad de la UE y especificar en mayor medida las disposiciones detalladas para asignar los servicios de apoyo proporcionados por 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. 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.

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

(39) ***Dado que los objetivos*** del presente Reglamento***, a saber, reforzar las capacidades de la Unión para la prevención, detección, respuesta y recuperación en materia de ciberamenazas y establecer un marco general que acabe con la compartimentación de la comunicación, no pueden ser alcanzados de manera suficiente por los Estados miembros,*** sino que pueden lograrse mejor a escala de la Unión. Por tanto, la Unión puede adoptar medidas con arreglo a los principios de subsidiariedad y proporcionalidad establecidos en el artículo 5 del Tratado de la Unión Europea. ***De conformidad con el principio de proporcionalidad enunciado en dicho artículo, el presente*** Reglamento no excede de lo necesario para alcanzar dicho objetivo.

HAN ADOPTADO EL PRESENTE REGLAMENTO:

Capítulo I

OBJETIVOS GENERALES, OBJETO Y DEFINICIONES

Artículo 1

Objeto y objetivos

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

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

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

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

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

a) afianzar la capacidad común de la Unión de detección y conciencia situacional de ciberamenazas y ciberincidentes, permitiendo así ***respaldar la capacidad industrial de la Unión y de los Estados miembros en el sector de la ciberseguridad, y*** reforzar la posición competitiva de la industria, ***en particular las microempresas, las pymes, también las empresas emergentes,*** y los sectores de servicios de la Unión en toda la economía digital y contribuir a la soberanía tecnológica de la Unión***, su autonomía estratégica abierta, su competitividad y su resiliencia en dicho sector, reforzar el sistema de ciberseguridad, con vistas a garantizar unas sólidas capacidades de la Unión, también en cooperación con socios internacionales***;

b) consolidar la preparación de las entidades que operan en sectores críticos y muy críticos en toda la Unión y reforzar la solidaridad mediante el desarrollo de capacidades comunes de respuesta frente a incidentes de ciberseguridad significativos o a gran escala, en particular poniendo el apoyo de la Unión a la respuesta a incidentes de ciberseguridad a disposición de terceros países asociados al programa Europa Digital;

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

c bis) desarrollar, de manera coordinada, las capacidades, los conocimientos técnicos y las competencias de la mano de obra, con vistas a garantizar la ciberseguridad y a crear sinergias con la Academia de Capacidades en Ciberseguridad.

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

Artículo 2

Definiciones

A los efectos del presente Reglamento, se entenderá por:

-1 bis) «centro de operaciones de seguridad nacional» («COS nacional»): una capacidad nacional centralizada que recopila y analiza continuamente información de inteligencia sobre ciberamenazas y mejora la posición en materia de ciberseguridad de conformidad con el artículo 4;

1) «centro de operaciones de seguridad transfronterizo» («COS transfronterizo»): una plataforma plurinacional que reúne en una estructura de red coordinada a los COS nacionales ***de conformidad con el artículo 5***;

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

3) «consorcio anfitrión»: un consorcio compuesto por Estados participantes, representados por los COS nacionales***, de conformidad con el artículo 5***;

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

4 bis) «entidad crítica»: entidad crítica tal como se define en el artículo 2, punto 1, de la Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo[2];

5) «entidades que operan en sectores críticos o muy críticos»: el tipo de entidades ***que operan en los sectores*** enumerados en los anexos I y II de la Directiva (UE) 2022/2555;

5 bis) «gestión de incidentes»: la gestión de incidentes según se define en el artículo 6, punto 8, de la Directiva (UE) 2022/2555;

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

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

6 bis) «ciberamenaza significativa»: una ciberamenaza significativa según se define en el artículo 6, punto 11, de la Directiva (UE) 2022/2555;

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

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

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

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

10 bis) «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;

11) «proveedores ***de servicios de seguridad gestionados*** de confianza»: los proveedores

---

[1] 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).

[2] ***Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo (DO L 333 de 27.12.2022, p. 164, ELI: http://data.europa.eu/eli/dir/2022/2557/oj).***

de servicios de seguridad gestionados seleccionados ***para formar parte de la Reserva de Ciberseguridad de la UE*** de conformidad con el artículo 16 del presente Reglamento.

Capítulo II

EL CIBERESCUDO EUROPEO

Artículo 3

Creación del Ciberescudo Europeo

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

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

2. El Ciberescudo Europeo:

a) reunirá y pondrá en común datos sobre ciberamenazas y ciberincidentes procedentes de diversas fuentes a través de los COS transfronterizos ***y, en su caso, a través del intercambio de información con la red de CSIRT***;

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

c) contribuirá a mejorar la protección frente a las ciberamenazas y la respuesta a ellas***, en particular proporcionando recomendaciones concretas a las entidades***;

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

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

Se desarrollará en cooperación con la infraestructura paneuropea de informática de alto

rendimiento creada en virtud del Reglamento (UE) 2021/1173.

Artículo 4

Centros de operaciones de seguridad nacionales

1. A fin de ***poder*** participar en el Ciberescudo Europeo, cada Estado miembro designará, al menos, a un COS nacional. El COS nacional será ***una capacidad centralizada en*** un organismo público. ***Cuando sea posible, los COS nacionales se incorporarán a los CSIRT o a otras infraestructuras y mecanismos de gobernanza de ciberseguridad existentes.***

Tendrá la capacidad de actuar como punto de referencia y pasarela a otras organizaciones públicas y privadas a nivel nacional, ***en particular sus COS nacionales,*** para recopilar y analizar información sobre amenazas e incidentes de ciberseguridad***, y, en su caso, compartir dicha información con los miembros de la red de los CSIRT de dicho Estado miembro,*** y contribuir a un COS transfronterizo. Estará equipado con tecnologías de vanguardia capaces de ***prevenir,*** detectar, agregar y analizar datos pertinentes para las amenazas e incidentes de ciberseguridad.

Cualquier COS nacional o CSIRT podrá solicitar datos de telemetría, sensores o registros de sus entidades críticas nacionales a proveedores de servicios de seguridad gestionados que presten un servicio a la entidad crítica. Dichos datos se compartirán de conformidad con la legislación de la Unión en materia de protección de datos y con el único fin de apoyar al COS nacional o al CSIRT en la detección y prevención de amenazas e incidentes de ciberseguridad.

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

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

Artículo 5

Centros de operaciones de seguridad transfronterizos

1. En las acciones destinadas a crear un COS transfronterizo podrá participar un consorcio anfitrión, compuesto por al menos tres Estados miembros, representados por COS nacionales, que se comprometan a colaborar para coordinar sus actividades de ciberdetección y seguimiento de amenazas. ***Deberá designarse un COS transfronterizo para detectar y analizar las ciberamenazas, prevenir incidentes y apoyar la producción de inteligencia de alta calidad, en particular mediante el intercambio de datos procedentes de diversas fuentes, públicas o privadas, así como mediante el intercambio de herramientas de vanguardia, y el desarrollo conjunto de capacidades de ciberdetección, análisis, prevención y protección en un entorno de confianza y seguro.***

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

2 bis. No obstante lo dispuesto en el artículo 176 del Reglamento (UE, Euratom) 2018/1046, las entidades establecidas en terceros países que no sean partes en el ACP no participarán en la adquisición conjunta de herramientas e infraestructuras.

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

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

Artículo 6

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

1. Los miembros de un consorcio anfitrión intercambiarán entre sí la información pertinente dentro del COS transfronterizo, incluida información relativa a ciberamenazas, cuasiincidentes, vulnerabilidades, técnicas y procedimientos, indicadores de compromiso, tácticas de los adversarios, información específica del agente de riesgo, alertas de

ciberseguridad y recomendaciones relativas a la configuración de las herramientas de ciberseguridad para detectar ciberataques, siempre que dicho intercambio de información:

a) ***mejore el intercambio de inteligencia sobre ciberamenazas entre los COS nacionales y transfronterizos y los ISAC del sector de la industria con el fin de prevenir, detectar o atenuar incidentes;***

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

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

a) el compromiso de poner en común ▌ los datos significativos a que se refiere el apartado 1 y las condiciones en las que se intercambiará dicha información;

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

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

3. Para fomentar el intercambio de información entre los COS transfronterizos y ***con los ISAC del sector de la industria***, los COS transfronterizos deberán garantizar un alto nivel de interoperabilidad entre sí y, ***en la medida de lo posible, con los ISAC del sector de la industria.*** Para facilitar la interoperabilidad entre los COS transfronterizos ***y con los ISAC del sector de la industria, las normas y protocolos de intercambio de información pueden armonizarse con las normas internacionales y las mejores prácticas del sector de la industria. También se fomentará la adquisición conjunta de infraestructuras, servicios y herramientas cibernéticos. Asimismo*****,*** previa consulta al ECCC y ***a la ENISA, la Comisión estará facultada durante... [seis meses desde la entrada en vigor del presente Reglamento] a adoptar actos delegados de conformidad con el artículo 20 bis para completar este Reglamento especificando*** las condiciones de dicha interoperabilidad ***en estrecha coordinación con los COS transfronterizos y con arreglo a las normas internacionales y las mejores prácticas de la industria.***

4. Los COS transfronterizos celebrarán acuerdos de cooperación entre sí ***y con, cuando corresponda, los ISAC del sector de la industria,*** especificando los principios de intercambio e interoperabilidad de información entre las plataformas transfronterizas, ***teniendo en cuenta los mecanismos de intercambio de información pertinentes ya disponibles en la Directiva (UE) 2022/2555. Cuando proceda, los COS transfronterizos celebrarán acuerdos de cooperación con los ISAC del sector de la industria. En el contexto de un incidente de ciberseguridad a gran escala potencial o en curso, los mecanismos de intercambio de información cumplirán las disposiciones pertinentes de la Directiva (UE) 2022/2555.***

Artículo 7

Cooperación e intercambio de información con *la red de CSIRT*

1. Cuando los COS transfronterizos obtengan información relativa a un incidente de ciberseguridad a gran escala potencial o en curso ***con el fin de poner en común la conciencia situacional, el COS coordinador facilitará*** la información pertinente a ***su CSIRT o a su autoridad competente, que la comunicará a*** EU-CyCLONe, a la red de CSIRT y a la Comisión ***y a la ENISA, con arreglo a*** sus respectivas funciones ***y procedimientos*** de gestión de crisis de conformidad con la Directiva (EU) 2022/2555. ***El presente apartado no impondrá nuevas obligaciones a las entidades públicas o privadas de comunicar un incidente de ciberseguridad a gran escala potencial o en curso para el cumplimiento de las obligaciones establecidas en la Directiva (UE) 2022/2555.***

2. La Comisión ***estará facultada para adoptar actos delegados, con arreglo al artículo 20 bis tras consultar a la red CSIRT para complementar el presente Reglamento estableciendo*** las disposiciones de procedimiento para el intercambio de información previsto en el apartado 1 ***del presente artículo y en consonancia con la Directiva (UE) 2022/2555***.

Artículo 8

Seguridad

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

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

3. La Comisión podrá adoptar actos de ejecución que establezcan requisitos técnicos para que los Estados miembros cumplan las obligaciones que les imponen los apartados 1 y 2. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 21, apartado 2, del presente Reglamento. ***Cumplirán las Directivas (UE) 2022/2555 y (UE) 2022/2557.*** En ***sus actos de ejecución*** la Comisión, con el apoyo del Alto Representante, tendrá en cuenta las normas de seguridad pertinentes en materia de defensa, con el fin de facilitar la cooperación con los mandos militares.

Capítulo III

MECANISMO DE EMERGENCIA EN MATERIA DE CIBERSEGURIDAD

Artículo 9

Creación del Mecanismo de Emergencia en materia de Ciberseguridad

1. Se crea un Mecanismo de ***Emergencia en materia de Ciberseguridad*** para mejorar la resiliencia de la Unión ante las principales amenazas para la ciberseguridad, prepararla para

los efectos a corto plazo de los incidentes de ciberseguridad significativos y a gran escala, y mitigar dichos efectos, en un espíritu de solidaridad (el «Mecanismo»).

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

Artículo 10

Tipos de acciones

1. El Mecanismo apoyará los siguientes tipos de acciones:

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

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

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

1 bis. Tras activar el Mecanismo, la Comisión informará, evaluará y publicará un informe cada año sobre el funcionamiento, tanto positivo como negativo, del Mecanismo, en especial sobre la necesidad de nuevos requisitos de cooperación o formación.

Artículo 11

Pruebas coordinadas de preparación de las entidades

1. Con el fin de apoyar las pruebas coordinadas de preparación de las entidades a que se refiere el artículo 10, apartado 1, letra a), en toda la Unión, la Comisión, previa consulta al Grupo de Cooperación SRI y a la ENISA, determinará, a partir de los sectores de alta criticidad enumerados en el anexo I de la Directiva (UE) 2022/2555, los sectores o subsectores afectados cuyas entidades podrán ser objeto de las pruebas coordinadas de preparación, teniendo en cuenta las evaluaciones de riesgos y las pruebas de resiliencia coordinadas existentes y previstas, ***con arreglo a las disposiciones establecidas para las entidades de los sectores de alta criticidad enumerados en el anexo I de la Directiva (UE) 2022/2555.***

2. El Grupo de Cooperación SRI, en colaboración con la Comisión, la ENISA, el Alto Representante ***y las entidades que pueden ser objeto de pruebas de preparación de conformidad con el apartado 1***, elaborará escenarios de riesgo y metodologías comunes para los ***ejercicios coordinados de preparación***, ***que culminarán en un plan de trabajo***

concertado**. **Las entidades sujetas a pruebas coordinadas de preparación elaborarán y aplicarán un plan de rehabilitación que lleve a cabo las recomendaciones resultantes de las pruebas de preparación.

El Grupo de cooperación SRI podrá informar sobre la priorización de sectores o subsectores para los ejercicios coordinados de preparación de pruebas.

Artículo 12

Creación de la Reserva de Ciberseguridad de la UE

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

Cuando resulte evidente que los servicios contratados no pueden utilizarse plenamente para prestar apoyo para responder a incidentes significativos o a gran escala, esos servicios podrán, excepcionalmente, convertirse en ejercicios o cursos de formación para hacer frente a incidentes, y ser prestados a los usuarios, previa solicitud, por el poder adjudicador.

2. La Reserva de Ciberseguridad de la UE consistirá en servicios de respuesta a incidentes prestados por proveedores ***de servicios de seguridad gestionados*** de confianza seleccionados de conformidad con los criterios establecidos en el artículo 16. La ***Reserva de Ciberseguridad de la UE*** incluirá servicios comprometidos previamente. ***Los servicios deberán poder desplegarse en todos los Estados miembros y reforzarán la soberanía tecnológica de la Unión, su autonomía estratégica abierta, su competitividad y resiliencia en el sector de la ciberseguridad, en particular impulsando la innovación en el mercado único digital en toda la Unión***.

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

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

b) las instituciones, órganos y organismos de la Unión ***según la definición del artículo 3, punto 1, del Reglamento (UE) .../2023 del Parlamento Europeo y del Consejo[1] y al CERT-UE***.

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

5. La Comisión tendrá la responsabilidad general de la ejecución de la Reserva de

---

1 ***Reglamento (UE) .../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 C , , p., , ELI: ...).***

Ciberseguridad de la UE. La Comisión, ***junto con el Grupo de Coordinación SRI 2***, determinará las prioridades y la evolución de la Reserva de Ciberseguridad de la UE, en consonancia con los requisitos de los usuarios a que se refiere el apartado 3, supervisará su aplicación y garantizará la complementariedad, la coherencia, las sinergias y los vínculos con otras acciones de apoyo en virtud del presente Reglamento, así como con otras acciones y programas de la Unión.

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

7. Con el fin de apoyar a la Comisión en la creación de la Reserva de Ciberseguridad de la UE, la ENISA elaborará una cartografía de los servicios necesarios, ***incluidas las capacidades y aptitudes que requiere el personal de ciberseguridad***, previa consulta a los Estados miembros y a la Comisión, ***y cuando proceda, a los servicios de seguridad gestionados y otros representantes de la industria de la ciberseguridad***. La ENISA elaborará una cartografía similar, previa consulta a la Comisión ***y en colaboración con los servicios de seguridad gestionados, y cuando proceda, otros representantes de la industria de la ciberseguridad***, para determinar las necesidades de los terceros países que puedan optar al apoyo de la Reserva de Ciberseguridad de la UE de conformidad con el artículo 17. La Comisión, cuando proceda, consultará al Alto Representante ***e informará al Consejo sobre las necesidades de terceros países***.

8. La Comisión ***estará facultada para adoptar actos delegados, con arreglo al artículo 20 bis, para complementar el presente Reglamento especificando*** los tipos y el número de servicios de respuesta necesarios para la Reserva de Ciberseguridad de la UE. ▌..

Artículo 13

Solicitudes de apoyo de la Reserva de Ciberseguridad de la UE

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

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

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

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

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

a) información adecuada sobre la entidad afectada y las posibles repercusiones del

incidente y sobre el uso previsto del apoyo solicitado, incluida una indicación de las necesidades estimadas;

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

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

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

7. La Comisión ***está facultada para adoptar actos delegados, con arreglo al artículo 20 bis, para complementar el presente Reglamento especificando*** las disposiciones detalladas para la asignación de los servicios de apoyo de la Reserva de Ciberseguridad de la UE. ▌

Artículo 14

Ejecución del apoyo de la Reserva de Ciberseguridad de la UE

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

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

a) la gravedad del incidente de ciberseguridad;

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

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

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

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

3. Los servicios de la Reserva de Ciberseguridad de la UE se prestarán de conformidad con acuerdos específicos entre el proveedor de servicios y el usuario al que se preste el apoyo en el marco de la Reserva de Ciberseguridad de la UE. Dichos acuerdos incluirán condiciones de responsabilidad ***y cualesquiera otras disposiciones que las partes del acuerdo consideren necesarias para la prestación del servicio correspondiente***.

4. Los acuerdos a que se refiere el apartado 3 se basarán en plantillas preparadas por la

ENISA, previa consulta a los Estados miembros ***y, cuando proceda, a otros usuarios de la Reserva de Ciberseguridad de la UE.***

5. La Comisión y la ENISA no asumirán responsabilidad contractual alguna por los daños causados a terceros por los servicios prestados en el marco de la ejecución de la Reserva de Ciberseguridad de la UE, ***salvo en casos de negligencia grave en la evaluación de la solicitud del proveedor de servicios, o en los casos en que la Comisión o la ENISA sean usuarios de la Reserva de Ciberseguridad de la UE, de conformidad con el artículo 14, apartado 3.***

6. En el plazo de un mes a partir del fin de la acción de apoyo, los usuarios facilitarán a la Comisión, la ENISA, ***la red de CSIRT y, cuando sea pertinente, a la EU-CyCLONe*** un informe resumido sobre el servicio prestado, los resultados obtenidos y las conclusiones extraídas. Cuando el usuario proceda de un tercer país, tal como se establece en el artículo 17, dicho informe se dará a conocer al Alto Representante.
El informe respetará la legislación nacional y de la Unión relativa a la protección de la información sensible o clasificada.

7. La Comisión informará de forma ***periódica y al menos dos veces al año*** al Grupo de cooperación SRI sobre el uso y los resultados del apoyo. ***Protegerá la información confidencial, de conformidad con la legislación nacional o de la Unión relativa a la protección de la información sensible o clasificada.***

Artículo 15

Coordinación con los mecanismos de gestión de crisis

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

2. En caso de incidente transfronterizo de ciberseguridad a gran escala en el que se active el Dispositivo de Respuesta Política Integrada a las Crisis (Dispositivo RPIC), el apoyo en virtud del presente Reglamento para responder a dicho incidente se gestionará de conformidad con los protocolos y procedimientos pertinentes en el marco del Dispositivo RPIC.

3. En consulta con el Alto Representante, el apoyo prestado en el marco del ***Mecanismo de 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. También podrá complementar o contribuir a la asistencia prestada por un Estado miembro a otro en el contexto del artículo 42, apartado 7, del ***TUE***.

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

[1] 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).

Artículo 16

Proveedores de confianza

1. En los procedimientos de contratación pública destinados a crear la Reserva de Ciberseguridad de la UE, el órgano de contratación actuará de conformidad con los principios establecidos en el Reglamento (UE, Euratom) 2018/1046 y con los siguientes principios:

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

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

c) garantizar que la Reserva de Ciberseguridad de la UE aporte valor añadido de la UE, al contribuir a los objetivos establecidos en el artículo 3 del Reglamento (UE) 2021/694, en particular promoviendo el desarrollo de capacidades de ciberseguridad en la UE, ***y el cumplimiento del equilibrio de género en el sector, y reforzando la soberanía tecnológica, la autonomía estratégica abierta, la competitividad y la resiliencia de 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 de selección:

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

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

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

d) el proveedor dispondrá de la habilitación de seguridad adecuada, al menos para el personal destinado a participar en el despliegue de servicios;

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

f) el proveedor estará equipado con el equipo técnico de hardware y software actualizado necesario para prestar el servicio solicitado ***y cumplirá con el Reglamento (UE) .../... aplicable; del Parlamento Europeo y del Consejo[1] (2022/0272(COD))*****;**

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

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

operan en sectores críticos o muy críticos;

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

i) el proveedor deberá poder prestar el servicio en el idioma local del Estado o Estados miembros, ***o en una de las lenguas de trabajo de las instituciones de la Unión***, en los que pueda prestar el servicio;

j) una vez que se haya establecido un esquema de certificación ***europeo*** para los servicios de seguridad gestionados, ***de conformidad con el*** Reglamento (UE) 2019/881, el proveedor será certificado de conformidad con dicho esquema ***dentro de un plazo de dos años tras la adopción de este***.

j bis) el proveedor podrá prestar el servicio de forma independiente y no como parte de un paquete, salvaguardando así la posibilidad del usuario de cambiar a otro proveedor de servicios;

j ter) a efectos del artículo 12, apartado 1, el proveedor incluirá en la propuesta de licitación la posibilidad de convertir los servicios de respuesta a incidentes no utilizados en ejercicios o formaciones;

j quater) el proveedor estará establecido y tendrá sus estructuras de gestión ejecutiva en la Unión, en un país asociado o en un tercer país que forme parte del Acuerdo sobre Contratación Pública en el contexto de la Organización Mundial del Comercio (ACP).

j quinquies) El proveedor no estará sujeto al control de un tercer país no asociado ni al de una entidad de un tercer país no asociado que no sea parte en el ACP o, alternativamente, esa entidad deberá haber sido objeto de control en el sentido del Reglamento (UE) 2019/452 y, cuando sea necesario, a medidas de atenuación, teniendo en cuenta los objetivos del presente Reglamento.

Artículo 17

Apoyo a terceros países

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

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

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

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

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

6. La Comisión notificará ***sin demora indebida al Consejo*** y coordinará con el Alto Representante las solicitudes recibidas y la ejecución del apoyo de la Reserva de Ciberseguridad de la UE concedido a terceros países.

Capítulo IV

MECANISMO DE REVISIÓN DE INCIDENTES DE CIBERSEGURIDAD

Artículo 18

Mecanismo de Revisión de Incidentes de Ciberseguridad

1. A petición de la Comisión, de EU-CyCLONe o de la red de CSIRT, la ENISA revisará y evaluará las amenazas, vulnerabilidades y medidas de mitigación con respecto a un incidente específico de ciberseguridad significativo o a gran escala. Una vez finalizada la revisión y evaluación de un incidente, la ENISA presentará un informe de revisión del incidente a la red de CSIRT, a EU-CyCLONe y a la Comisión para ayudarlos en el desempeño de sus cometidos, en particular a la luz de los establecidos en los artículos 15 y 16 de la Directiva (UE) 2022/2555. Cuando proceda, la Comisión dará a conocer el informe al Alto Representante.

2. Para preparar el informe de revisión del incidente a que se refiere el apartado 1, la ENISA ***colaborará y recabará información de*** todas las partes interesadas pertinentes, incluidos los representantes de los Estados miembros, la Comisión, otras instituciones, órganos, organismos y agencias pertinentes de la UE, los proveedores de servicios de seguridad gestionados en los COS ***nacionales y transfronterizos*** y los usuarios de servicios de ciberseguridad, ***con el complemento de unas garantías y una supervisión adecuadas para garantizar que las lecciones aprendidas y las mejores prácticas identificadas reciban el respaldo de los agentes de la industria y el sector de servicios***. Cuando proceda, la ENISA también colaborará con las entidades afectadas por incidentes de ciberseguridad significativos o a gran escala. Para apoyar la revisión, la ENISA también podrá consultar a otros tipos de partes interesadas. Los representantes consultados revelarán cualquier posible conflicto de intereses.

3. El informe incluirá una revisión y un análisis del incidente específico de ciberseguridad significativo o a gran escala, incluidas las principales causas, vulnerabilidades y conclusiones extraídas. Protegerá la información confidencial, de conformidad con la legislación nacional o de la Unión relativa a la protección de la información sensible o clasificada. ***No incluirá ningún dato sobre las vulnerabilidades explotadas activamente que permanezcan sin subsanar.***

3 bis. El informe mencionado en el apartado 1 de este artículo incluirá las enseñanzas

extraídas de las revisiones inter pares realizadas de conformidad con el artículo 19 de la Directiva (UE) 2022/2555.

4. Cuando proceda, el informe formulará recomendaciones***, también para todas las partes interesadas pertinentes***, para mejorar la posición de la Unión en materia de ciberseguridad.

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

Capítulo V

DISPOSICIONES FINALES

Artículo 19

Modificaciones del Reglamento (UE) 2021/694

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

1) el artículo 6 se modifica como sigue:

a) el apartado 1 se modifica como sigue:

i) se añade la letra a bis) siguiente:

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

ii) se añade la letra g) siguiente:

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

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*, con excepción de las acciones de ejecución de la Reserva de Ciberseguridad de la UE, que serán ejecutadas por la Comisión y la 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), ***ELI: http://data.europa.eu/eli/reg/2021/887/oj).»*;**

2) El artículo 9 se modifica como sigue:

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

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

c) ***1 620 566 000*** EUR para el objetivo específico 3 – Ciberseguridad y confianza;

d) ***500 347 000*** EUR para el objetivo específico 4 – Capacidades digitales avanzadas;»;

a bis) se añade el apartado 2 bis siguiente:

«2 bis. El importe a que se refiere el apartado 2, letra c), se utilizará principalmente para alcanzar los objetivos operativos mencionados en el artículo 6, apartado 1, letras a) a f), del Programa.»;

a ter) se añade el apartado 2 ter siguiente:

«2 ter. El importe para el establecimiento y ejecución de la Reserva de Ciberseguridad de la UE no excederá los 27 millones EUR durante el plazo de vigencia previsto del Reglamento 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.»;

b) se añade el apartado 8 siguiente:

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

La Comisión informará al Parlamento y al Consejo de los créditos prorrogados de conformidad con el artículo 12, apartado 6, del Reglamento (UE, Euratom) 2018/1046.

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

«2. El Programa podrá proporcionar financiación en cualquiera de las formas establecidas en el Reglamento ***(UE, Euratom) 2018/1046***, en particular mediante contratos públicos principalmente, así como subvenciones y premios.

Cuando el logro del objetivo de una acción requiera la contratación de bienes y servicios innovadores, podrán concederse subvenciones solo a los beneficiarios que

sean poderes adjudicadores o entidades adjudicadoras como se definen en las Directivas 2014/24/UE[27] y 2014/25/UE[28] del Parlamento Europeo y del Consejo.

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

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

Al ejecutar los procedimientos de contratación pública para la Reserva de Ciberseguridad de la UE establecida por el artículo 12 del Reglamento (UE) 2023***/…***, la Comisión y la ENISA podrán actuar como central de compras para la contratación en nombre o por cuenta de terceros países asociados al Programa, de conformidad con el artículo 10. La Comisión y la ENISA también podrán actuar como mayoristas, comprando, almacenando, revendiendo o donando suministros y servicios, incluidos los alquileres, a esos terceros países. Como excepción a lo dispuesto en el artículo 169, apartado 3 del Reglamento (UE). ***…/…***, la solicitud de un único tercer país es suficiente para otorgar un mandato a la Comisión o a la ENISA para que actúen.

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

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

4) se añade el artículo 16 bis siguiente:

«Artículo 16 bis

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

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

«Las subvenciones en el marco del Programa se concederán y gestionarán de conformidad con el título VIII del ***Reglamento (UE, Euratom) 2018/1046*** y podrán cubrir hasta el 100 % de los costes admisibles, sin perjuicio del principio de cofinanciación establecido en el artículo 190 del ***Reglamento (UE, Euratom) 2018/1046***. Tales subvenciones se concederán y gestionarán conforme a lo especificado para cada objetivo específico.

El apoyo en forma de subvenciones podrá ser concedido directamente por el ECCC sin convocatoria de propuestas a los COS nacionales a que se refiere el artículo 4 del Reglamento ***(UE) .../...*** y al consorcio anfitrión a que se refiere el artículo 5 del Reglamento ***(UE) .../...***, de conformidad con el artículo 195, apartado 1, letra d), del ***Reglamento (UE, Euratom) 2018/1046***.

El apoyo en forma de subvenciones para el ***Mecanismo de Emergencia en materia de Ciberseguridad***, tal como se establece en el artículo 10 del Reglamento (UE) ***.../...***, 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 (UE, Euratom) 2018/1046***.

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

Para el apoyo a la asistencia mutua en respuesta a un incidente de ciberseguridad significativo o a gran escala, tal como se define en el artículo 10, letra c), del Reglamento ***(UE) .../...***, y de conformidad con el artículo 193, apartado 2, párrafo segundo, letra a), del ***Reglamento (UE, Euratom) 2018/1046***, en casos debidamente justificados, los costes podrán considerarse subvencionables aunque se haya incurrido en ellos antes de la presentación de la solicitud de subvención.»;

6) Los anexos I y II del Reglamento (UE) 2021/694 quedan modificados de conformidad con el anexo del presente Reglamento.

Artículo 19 bis
Recursos adicionales para ENISA

La ENISA recibirá recursos adicionales para llevar a cabo las tareas adicionales que el presente Reglamento le confiere. Este apoyo adicional, incluida la financiación, no pondrá en peligro la consecución de los objetivos de otros programas de la Unión, en particular el programa Europa Digital.

Artículo 20

Evaluación *y revisión*

1. A más tardar [***dos*** años ***desde*** la fecha de aplicación del presente Reglamento] ***y cada dos años a partir de entonces***, la Comisión ***llevará a cabo*** una evaluación ***del funcionamiento de las medidas establecidas en el*** presente Reglamento y presentará al Parlamento Europeo y al Consejo un informe.

2. En la evaluación se analizarán, en concreto:

a) el uso y el valor añadido de los COS transfronterizos y la medida en que contribuyen a acelerar la detección y la respuesta a las ciberamenazas y el conocimiento de la situación; la participación activa de los COS nacionales en el Ciberescudo Europeo, incluido el número de COS nacionales y transfronterizos establecidos y la medida en que han contribuido a la producción e intercambio de información viable de alta calidad y de inteligencia sobre ciberamenazas; el número y el coste de las infraestructuras o herramientas de ciberseguridad contratadas conjuntamente; el número de acuerdos de cooperación celebrados entre los COS transfronterizos y los ISAC del sector de la industria; el número de incidentes notificados a la red de CSIRT y su impacto en el trabajo de la red;

b) el trabajo positivo y negativo del Mecanismo de Emergencia en materia de Ciberseguridad, en particular si se necesitan más cooperación o requisitos de formación;

c) la contribución del presente Reglamento a reforzar la resiliencia y la autonomía estratégica abierta de la Unión, a mejorar la competitividad de los sectores industriales pertinentes, las microempresas, las pymes, en particular las empresas emergentes, y el desarrollo de capacidades en materia de ciberseguridad en la UE;

d) el uso y el valor añadido de la Reserva de Ciberseguridad de la UE, incluido el número de proveedores de seguridad de confianza que forman parte de la Reserva de Ciberseguridad de la UE; el número, el tipo, los costes y el impacto de las acciones llevadas a cabo en apoyo de la respuesta a incidentes de ciberseguridad, así como de sus usuarios y proveedores; el tiempo medio para que la Comisión reconozca, la Reserva de Ciberseguridad de la UE que debe desplegarse y responder, y el usuario para recuperarse de incidentes; si el ámbito de aplicación de la Reserva de Ciberseguridad de la UE debe ampliarse a los servicios de preparación ante incidentes o a ejercicios comunes con los proveedores de servicios de seguridad gestionados de confianza y los usuarios potenciales de la Reserva de Ciberseguridad para garantizar el funcionamiento eficiente de esta cuando sea necesario;

e) la contribución del presente Reglamento al desarrollo y mejora de las capacidades y competencias de la mano de obra en el sector de la ciberseguridad necesarias para

reforzar la capacidad de la Unión de detectar y prevenir amenazas e incidentes de ciberseguridad, reaccionar a ellos y recuperarse;

f) la contribución del presente Reglamento al despliegue y desarrollo de tecnologías punteras en la Unión.

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 20 bis (nuevo)

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 6, apartado 3; el artículo 7, apartado 2; el artículo 12, apartado 8; y el artículo 13, apartado 7, se otorgan a la Comisión por un período de … años a partir de ... [fecha de entrada en vigor del acto legislativo de base o cualquier otra fecha fijada por los colegisladores]. La Comisión elaborará un informe sobre la delegación de competencias a más tardar nueve meses antes de que finalice el período de … 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 6, apartado 3, el artículo 7, apartado 2, el artículo 12, apartado 8, y el artículo 13, apartado 7, podrá ser revocada en cualquier momento por el Parlamento Europeo o por el Consejo. La decisión de revocación pondrá término a la delegación de los poderes que en ella se especifiquen. La decisión surtirá efecto el día siguiente al de su publicación en el Diario Oficial de la Unión Europea o en una fecha posterior indicada en ella. No afectará a la validez de los actos delegados que ya estén en vigor.

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

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

6. Los actos delegados adoptados en virtud del artículo 6, apartado 3, el artículo 7, apartado 2, el artículo 12, apartado 8, y el artículo 13, 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 21

Procedimiento de comité

1. La Comisión estará asistida por el Comité de Coordinación del programa Europa Digital establecido por el Reglamento (UE) 2021/694. Dicho comité será un comité en el sentido del Reglamento (UE) n.º 182/2011.
2. En los casos en que se haga referencia al presente apartado, se aplicará el artículo 5 del Reglamento (UE) n.º 182/2011.

Artículo 22

Entrada en vigor

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

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

Hecho en Estrasburgo, el

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

ANEXO

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

(1) en el anexo I, la sección/capítulo «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 amenazas cibernéticas, 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 COS nacionales y transfronterizos que forman el Ciberescudo Europeo***, 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 un amplio despliegue de soluciones punteras eficaces en materia de ciberseguridad y confianza en los Estados miembros. Dicho despliegue 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 ***prestando especial atención a lograr el equilibrio de género***, por ejemplo alineando los programas de capacidades en materia de ciberseguridad, adaptándolos a las necesidades sectoriales específicas, ***incluido un enfoque interdisciplinario y general***, y facilitando el acceso a una formación especializada específica ***para capacitar a todas las personas y territorios, sin perjuicio de la posibilidad de beneficiarse de las oportunidades que ofrece el presente Reglamento***.

5. La promoción de la solidaridad entre los Estados miembros por lo que respecta a la preparación frente a incidentes significativos de ciberseguridad y la respuesta a ellos mediante el despliegue 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 ***servicios de seguridad gestionados*** de confianza a escala de la Unión.»;

(2) en el anexo II, la sección/capítulo «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 contratadas conjuntamente como parte del ***escudo europeo de la ciberseguridad.***

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

3.3. Número, tipo, costes e impacto de las acciones de apoyo a la preparación y la respuesta ante incidentes de ciberseguridad en el marco del Mecanismo de Emergencia ***en materia de Ciberseguridad***. ***La medida en que el usuario ha aplicado y llevado a cabo las recomendaciones de las pruebas de preparación, así como el tiempo medio para que la Comisión reconozca, la Reserva de Ciberseguridad de la UE para responder y el usuario para recuperarse de incidentes.».***