Parlamento Europeo
2019-2024

Comisión de Asuntos Exteriores

2023/0109(COD)

27.10.2023

OPINIÓN

de la Comisión de Asuntos Exteriores

para la Comisión de Industria, Investigación y Energía

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

Ponente de opinión: Dragoş Tudorache

PA_Legapp

Enmienda 1

Propuesta de Reglamento
Considerando 1

Texto de la Comisión	*Enmienda*
(1) La utilización y dependencia de las tecnologías de la información y la comunicación constituyen un elemento esencial en todos los sectores de actividad económica, ya que tanto nuestras administraciones públicas como nuestras empresas y ciudadanos están más interconectados y son más interdependientes que nunca, en todos los sectores y por encima de todas las fronteras.	(1) La utilización y dependencia de las tecnologías de la información y la comunicación constituyen un elemento esencial en todos los sectores de actividad económica***, y también militar,*** ya que tanto nuestras administraciones públicas como nuestras empresas y ciudadanos***, así como los entes militares y de defensa,*** están más interconectados y son más interdependientes que nunca, en todos los sectores y por encima de todas las fronteras.

Enmienda 2

Propuesta de Reglamento
Considerando 2

Texto de la Comisión	*Enmienda*
(2) La magnitud, la frecuencia y los efectos de los incidentes de ciberseguridad están aumentando, incluidos los ataques a la cadena de suministro con fines de ciberespionaje, secuestro de archivos o perturbación. Representan una grave amenaza para el funcionamiento de las redes y los sistemas de información. En vista de la rápida evolución del panorama de amenazas, la amenaza de un posible incidente a gran escala que provoque perturbaciones y daños significativos en las infraestructuras críticas exige una mayor preparación a todos los niveles del marco de ciberseguridad de la UE. ***Esa amenaza va*** más allá de la agresión militar de Rusia a Ucrania y probablemente persistirá, dada la multiplicidad de agentes estatales, criminales y hacktivistas implicados en las tensiones geopolíticas actuales. Tales incidentes pueden obstaculizar la	(2) La magnitud, la frecuencia y los efectos de los incidentes de ciberseguridad están aumentando, incluidos los ataques a la cadena de suministro con fines de ciberespionaje, secuestro de archivos o perturbación. Representan una grave amenaza para el funcionamiento de las redes y los sistemas de información. En vista de la rápida evolución del panorama de amenazas, la amenaza de un posible incidente a gran escala que provoque perturbaciones y daños significativos en las infraestructuras críticas exige una mayor preparación a todos los niveles del marco de ciberseguridad de la UE. ***La gravedad de estas amenazas cobró aún más importancia debido al regreso de la guerra a nuestro continente. Esas amenazas van*** más allá de la agresión militar de Rusia a Ucrania y probablemente ***persistirán***, dada la multiplicidad de

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.	agentes estatales, criminales y hacktivistas implicados en las tensiones geopolíticas actuales. Tales incidentes pueden obstaculizar la prestación de servicios públicos y el desarrollo de actividades económicas, incluso en sectores críticos o muy críticos, generar pérdidas económicas sustanciales, socavar la confianza de los usuarios, causar graves daños a la economía ***y la seguridad*** de la Unión e incluso suponer una amenaza para la salud o la vida***, comprometiendo eventualmente las instalaciones relacionadas con la seguridad local o nacional***. 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. ***La ciberseguridad es importante para proteger nuestros valores europeos y garantizar el funcionamiento de nuestras democracias a través de la protección de nuestra infraestructura electoral y nuestros procedimientos democráticos ante cualquier injerencia extranjera.***

Enmienda 3

Propuesta de Reglamento
Considerando 2 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(2 bis) La ciberseguridad es fundamental para mantener a salvo nuestra Unión y evitar que agentes malintencionados, estatales y no estatales, socaven nuestra democracia, economía y seguridad. Es necesario evitar un panorama fragmentado, ya que tal situación no supondría un enfoque adecuado, en particular ante el reto de futuros ciberataques a gran escala dirigidos a varios Estados miembros al mismo tiempo o a infraestructuras críticas

	transnacionales. Por consiguiente, hace falta un organismo de la Unión que actúe como plataforma de coordinación para todos los instrumentos, fondos y mecanismos de ciberseguridad existentes y futuros.

Enmienda 4

Propuesta de Reglamento
Considerando 3

Texto de la Comisión	*Enmienda*
(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 [16], es necesario aumentar la resiliencia de los ciudadanos, las empresas y las entidades que gestionan infraestructuras críticas frente a las crecientes amenazas a la ciberseguridad, que pueden tener repercusiones sociales y económicas devastadoras. Por lo tanto, es necesaria la inversión en infraestructuras y servicios que apoyen una detección de las amenazas e incidentes de ciberseguridad y una respuesta a ellos más rápidas, y los Estados miembros precisan de asistencia para prepararse mejor y responder a los incidentes de ciberseguridad significativos y a gran escala. La Unión también debe aumentar sus capacidades en estos ámbitos, en particular en lo que se refiere a la recopilación y el análisis de datos sobre amenazas e incidentes de ciberseguridad.	(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 [16], es necesario aumentar la resiliencia de los ciudadanos, las empresas y las entidades que gestionan infraestructuras críticas frente a las crecientes amenazas a la ciberseguridad, que pueden tener repercusiones sociales y económicas devastadoras. Por lo tanto, es necesaria la inversión en infraestructuras y servicios que apoyen una detección de las amenazas e incidentes de ciberseguridad y una respuesta a ellos más rápidas, y los Estados miembros precisan de asistencia para prepararse mejor y responder a los incidentes de ciberseguridad significativos y a gran escala. La Unión también debe aumentar sus capacidades en estos ámbitos, en particular en lo que se refiere a la recopilación y el análisis de datos sobre amenazas e incidentes de ciberseguridad***, así como su capacidad de actuar de forma proactiva y de reaccionar con decisión en estos casos***.
[16] https://futureu.europa.eu/es/	[16] https://futureu.europa.eu/es/

Enmienda 5

Propuesta de Reglamento
Considerando 4

Texto de la Comisión	*Enmienda*
(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[17], la Recomendación (UE) 2017/1584[18] de la Comisión, la Directiva 2013/40/UE del Parlamento Europeo y del Consejo[19] y el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo[20]. Además, la Recomendación del Consejo sobre un enfoque coordinado a escala de la Unión para reforzar la resiliencia de las infraestructuras críticas invita a los Estados miembros a tomar medidas urgentes y eficaces y a cooperar de manera leal, eficiente, solidaria y coordinada entre sí, con la Comisión y otras autoridades públicas pertinentes, así como con las entidades afectadas, a fin de aumentar la resiliencia de las infraestructuras críticas utilizadas para prestar servicios esenciales en el mercado interior.	(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[17], la Recomendación (UE) 2017/1584[18] de la Comisión, la Directiva 2013/40/UE del Parlamento Europeo y del Consejo[19] y el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo[20]. Además, la Recomendación del Consejo sobre un enfoque coordinado a escala de la Unión para reforzar la resiliencia de las infraestructuras críticas invita a los Estados miembros a tomar medidas urgentes y eficaces y a cooperar de manera leal, eficiente ***y proactiva***, 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. ***Asimismo, la Unión aprobó y puso en marcha en marzo de 2022 su Brújula Estratégica para la Seguridad y la Defensa, que se centra, entre otros puntos, en reforzar la ciberseguridad y mejorar la cooperación internacional con aliados afines y socios democráticos, especialmente a este respecto. Además, la ciberseguridad ha sido un elemento central de la reciente tercera declaración conjunta sobre cooperación UE-OTAN, de enero de 2023. En particular, en el informe de evaluación final del grupo de trabajo UE-OTAN se recomendaba aprovechar al máximo las sinergias entre***

la UE y la OTAN[1], incluido el intercambio de buenas prácticas entre los actores civiles y militares sobre la aplicación de las políticas y la legislación pertinentes relacionadas con el entorno cibernético.

[1] https://commission.europa.eu/document/34209534-3c59-4b01-b4f0-b2c6ee2df736_es

---

[17] 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).

[18] 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).

[19] 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).

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

---

[17] 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).

[18] 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).

[19] 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).

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

Enmienda 6

Propuesta de Reglamento
Considerando 6

Texto de la Comisión	*Enmienda*
(6) La Comunicación conjunta sobre la política de ciberdefensa de la UE [22], adoptada el 10 de noviembre de 2022, anunció una Iniciativa de Cibersolidaridad de la UE con los siguientes objetivos: refuerzo de las capacidades comunes de detección, conciencia situacional y respuesta de la UE mediante la promoción del despliegue de una infraestructura de la UE de centros de operaciones de seguridad («COS»), el apoyo a la creación gradual de una reserva de ciberseguridad a escala de la UE con servicios de proveedores privados de confianza y la realización de pruebas de entidades críticas para detectar posibles vulnerabilidades basadas en evaluaciones de riesgos de la UE.	(6) La Comunicación conjunta sobre la política de ciberdefensa de la UE [22], adoptada el 10 de noviembre de 2022, anunció una Iniciativa de Cibersolidaridad de la UE con los siguientes objetivos: refuerzo de las capacidades comunes de detección, conciencia situacional y respuesta de la UE mediante la promoción del despliegue de una infraestructura de la UE de centros de operaciones de seguridad («COS»), el apoyo a la creación gradual de una reserva de ciberseguridad a escala de la UE con servicios de proveedores privados de confianza y la realización de pruebas de entidades críticas para detectar posibles vulnerabilidades basadas en evaluaciones de riesgos de la UE. ***Además, la rápida evolución del panorama de las ciberamenazas y el ritmo vertiginoso del desarrollo tecnológico también demuestran la necesidad de reforzar la coordinación y la cooperación entre los ámbitos civil y militar, tal y como subrayó el Consejo en sus Conclusiones sobre la política de ciberdefensa de la UE[1].*** ***[1] Conclusiones del Consejo sobre la política de ciberdefensa de la UE aprobadas por el Consejo en su reunión del 22 de mayo de 2023 (9618/23)***
[22] Comunicación conjunta al Parlamento Europeo y al Consejo, Política de ciberdefensa de la UE, JOIN(2022) 49 final.	[22] Comunicación conjunta al Parlamento Europeo y al Consejo, Política de ciberdefensa de la UE, JOIN(2022) 49 final.

Enmienda 7

Propuesta de Reglamento
Considerando 6 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(6 bis) Habida cuenta de lo difuso de las líneas que separan los ámbitos de los asuntos civiles y militares y del uso dual que caracteriza a las herramientas y las tecnologías informáticas, es necesario adoptar un enfoque exhaustivo y global respecto al ámbito digital. En caso de incidente y crisis de ciberseguridad a gran escala que afecte a más de un Estado miembro, deben establecerse una gestión y una gobernanza de crisis adecuadas. Esas estructuras deben organizar el intercambio de información, la coordinación y la cooperación con las estructuras de la Unión dedicadas a la gestión de las crisis militares y de seguridad exterior, así como con los organismos de los Estados miembros encargados de la seguridad y la defensa (la comunidad de ciberdefensa). Lo mismo debe ser aplicable también a las operaciones y las misiones de la política común de seguridad y defensa que lleva a cabo la Unión para garantizar la paz y la estabilidad en los países de su vecindad y en otras regiones.

Enmienda 8

Propuesta de Reglamento
Considerando 7

Texto de la Comisión	*Enmienda*
(7) Es necesario reforzar la capacidad de detección y conciencia situacional de las ciberamenazas y ciberincidentes en toda la Unión y afianzar la solidaridad mejorando la preparación y las capacidades de los Estados miembros y de la Unión para responder a incidentes de ciberseguridad significativos y a gran escala. Procede, por lo tanto, desplegar una infraestructura paneuropea de COS (el Ciberescudo Europeo) para desarrollar y mejorar las	(7) Es necesario reforzar la capacidad de detección y conciencia situacional de las ciberamenazas y ciberincidentes en toda la Unión y afianzar la solidaridad mejorando la preparación y las capacidades de los Estados miembros y de la Unión para responder a incidentes de ciberseguridad significativos y a gran escala. Procede, por lo tanto, desplegar una infraestructura paneuropea de COS (el Ciberescudo Europeo) para desarrollar y mejorar las

capacidades comunes de detección y conciencia situacional; debe crearse un Mecanismo de Ciberemergencia para ayudar a los Estados miembros a prepararse, responder a incidentes de ciberseguridad significativos y a gran escala y recuperarse inmediatamente de ellos; conviene establecer un Mecanismo de Revisión de Incidentes de Ciberseguridad para revisar y evaluar incidentes específicos significativos o a gran escala. Estas acciones deben entenderse sin perjuicio de lo dispuesto en los artículos 107 y 108 del Tratado de Funcionamiento de la Unión Europea (TFUE).

capacidades comunes de detección y conciencia situacional; debe crearse un Mecanismo de Ciberemergencia para ayudar a los Estados miembros a prepararse, responder a incidentes de ciberseguridad significativos y a gran escala y recuperarse inmediatamente de ellos***, incluidos los incidentes que afecten a más de un Estado miembro. Cuando sea viable y necesario, un mecanismo de emergencia en materia de ciberseguridad debe organizar el intercambio de información y la cooperación entre las autoridades de defensa de los Estados miembros, con el apoyo de las instituciones, órganos y organismos de la Unión (la comunidad de ciberdefensa de la UE);*** conviene establecer un Mecanismo de Revisión de Incidentes de Ciberseguridad para revisar y evaluar incidentes específicos significativos o a gran escala. ***Estas nuevas estructuras también deben apoyar las operaciones y misiones de la PCSD de la UE.*** Estas acciones deben entenderse sin perjuicio de lo dispuesto en los artículos 107 y 108 del Tratado de Funcionamiento de la Unión Europea (TFUE).

Enmienda 9

Propuesta de Reglamento
Considerando 11

Texto de la Comisión	*Enmienda*
(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	(11) A efectos de una buena gestión financiera, deben establecerse normas específicas para la prórroga de los créditos de compromiso y de pago no utilizados. Al tiempo que se respeta el principio de que el presupuesto de la Unión se establece anualmente, el presente Reglamento, debido al carácter impredecible, excepcional y específico del panorama de la ciberseguridad, debe prever la posibilidad de prorrogar los fondos no utilizados más allá de los establecidos en el

Reglamento Financiero, maximizando así la capacidad del Mecanismo de Ciberemergencia para ayudar a los Estados miembros a hacer frente eficazmente a las ciberamenazas.

Reglamento Financiero, maximizando así la capacidad del Mecanismo de Ciberemergencia para ayudar a los Estados miembros a hacer frente eficazmente a las ciberamenazas. ***Estas normas específicas también permitirían un apoyo financiero a más largo plazo para la adquisición conjunta de herramientas e infraestructuras ultraseguras de última generación, con el fin de mejorar las capacidades de detección colectiva mediante el uso de los avances más recientes en inteligencia artificial (IA) y análisis de datos.***

Enmienda 10

Propuesta de Reglamento
Considerando 13

Texto de la Comisión	*Enmienda*
(13) Cada Estado miembro debe designar un organismo público a nivel nacional encargado de coordinar las actividades de detección de ciberamenazas en dicho Estado miembro. Estos COS nacionales deben actuar como punto de referencia y pasarela a nivel nacional para la participación en el Ciberescudo Europeo y deben garantizar que la información sobre ciberamenazas procedente de entidades públicas y privadas se comparta y recopile a nivel nacional de manera eficaz y racional.	(13) Cada Estado miembro debe designar un organismo público a nivel nacional encargado de coordinar las actividades de detección de ciberamenazas en dicho Estado miembro. Estos COS nacionales deben actuar como punto de referencia y pasarela a nivel nacional para la participación en el Ciberescudo Europeo y deben garantizar que la información sobre ciberamenazas procedente de entidades públicas y privadas se comparta y recopile a nivel nacional de manera eficaz y racional. ***Cuando sea viable y necesario, los COS también deben permitir la participación de entidades de defensa, estableciendo un «pilar de defensa» en términos de gobernanza y tipo de información compartida, como se establece en la Comunicación conjunta sobre la política de ciberdefensa de la UE[1] y apoya el Alto Representante.*** ***[1] Comunicación conjunta al Parlamento Europeo y al Consejo, Política de ciberdefensa de la UE, JOIN(2022) 49 final.***

Enmienda 11

Propuesta de Reglamento
Considerando 14

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

Enmienda 12

Propuesta de Reglamento
Considerando 15

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

Enmienda 13

Propuesta de Reglamento
Considerando 16

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

contextualizada sobre incidentes, amenazas y vulnerabilidades. Además, los COS transfronterizos también deben celebrar acuerdos de cooperación con otros COS transfronterizos.

indicadores de compromiso e información contextualizada sobre incidentes, amenazas y vulnerabilidades. Además, los COS transfronterizos también deben celebrar acuerdos de cooperación con otros COS transfronterizos ***y con la red operativa para CERT militares (MICNET) cuando se cree esta***.

Enmienda 14

Propuesta de Reglamento
Considerando 17

Texto de la Comisión	*Enmienda*
(17) Que las autoridades pertinentes compartan la conciencia situacional es un requisito indispensable para la preparación y la coordinación a escala de la Unión con respecto a los incidentes de ciberseguridad significativos y a gran escala. La Directiva (UE) 2022/2555 crea EU-CyCLONe a fin de respaldar la gestión coordinada de los incidentes y las crisis de ciberseguridad a gran escala en el ámbito operativo y de garantizar el intercambio periódico de información pertinente entre los Estados miembros y las instituciones, órganos y organismos de la Unión. La Recomendación (UE) 2017/1584 sobre la respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala aborda el papel de todos los agentes pertinentes. La Directiva (UE) 2022/2555 también recuerda las responsabilidades de la Comisión en el Mecanismo de Protección Civil de la Unión («UCPM») establecido por la Decisión 1313/2013/UE del Parlamento Europeo y del Consejo, así como en lo relativo a la presentación de informes analíticos para el Dispositivo de Respuesta Política Integrada a las Crisis («Dispositivo RPIC») en virtud de la Decisión de Ejecución (UE) 2018/1993. Por lo tanto, en situaciones en las que los COS transfronterizos obtengan información relacionada con un incidente	(17) Que las autoridades pertinentes compartan la conciencia situacional es un requisito indispensable para la preparación y la coordinación a escala de la Unión con respecto a los incidentes de ciberseguridad significativos y a gran escala. La Directiva (UE) 2022/2555 crea EU-CyCLONe a fin de respaldar la gestión coordinada de los incidentes y las crisis de ciberseguridad a gran escala en el ámbito operativo y de garantizar el intercambio periódico de información pertinente entre los Estados miembros y las instituciones, órganos y organismos de la Unión. La Recomendación (UE) 2017/1584 sobre la respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala aborda el papel de todos los agentes pertinentes. La Directiva (UE) 2022/2555 también recuerda las responsabilidades de la Comisión en el Mecanismo de Protección Civil de la Unión («UCPM») establecido por la Decisión 1313/2013/UE del Parlamento Europeo y del Consejo, así como en lo relativo a la presentación de informes analíticos para el Dispositivo de Respuesta Política Integrada a las Crisis («Dispositivo RPIC») en virtud de la Decisión de Ejecución (UE) 2018/1993. Por lo tanto, en situaciones en las que los COS transfronterizos obtengan información relacionada con un incidente

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

de ciberseguridad a gran escala potencial o en curso, deben proporcionar la información pertinente a EU-CyCLONe, a la red de CSIRT***, a la comunidad de ciberdefensa*** y a la Comisión. En particular, dependiendo de la situación, la información que debe compartirse podría incluir información técnica, información sobre la naturaleza y los motivos del agresor o posible agresor, e información no técnica de nivel superior sobre un incidente de ciberseguridad a gran escala potencial o en curso. En este contexto, debe prestarse la debida atención al principio de la necesidad de conocer y al carácter potencialmente sensible de la información compartida.

Enmienda 15

Propuesta de Reglamento
Considerando 19

Texto de la Comisión	*Enmienda*
(19) A fin de permitir el intercambio de datos sobre amenazas a la ciberseguridad procedentes de diversas fuentes, a gran escala, en un entorno de confianza, las entidades que participen en el Ciberescudo Europeo deben estar dotadas de herramientas, equipos e infraestructuras de última generación y de alta seguridad. Esto debería permitir mejorar las capacidades de detección colectiva y las alertas oportunas a las autoridades y entidades pertinentes, en particular mediante el uso de las últimas tecnologías de inteligencia artificial y análisis de datos.	(19) A fin de permitir el intercambio de datos sobre amenazas a la ciberseguridad procedentes de diversas fuentes, a gran escala, en un entorno de confianza, las entidades que participen en el Ciberescudo Europeo deben estar dotadas de herramientas, equipos e infraestructuras de última generación y de alta seguridad***, excluyendo a los proveedores de alto riesgo de productos críticos con elementos digitales***. 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. ***Debe preverse la supervisión humana cuando se utilice inteligencia artificial, y debe garantizarse un nivel suficiente de alfabetización en materia de inteligencia artificial, así como el apoyo y la autoridad necesarios para ejercer esa función.***

Enmienda 16

Propuesta de Reglamento
Considerando 19 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(19 bis) De conformidad con el Reglamento [XX/XXXX (Ley de Ciberresiliencia)], las entidades que participen en el Ciberescudo Europeo también deben abarcar los requisitos establecidos en el presente Reglamento para todos los productos con elementos digitales. En vista de los crecientes riesgos originados por las dependencias económicas, es necesario minimizar la exposición a los proveedores de alto riesgo de productos críticos a través de un marco estratégico común para la seguridad económica de la Unión. La dependencia de proveedores de alto riesgo de productos críticos con elementos digitales plantea un riesgo estratégico que debe abordarse a escala de la Unión, sobre todo si un país practica el espionaje económico o la coacción económica y su legislación obliga a acceder arbitrariamente a cualquier tipo de operaciones o datos de la empresa, especialmente cuando los productos críticos están destinados al uso de las entidades esenciales a que se refiere la Directiva (UE) 2022/2555.

Enmienda 17

Propuesta de Reglamento
Considerando 20

Texto de la Comisión	*Enmienda*
(20) Al recopilar, compartir e intercambiar datos, el Ciberescudo Europeo debe reforzar la soberanía tecnológica de la Unión. La puesta en	(20) Al recopilar, compartir e intercambiar datos, el Ciberescudo Europeo debe reforzar la soberanía tecnológica de la Unión***, su autonomía***

común de datos gestionados de alta calidad también debería contribuir al desarrollo de tecnologías avanzadas de inteligencia artificial y análisis de datos. Debe facilitarse mediante la conexión del Ciberescudo Europeo con la infraestructura paneuropea de informática de alto rendimiento establecida por el Reglamento (UE) 2021/1173 del Consejo [25].

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

estratégica, su competitividad y su resiliencia. La puesta en común de datos gestionados de alta calidad también debería contribuir al desarrollo de tecnologías avanzadas de inteligencia artificial y análisis de datos. Debe facilitarse mediante la conexión del Ciberescudo Europeo con la infraestructura paneuropea de informática de alto rendimiento establecida por el Reglamento (UE) 2021/1173 del Consejo [25].

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

Enmienda 18

Propuesta de Reglamento
Considerando 25

Texto de la Comisión	*Enmienda*
(25) El Mecanismo de Ciberemergencia debe prestar apoyo a los Estados miembros complementando sus propias medidas y recursos, así como otras opciones de apoyo existentes para la respuesta y recuperación inmediata de incidentes de ciberseguridad significativos y a gran escala, como los servicios prestados por la Agencia de la Unión Europea para la Ciberseguridad (la «ENISA») de conformidad con su mandato, la respuesta coordinada y la asistencia de la red de CSIRT, el apoyo a la mitigación de EU-CyCLONe, así como la asistencia mutua entre los Estados miembros, también en el contexto del artículo 42, apartado 7, del TUE, los equipos de respuesta telemática rápida de la CEP ***26*** y los equipos de respuesta rápida contra amenazas híbridas. Debe abordar la necesidad de garantizar la disponibilidad de medios especializados para apoyar la	(25) El Mecanismo de Ciberemergencia debe prestar apoyo a los Estados miembros complementando sus propias medidas y recursos, así como otras opciones de apoyo existentes para la respuesta y recuperación inmediata de incidentes de ciberseguridad significativos y a gran escala, como los servicios prestados por la Agencia de la Unión Europea para la Ciberseguridad (la «ENISA») de conformidad con su mandato, la respuesta coordinada y la asistencia de la red de CSIRT, el apoyo a la mitigación de EU-CyCLONe, así como la asistencia mutua entre los Estados miembros, también en el contexto del artículo 42, apartado 7, del TUE, los equipos de respuesta telemática rápida de la CEP***[1], el nuevo Centro de Coordinación del Ámbito del Ciberespacio y de la Información (CIDCC) del proyecto CEP y su sucesor propuesto, el Centro de***

preparación y la respuesta a los incidentes de ciberseguridad en toda la Unión y en terceros países.

Coordinación de la Ciberdefensa de la UE (EUCDCC) 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***, especialmente los países candidatos a la adhesión a la Unión alineados con la política exterior y de seguridad común y de la política común de seguridad y defensa, ayudándoles a desarrollar sus cibercapacidades y a mejorar la cooperación transfronteriza y regional entre dichos países candidatos en el ámbito cibernético***.

[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.

[26] 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.

[26] 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.

Enmienda 19

Propuesta de Reglamento
Considerando 26

Texto de la Comisión	*Enmienda*
(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 [27], el Dispositivo RPIC [28], 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	(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 [27], el Dispositivo RPIC [28], 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***.

uso del presente instrumento también debe coordinarse con la aplicación de las medidas del conjunto de instrumentos de ciberdiplomacia, ***impulsando la cooperación en los planos estratégico, operativo y técnico entre la comunidad de ciberdefensa y otras cibercomunidades, en particular con el fin de reforzar las capacidades contra las amenazas a la ciberseguridad procedentes de fuera de la Unión, incluidas las medidas restrictivas, que pueden utilizarse para prevenir y responder a actividades informáticas malintencionadas***.

---

[27] 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).

[28] 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.

[27] 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).

[28] 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.

Enmienda 20

Propuesta de Reglamento
Considerando 28

Texto de la Comisión	*Enmienda*
(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	(28) La Directiva (UE) 2022/2555 exige a los Estados miembros que designen o establezcan una o varias autoridades de gestión de crisis de ciberseguridad y velen por que estas dispongan de los recursos adecuados para llevar a cabo sus cometidos de manera eficaz y eficiente. También exige a los Estados miembros que determinen las capacidades, los activos y los procedimientos que se pueden desplegar en caso de crisis, así como que

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

adopten un plan nacional de respuesta a incidentes y crisis de ciberseguridad a gran escala en el que se fijen los objetivos y las disposiciones de la gestión de los incidentes y las crisis de ciberseguridad a gran escala. Asimismo, los Estados miembros están obligados a establecer uno o varios CSIRT encargados de las responsabilidades de gestión de incidentes de conformidad con un proceso bien definido y que abarquen al menos los sectores, subsectores y tipos de entidades incluidos en el ámbito de aplicación de dicha Directiva, y a velar por que dispongan de los recursos adecuados para llevar a cabo eficazmente sus cometidos. El presente Reglamento se entiende sin perjuicio del papel de la Comisión a la hora de garantizar el cumplimiento por parte de los Estados miembros de las obligaciones que les impone la Directiva (UE) 2022/2555. El Mecanismo de Ciberemergencia debe proporcionar asistencia para las acciones destinadas a reforzar la preparación, así como las acciones de respuesta a incidentes para mitigar los efectos de incidentes de ciberseguridad significativos y a gran escala, apoyar la recuperación inmediata o restablecer el funcionamiento de los servicios esenciales***, utilizando adecuadamente toda una serie de opciones defensivas disponibles para las comunidades civiles y militares***.

Enmienda 21

Propuesta de Reglamento
Considerando 29

Texto de la Comisión	*Enmienda*
(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	(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***[29]***. La selección de los sectores también debe

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. ***En su caso, el Servicio Europeo de Acción Exterior (SEAE), en particular a través del Centro de Inteligencia de la UE (INTCEN) y su Célula de Fusión contra las Amenazas Híbridas, con el apoyo de la Dirección de Inteligencia del Estado Mayor de la Unión Europea (EMUE) dentro de la Capacidad Única de Análisis de Inteligencia (SIAC), también deberá asociarse para proporcionar evaluaciones actualizadas y contribuir de este modo a la identificación de*** los sectores o subsectores ***que*** 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. ***Estos ejercicios también deben desempeñar un importante papel para la mejora de la cooperación entre entidades civiles y militares. Al organizar los ejercicios, la Comisión, el SEAE y la ENISA deben, por tanto, valorar de forma sistemática la inclusión de participantes procedentes de otras comunidades, como la Agencia Europea de Defensa (AED) y otras entidades pertinentes.*** 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

tener en cuenta la Recomendación del Consejo relativa a un enfoque coordinado en toda la Unión para reforzar la resiliencia de las infraestructuras críticas.

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.

[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).

---

[29] 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).

[29] 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).

Enmienda 22

Propuesta de Reglamento
Considerando 32

Texto de la Comisión	*Enmienda*
(32) El Mecanismo de Ciberemergencia debe apoyar la asistencia prestada por los Estados miembros a un Estado miembro afectado por un incidente de ciberseguridad significativo o a gran escala, incluida la red de CSIRT establecida en el artículo 15 de la Directiva (UE) 2022/2555. Los Estados miembros que presten asistencia deben poder presentar solicitudes para cubrir los costes relacionados con el envío de equipos de expertos en el marco de la asistencia mutua. Los costes subvencionables podrían incluir los gastos de viaje, alojamiento y dietas de los expertos en ciberseguridad.	(32) El Mecanismo de Ciberemergencia debe apoyar la asistencia prestada por los Estados miembros a un Estado miembro afectado por un incidente de ciberseguridad significativo o a gran escala, incluida la red de CSIRT establecida en el artículo 15 de la Directiva (UE) 2022/2555. Los Estados miembros que presten asistencia deben poder presentar solicitudes para cubrir los costes relacionados con el envío de equipos de expertos en el marco de la asistencia mutua***, garantizando una coordinación eficiente entre los programas e instrumentos pertinentes de la Unión, incluidos el Fondo Europeo de Apoyo a la Paz (FEAP), la PESC y el IVCDCI, a la hora de prestar ayuda a terceros países, en particular Ucrania y Moldavia***. Los costes subvencionables podrían incluir los gastos de viaje, alojamiento y dietas de los expertos en ciberseguridad.

Enmienda 23

Propuesta de Reglamento
Considerando 33

Texto de la Comisión	*Enmienda*
(33) Debe crearse gradualmente una reserva de ciberseguridad a escala de la Unión, compuesta por servicios de proveedores privados de servicios de seguridad gestionados para apoyar las acciones de respuesta y recuperación inmediata en caso de incidentes de ciberseguridad significativos o a gran escala. La Reserva de Ciberseguridad de la UE debe garantizar la disponibilidad y el estado de preparación de los servicios. Los servicios de la Reserva de Ciberseguridad	(33) Debe crearse gradualmente una reserva de ciberseguridad a escala de la Unión, compuesta por servicios de proveedores privados de servicios de seguridad gestionados para apoyar las acciones de respuesta y recuperación inmediata en caso de incidentes de ciberseguridad significativos o a gran escala. La Reserva de Ciberseguridad de la UE debe garantizar la disponibilidad y el estado de preparación de los servicios. Los servicios de la Reserva de Ciberseguridad

de la UE deben servir para ayudar a las autoridades nacionales a prestar asistencia a las entidades afectadas que operen en sectores críticos o muy críticos como complemento de sus propias acciones a nivel nacional. Al solicitar el apoyo de la Reserva de Ciberseguridad de la UE, los Estados miembros deben especificar el apoyo prestado a la entidad afectada a nivel nacional, que debe tenerse en cuenta al evaluar la solicitud del Estado miembro. Los servicios de la Reserva de Ciberseguridad de la UE también pueden servir para apoyar a las instituciones, órganos y organismos de la Unión, en condiciones similares.	de la UE deben servir para ayudar a las autoridades nacionales a prestar asistencia a las entidades afectadas que operen en sectores críticos o muy críticos como complemento de sus propias acciones a nivel nacional. Al solicitar el apoyo de la Reserva de Ciberseguridad de la UE, los Estados miembros deben especificar el apoyo prestado a la entidad afectada a nivel nacional, que debe tenerse en cuenta al evaluar la solicitud del Estado miembro. Los servicios de la Reserva de Ciberseguridad de la UE también pueden servir para apoyar a las instituciones, órganos y organismos de la Unión, ***incluidas las misiones de la PCSD*** en condiciones similares.

Enmienda 24

Propuesta de Reglamento
Considerando 34

Texto de la Comisión	*Enmienda*
(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.	(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***, teniendo en cuenta también los riesgos asociados a la participación de los proveedores de países competidores estratégicos, que podrían dar origen a riesgos para la seguridad económica, así como las implicaciones para la seguridad estratégica de la Unión***.

Enmienda 25

Propuesta de Reglamento
Considerando 36

Texto de la Comisión	*Enmienda*
(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	(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. ***En vista del desarrollo de un sistema de conectividad seguro, basado en la infraestructura europea de comunicación cuántica (EuroQCI) y la comunicación gubernamental por satélite de la Unión Europea (Govsatcom), y en particular de la ejecución del GNSS GALILEO para usuarios de defensa, todo posible desarrollo futuro ha de tener en cuenta el advenimiento de la «hiperguerra», que combina la velocidad y la sofisticación de la informática cuántica con unos sistemas militares altamente autónomos.*** 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

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.

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***, el SEAE y cualquier misión de la PCSD en el país afectado por el incidente a través de sus respectivas sedes***.

Enmienda 26

Propuesta de Reglamento
Considerando 37

Texto de la Comisión	*Enmienda*
(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	(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***, en particular Ucrania y Moldavia,*** 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 ***deben*** recibir apoyo de la Reserva de Ciberseguridad de la UE***. El apoyo también debe aplicarse a aquellos terceros países en los que se despliegue una misión***

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.

de la PCSD con un mandato específico de reforzar la resiliencia frente a amenazas híbridas, incluida la cibernética, o en los que se haya adoptado una medida de ayuda del Mecanismo Europeo para la Paz para reforzar la ciberresiliencia del país. 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.

Enmienda 27

Propuesta de Reglamento
Artículo 1 – apartado 1 – letra c

Texto de la Comisión	*Enmienda*
c) el establecimiento de un Mecanismo Europeo de Revisión de Incidentes de Ciberseguridad para revisar y evaluar incidentes significativos o a gran escala.	c) el establecimiento de un Mecanismo Europeo de Revisión de Incidentes de Ciberseguridad para revisar y evaluar incidentes ***o amenazas*** significativos o a gran escala.

Enmienda 28

Propuesta de Reglamento
Artículo 1 – apartado 2 – letra a

Texto de la Comisión	*Enmienda*
a) afianzar la capacidad común de la Unión de detección y conciencia situacional de ciberamenazas y ciberincidentes, permitiendo así reforzar la posición competitiva de la industria y los	a) afianzar la capacidad común de la Unión de detección y conciencia situacional de ciberamenazas y ciberincidentes, permitiendo así reforzar la posición competitiva de la industria y los

sectores de servicios de la Unión en toda la economía digital y contribuir a la ***soberanía*** tecnológica de la Unión en el ámbito de la ciberseguridad;	sectores de servicios de la Unión en toda la economía digital y contribuir a la ***resiliencia*** tecnológica de la Unión en el ámbito de la ciberseguridad;

Enmienda 29

Propuesta de Reglamento
Artículo 1 – apartado 2 – letra b

Texto de la Comisión	*Enmienda*
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;	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 ***o de aquellos terceros países que sean candidatos para la adhesión a la Unión y no sean contrarios a los intereses de seguridad y defensa de la Unión y de sus Estados miembros, tal como se establece en el marco de la PESC de conformidad con el título V del TUE***; ***Los Estados miembros deben considerar la posibilidad de integrar en su estrategia nacional de ciberseguridad un programa de ciberdefensa activo que incorpore ejercicios de formación conjuntos de los Estados miembros y las diferentes organizaciones internacionales. Dicho programa debe proporcionar una capacidad sincronizada y en tiempo real para descubrir, detectar, analizar y mitigar amenazas;***

Enmienda 30

Propuesta de Reglamento
Artículo 1 – apartado 2 bis (nuevo)

Texto de la Comisión	*Enmienda*
	2 bis. reducir los riesgos sistémicos de ciberseguridad que plantean las dependencias de equipos críticos de países que sean contrarios a los intereses de seguridad y defensa de la Unión y de sus Estados miembros, tal como se establece en el marco de la PESC de conformidad con el título V del TUE;

Enmienda 31

Propuesta de Reglamento
Artículo 2 – párrafo 2 bis (nuevo)

Texto de la Comisión	*Enmienda*
	«comunidad de ciberdefensa»: las autoridades de defensa de los Estados miembros y el apoyo de las instituciones, órganos y organismos de la Unión, tal y como se establece en la Comunicación conjunta sobre la política de ciberdefensa de la Unión[1]
	[1] Comunicación conjunta al Parlamento Europeo y al Consejo, Política de ciberdefensa de la UE, JOIN(2022) 49 final.

Enmienda 32

Propuesta de Reglamento
Artículo 3 – apartado 2 – párrafo 1 – letra b bis (nueva)

Texto de la Comisión	*Enmienda*
	b bis) contribuir a modernizar la totalidad de los sistemas de ciberdefensa, aumentando la calidad de las capacidades de ciberdefensa mediante el despliegue de sistemas de IA, y a acelerar el intercambio de información entre los COS nacionales y los COS transfronterizos;

Enmienda 33

Propuesta de Reglamento
Artículo 3 – apartado 2 – párrafo primero – letra d *bis* (nueva)

Texto de la Comisión	*Enmienda*
	d bis) revisar y evaluar las tecnologías y equipos críticos de ciberseguridad desplegados por los COS en respuesta a incidentes de ciberseguridad para detectar riesgos sistémicos originados por el control de proveedores de alto riesgo por parte de países que sean contrarios a los intereses de seguridad y defensa de la Unión y de sus Estados miembros, tal como se establece en el marco de la PESC de conformidad con el título V del TUE;

Enmienda 34

Propuesta de Reglamento
Artículo 4 – apartado 1 – párrafo 2

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

Enmienda 35

Propuesta de Reglamento
Artículo 4 – apartado 2

Texto de la Comisión	*Enmienda*
2. Tras una convocatoria de	2. Tras una convocatoria de

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

manifestaciones de interés, el Centro Europeo de Competencia en Ciberseguridad («ECCC», por sus siglas en inglés) seleccionará a COS nacionales para que participen con él en una adquisición conjunta de herramientas e infraestructuras. El ECCC podrá conceder subvenciones a los COS nacionales seleccionados para financiar el funcionamiento de dichas herramientas e infraestructuras***, sujeto a la condición estricta de que dichas herramientas e infraestructuras las faciliten proveedores de confianza conforme al artículo 16***. 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.

Enmienda 36

Propuesta de Reglamento
Artículo 5 – apartado 2

Texto de la Comisión	*Enmienda*
2. Tras una convocatoria de manifestaciones de interés, el ECCC seleccionará un consorcio anfitrión para que participe con él en una adquisición conjunta de herramientas e infraestructuras. El ECCC podrá conceder al consorcio anfitrión una subvención para financiar el funcionamiento de dichas herramientas e infraestructuras. La contribución financiera de la Unión sufragará hasta el 75 % de los costes de adquisición de las herramientas e infraestructuras y hasta el 50 % de los costes de funcionamiento, y los costes restantes correrán a cargo del consorcio anfitrión. Antes de iniciar el procedimiento	2. Tras una convocatoria de manifestaciones de interés, el ECCC seleccionará un consorcio anfitrión para que participe con él en una adquisición conjunta de herramientas e infraestructuras. El ECCC podrá conceder al consorcio anfitrión una subvención para financiar el funcionamiento de dichas herramientas e infraestructuras***, sujeto a la condición estricta de que dichas herramientas e infraestructuras las faciliten proveedores de confianza conforme al artículo 16***. La contribución financiera de la Unión sufragará hasta el 75 % de los costes de adquisición de las herramientas e

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.	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.

Enmienda 37

Propuesta de Reglamento
Artículo 5 – párrafo 2 bis (nuevo)

Texto de la Comisión	*Enmienda*
	2 bis. Cualquier infraestructura o proveedor originario de un tercer país de alto riesgo quedará automáticamente excluido.

Enmienda 38

Propuesta de Reglamento
Artículo 6 – apartado 1 – letra b bis (nueva)

Texto de la Comisión	*Enmienda*
	b bis) apoye directamente el refuerzo de las capacidades militares y de defensa de los miembros participantes o evite una amenaza directa e inminente para su seguridad. Dado que la explotación de las vulnerabilidades en el sector de la defensa puede causar perturbaciones y daños considerables, la ciberseguridad de la industria de la defensa requiere medidas especiales que garanticen la seguridad de las cadenas de suministro, particularmente en el caso de las entidades situadas en los tramos finales de tales cadenas, que no necesitan tener acceso a información clasificada pero que podrían comportar graves riesgos para el sector en su conjunto. Debe prestarse especial atención a las repercusiones de

	un posible incidente y al riesgo derivado de cualquier posible manipulación de los datos de red que pueda inutilizar los mecanismos de defensa esenciales o incluso neutralizar sus sistemas operativos, y los haga vulnerables a la piratería.

Enmienda 39

Propuesta de Reglamento
Artículo 6 – apartado 1 – letra b bis (nueva)

Texto de la Comisión	*Enmienda*
	b ter) apoye el refuerzo de las capacidades militares y de defensa de los miembros participantes o evite una amenaza directa e inminente para su seguridad, garantizando la seguridad de las cadenas de suministro, particularmente en el caso de las entidades situadas en los tramos finales de tales cadenas, lo que no requiere el acceso a información clasificada, pero podría comportar riesgos graves para el sector en su conjunto.

Enmienda 40

Propuesta de Reglamento
Artículo 7 – apartado 1

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

(UE) 2022/2555.

Enmienda 41

Propuesta de Reglamento
Artículo 8 – apartado 1

Texto de la Comisión	*Enmienda*
1. Los Estados miembros que participen en el Ciberescudo Europeo garantizarán un alto nivel de seguridad de los datos y de seguridad física de la infraestructura del Ciberescudo Europeo, y velarán por que la infraestructura se gestione y controle adecuadamente, de tal manera que se proteja de las amenazas y se garantice su seguridad y la de los sistemas, incluida la de los datos intercambiados a través de la infraestructura.	1. Los Estados miembros que participen en el Ciberescudo Europeo garantizarán un alto nivel de seguridad de los datos y de seguridad física de la infraestructura del Ciberescudo Europeo, y velarán por que la infraestructura se gestione y controle adecuadamente, de tal manera que se proteja de las amenazas y se garantice su seguridad y la de los sistemas, ***la supresión de riesgos y el impulso de la ventaja tecnológica de la Unión en sectores críticos, incluidas medidas para restringir o excluir a proveedores de alto riesgo, así como proteger la seguridad*** de los datos intercambiados a través de la infraestructura.

Enmienda 42

Propuesta de Reglamento
Artículo 8 – apartado 2

Texto de la Comisión	*Enmienda*
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.	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 ***y que todo intercambio de información con proveedores de alto riesgo tenga un alcance limitado y no perjudique los intereses de seguridad y estratégicos de la Unión***.

Enmienda 43

Propuesta de Reglamento
Artículo 8 – apartado 3

Texto de la Comisión	*Enmienda*
3. La Comisión podrá adoptar actos de ejecución que establezcan requisitos técnicos para que los Estados miembros cumplan las obligaciones que les imponen los apartados 1 y 2. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 21, apartado 2. Al hacerlo, la Comisión, con el apoyo del Alto Representante, tendrá en cuenta las normas de seguridad pertinentes en materia de defensa, con el fin de facilitar la cooperación con los mandos militares.	3. La Comisión podrá adoptar actos de ejecución que establezcan requisitos técnicos para que los Estados miembros cumplan las obligaciones que les imponen los apartados 1 y 2. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 21, apartado 2. Al hacerlo, la Comisión, con el apoyo del Alto Representante, tendrá en cuenta las normas de seguridad pertinentes en materia de defensa, con el fin de facilitar la cooperación con los mandos militares***, utilizando adecuadamente toda una serie de opciones defensivas a disposición de las comunidades civiles y militares para la seguridad y la defensa generales de la Unión, e informará al Parlamento Europeo***.

Enmienda 44

Propuesta de Reglamento
Artículo 9 – apartado 2

Texto de la Comisión	*Enmienda*
2. Las acciones por las que se aplica el Mecanismo de Ciberemergencia recibirán financiación del programa Europa Digital y se ejecutarán de conformidad con el Reglamento (UE) 2021/694 y, en particular, con su objetivo específico 3.	2. Las acciones por las que se aplica el Mecanismo de Ciberemergencia recibirán financiación del programa Europa Digital y se ejecutarán de conformidad con el Reglamento (UE) 2021/694 y, en particular, con su objetivo específico 3***, y del Fondo Europeo de Apoyo a la Paz al facilitar medidas de asistencia a terceros países, en particular a Ucrania y Moldavia***.

Enmienda 45

Propuesta de Reglamento
Artículo 10 – apartado 1 – letra a

Texto de la Comisión	*Enmienda*
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;	a) acciones de preparación, incluida la realización de pruebas coordinadas de preparación de las entidades que operan en sectores muy críticos***, como las infraestructuras públicas, las infraestructuras electorales, el transporte, la asistencia sanitaria, las finanzas, las telecomunicaciones, el suministro de alimentos y la seguridad*** en toda la Unión;

Enmienda 46

Propuesta de Reglamento
Artículo 10 – apartado 1 – letra c

Texto de la Comisión	*Enmienda*
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.	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 ***y en el contexto del artículo 42, apartado 7, del TUE y del artículo 222 del TFUE;***

Enmienda 47

Propuesta de Reglamento
Artículo 10 – apartado 1 – letra c bis (nueva)

Texto de la Comisión	*Enmienda*
	c bis) sustitución y retirada gradual de equipos críticos procedentes de proveedores de alto riesgo que sean contrarios a los intereses de seguridad y defensa de la Unión y de sus Estados miembros, tal como se establece en el

marco de la PESC de conformidad con el título V del TUE.

Enmienda 48

Propuesta de Reglamento
Artículo 11 – apartado 2

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

Enmienda 49

Propuesta de Reglamento
Artículo 12 – apartado 2

Texto de la Comisión	*Enmienda*
2. La Reserva de Ciberseguridad de la UE consistirá en servicios de respuesta a incidentes prestados por proveedores de confianza seleccionados de conformidad con los criterios establecidos en el artículo 16. La Reserva incluirá servicios comprometidos previamente. Los servicios deberán poder desplegarse en todos los Estados miembros.	2. La Reserva de Ciberseguridad de la UE consistirá en servicios de respuesta a incidentes prestados por proveedores de confianza seleccionados de conformidad con los criterios establecidos en el artículo 16. La Reserva incluirá servicios comprometidos previamente. Los servicios deberán poder desplegarse en todos los Estados miembros ***y en los terceros países que reúnan los requisitos aplicables del presente Reglamento***.

Enmienda 50

Propuesta de Reglamento
Artículo 12 – apartado 3 – letra b

Texto de la Comisión	*Enmienda*
b) las instituciones, órganos y organismos de la Unión.	b) las instituciones, órganos y organismos de la Unión***, incluidas las***

	misiones de la PCSD.

Enmienda 51

Propuesta de Reglamento
Artículo 12 – apartado 4

Texto de la Comisión	*Enmienda*
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.	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 ***—como las infraestructuras públicas, las infraestructuras electorales, el transporte, la asistencia sanitaria, las finanzas, las telecomunicaciones, el suministro de alimentos y la seguridad—*** y la recuperación inmediata de tales incidentes.

Enmienda 52

Propuesta de Reglamento
Artículo 12 – apartado 5

Texto de la Comisión	*Enmienda*
5. La Comisión tendrá la responsabilidad general de la ejecución de la Reserva de Ciberseguridad de la UE. La Comisión determinará las prioridades y la evolución de la Reserva de Ciberseguridad de la UE, en consonancia con los requisitos de los usuarios a que se refiere el apartado 3, supervisará su aplicación y garantizará la complementariedad, la coherencia, las sinergias y los vínculos con otras acciones de apoyo en virtud del presente Reglamento, así como con otras acciones y programas de la Unión.	5. La Comisión tendrá la responsabilidad general de la ejecución de la Reserva de Ciberseguridad de la UE. La Comisión determinará las prioridades y la evolución de la Reserva de Ciberseguridad de la UE, en consonancia con los requisitos de los usuarios a que se refiere el apartado 3, supervisará su aplicación y garantizará la complementariedad, la coherencia, las sinergias y los vínculos con otras acciones de apoyo en virtud del presente Reglamento, así como con otras acciones y programas de la Unión***, en particular el objetivo estratégico de reducir las dependencias con respecto a los proveedores de alto riesgo que sean contrarios a los intereses de seguridad y***

	defensa de la Unión y de sus Estados miembros, tal como se establece en el marco de la PESC de conformidad con el título V del TUE.

Enmienda 53

Propuesta de Reglamento
Artículo 12 – apartado 7

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

Enmienda 54

Propuesta de Reglamento
Artículo 14 – apartado 2 – letra a bis (nueva)

Texto de la Comisión	*Enmienda*
	a bis) el impacto del incidente en la seguridad y la defensa de la Unión;

Enmienda 55

Propuesta de Reglamento
Artículo 15 – apartado 3

Texto de la Comisión	*Enmienda*
3. En consulta con el Alto Representante, el apoyo prestado en el	3. En consulta con el Alto Representante, el apoyo prestado en el

marco del Mecanismo de Ciberemergencia podrá complementar la asistencia prestada en el contexto de la política exterior y de seguridad común y de la política común de seguridad y defensa, en particular a través de los Equipos de Respuesta Telemática Rápida. También podrá complementar o contribuir a la asistencia prestada por un Estado miembro a otro en el contexto del artículo 42, apartado 7, del Tratado de la Unión Europea.	marco del Mecanismo de Ciberemergencia podrá complementar la asistencia prestada en el contexto de la política exterior y de seguridad común y de la política común de seguridad y defensa, en particular a través de los Equipos de Respuesta Telemática Rápida***, con el fin de prestar un mayor apoyo a los Estados miembros de la Unión, a las misiones y operaciones de la PCSD y a los terceros países alineados con la política exterior y de seguridad común y la política común de seguridad y defensa de la Unión en sus esfuerzos por desarrollar capacidades de ciberdefensa, en particular a Ucrania y Moldavia***. También podrá complementar o contribuir a la asistencia prestada por un Estado miembro a otro en el contexto del artículo 42, apartado 7, del Tratado de la Unión Europea.

Enmienda 56

Propuesta de Reglamento
Artículo 16 – apartado 2 – letra b bis (nueva)

Texto de la Comisión	*Enmienda*
	a bis) el proveedor demostrará que sus estructuras de decisión y gestión están libres de cualquier influencia indebida de Gobiernos de Estados que sean contrarios a los intereses de seguridad y defensa de la Unión y de sus Estados miembros, tal como se establece en el marco de la PESC de conformidad con el título V del TUE;

Enmienda 57

Propuesta de Reglamento
Artículo 16 – apartado 2 – letra f

Texto de la Comisión	*Enmienda*
f) el proveedor estará equipado con el equipo técnico de hardware y software necesario para prestar el servicio	f) el proveedor estará equipado con el equipo técnico de *hardware* y *software* necesario para prestar el servicio solicitado

solicitado;	***y cumple los requisitos establecidos en el artículo X del Reglamento XX/XXXX (Ley de Ciberresiliencia)***;

Enmienda 58

Propuesta de Reglamento
Artículo 16 – apartado 2 – letra j bis (nueva)

Texto de la Comisión	*Enmienda*
	j bis) ningún proveedor originario de un tercer país de alto riesgo será elegible.

Enmienda 59

Propuesta de Reglamento
Artículo 16 – apartado 2 – letra j ter (nueva)

Texto de la Comisión	*Enmienda*
	j ter) el proveedor cooperará estrechamente con las pymes pertinentes, cuando sea posible;

Enmienda 60

Propuesta de Reglamento
Artículo 17 – apartado 1

Texto de la Comisión	*Enmienda*
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.	1. Los terceros países podrán solicitar el apoyo de la Reserva de Ciberseguridad de la UE cuando***:***
	a) así lo contemplen los acuerdos de asociación celebrados en relación con su participación en el programa Europa Digital***;***
	b) aquellos terceros países en los que se despliegue una misión de la PCSD con un mandato específico de reforzar la

	resiliencia frente a amenazas híbridas, incluida la cibernética, o en los que se haya adoptado una medida de ayuda del Mecanismo Europeo para la Paz para reforzar la ciberresiliencia del país.

Enmienda 61

Propuesta de Reglamento
Artículo 17 – apartado 2

Texto de la Comisión	*Enmienda*
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.	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 ***excepto aquellos terceros países incluidos en las disposiciones establecidas en el apartado 1, letra b)***.

Enmienda 62

Propuesta de Reglamento
Artículo 18 – apartado 1

Texto de la Comisión	*Enmienda*
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	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, ***en especial cuando el incidente se refiera a un tercer país,*** la Comisión dará a conocer

Representante.	el informe al Alto Representante ***y al SEAE***.

Enmienda 63

Propuesta de Reglamento
Artículo 18 – apartado 3 bis (nuevo)

Texto de la Comisión	*Enmienda*
	3 bis. El informe será transmitido al Parlamento Europeo de conformidad con el Derecho de la Unión o nacional para la protección de la información clasificada sensible.

Enmienda 64

Propuesta de Reglamento
Artículo 19 – párrafo 1 – punto 1 – letra a – punto 1
Reglamento (UE) 2021/694
Artículo 6 – apartado 1

Texto de la Comisión	*Enmienda*
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;	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 ***y a reducir la dependencia de la Unión con respeto a proveedores de alto riesgo de equipos o componentes de ciberseguridad críticos que sean contrarios a los intereses de seguridad y defensa de la Unión y de sus Estados miembros, tal como se establece en el marco de la PESC de conformidad con el título V del TUE***;

Enmienda 65

Propuesta de Reglamento
Artículo 20 – apartado 1

Texto de la Comisión	*Enmienda*
A más tardar [cuatro años después de la fecha de aplicación del presente Reglamento], la Comisión presentará al Parlamento Europeo y al Consejo un informe sobre la evaluación y revisión del presente Reglamento.	A más tardar [***tres*** años después de la fecha de aplicación del presente Reglamento ***y cada dos años a partir de ese momento***], la Comisión presentará al Parlamento Europeo y al Consejo un informe sobre la evaluación y revisión del presente Reglamento.

PROCEDIMIENTO DE LA COMISIÓN COMPETENTE PARA EMITIR OPINIÓN

Título	Establecimiento de 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
Referencias	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)
Comisión competente para el fondo Fecha del anuncio en el Pleno	ITRE 1.6.2023
Opinión emitida por Fecha del anuncio en el Pleno	AFET 1.6.2023
Ponente de opinión Fecha de designación	Dragoş Tudorache 16.6.2023
Examen en comisión	18.9.2023
Fecha de aprobación	24.10.2023
Resultado de la votación final	+: 39 –: 4 0: 0
Miembros presentes en la votación final	Alexander Alexandrov Yordanov, Petras Auštrevičius, Traian Băsescu, Anna Bonfrisco, Włodzimierz Cimoszewicz, Katalin Cseh, Michael Gahler, Giorgos Georgiou, Sunčana Glavak, Bernard Guetta, Sandra Kalniete, Dietmar Köster, Andrius Kubilius, David Lega, Leopoldo López Gil, Jaak Madison, Pedro Marques, David McAllister, Vangelis Meimarakis, Sven Mikser, Francisco José Millán Mon, Matjaž Nemec, Demetris Papadakis, Kostas Papadakis, Tonino Picula, Thijs Reuten, Nacho Sánchez Amor, Andreas Schieder, Jordi Solé, Sergei Stanishev, Tineke Strik, Dominik Tarczyński, Dragoş Tudorache, Thomas Waitz, Bernhard Zimniok, Željana Zovko
Suplentes presentes en la votación final	Attila Ara-Kovács, Lars Patrick Berg, Andrey Kovatchev, Georgios Kyrtsos, Sergey Lagodinsky, Giuliano Pisapia, Mick Wallace

VOTACIÓN FINAL NOMINAL
EN LA COMISIÓN COMPETENTE PARA EMITIR OPINIÓN

39	+
ECR	Lars Patrick Berg, Dominik Tarczyński
ID	Anna Bonfrisco, Jaak Madison
PPE	Alexander Alexandrov Yordanov, Traian Băsescu, Michael Gahler, Sunčana Glavak, Sandra Kalniete, Andrey Kovatchev, Andrius Kubilius, David Lega, Leopoldo López Gil, David McAllister, Vangelis Meimarakis, Francisco José Millán Mon, Željana Zovko
Renew	Petras Auštrevičius, Katalin Cseh, Bernard Guetta, Georgios Kyrtsos, Dragoş Tudorache
S&D	Attila Ara-Kovács, Włodzimierz Cimoszewicz, Dietmar Köster, Pedro Marques, Sven Mikser, Matjaž Nemec, Demetris Papadakis, Tonino Picula, Giuliano Pisapia, Thijs Reuten, Nacho Sánchez Amor, Andreas Schieder, Sergei Stanishev
Verts/ALE	Sergey Lagodinsky, Jordi Solé, Tineke Strik, Thomas Waitz

4	-
ID	Bernhard Zimniok
NI	Kostas Papadakis
The Left	Giorgos Georgiou, Mick Wallace

0	0

Explicación de los signos utilizados
+ : a favor
- : en contra
0 : abstenciones