COMISIÓN
EUROPEA

Bruselas, 24.2.2025
COM(2025) 66 final

2025/0036 (NLE)

Propuesta de

RECOMENDACIÓN DEL CONSEJO

de Plan Director de la UE para la Gestión de Crisis de Ciberseguridad

EXPOSICIÓN DE MOTIVOS

1. CONTEXTO DE LA PROPUESTA

• Razones y objetivos de la propuesta

El Consejo, en sus Conclusiones sobre el futuro de la ciberseguridad, de 22 de mayo de 2024,

> *«(instó) a la Comisión a que evalúe con rapidez el actual plan director de ciberseguridad y, sobre esta base, proponga un plan director de ciberseguridad revisado que adopte la forma de una Recomendación del Consejo en la que se aborden los desafíos actuales y el complejo panorama de las ciberamenazas, se refuercen las redes existentes, se mejore la cooperación y se ponga fin a la compartimentación entre organizaciones, utilizando para ello, ante todo, las estructuras existentes. Además, el plan director revisado debe basarse en unos principios rectores de cooperación que hayan superado la prueba del tiempo (proporcionalidad, subsidiariedad, complementariedad y confidencialidad de la información) y ampliarlos a todo el ciclo de vida de la gestión de crisis, y debe contribuir a armonizar y mejorar la comunicación segura en el ámbito de la ciberseguridad. El plan director revisado debe ser compatible con los marcos existentes, como el Dispositivo de Respuesta Política Integrada a las Crisis, el conjunto de instrumentos de ciberdiplomacia de la UE, el conjunto de instrumentos de la UE contra las amenazas híbridas, el Protocolo de Respuesta Policial ante Emergencias de la UE, marcos emergentes como el Plan Director de Infraestructuras Críticas, procedimientos sectoriales y estructuras generales de gestión de crisis en las entidades de la Unión, también con la participación del Alto Representante y Europol. En este plan director revisado, el papel de la Comisión, del Alto Representante y de la ENISA, en consonancia con sus competencias, debe centrarse, en particular, en apoyar la coordinación horizontal.*».

El objetivo del presente proyecto de Recomendación del Consejo sobre el Plan director de la Unión para la gestión de crisis de ciberseguridad (Plan Director de Ciberseguridad) es presentar, de manera clara, sencilla y accesible, el marco de la Unión Europea (UE) para la gestión de crisis de ciberseguridad. Ello debe permitir a los agentes pertinentes de la Unión (es decir, entidades individuales y redes de entidades de la Unión) comprender cómo interactuar y hacer el mejor uso posible de los mecanismos disponibles a lo largo de todo el ciclo de vida de la gestión de crisis. Su objetivo es explicar qué es una crisis cibernética y qué desencadena un mecanismo de crisis cibernética a escala de la Unión. Explica el uso de los mecanismos disponibles, como el Mecanismo de Emergencia de Ciberseguridad, incluida la Reserva de Ciberseguridad de la UE, para preparar cómo gestionar, responder y recuperarse de una crisis derivada de un incidente de ciberseguridad a gran escala. Además, pretende fomentar una cooperación más estructurada entre los agentes civiles y militares, incluida la cooperación con la Organización del Tratado del Atlántico Norte (OTAN), dado que un ciberincidente a gran escala que afecte a infraestructuras civiles de la Unión de las que dependan los militares también puede activar los mecanismos de respuesta de la OTAN.

El Plan Director de Ciberseguridad es un instrumento no vinculante que identifica acciones específicas para los agentes pertinentes en una crisis cibernética y que puede mejorar la eficacia general del marco de gestión de crisis de ciberseguridad. Actualiza el plan establecido en la Recomendación (UE) 2017/1584 de la Comisión sobre la respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala, y se basa en los resultados y lecciones extraídas de los ejercicios a escala de la Unión desde la adopción de dicha Recomendación. Forma parte de prioridades políticas más amplias en los ámbitos de la preparación y la seguridad.

Tal como se define en la Directiva (UE) 2022/2555 (SRI 2), un incidente de ciberseguridad a gran escala es un incidente que causa perturbaciones que superan la capacidad de un Estado miembro para responder a él o que afecta significativamente por lo menos a dos Estados miembros. Dicho incidente, dependiendo de su causa e impacto, puede intensificarse y convertirse en una crisis propiamente dicha que afecte al correcto funcionamiento del mercado interior o plantee graves riesgos para la seguridad y la protección públicas de las entidades o los ciudadanos de varios Estados miembros o del conjunto de la Unión.

- **Coherencia con las disposiciones existentes en la misma política sectorial**

La propuesta es coherente con los instrumentos pertinentes de la Unión en el ámbito de la ciberseguridad, en particular la Directiva SRI 2 y el Reglamento (UE) 2023/2841 por el que se establecen medidas destinadas a garantizar un elevado nivel común de ciberseguridad en las instituciones, los órganos y los organismos de la Unión. Asimismo, es coherente con el marco del Mecanismo de Protección Civil de la Unión, establecido por la Decisión n.º 1313/2013/UE del Parlamento Europeo y del Consejo, la Decisión de Ejecución (UE) 2018/1993, sobre el dispositivo de la UE de respuesta política integrada a las crisis (RPIC), y las disposiciones e instrumentos sectoriales para el conocimiento de la situación y la gestión de crisis, también en el sector de la electricidad.

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

El Plan Director de Ciberseguridad complementa y es coherente con la Recomendación del Consejo sobre un Plan director para coordinar la respuesta a escala de la Unión en caso de perturbaciones de infraestructuras críticas con importancia transfronteriza significativa, recientemente adoptada, ya que esta última abarca las perturbaciones relacionadas con la resiliencia física no cibernética. Interactúa estrechamente con los mecanismos y herramientas de gestión de crisis de la política exterior y de seguridad común (PESC) y la política común de seguridad y defensa (PCSD), tal como se establece en la Brújula Estratégica para la Seguridad y la Defensa del Consejo. Además, las iniciativas de la Unión para luchar contra la ciberdelincuencia pueden apoyar los objetivos perseguidos por la presente Recomendación.

2. BASE JURÍDICA, SUBSIDIARIEDAD Y PROPORCIONALIDAD

- **Base jurídica**

La propuesta se basa en el artículo 292 del TFUE, que establece las normas pertinentes relativas a la adopción de recomendaciones.

La propuesta complementaría todo el marco legislativo en materia de ciberseguridad establecido a escala de la Unión. No aborda la gestión de incidentes graves que afecten a entidades de la Unión en el sentido del Reglamento (UE, Euratom) 2023/2841, adoptado sobre la base del artículo 298 del TFUE. No obstante, sí aborda el intercambio de información entre las entidades de la Unión y los Estados miembros, incluidas las disposiciones del Reglamento (UE) 2023/2841 para que el representante de la Comisión en el Consejo Interinstitucional de Ciberseguridad (CIIC) sea el punto de contacto para facilitar que este comparta información pertinente en relación con incidentes graves con la Red europea de organizaciones de enlace nacionales para las crisis de ciberseguridad la EU-CyCLONe, como contribución al conocimiento común de la situación.

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

Aunque responder a las perturbaciones de las infraestructuras críticas o de los servicios prestados por entidades esenciales e importantes es sobre todo responsabilidad de los Estados

miembros, determinadas actividades informáticas malintencionadas de carácter transfronterizo pueden perturbar y dañar las infraestructuras críticas de información de las que depende el buen funcionamiento del mercado interior. Por ello, la Unión desempeña un papel importante en caso de crisis o incidente significativo. Esta perturbación puede afectar a varios o incluso a todos los sectores de la actividad económica dentro del mercado único, y podría afectar a la seguridad y a las relaciones internacionales de la Unión. Con el fin de garantizar el funcionamiento del mercado interior, la coordinación a escala de la Unión en caso de perturbaciones de infraestructuras críticas con efectos transfronterizos significativos no solo es adecuada, sino también necesaria. Las respuestas coordinadas a escala de la Unión apoyarán las respuestas de los Estados miembros a la perturbación mediante el conocimiento común de la situación, la comunicación pública coordinada y la mitigación de las consecuencias de la perturbación en el mercado interior.

- **Proporcionalidad**

La presente propuesta se ajusta al principio de proporcionalidad establecido en el artículo 5, apartado 4, del Tratado de la Unión Europea. Ni el contenido ni la forma de la presente propuesta de Recomendación del Consejo exceden de lo necesario para alcanzar sus objetivos. Las acciones propuestas son proporcionales a los objetivos perseguidos, que se centran en garantizar una gestión coordinada de las crisis de ciberseguridad por parte de la Unión.

- **Elección del instrumento**

Para alcanzar los objetivos mencionados, el TFUE, en particular en su artículo 292, prevé que el Consejo adopte recomendaciones basadas en una propuesta de la Comisión. De conformidad con el artículo 288 del TFUE, las recomendaciones no tienen carácter vinculante. Una Recomendación del Consejo es un instrumento adecuado en este caso, ya que señala el compromiso de los Estados miembros con las medidas que incluye y proporciona una base sólida para la cooperación en el ámbito de la coordinación de la gestión de incidentes y crisis de ciberseguridad a gran escala. De este modo, la Recomendación propuesta complementaría el marco jurídico vinculante (en particular, la Directiva SRI 2).

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

- **Consultas con las partes interesadas**

Para elaborar esta propuesta, la Comisión realizó una consulta sobre la revisión del Plan Director de Ciberseguridad e invitó a los Estados miembros y a las entidades pertinentes de la Unión a presentar sus aportaciones. Tuvo en cuenta los puntos de vista de los expertos de los Estados miembros, así como de la ENISA, expresados en el taller que la Comisión y Polonia organizaron de forma conjunta en Karpacz el 5 de septiembre de 2024.

La Comisión consultó a los representantes de los Estados miembros en la red de CSIRT, EU-CyCLONe y el Grupo de Cooperación SRI en las reuniones de septiembre de 2024 e invitó a presentar contribuciones por escrito.

La Comisión presentó y recabó información del Consejo durante dos debates específicos en el Grupo horizontal sobre cuestiones cibernéticas celebrado en octubre y noviembre de 2024.

La Comisión consultó a representantes del sector privado, así como a los Estados miembros, al Servicio Europeo de Acción Exterior (SEAE) y a la ENISA, en un taller organizado por la Representación Permanente de Polonia ante la UE en Bruselas en noviembre de 2024.

La Comisión consultó a las entidades pertinentes de la Unión, a saber el SEAE, la ENISA, Europol y el CERT-EU, en particular a través de debates de alto nivel en las reuniones del Grupo de Trabajo sobre Crisis Cibernéticas[1] celebradas en julio y noviembre de 2024.

Se alcanzó un consenso sobre la necesidad de un documento actualizado, claro, sencillo y operativo que permita a los agentes pertinentes comprender el marco para la gestión de crisis de ciberseguridad y utilizar de forma eficaz los mecanismos disponibles. También hubo consenso sobre la necesidad de evitar la duplicación de instrumentos y hacer un buen uso de los mecanismos existentes a escala de la Unión para la coordinación, el intercambio de información y la respuesta, sin crear nuevas estructuras ni interferir en los procedimientos operativos normalizados internos de las redes y de los mecanismos sectoriales existentes.

[1] Un grupo informal compuesto por los servicios de la Comisión y otros servicios de la UE.

2025/0036 (NLE)

Propuesta de

RECOMENDACIÓN DEL CONSEJO

de Plan Director de la UE para la Gestión de Crisis de Ciberseguridad

EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular su artículo 292,

Vista la propuesta de la Comisión Europea,

Considerando lo siguiente:

(1) La tecnología digital y la conectividad mundial son la columna vertebral del crecimiento económico, la competitividad y la transformación de la infraestructura crítica de la Unión. Sin embargo, una economía interconectada y cada vez más digital también aumenta el riesgo de ciberincidentes y ciberataques. Además, el aumento de las tensiones geopolíticas, los conflictos y la rivalidad estratégica se reflejan en el impacto, el volumen y la sofisticación de las actividades informáticas malintencionadas. Estas actividades pueden formar parte de amenazas híbridas multidimensionales o de operaciones militares. También pueden afectar directamente a la seguridad, la economía y la sociedad de la Unión. Asimismo, pueden extenderse, especialmente cuando estas actividades tienen como objetivo a países socios estratégicos internacionales, como los países candidatos o vecinos.

(2) Un incidente de ciberseguridad a gran escala puede causar perturbaciones que superan la capacidad de un Estado miembro para responder a él o afecta significativamente por lo menos a dos Estados miembros. Este incidente, dependiendo de su causa e impacto, podría intensificarse y convertirse en una crisis propiamente dicha que impida el correcto funcionamiento del mercado interior o plantee graves riesgos para la seguridad y la protección públicas de las entidades o los ciudadanos de varios Estados miembros o del conjunto de la Unión. Una gestión eficaz de las crisis es esencial para mantener la estabilidad económica y proteger a los Gobiernos, la infraestructura crítica, las empresas y los ciudadanos europeos, así como para contribuir a la seguridad y la estabilidad internacionales en el ciberespacio. Por consiguiente, la gestión de las crisis de ciberseguridad forma parte del marco general de gestión de crisis de la UE.

(3) De conformidad con los procedimientos establecidos en la Decisión de Ejecución (UE) 2018/1993 del Consejo[2], la Presidencia del Consejo, que consulta (excepto cuando se haya invocado la cláusula de solidaridad) a los Estados miembros afectados, a la Comisión y al Alto Representante (AR), toma la decisión de activar y desactivar el Dispositivo de la UE de Respuesta Política Integrada a las Crisis (Dispositivo RPIC).

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

Además, de conformidad con los procedimientos del Dispositivo RPIC, la Secretaría General del Consejo, los servicios de la Comisión y el SEAE también pueden acordar en consulta con la Presidencia activar el Dispositivo RPIC en modo de intercambio de información. Los debates en el marco del Dispositivo RPIC se basan en Informes de la Capacidad de Conocimiento y Análisis Integrados de la Situación elaborados por los servicios de la Comisión y el Servicio Europeo de Acción Exterior (SEAE).

(4) Aunque los Estados miembros tienen una responsabilidad primordial en la gestión de las crisis de ciberseguridad nacionales, el posible carácter transfronterizo e intersectorial de los incidentes de ciberseguridad requiere que los Estados miembros y las entidades pertinentes de la Unión colaboren a nivel técnico, operativo y político para coordinarse de forma eficaz en toda la Unión. Al mismo tiempo, la respuesta a las crisis y la recuperación son costosas para las entidades y sectores afectados. Por tanto, la gestión de crisis a lo largo de todo su ciclo de vida incluye la preparación y el conocimiento común de la situación para anticipar los incidentes de ciberseguridad, las capacidades de detección necesarias para identificarlos y las herramientas de respuesta y recuperación necesarias para mitigar, disuadir y contener los incidentes de ciberseguridad.

(5) La Recomendación (UE) 2017/1584 de la Comisión[3], sobre la respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala, establece los objetivos y los modos de cooperación entre los Estados miembros y las entidades de la Unión en la respuesta a incidentes y crisis de ciberseguridad a gran escala. Enumera los agentes pertinentes a nivel técnico, operativo y político, y explica su integración en la gestión de crisis más amplia de la Unión, como el Dispositivo RPIC. Los principios fundamentales establecidos en la Recomendación (UE) 2017/1584 siguen siendo válidos, a saber, la subsidiariedad, la complementariedad y la confidencialidad de la información, así como el planteamiento de tres niveles (técnico, operativo y político).

(6) Desde 2017, la Unión ha desarrollado su marco de ciberseguridad a través de varios instrumentos que contienen disposiciones pertinentes para la gestión de las crisis de ciberseguridad: El Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo[4], la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo[5], el Reglamento de Ejecución (UE, Euratom) 2024/2690 de la Comisión[6], el Reglamento

---

3 Recomendación (UE) 2017/1584 de la Comisión, de 13 de septiembre de 2017, sobre la respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala (DO L 239 de 19.9.2017, p. 36, ELI: http://data.europa.eu/eli/reco/2017/1584/oj).

4 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, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

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

6 Reglamento de Ejecución (UE) 2024/2690 de la Comisión, de 17 de octubre de 2024, por el que se establecen las disposiciones de aplicación de la Directiva (UE) 2022/2555 en lo que respecta a los requisitos técnicos y metodológicos de las medidas para la gestión de riesgos de ciberseguridad y en el que se detallan los casos en que un incidente se considera significativo con respecto a los proveedores de servicios de DNS, los registros de nombres de dominio de primer nivel, los proveedores de servicios de computación en nube, los proveedores de servicios de centro de datos, los proveedores de redes de distribución de contenidos, los proveedores de servicios gestionados, los proveedores de servicios de

(UE, Euratom) 2023/2841 del Parlamento Europeo y del Consejo[7], el Reglamento (UE) 2021/887 del Parlamento Europeo y del Consejo[8], el Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo[9] y el Reglamento (UE) 2025/38 del Parlamento Europeo y del Consejo («Reglamento de Cibersolidaridad»)[10]. Entre las medidas sectoriales específicas en materia de crisis de ciberseguridad figuran el Reglamento Delegado (UE) 2024/1366[11] de la Comisión y el próximo marco de coordinación de ciberincidentes sistémicos (EU-SCICF) en el contexto del Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo[12]. La Directiva 2013/40[13] proporciona la referencia para la definición de las actividades delictivas relacionadas con los ciberataques y las normas de la Unión sobre el acceso transfronterizo a las pruebas electrónicas y, en particular, el Reglamento (UE) 2023/1543 del Parlamento Europeo y del Consejo[14], tras su aplicación, facilitará considerablemente las medidas policiales en este ámbito. La política de ciberdefensa de la UE[15] esboza las funciones de una red de la UE de la red operativa de equipos

---

seguridad gestionados, los proveedores de mercados en línea, motores de búsqueda en línea y plataformas de servicios de redes sociales, y los proveedores de servicios de confianza (DO L, 2024/2690, 18.10.2024).

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

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

9 Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE) n.º 168/2013 y el Reglamento (UE) 2019/1020 y la Directiva (UE) 2020/1828 (Reglamento de Ciberresiliencia) (DO L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

10 Reglamento (UE) 2025/38 del Parlamento Europeo y del Consejo, de 19 de diciembre de 2024, por el que se establecen medidas destinadas a reforzar la solidaridad y las capacidades en la Unión a fin de detectar ciberamenazas e incidentes, prepararse y responder a ellos y por el que se modifica el Reglamento (UE) 2021/694 (Reglamento de Cibersolidaridad) (DO L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

11 Reglamento Delegado (UE) 2024/1366 de la Comisión, de 11 de marzo de 2024, por el que se completa el Reglamento (UE) 2019/943 del Parlamento Europeo y del Consejo mediante el establecimiento de un código de red sobre normas sectoriales específicas para los aspectos relativos a la ciberseguridad de los flujos transfronterizos de electricidad (DO L, 2024/1366, 24.5.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1366/oj).

12 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 (DO L 333 de 27.12.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

13 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, ELI: http://data.europa.eu/eli/dir/2013/40/oj).

14 Reglamento (UE) 2023/1543 del Parlamento Europeo y del Consejo, de 12 de julio de 2023, sobre las órdenes europeas de producción y las órdenes europeas de conservación a efectos de prueba electrónica en procesos penales y de ejecución de penas privativas de libertad a raíz de procesos penales, y Directiva (UE) 2023/1544 del Parlamento Europeo y del Consejo, de 12 de julio de 2023, por la que se establecen normas armonizadas para la designación de establecimientos designados y de representantes legales a efectos de recabar pruebas electrónicas en procesos penales (DO L 191 de 28.7.2023, p. 118, ELI: http://data.europa.eu/eli/reg/2023/1543/oj).

15 JOIN(2022) 49 final.

militares de respuesta a emergencias informáticas (MICNET) y de la Conferencia de cibermandos de la UE, y prevé la creación de un Centro de Coordinación de la Ciberdefensa de la UE (EUCDCC). Existen otros mecanismos de conciencia situacional y de respuesta a las crisis no relacionados con la ciberseguridad en algunos de los sectores críticos enumerados en los anexos I y II de la Directiva (UE) 2022/2555. La «Recomendación del Consejo sobre un plan director para coordinar la respuesta a escala de la Unión en caso de perturbaciones de infraestructuras críticas con importancia transfronteriza significativa»[16] prevé la cooperación entre los agentes pertinentes cuando un incidente afecte tanto a aspectos físicos como a la ciberseguridad de las infraestructuras críticas.

(7) En la Unión, entre los agentes pertinentes que tienen responsabilidades de gestión de crisis de ciberseguridad figuran la Comisión, el SEAE, incluida la Capacidad Única de Análisis de Inteligencia (SIAC), la Agencia de la Unión Europea para la Ciberseguridad (ENISA), el Equipo de respuesta a emergencias informáticas de las instituciones, órganos y organismos de la Unión (CERT-EU), Europol a través de su Centro Europeo de Ciberdelincuencia (EC3), la Red de organizaciones de enlace para la gestión de cibercrisis (EU-CyCLONe), la Red de equipos de respuesta a incidentes de seguridad informática (CSIRT), el Centro de Satélites de la Unión Europea (Satcen), el Centro de Supervisión de la Seguridad de Galileo y la red de delegaciones de la Unión. Estos agentes de la Unión deben determinar de forma conjunta los ámbitos de cooperación y contribuir a la aplicación del marco de gestión de crisis de ciberseguridad de la Unión, de conformidad con sus competencias en virtud de la legislación aplicable.

(8) Es necesaria una Recomendación actualizada que establezca un plan director sobre ciberseguridad («Plan Director de Ciberseguridad») para proporcionar unas orientaciones claras y accesibles que expliquen qué es una crisis cibernética a escala de la Unión, cómo se activa el marco de gestión de crisis y cuáles son las funciones de los agentes y mecanismos pertinentes en la Unión, así como la interacción entre estos agentes y mecanismos en todo el ciclo de vida de las crisis de ciberseguridad. El Plan Director de Ciberseguridad debe considerarse en el contexto más amplio de las relaciones civiles, militares y entre la UE y la OTAN.

(9) La presente Recomendación complementa el dispositivo de respuesta política integrada a las crisis (Dispositivo RPIC) y a mecanismos de crisis más amplios de la Unión, como el sistema de alerta rápida general de la Comisión (ARGUS), el Mecanismo de Protección Civil de la Unión con el apoyo del Centro de Coordinación de la Respuesta a Emergencias (CECRE), el Mecanismo de Respuesta a las Crisis (CRM) del Servicio Europeo de Acción Exterior, así como otros procesos, como los descritos en el conjunto de instrumentos de la UE contra las amenazas híbridas[17] y en el Protocolo revisado de la UE para contrarrestas las amenazas híbridas. También complementa y debe ser coherente con la Recomendación del Consejo sobre un plan director para coordinar la respuesta a escala de la Unión en caso de perturbaciones de infraestructuras críticas con importancia transfronteriza significativa («Plan Director de Infraestructuras Críticas»), que abarca la resiliencia física no cibernética y tiene por objeto mejorar la coordinación de la respuesta a escala de la Unión en este ámbito.

---

16 DO C, C/2024/4371, 5.7.2024.

17 Conclusiones del Consejo sobre un marco para una respuesta coordinada de la UE a las campañas híbridas, de 22 de junio de 2022.

(10) Debe fomentarse un enfoque global e integrado de la gestión de crisis en todos los sectores y niveles de gobernanza. Debe reforzarse la gestión intersectorial de crisis a escala de la Unión para permitir una respuesta integrada a las crisis, en particular en los casos en que los ciberincidentes tengan consecuencias en la vida real. Cuando los incidentes de ciberseguridad formen parte de una campaña o crisis híbrida más amplia, los agentes pertinentes deben apoyar los esfuerzos para desarrollar una visión de la situación unificada en varios sectores y ámbitos. La Recomendación contribuye a medidas de preparación más amplias que la Unión requiere frente a las amenazas híbridas multidimensionales (en consonancia con los principios integrados en la Estrategia de Preparación de la Unión).

(11) La seguridad de las infraestructuras digitales críticas es fundamental para la resiliencia de la economía, la sociedad y la defensa de la Unión. Las entidades que entran en el ámbito de aplicación de la Directiva (UE) 2022/2555, incluidas aquellas que suministran cables de comunicación submarinos, deben adoptar medidas para proteger la seguridad física y ambiental de las redes, así como los sistemas de información sobre la base de un enfoque que contemple todas las amenazas, como fallos del sistema, errores humanos, actos malintencionados o fenómenos naturales. Además, dichas entidades deben notificar los incidentes, también los relacionados con los cables de comunicación submarinos, a los CSIRT o, en su caso, a la autoridad competente. Aunque los principios fundamentales en los que se basa el Plan Director de Ciberseguridad son pertinentes para la seguridad de los cables submarinos, los mecanismos que establece no son suficientemente exhaustivos para cubrir el ciclo completo de resiliencia frente a las crisis. Su naturaleza específica justifica un esfuerzo concertado y a medida para abordar las necesidades de vigilancia integrada de las amenazas y conocimiento de la situación de las cuencas marítimas alrededor de la UE, inversiones estratégicas para crear redundancias y un enfoque común europeo para aumentar las capacidades de reparación y recuperación. La Estrategia de Seguridad Marítima de la Unión Europea incluye acciones para mejorar la ciberseguridad en el ámbito marítimo y mejorar la vigilancia y la protección de las infraestructuras marítimas críticas, incluidos los cables submarinos. Para la gestión de crisis a escala de la Unión, una red específica de puntos de contacto nacionales y estrechas interacciones civiles y militares, también con la OTAN, sería una vía que considerar.

(12) La preparación ante una crisis requiere una evaluación exhaustiva de los riesgos que contemple todos los peligros y amenazas, dada la convergencia de los intereses económicos y de seguridad de la UE. Un conocimiento común de la situación de la Unión entre los Estados miembros y las entidades de la Unión, facilitado por el acuerdo sobre una taxonomía común y unos canales de comunicación seguros, debe permitir una respuesta coordinada y fundamentada a los incidentes de ciberseguridad potenciales y a gran escala, así como la disuasión de los agentes de amenaza persistentes. Sobre la base del principio de la necesidad de conocer y teniendo en cuenta la importancia de la confianza en el intercambio de información, los grupos de Estados miembros con diferentes configuraciones y, en su caso, las entidades pertinentes de la Unión, podrían desear cooperar y compartir información pertinente para la gestión de ciberincidentes. Los Estados miembros y las entidades de la Unión que comparten amenazas, riesgos y diferencias de madurez deben facilitar la determinación de las prioridades adecuadas para una inversión sólida y acciones tangibles que conduzcan a una mayor ciberresiliencia.

(13) De conformidad con el artículo 6 del Reglamento (UE) 2019/881, la ENISA, en estrecha colaboración con los Estados miembros, prepara un informe periódico y

detallado sobre la situación técnica de la ciberseguridad en la UE relativo a incidentes y ciberamenazas. Este informe se denomina Informe conjunto de evaluación de la ciberseguridad de la UE (EU-JCAR) y se elabora con Europol/EC3 y el CERT-EU, con el objetivo de reforzar la preparación de la Unión, ya que proporciona un conocimiento de la situación basado en un análisis de incidentes y ciberamenazas.

(14) Las infraestructuras críticas clave, como la energía, el transporte, la infraestructura digital, la sanidad o los servicios financieros, así como las soluciones de seguridad implantadas para protegerla, suelen gestionarlas empresas privadas. La protección de esta infraestructura frente a los ciberincidentes a gran escala requiere una estrecha colaboración entre las entidades públicas y privadas, también los fabricantes y los desarrolladores de código abierto, basada en la confianza y en procedimientos claros y específicos para el intercambio y la difusión de información, así como para la coordinación de la respuesta.

(15) Los ejercicios de ciberseguridad de la Unión son una herramienta muy eficaz en los procedimientos de prueba y los mecanismos de cooperación, mejorando así la preparación. Dado que los ejercicios requieren un uso intensivo de recursos, el programa de ejercicios debe racionalizarse y consolidarse lo más posible. Además, deben tener en cuenta las hipótesis desarrolladas en las evaluaciones de riesgos coordinadas de la Unión y en otras iniciativas pertinentes.

(16) Las infraestructuras digitales europeas tienen muchas dependencias técnicas profundamente arraigadas y estas deben abordarse para garantizar la continuidad de las actividades en caso de crisis. Esto afecta, por ejemplo, al sistema de nombres de dominio (DNS), que es un componente crucial que sustenta el funcionamiento de internet. Los servicios de resolución de DNS son esenciales para acceder a internet, incluso durante una crisis cibernética importante, ya que traducen los nombres de dominios de internet en direcciones IP. La Directiva (UE) 2022/2555 anima a que las partes interesadas pertinentes adopten una estrategia de diversificación de la resolución de DNS. También anima a los Estados miembros a fomentar el desarrollo y el uso de un servicio de resolución de DNS europeo público y seguro como medida clave para garantizar la preparación y la resiliencia frente a las crisis.

(17) Además, para mejorar la resiliencia de otros componentes críticos, como el sistema de enrutamiento, y garantizar su funcionalidad durante las crisis de ciberseguridad graves, es esencial aplicar de forma oportuna las mejores prácticas correspondientes y las normas disponibles más recientes. En consecuencia, el Reglamento de Ejecución (UE) 2024/2690 encomienda la creación de un foro multilateral para determinar las mejores normas disponibles y técnicas de implantación para los elementos de ciberseguridad esenciales y fomenta la participación de las entidades pertinentes.

(18) Para detectar de forma eficaz las actividades malintencionadas en las cadenas de suministro mundiales cada vez más complejas que pueden tener un impacto en la Unión, es necesario un enfoque coordinado. Esto es especialmente pertinente en los ámbitos en los que la Unión depende de la tecnología de proveedores de alto riesgo sujetos a la jurisdicción de un tercer país que exige comunicar a sus autoridades información sobre vulnerabilidades de *software* o *hardware* antes de que se sepa que están siendo explotadas. Los agentes patrocinados por los Estados también pueden preposicionarse en infraestructuras críticas con la intención de causar perturbaciones en un momento posterior, por ejemplo durante un conflicto. Resulta difícil detectarlo utilizando métodos tradicionales, ya que los agentes de amenazas disimulan sus actividades mezclando el tráfico legítimo y fusionando técnicas como la técnica

conocida como «living off the land» en la que se utilizan herramientas y procesos legítimos para ocultar actividades malintencionadas. Lo mismo puede decirse de terceros países en los que, según declaraciones públicas de la Unión o de sus Estados miembros, agentes de amenaza que operan fuera de los territorios de estos países han llevado a cabo actividades informáticas malintencionadas contra la Unión. Las cadenas de suministro deben ser más resilientes y estar más diversificadas y, al mismo tiempo, mantener una base común de preparación.

(19) A nivel técnico, los CSIRT, los servicios policiales y los centros cibernéticos nacionales y transfronterizos que se crearán en virtud del Reglamento (UE) 2025/38 desempeñan un papel esencial en la detección de incidentes, ciberamenazas y vulnerabilidades, el apoyo a las atribuciones técnicas y la recuperación de los ciberataques. Unas disposiciones de procedimiento eficaces son esenciales para la colaboración entre la red de CSIRT y EU-CyCLONe, tal como establece la Directiva (UE) 2022/2555. El Mecanismo Europeo de Alerta de Ciberseguridad tiene el objetivo de apoyar el desarrollo de capacidades avanzadas para que la Unión mejore las capacidades de detección, análisis y tratamiento de datos en relación con las ciberamenazas y la prevención de incidentes en la Unión.

(20) En términos de respuesta inmediata, los mecanismos a disposición de los Estados miembros incluyen la Reserva de Ciberseguridad de la UE y las acciones de apoyo para la asistencia mutua establecidas en virtud del Reglamento (UE) 2025/38, los equipos de respuesta rápida contra amenazas híbridas y los equipos de respuesta telemática rápida de la Cooperación Estructurada Permanente (CEP), así como los mecanismos previstos para los aliados de la OTAN. Además, el Protocolo de Respuesta Policial ante Emergencias de la UE apoya a los servicios policiales de la UE para dar una respuesta inmediata a los ciberataques transfronterizos importantes mediante una evaluación rápida, el intercambio seguro y oportuno de información crítica y la coordinación eficaz de los aspectos internacionales de sus investigaciones, incluida la prevención de conflictos a nivel policial y la coordinación con socios no policiales. Lograr una visión clara de las opciones de respuesta disponibles en caso de ciberincidentes y actividades híbridas y cómo se utilizan puede asegurar una asignación eficiente de los recursos y evitar su duplicación. En consecuencia, en virtud del Reglamento (UE) 2025/38, los Estados miembros deben informar a la red de CSIRT y a la EU-CyCLONe cuando soliciten servicios de la Reserva de Ciberseguridad de la UE.

(21) Una lucha eficaz contra la ciberdelincuencia es esencial para la ciberseguridad. La disuasión no puede lograrse únicamente a través de la resiliencia, sino que también requiere la identificación, la persecución y la respuesta a los delincuentes. La cooperación a través de plataformas y sistemas técnicos adaptados y el intercambio de información pertinente entre los agentes de ciberseguridad, las entidades de ciberdiplomacia y los servicios policiales son, por tanto, esenciales para garantizar una comprensión global del panorama de amenazas y poder responder de una manera coherente y coordinada.

(22) Las crisis generan una incertidumbre que los adversarios pueden aprovechar fácilmente para difundir desinformación y sembrar la desconfianza. Para contrarrestar esta situación, es esencial una comunicación pública clara y coherente sobre la situación y las medidas que se están tomando para remediarla. Una comunicación estratégica coordinada también puede apoyar las acciones diplomáticas dirigidas a los agentes de amenaza persistentes y la elaboración de una narrativa sobre las amenazas a

la Unión, sus acciones disuasorias y la necesidad de promover un comportamiento responsable de los Estados en el ciberespacio.

(23) Para una gestión eficaz de las crisis, es necesario determinar las soluciones comunes de comunicación seguras para el ámbito cibernético y aplicarlas en toda la Unión, también cuando sea necesario para el intercambio de información clasificada de la UE. A petición del Consejo, la Comisión y otras entidades pertinentes de la Unión hicieron un inventario de las herramientas de comunicación seguras existentes y presentaron los resultados en diciembre de 2022. Las entidades de la Unión tienen en marcha varios esfuerzos independientes para desarrollar capacidades de comunicación seguras en una crisis que requieren una mejor coordinación y movilización. Esto incluye el establecimiento de un sistema de europeo de comunicación crítica para aumentar la resiliencia de la infraestructura de comunicación pública frente a las interferencias malintencionadas y mejorar la cooperación operativa diaria, también a través de las fronteras.

(24) El entorno de seguridad de la Unión requiere un planteamiento de preparación y disposición en los ámbitos civil y militar que abarque todos los riesgos, la Administración en su conjunto y la sociedad en su conjunto. Los organismos militares dependen de infraestructuras civiles críticas, como las comunicaciones, la energía, la salud, el transporte y la logística. En consecuencia, y como se subraya en la política de ciberdefensa de la UE[18], la ciberseguridad de la UE requiere una mayor cooperación y sinergias entre las capacidades de preparación y respuesta de las redes civiles y militares, también en caso de ataque armado. Los agentes de ciberseguridad deben colaborar en todos los compartimentos institucionales y operativos para anticipar y abordar la amenaza de perturbaciones multisectoriales y multidimensionales, en consonancia con los principios que (se integrarán) en la Estrategia de Preparación de la Unión. Además, la actividad informática malintencionada desempeña un papel cada vez más importante en campañas híbridas más amplias contra la Unión, sus Estados miembros y sus socios estratégicos. Por tanto, es necesaria una cooperación más estrecha entre la Unión y la OTAN.

(25) En la comunidad militar, el futuro Centro de Coordinación de la Ciberdefensa de la UE y la Capacidad Única de Análisis de Inteligencia (SIAC) dentro del Servicio Europeo de Acción Exterior, la red operativa de equipos militares de respuesta a emergencias informáticas (MICNET) y la Conferencia de Cibermandos de la UE, facilitada por la Agencia Europea de Defensa (AED), así como los proyectos pertinentes en el marco de la Cooperación Estructurada Permanente (CEP), representan agentes e iniciativas importantes para la coordinación y la cooperación en materia de preparación para la detección, la disuasión y la defensa contra las ciberamenazas que afectan a la Unión y a los Estados miembros y la recuperación frente a ellas. Por consiguiente, debe fomentarse la cooperación entre los agentes civiles y militares, como la cooperación entre la EU-CyCLONe y la Conferencia de cibermandos de la UE, así como la posible colaboración entre la red operativa de equipos militares de respuesta a emergencias informáticas (MICNET) y la red de CSIRT.

(26) La cooperación con organizaciones internacionales y países socios estratégicos fuera de la Unión refuerza las capacidades de ciberseguridad de la Unión. Al fomentar la cooperación internacional, la Unión y sus socios pueden garantizar un conocimiento

[18] Política de ciberdefensa de la UE; JOIN(2022) 49 final.

común de la situación y la coherencia en la gestión de las crisis de ciberseguridad, así como una sólida postura de ciberseguridad, contribuyendo a un ciberespacio mundial, abierto, estable, seguro y resiliente. Esta colaboración debe basarse en la confianza y el objetivo compartido de proteger las infraestructuras críticas y los servicios esenciales de las ciberamenazas, en particular mediante la promoción de un comportamiento responsable del Estado en el ciberespacio basado en el marco de las Naciones Unidas (ONU) y la exigencia de responsabilidades a los agentes de amenaza por su comportamiento irresponsable e ilegal en el ciberespacio. Las medidas de ciberdiplomacia contribuyen a la disuasión y a la respuesta ante las actividades informáticas malintencionadas y prevén la coordinación y la cooperación con países socios estratégicos internacionales.

HA ADOPTADO LA PRESENTE RECOMENDACIÓN:

I: Objetivo, ámbito de aplicación y principios del marco de gestión de crisis de ciberseguridad de la UE

1) La presente Recomendación establece el marco de la Unión para la gestión de crisis de ciberseguridad en el contexto de la preparación general de la UE frente a amenazas híbridas multidimensionales. En el anexo 1 se ilustra y resume cómo un incidente puede pasar a ser un incidente a gran escala y, a su vez, convertirse en una crisis a escala de la UE, incluso cuando este incidente coincida con otras amenazas híbridas que requieran interacción entre las respuestas necesarias. El marco de gestión de crisis de ciberseguridad debe permitir que los agentes pertinentes de la Unión, también las entidades y las redes, comprendan cómo interactuar y hacer el mejor uso posible de los mecanismos existentes mencionados en el anexo II a lo largo de todo el ciclo de vida de la gestión de crisis. Además, recomienda a estos agentes de la Unión la forma de mejorar la eficacia de los mecanismos existentes.

2) La Unión y sus Estados miembros deben seguir el Plan Director de Ciberseguridad en la gestión de una crisis derivada de un incidente de ciberseguridad a gran escala, tal como se define en el artículo 6, punto 7), de la Directiva (UE) 2022/2555, que afecte al correcto funcionamiento del mercado interior o plantee riesgos graves para la seguridad y la protección públicas de las entidades o los ciudadanos de varios Estados miembros o de la Unión en su conjunto («crisis de ciberseguridad»).

3) Cuando un incidente de ciberseguridad detectado a nivel técnico por un CSIRT o un centro cibernético dé lugar a una escalada con arreglo a los procedimientos internos de la red de CSIRT, debe compartirse la información adecuada con la EU-CyCLONe con arreglo a las disposiciones de procedimiento pertinentes, que, a su vez, debe considerar si representa un incidente a gran escala potencial o en curso, tal como se define en el artículo 6, punto 7), de la Directiva (UE) 2022/2555. La determinación de si existe o ha dejado de existir una crisis de ciberseguridad como consecuencia de este incidente a gran escala debe llevarse a cabo de conformidad con la Decisión de Ejecución (UE) 2018/1993 y, en particular, con sus artículos 4 y 5.

4) De conformidad con los principios de proporcionalidad, subsidiariedad, complementariedad y confidencialidad de la información establecidos en el anexo III, los Estados miembros y las entidades de la Unión deben profundizar su cooperación en materia de gestión de crisis de ciberseguridad, fomentando la confianza mutua y aprovechando las redes y mecanismos existentes. Aunque el Plan Director de Ciberseguridad no interfiere en la manera en que las entidades definen sus procedimientos internos, cada entidad debe definir claramente las interfaces que

utilizan para trabajar con otras entidades. Estas interfaces deben acordarse de manera conjunta entre las entidades afectadas y estar claramente documentadas.

5) El Plan Director de Ciberseguridad debe aplicarse de manera coherente con el Plan Director de Infraestructuras Críticas, en particular en caso de incidentes que afecten tanto a la resiliencia física como a la ciberseguridad de las infraestructuras críticas[19]. Cuando existan medidas sectoriales de gestión de crisis que abarquen incidentes de ciberseguridad, dichas medidas deben aplicarse de manera coherente con la presente Recomendación.

II: Prepararse para una crisis de ciberseguridad a escala de la Unión

a) Conocimiento de la situación e intercambio de información

6) Los datos verificados y fiables, incluidas las tendencias en materia de incidentes, tácticas, técnicas y procedimientos, y las vulnerabilidades aprovechadas activamente deben constituir la base de un conocimiento común de la situación entre los Estados miembros y las entidades de la Unión sobre el panorama de las ciberamenazas. Los Estados miembros y las entidades de la Unión deben utilizar este conocimiento compartido para anticipar, prepararse y detectar ciberataques, en consonancia con sus respectivos ámbitos de responsabilidad. Este conocimiento común de la situación debe:

   a) aplicarse a todos los sectores críticos mencionados en la Directiva (UE) 2022/2555, en particular las comunicaciones, la infraestructura digital, la energía, el transporte, las finanzas, el espacio y la salud, y también deben aplicarse, a través del CERT-EU, a las redes y sistemas de las entidades de la Unión de conformidad con el Reglamento (UE, Euratom) 2023/2841;

   b) basarse en conjuntos de datos diversificados e integrados de alta calidad que se recopilen, se traten y se compartan en tiempo real;

   c) tenerse en cuenta en el informe conjunto de evaluación de la ciberseguridad (EU-JCAR) y en otros productos pertinentes;

   d) tener en cuenta las amenazas híbridas conexas, incluida la manipulación de información y la injerencia por parte de agentes extranjeros, así como la desinformación;

   e) apoyar acciones y medidas de respuesta a corto plazo, así como contribuir a la planificación de políticas a largo plazo en el contexto de la preparación y la disuasión;

   f) (vincularse a otras evaluaciones de riesgos y amenazas realizadas periódicamente y reforzadas por la Estrategia de Preparación de la Unión con el fin de garantizar sinergias y la simplificación de las obligaciones de información para los Estados miembros).

7) La EU-CyCLONe y la red de CSIRT deben:

   a) cooperar para mejorar el intercambio de información entre el nivel técnico y operativo, así como el conocimiento de la situación en su conjunto;

   b) seguir construyendo un clima de confianza entre los miembros;

[19] . El Plan Director de Infraestructuras Críticas detalla la coordinación en tales casos en la sección 4 de la parte I de su anexo.

c) hacer pleno uso de las herramientas disponibles para el intercambio de información.

8) Los Estados miembros y las entidades pertinentes de la Unión deben mejorar las formas de coordinarse y asociarse con el sector privado, en particular las comunidades de código abierto y los fabricantes, con el fin de mejorar el intercambio de información, basándose en los centros de puesta en común y análisis de información existentes a nivel nacional y de la UE, mejorar la capacidad de ciberseguridad y responder a los incidentes de ciberseguridad, en particular mediante mesas redondas con EUCyCLONe y la red de CSIRT.

9) Los Estados miembros y las entidades pertinentes de la Unión podrían decidir, con el fin de promover la cooperación y reforzar la confianza, y basándose en los mecanismos de intercambio de información sobre ciberseguridad de la Directiva (UE) 2022/2555 y las disposiciones del Reglamento (UE) 2025/38 relativas a los centros cibernéticos, crear grupos colaborativos voluntarios sobre la base de la necesidad de saber cuando existan preocupaciones comunes, como la disuasión, la detección o la respuesta a un tipo particular de amenaza a la que se enfrentan de manera única. Tales grupos deben respetar el mandato de los agentes pertinentes, así como las estructuras ya establecidas. Estos grupos colaborativos podrían pedir a las entidades de la Unión que faciliten su colaboración, también a través de la infraestructura adecuada.

10) Los Estados miembros, a través del Grupo de Cooperación SRI establecido por la Directiva (UE) 2022/2555, deben elaborar, en un plazo de doce meses a partir de la adopción del Plan Director de Ciberseguridad, una taxonomía común con respecto a la gestión de crisis de ciberseguridad y proporcionar una guía sobre el tratamiento seguro y el intercambio de información relacionada con los incidentes y las crisis de ciberseguridad, incluida una sección dedicada a determinar el nivel de confidencialidad de esta información (categorización).

11) A la hora de determinar el nivel de confidencialidad de la información disponible, los Estados miembros y las entidades pertinentes de la Unión deben tener en cuenta el posible impacto que una clasificación excesiva puede tener en el intercambio voluntario de información y la consecución de un conocimiento común de la situación. A la hora de compartir información no clasificada, los Estados miembros deben hacer pleno uso de las plataformas existentes para la cooperación técnica y operativa, como las que utilizan la red de CSIRT y la EU-CyCLONe.

b) Ejercicios comunes

12) Los Estados miembros y las entidades pertinentes de la Unión deben desarrollar un ciclo continuo y eficiente de ejercicios de ciberseguridad con el fin de prepararse para las crisis de ciberseguridad y mejorar la eficiencia organizativa. Estos ejercicios deben basarse en las hipótesis elaboradas sobre la base de evaluaciones de riesgos coordinadas a escala de la UE, incluidas las relativas a crisis multisectoriales. El ciclo continuo de ejercicios de ciberseguridad debe tener en cuenta el Mecanismo de Protección Civil de la Unión y otros mecanismos de la Unión de respuesta a las crisis. Debe garantizar la aplicación efectiva de las lecciones extraídas de los ejercicios.

13) Los agentes pertinentes de la Unión podrían llevar a cabo ejercicios más pequeños para probar sus interacciones e interfaces en caso de una escalada de ciberincidentes.

14) Se invita a los servicios de la Comisión, al SEAE y a la ENISA a que organicen un ejercicio para probar el Plan Director de Ciberseguridad en un plazo de dieciocho meses a partir de la adopción del Plan en el que participen todos los agentes pertinentes, incluido el sector privado.

c) Capacidades de resolución de DNS

15) Los Estados miembros, las entidades pertinentes de la Unión, así como las entidades privadas, como los operadores de infraestructuras críticas, deben mejorar su estrategia de diversificación de la resolución de los sistemas de nombres de dominio (DNS), incluido el uso de al menos una infraestructura DNS con sede en la Unión, como el DNS4EU, para garantizar una resolución de DNS fiable durante las crisis graves. La ENISA y la EU-CyCLONe deben elaborar y publicar unas directrices de conmutación automática de emergencia que describan los pasos para pasar a la infraestructura DNS con sede en la Unión en caso de fallo de otros servicios de DNS, garantizando la continuidad de los servicios críticos durante una crisis.

16) Además, los centros cibernéticos nacionales y los transfronterizos deben compartir información pertinente sobre amenazas con estas infraestructuras de DNS con sede en la Unión para ayudarles a proporcionar un alto nivel de protección frente a amenazas específicas de la Unión y, de este modo, seguir aumentando las capacidades para detectar y mitigar amenazas específicas de la Unión.

17) Para reforzar en general la seguridad y la disponibilidad de infraestructuras críticas de internet, también durante las crisis, los Estados miembros deben promover activamente la participación de todas las partes interesadas pertinentes, incluidas las que no se abordan directamente en el acto de aplicación de la SRI 2, en el foro multilateral encargado de determinar las mejores normas disponibles y las técnicas de implantación de medidas esenciales de seguridad de las redes. Además, los Estados miembros deben considerar la posibilidad de participar en el foro y adoptar ellos mismos las directrices recomendadas.

d) Recursos

18) Los Estados miembros deben hacer pleno uso de los recursos financieros disponibles para la ciberseguridad proporcionados por los programas pertinentes de la Unión.

III: Detectar un incidente que podría convertirse en una crisis de ciberseguridad

19) Para afrontar la creciente complejidad de los ciberincidentes y las dificultades cada vez mayores para su detección, tanto las entidades públicas como las privadas deben aplicar estrategias de detección basadas en amenazas en todas sus infraestructuras digitales con el fin de identificar un posible posicionamiento previo que pueda aprovecharse posteriormente con fines de perturbación. Cuando se identifiquen operaciones encubiertas, las entidades deben compartir de forma proactiva la información pertinente con sus socios mucho antes de que las situaciones se conviertan en crisis.

20) Todos los agentes deben aportar, de conformidad con sus respectivos mandatos y sobre la base de un enfoque que contemple todos los riesgos, información que indique una posible crisis de ciberseguridad a las redes pertinentes.

21) La red de CSIRT y la EU-CyCLONe deben establecer disposiciones de procedimiento en caso de incidente de ciberseguridad a gran escala, potencial o en curso, con el fin de garantizar la coordinación técnica y operativa y la información oportuna y pertinente a nivel político.

22) La red de CSIRT debe asesorar a la EU-CyCLONe sobre si un incidente de ciberseguridad observado puede considerarse un incidente a gran escala potencial o en curso.

23) Los centros cibernéticos transfronterizos, ya establecidos o pendientes de creación en virtud del Reglamento (UE) 2025/38, deben contribuir con información pertinente a los mecanismos de la Unión en caso de incidente de ciberseguridad a gran escala, potencial o en curso, sobre la base de un enfoque que contemple todos los peligros, incluidos los daños físicos a infraestructuras críticas que comprometan la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados o de los servicios ofrecidos por las redes y los sistemas de información, o accesibles a través de ellos.

24) Cuando se detecte un incidente de ciberseguridad potencial o a gran escala con impacto multisectorial:

a) la Comisión debe facilitar el flujo de la información necesaria entre los puntos de contacto para los mecanismos de crisis horizontales y sectoriales pertinentes a escala de la Unión mencionados en el anexo II y la EU-CyCLONe;

b) las entidades pertinentes de la Unión deben apoyar a la EU-CyCLONe en la evaluación de las consecuencias para los sectores y la población.

IV: Responder a una crisis de ciberseguridad a escala de la Unión

25) En caso de una crisis de ciberseguridad establecida en el marco de la RPIC, todos los agentes deben responder en estrecha coordinación con otras entidades que respondan a amenazas híbridas más amplias con una perspectiva de la Administración en su conjunto de la siguiente manera:

a) el Estado o los Estados miembros afectados y la red de CSIRT deben cooperar para restablecer de forma rápida los sistemas comprometidos, garantizando una perturbación operativa mínima;

b) La EU-CyCLONe, en colaboración con la red de CSIRT, debe proporcionar información clara al nivel político sobre el impacto, las posibles consecuencias y las medidas de respuesta y reparación del incidente, en particular contribuyendo al Informe de la Capacidad de Conocimiento y Análisis Integrados de la Situación (ISAA) en el marco del Dispositivo RPIC;

c) la Comisión, en colaboración con el Alto Representante, cuando proceda, debe garantizar la coherencia y la coordinación entre las respuestas a la crisis y las acciones conexas de respuesta a la crisis a escala de la Unión, en particular los mecanismos sectoriales de gestión de crisis pertinentes de la Unión mencionados en el anexo 2, y en relación con la solicitud de asistencia a través del Mecanismo de Protección Civil de la Unión;

d) la Presidencia del Consejo debe considerar la posibilidad de invitar a la persona que presida la EU-CyCLONe a las mesas redondas informales y a otras reuniones pertinentes del Consejo en el marco del Dispositivo RPIC;

e) el Consejo, con el apoyo de la EU-CyCLONe y las entidades pertinentes de la Unión, debe coordinar los esfuerzos de comunicación pública, también para garantizar que la situación de crisis no se utilice para difundir información inexacta;

f) el Alto Representante, en estrecha cooperación con la Comisión y otras entidades pertinentes de la Unión, debe apoyar la toma de decisiones en el Consejo, en particular mediante análisis e informes, sobre el uso de posibles medidas en el marco del conjunto de instrumentos de ciberdiplomacia. Esto permitirá el uso de todo el espectro de herramientas de la Unión disponibles para prevenir, disuadir y responder a las actividades informáticas malintencionadas, reforzando su sólida postura de ciberseguridad y promoviendo la paz, la seguridad y la estabilidad internacionales en el ciberespacio;

g) la Comisión, el Alto Representante y los Estados miembros también deben aprovechar herramientas económicas como las prohibiciones comerciales de una manera más eficaz para prevenir, disuadir y responder mejor a las actividades informáticas malintencionadas persistentes por parte de agentes estatales.

26) Cuando un usuario de los servicios prestados por la Reserva de Ciberseguridad de la UE[20] solicite servicios dicha Reserva de conformidad con el artículo 15 del Reglamento (UE) 2025/38, y sin perjuicio de cualquier futuro acto de ejecución en virtud de dicho Reglamento:

a) los servicios deben implementarse en un plazo de veinticuatro horas a partir de la solicitud;

b) la Comisión y el Alto Representante deben garantizar la coordinación con medidas adicionales, en consonancia con el conjunto de instrumentos contra las amenazas híbridas[21], en el caso de actividades informáticas malintencionadas que formen parte de una campaña híbrida más amplia;

c) en el caso de actividades informáticas malintencionadas con una dimensión militar, el Estado miembro solicitante debe informar de su solicitud a la Conferencia de cibermandos de la Unión.

27) En caso de incidente de ciberseguridad a gran escala que afecte al correcto funcionamiento de los servicios espaciales esenciales para la seguridad de la Unión o de sus Estados miembros, la EU-CyCLONe debe informar al Alto Representante con vistas a coordinar la posible respuesta con la arquitectura de respuesta a amenazas espaciales establecida de conformidad con la Decisión (PESC) 2021/698 del Consejo.

V: Recuperación de una crisis de ciberseguridad

28) Los Estados miembros, las entidades y redes pertinentes de la Unión deben colaborar en la fase de recuperación basándose en las lecciones extraídas de los ejercicios realizados, así como en los informes de incidentes, en particular en el contexto del

---

20 La Reserva de Ciberseguridad de la UE es un mecanismo que consiste en servicios de proveedores de servicios de seguridad gestionados de confianza para, previa petición, apoyar la respuesta e iniciar acciones de recuperación en caso de incidentes de ciberseguridad significativos, a gran escala o equivalentes a gran escala que afecten a los Estados miembros, a las instituciones, órganos y organismos de la Unión o a terceros países asociados al Programa Europa Digital.

21 El conjunto de instrumentos contra las amenazas híbridas es un marco para una respuesta coordinada a las campañas híbridas que afectan a la UE y a sus Estados miembros, que incluye, por ejemplo, medidas preventivas, de cooperación, de estabilidad, restrictivas y de recuperación, y apoyo a la solidaridad y la asistencia mutua.

Mecanismo Europeo de Revisión de Incidentes de Ciberseguridad establecido por el Reglamento (UE) 2025/38.

VI: Comunicación segura

29) Sobre la base de un inventario de las herramientas de comunicación segura existentes[22], la Comisión, el Alto Representante, la EU-CyCLONe, la red de CSIRT y las entidades pertinentes de la Unión deben acordar para finales de 2026 un conjunto interoperable de soluciones de comunicación seguras para los agentes pertinentes de la Unión. Estas soluciones deben abarcar toda la gama de modos de comunicación necesarios (voz, datos, videoconferencia, mensajería, colaboración, intercambio de documentos y consulta). Las soluciones deben reflejar principios clave como los intereses de seguridad de la Unión, la soberanía tecnológica y la confidencialidad, así como características como la facilidad de uso, la seguridad desde el diseño, la certificación por parte de los organismos europeos de seguridad de la información, el cifrado de extremo a extremo, la autenticación, la disponibilidad y la criptografía poscuántica. Las soluciones deben cumplir los requisitos comúnmente definidos para la protección de la información delicada no clasificada e incluir herramientas para el intercambio de información RESTREINT UE/EU RESTRICTED.

30) Sobre esta base, los agentes a escala de la Unión deben utilizar soluciones basadas en el protocolo Matrix para la comunicación en tiempo real. El Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad, creado en virtud del Reglamento (UE) 2021/887, sin perjuicio del futuro marco financiero plurianual, debe considerar la posibilidad de proporcionar financiación a través del programa Europa Digital para ayudar a los Estados miembros a implantar estas herramientas.

31) En particular, las entidades de la UE y los Estados miembros deben desarrollar contingencias en caso de crisis graves en las que los canales de comunicación normales que dependen de internet o de las redes de telecomunicaciones se vean perturbados o no estén disponibles.

32) A medio plazo, para dar una respuesta eficaz a las crisis, deben establecerse mecanismos de comunicación e intercambio de información entre los servicios policiales y las redes de ciberseguridad, en particular a nivel técnico. Estos mecanismos deben respetar el papel de cada parte y evitar interferir en las operaciones en curso. La Comisión colabora con los Estados miembros para crear el Sistema Europeo de Comunicación Crítica, que debería conectar de aquí a 2030 las redes de comunicación de protección civil y policiales en todo el espacio Schengen, de tal modo que los equipos de comunicación críticos puedan utilizarse en el territorio de otros Estados miembros. Por tanto, el Sistema Europeo de Comunicación Crítica también puede ser beneficioso para la respuesta conjunta con las comunidades cibernéticas pertinentes. Este sistema debe incluir comunicaciones de respaldo a través, por ejemplo, de comunicaciones por satélite.

VII: Coordinación de las crisis de ciberseguridad con los agentes militares

33) La EU-CyCLONe y la Conferencia de cibermandos de la UE, la red operativa de equipos militares de respuesta a emergencias informáticas y la red de CSIRT, así como un futuro Centro de Coordinación de la Ciberdefensa de la UE y sus

[22] HWPCI WK 862/23.

homólogos civiles de la Unión deben cooperar para desarrollar un conocimiento común de la situación entre los agentes civiles y militares.

34) La Unión, teniendo en cuenta los acuerdos existentes, como el acuerdo técnico CERT-EU/OTAN de 2016, debe esforzarse por establecer puntos de contacto para la coordinación con la OTAN en caso de crisis cibernética a fin de intercambiar la información necesaria sobre la situación y el uso de los mecanismos de respuesta a las crisis. A tal fin, la Unión debe explorar formas de mejorar las capacidades de intercambio de información con la OTAN, en particular mediante posibles interconexiones entre sus respectivos sistemas de comunicación e información.

35) Cuando un Estado miembro, en el contexto de un incidente de ciberseguridad, utilice iniciativas de defensa pertinentes, como los Equipos de Respuesta Telemática Rápida de la CEP u otras iniciativas pertinentes, como los equipos de respuesta rápida contra amenazas híbridas de la Unión, debe informar a la EU-CyCLONe, así como a la Conferencia de cibermandos de la UE.

VIII: Cooperación con socios estratégicos

36) El Alto Representante, en estrecha colaboración con la Comisión y otras entidades pertinentes de la Unión, debe:

a) facilitar el flujo de la información necesaria con los socios estratégicos cuando se detecte un incidente relevante;

b) mejorar la coordinación con los socios estratégicos en la respuesta a actividades informáticas malintencionadas realizadas por agentes de amenazas persistentes, en particular a la hora de utilizar el conjunto de instrumentos de ciberdiplomacia, en consonancia con sus directrices de aplicación.

37) Los Estados miembros, el Alto Representante, la Comisión y otras entidades pertinentes de la Unión deben colaborar con socios estratégicos y organizaciones internacionales para promover las buenas prácticas y el comportamiento responsable de los Estados en el ciberespacio y garantizar una reacción rápida y coordinada en caso de ciberincidentes potenciales o a gran escala.

38) En el marco del ciclo continuo de ejercicios a que se refiere la sección II, los servicios de la Comisión y el SEAE deben considerar la posibilidad de organizar un ejercicio conjunto de personal para probar la cooperación entre los componentes civiles y militares en caso de ciberincidente a gran escala que afecte a Estados miembros de la Unión y a aliados de la OTAN, incluso cuando se activen o puedan activarse los artículos 4 o 5 del Tratado de la OTAN.

39) Dada la exposición de los países candidatos y el potencial de ciberincidentes existente en los países vecinos de la Unión, deben considerarse ejercicios conjuntos en los que participen los países candidatos.

Hecho en Bruselas, el

Por el Consejo

La Presidenta / El Presidente