C/2025/3445

20.6.2025

RECOMENDACIÓN DEL CONSEJO

de 6 de junio de 2025

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

(C/2025/3445)

EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular sus artículos 114 y 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 incidentes de ciberseguridad 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 campañas híbridas o de operaciones militares. También pueden afectar directamente a la seguridad, la economía y la sociedad de la Unión. Asimismo, entrañan un riesgo de efectos indirectos, especialmente cuando estas actividades tienen como objetivo a países socios estratégicos internacionales, como países candidatos o países 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. Es esencial gestionar eficazmente las crisis para mantener la estabilidad económica y proteger a los Gobiernos, la infraestructura crítica, los ciudadanos y las empresas 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) Dadas las interdependencias e interconexiones entre los entornos de tecnologías de la información y de las comunicaciones (TIC) de las entidades de la Unión y de los Estados miembros, el hecho de que ocurra un incidente en alguna entidad de la Unión podría suponer un riesgo de ciberseguridad para los Estados miembros y viceversa. La puesta en común de información pertinente y la coordinación con respecto tanto a los incidentes de ciberseguridad a gran escala como a los incidentes graves, tal como se definen en el artículo 3, apartado 8, del Reglamento (UE, Euratom ([1])) 2023/2841 del Parlamento Europeo y del Consejo, es crucial en el contexto del Plan Director de la UE para la Gestión de Crisis de Ciberseguridad («Plan Director de Ciberseguridad»).

(4) En las crisis en las que se haya activado la Respuesta Política Integrada de la UE a las Crisis ([2]) (RPIC) en virtud de la Decisión de Ejecución (UE) 2018/1993 del Consejo («dispositivo RPIC»), el Plan Director de Ciberseguridad debe respetar plenamente el dispositivo RPIC para la coordinación y la respuesta. La coordinación política y estratégica tendría lugar en la RPIC. El dispositivo RPIC es la herramienta de coordinación horizontal y respuesta de la Unión a nivel político. De conformidad con el dispositivo RPIC, la Presidencia del Consejo de la Unión Europea es quien toma la decisión de activar o desactivar la RPIC. Los informes de la capacidad de conocimiento y análisis integrados de la situación (ISAA) elaborados por los servicios de la Comisión y el Servicio Europeo de Acción Exterior (SEAE) apoyan la labor de la RPIC, tanto en su modo de puesta en común de información como en su modo de activación plena.

(5) Los Estados miembros son responsables en primera instancia de la gestión los incidentes y las crisis de ciberseguridad. No obstante, 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. La gestión de crisis de ciberseguridad a lo largo de todo su ciclo de vida incluye la preparación y la conciencia situacional común para anticipar los incidentes de ciberseguridad a gran escala, las capacidades de detección necesarias para identificar las herramientas de respuesta y recuperación precisas destinadas a mitigar y contener los incidentes de ciberseguridad a gran escala, así como las capacidades de reacción para disuadir y prevenir nuevos incidentes.

([1]) 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, p. 1).

([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).

(6) La Recomendación (UE) 2017/1584 ([3]) de la Comisión 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 este tipo de incidentes y crisis de ciberseguridad. Enumera los agentes pertinentes a nivel técnico, operativo y político, y explica su integración en los mecanismos de gestión de crisis de la Unión existentes, 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). La presente Recomendación se basa en estos principios fundamentales y tiene por objeto sustituir a la Recomendación (UE) 2017/1584 con el fin de establecer un nuevo marco de la Unión para la gestión de crisis de ciberseguridad.

(7) Algunas de las definiciones utilizadas en la presente Recomendación se basan en las definiciones y los términos utilizados en la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo ([4]). Sin embargo, el ámbito de aplicación de la presente Recomendación es diferente del de dicha Directiva. 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 incidentes de ciberseguridad a gran escala y crisis de ciberseguridad derivadas de dichos incidentes, independientemente del sector o la entidad que se vean afectados. En la medida de lo posible, las definiciones se basan en las que figuran en la Directiva (UE) 2022/2555.

(8) Se necesita un Plan Director de Ciberseguridad actualizado que proporcione orientaciones claras y accesibles que expliquen qué es un incidente de ciberseguridad a gran escala o una crisis de ciberseguridad a nivel de la Unión, cómo se activa el marco de gestión de crisis y cuáles son las funciones de las redes, los agentes y los 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 tiene por objeto apoyar, en el ámbito de la gestión de crisis de ciberseguridad, el marco más amplio de las relaciones en materia civil y militar de la UE, también en el contexto del estrechamiento de lazos entre la UE y la OTAN, en la medida de lo posible mediante mecanismos reforzados de puesta en común de información inclusivos, recíprocos y no discriminatorios en la gestión de crisis de ciberseguridad.

(9) Debe reforzarse la gestión intersectorial de crisis a nivel de la Unión para permitir una respuesta integrada a las crisis, en particular en los casos en que los incidentes y crisis de ciberseguridad a gran escala tengan consecuencias físicas. La presente Recomendación complementa el dispositivo RPIC y otros mecanismos de gestión de crisis de la Unión, como el sistema de alerta rápida general de la Comisión (ARGUS), el Mecanismo de Protección Civil de la Unión (MPCU) con el apoyo del Centro de Coordinación de la Respuesta a Emergencias (CECRE) creado en virtud del MPCU mediante la Decisión n.º 1313/2013/UE del Parlamento Europeo y del Consejo ([5]) («Decisión MPCU»), el Mecanismo de Respuesta a las Crisis del SEAE, así como otros procesos, como los descritos en el conjunto de instrumentos de ciberdiplomacia de la UE ([6]), el conjunto de instrumentos contra las amenazas híbridas ([7]) y el protocolo revisado de la UE para la lucha contra las amenazas híbridas ([8]). También complementa y debe ser coherente con la Recomendación del Consejo sobre un plan director para coordinar la respuesta a nivel de la Unión en caso de perturbaciones de infraestructuras críticas con importancia transfronteriza significativa ([9]) («Plan Director de la UE de Infraestructuras Críticas»), que abarca la resiliencia física no cibernética y tiene por objeto mejorar la coordinación de la respuesta a nivel de la Unión en este ámbito.

(10) La Red Europea de Organizaciones de Enlace Nacionales para las Crisis de Ciberseguridad («EU-CyCLONe») es la red destinada a la coordinación de la gestión de incidentes y crisis de ciberseguridad a gran escala a nivel operativo, también en caso de incidentes de ciberseguridad intersectoriales a gran escala y crisis de ciberseguridad. Con el fin de no complicar aún más los marcos existentes, debe evitarse la creación de estructuras sectoriales que dupliquen las tareas de EU-CyCLONe. EU-CyCLONe también debe recibir de los sectores información operativa relacionada con la ciberseguridad y transmitir dicha información a las instancias políticas.

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

([4]) Directiva (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).

([5]) 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).

([6]) Conclusiones del Consejo sobre un marco para una respuesta diplomática conjunta de la UE a las actividades informáticas malintencionadas (9916/17)

([7]) Conclusiones del Consejo sobre un marco para una respuesta coordinada de la UE a las campañas híbridas, 22 de junio de 2022.

([8]) Documento de trabajo conjunto de los servicios de la Comisión: protocolo de la UE para la lucha contra las amenazas híbridas [SWD(2023) 116 final; documento en inglés].

([9]) DO C, C/2024/4371, 5.7.2024.

(11) Se anima a los Estados miembros a que hagan pleno uso de los recursos financieros disponibles para la ciberseguridad previstos por los programas pertinentes de la Unión. Debe garantizarse que la carga administrativa que impongan estos programas a los solicitantes de financiación sea mínima y que se facilite la participación de los Estados miembros en dichos programas proporcionando información pertinente sobre opciones viables de apoyo financiero.

(12) La presente Recomendación contribuye a la adopción de medidas de preparación más amplias que la Unión necesita frente a las crisis intersectoriales, en consonancia con los principios integrados en la Estrategia de Preparación de la Unión, a saber, un enfoque integrado que abarque todos los riesgos, a todas las instancias de la Administración y a la sociedad en su conjunto, en particular en lo que respecta a mejorar la sensibilización sobre los riesgos y amenazas y la respuesta intersectorial a las crisis.

HA ADOPTADO LA PRESENTE RECOMENDACIÓN:

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

Objetivo y ámbito de aplicación

1) La presente Recomendación del Consejo de Plan Director de la UE para la Gestión de Crisis de Ciberseguridad («Plan Director de Ciberseguridad») 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 incidentes de ciberseguridad a gran escala y crisis de ciberseguridad. El marco refleja las funciones tanto de los Estados miembros como de las instituciones, órganos y organismos de la Unión («entidades de la Unión») en el marco de sus respectivas competencias, respetando plenamente el Derecho nacional y las normas internas, a fin de garantizar una actuación global y coordinada a nivel de la Unión.

2) El Plan Director de Ciberseguridad debe aplicarse de manera coherente con el Plan Director de la UE de Infraestructuras Críticas, en particular en caso de incidentes que afecten tanto a la resiliencia física como a la ciberseguridad de las infraestructuras críticas ([10]).

3) El Plan Director de Ciberseguridad contiene orientaciones para la respuesta a incidentes de ciberseguridad a gran escala o crisis de ciberseguridad, y debe utilizarse de forma complementaria con otros mecanismos de respuesta sectorial pertinentes como los que figuran en el anexo II. Las partes interesadas correspondientes en materia de ciberseguridad deben prestar ayuda y asistencia para alcanzar los objetivos de dichos mecanismos sectoriales, tanto a nivel nacional como de la Unión.

4) En caso de que surja una crisis intersectorial en el ámbito de la UE con aspectos cibernéticos que requiera la activación de la RPIC, el Consejo debe coordinar la respuesta en el nivel político de la Unión por medio del dispositivo RPIC. Cuando se haya activado la RPIC, las medidas que se adopten en el marco del Plan Director de Ciberseguridad deben respaldar la respuesta de la UE a nivel político y prestar apoyo específico en materia de ciberseguridad.

Principios rectores

5) Los siguientes principios rectores se aplican a la gestión de crisis de ciberseguridad a nivel de la Unión:

a) *Proporcionalidad:* la mayoría de los incidentes de ciberseguridad que afectan a los Estados miembros no reúnen los elementos que permiten considerarlos incidentes de ciberseguridad a gran escala o crisis de ciberseguridad nacionales o de la Unión. En caso de incidentes y amenazas de ciberseguridad, los Estados miembros cooperan e intercambian información de forma voluntaria y periódica dentro de la red de equipos de respuesta a incidentes de seguridad informática («red de CSIRT») y EU-CyCLONe, en consonancia con los procedimientos operativos estándar de las redes.

b) *Subsidiariedad*: los Estados miembros son responsables en primera instancia de la respuesta y la reparación en caso de incidentes ciberseguridad, incidentes de ciberseguridad a gran escala o crisis de ciberseguridad que les afecten. De cara a posibles efectos transfronterizos, el Consejo, la Comisión, el Alto Representante, la Agencia de la Unión Europea para la Ciberseguridad (ENISA), el Servicio de Ciberseguridad para las Instituciones, los Órganos y los Organismos de la Unión (CERT-UE), Europol y todas las demás entidades pertinentes de la Unión deben cooperar a lo largo de todo el ciclo de vida de la crisis. Esta función se desprende del Derecho de la Unión y refleja el modo en que los incidentes de ciberseguridad a gran escala y las crisis de ciberseguridad afectan a uno o más sectores de la actividad económica dentro del mercado único, a la seguridad y las relaciones internacionales de la Unión, así como a las propias entidades de la Unión.

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

c) *Complementariedad*: la presente Recomendación tiene plenamente en cuenta los mecanismos de gestión de crisis existentes en el ámbito de la Unión que figuran en el anexo II, en particular el dispositivo RPIC, ARGUS y el Mecanismo de Respuesta a las Crisis del SEAE. La presente Recomendación tiene en cuenta los mandatos de la red de CSIRT y EU-CyCLONe, así como el Reglamento (UE, Euratom) 2023/2841. Cuando se active la RPIC, el trabajo de las redes, entidades y mecanismos sectoriales activados debe continuar y debe contribuir a la coordinación política y estratégica que tiene lugar en el marco de la RPIC y respaldarla.

d) *Confidencialidad de la información*: todos los intercambios de información en el contexto de la presente Recomendación deben cumplir las normas aplicables sobre seguridad y sobre la protección de datos personales. Cuando proceda, deben tenerse en cuenta los acuerdos informales de confidencialidad, como el protocolo TLP para etiquetar la información delicada. Para el intercambio de información clasificada, independientemente del sistema de clasificación aplicado, deben seguirse las normas y los acuerdos vinculantes que existan en materia de tratamiento de información clasificada junto con las herramientas acreditadas disponibles.

6) De conformidad con los principios rectores mencionados, 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. Esta cooperación, en el marco del Plan Director de Ciberseguridad, se beneficia de la aplicación de los artículos 22 y 23 del Reglamento (UE, Euratom) 2023/2841. En particular, el plan de gestión de crisis de ciberseguridad establecido con arreglo al artículo 23 del Reglamento (UE, Euratom) 2023/2841 contribuye, entre otras cosas, al intercambio periódico de información pertinente entre las entidades de la Unión y con los Estados miembros, y define mecanismos para la coordinación y el flujo de información entre las entidades de la Unión.

II: Definiciones

7) A los efectos del presente Plan Director de Ciberseguridad, se entenderá por:

a) «incidente»: todo hecho que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios ofrecidos por sistemas de redes y de información o accesibles a través de ellos;

b) «incidente significativo»: un incidente que:

a. ha causado o puede causar graves perturbaciones operativas de los servicios o pérdidas económicas para la entidad afectada;

b. ha afectado o puede afectar a otras personas físicas o jurídicas al causar perjuicios materiales o inmateriales considerables;

c) «incidente de ciberseguridad a gran escala»: un incidente que cause perturbaciones que superen la capacidad de un Estado miembro para responder a él o que afecte significativamente por lo menos a dos Estados miembros;

d) «crisis de ciberseguridad»: incidente de ciberseguridad a gran escala que se haya intensificado hasta 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.

III: Estructuras y responsabilidades nacionales de gestión de crisis de ciberseguridad

8) Los Estados miembros son responsables en primera instancia de la respuesta en caso de incidentes de ciberseguridad a gran escala o crisis de ciberseguridad que les afecten. Cada Estado miembro, de conformidad con la Directiva (UE) 2022/2555, cuenta con una o varias autoridades de gestión de crisis de ciberseguridad, así como con uno o varios CSIRT.

9) Con la adopción de la Directiva (UE) 2022/2555 y otros instrumentos legislativos y no legislativos en materia de ciberseguridad, los Estados miembros han ido armonizando sus marcos de ciberseguridad mediante la definición de normas mínimas relativas al funcionamiento del marco regulador coordinado, el establecimiento de mecanismos para que las autoridades competentes de cada Estado miembro cooperen de manera eficaz, y la disponibilidad de vías de recurso y medidas de ejecución eficaces que son fundamentales para garantizar el cumplimiento efectivo de dichas obligaciones.

10) De conformidad con el artículo 9, apartado 4, de la Directiva (UE) 2022/2555, los Estados miembros deben adoptar planes nacionales de respuesta a incidentes y crisis de ciberseguridad a gran escala. Estos planes incluyen, entre otras cosas, medidas nacionales de preparación, procedimientos de gestión de crisis de ciberseguridad, y procedimientos y mecanismos nacionales entre las autoridades y los organismos nacionales para garantizar su participación efectiva en la gestión coordinada de incidentes de ciberseguridad a gran escala y crisis de ciberseguridad a nivel de la Unión y su apoyo a ella. Los procedimientos de gestión de crisis de ciberseguridad contemplan también disposiciones sobre su integración en el marco nacional general de gestión de crisis y los canales para el intercambio de información.

11) De conformidad con el artículo 9, apartado 1, de la Directiva (UE) 2022/2555, los Estados miembros velarán por la coherencia con los marcos nacionales generales de gestión de crisis vigentes. En caso de activación de la RPIC, las autoridades nacionales de gestión de crisis deben recabar información de las autoridades de gestión de crisis de ciberseguridad y de los mecanismos sectoriales nacionales de crisis con el fin de comunicársela a la RPIC.

12) De conformidad con el artículo 9, apartado 5, de la Directiva (UE) 2022/2555, EU-CyCLONe, a petición de un Estado miembro afectado, debe intercambiar información sobre las partes pertinentes de los planes nacionales de respuesta a incidentes y crisis de ciberseguridad a gran escala, en particular sobre las disposiciones destinadas a garantizar la participación efectiva en la gestión coordinada de incidentes de ciberseguridad a gran escala y crisis de ciberseguridad a nivel de la Unión y su apoyo a dicha gestión, con el fin de intercambiar mejores prácticas y comprobar si el marco general funcionaría en la práctica.

13) Se invita a EU-CyCLONe y al Consejo Interinstitucional de Ciberseguridad (CIIC) a intercambiar información, cuando proceda, sobre la coherencia del plan de gestión de crisis establecido por el CIIC, de conformidad con el artículo 23 del Reglamento (UE, Euratom) 2023/2841, con los planes nacionales de respuesta a incidentes de ciberseguridad a gran escala y crisis de ciberseguridad.

14) EU-CyCLONe, con el apoyo de ENISA en sus funciones de secretaría, debe mantener una lista actualizada de las autoridades de gestión de crisis de ciberseguridad con los datos de contacto de los funcionarios y ejecutivos de EU-CyCLONe, y ponerla a disposición de los miembros de EU-CyCLONe.

IV: Principales redes y agentes del ecosistema de gestión de crisis de ciberseguridad de la UE

15) La red de CSIRT es la principal red técnica para intercambiar información pertinente sobre incidentes, en particular en el ámbito de aplicación de la presente Recomendación, de conformidad con los cometidos correspondientes que se describen en el artículo 15, apartado 3, de la Directiva (UE) 2022/2555. Contribuye al refuerzo de la confianza y la seguridad y fomenta una cooperación operativa rápida y eficaz entre los Estados miembros. El presidente de la red de CSIRT podrá participar como observador en el CIIC.

16) El CERT-EU es el servicio de ciberseguridad de todas las entidades de la Unión. Funciona como centro de coordinación de las entidades de la Unión para el intercambio de información sobre ciberseguridad y la respuesta a incidentes, de conformidad con el artículo 13 del Reglamento (UE) 2023/2841. El CERT-EU es miembro de la red de CSIRT y presta apoyo a la Comisión en EU-CyCLONe. Opera a nivel técnico y es responsable de coordinar la gestión de los incidentes graves que afecten a las entidades de la Unión.

17) EU-CyCLONe actúa como intermediario entre el nivel técnico y el político, en particular durante los incidentes de ciberseguridad a gran escala y las crisis de ciberseguridad. Respalda la gestión coordinada de los incidentes de ciberseguridad a gran escala y las crisis de ciberseguridad en el ámbito operativo y garantiza el intercambio regular de información relevante entre los Estados miembros y las instituciones, los órganos y los organismos de la Unión, de conformidad con el artículo 16 de la Directiva (UE) 2022/2555. El presidente de EU-CyCLONe podrá participar como observador en el CIIC.

18) ENISA es la agencia de la Unión que desempeña el cometido que se le asigna en virtud del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo ([11]) con el fin de lograr un elevado nivel de ciberseguridad común en toda la Unión, especialmente mediante el apoyo activo a los Estados miembros y a las instituciones, órganos y organismos de la Unión. ENISA se hace cargo, entre otras cosas, de la secretaría de la red de CSIRT y EU-CyCLONe, de servicios de conciencia situacional, y asiste a los Estados miembros organizando periódicamente ejercicios de ciberseguridad a nivel de la Unión. De conformidad con la Directiva (UE) 2022/2555 y el Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo ([12]), ENISA recibe información sobre incidentes transfronterizos significativos, vulnerabilidades aprovechadas activamente e incidentes que afectan a productos digitales.

([11]) 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).

([12]) 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).

19) El Consejo de la Unión Europea (en lo sucesivo, «Consejo»), en virtud del artículo 16 del Tratado de la Unión Europea (TUE), es la institución que ejerce funciones de definición de políticas y de coordinación y tiene a su cargo la RPIC, que está relacionado con la coordinación y la respuesta en el nivel político de la Unión. El Consejo actúa a través de las formaciones del Consejo, el Comité de Representantes Permanentes y los órganos preparatorios del Consejo pertinentes, especialmente el Grupo Horizontal «Cuestiones Cibernéticas», así como, cuando proceda, el dispositivo RPIC.

20) La Comisión, como institución que, en virtud del artículo 17 del TUE, promueve el interés general de la Unión y toma las iniciativas adecuadas con este fin, y vela por que se apliquen los Tratados y las medidas adoptadas por las instituciones, es responsable de determinadas acciones de preparación general a nivel de la Unión y de determinadas acciones de conciencia situacional, incluida la gestión del CECRE y del Sistema Común de Comunicación e Información de Emergencia (SCCIE), en consonancia con la Decisión MPCU. Facilita la coherencia y la coordinación entre las acciones conexas de respuesta a las crisis a nivel de la Unión en el ámbito operativo. Se le consulta sobre las decisiones de activar o desactivar la RPIC. Los servicios de la Comisión elaboran, junto con el SEAE, los informes ISAA. La Comisión es miembro de EU-CyCLONe cuando un incidente de ciberseguridad a gran escala, potencial o en curso, tenga o pueda tener repercusiones significativas en los servicios y actividades incluidos en el ámbito de aplicación de la Directiva (UE) 2022/2555, y asume funciones de observador en otros casos. Es el punto de contacto del CIIC con EU-CyCLONe. Participa como observador en la red de CSIRT.

21) El Alto Representante para Asuntos Exteriores y Política de Seguridad (en lo sucesivo, «Alto Representante»), con la asistencia del SEAE, está al frente de la política exterior y de seguridad común (PESC) de la Unión y contribuye con sus propuestas a elaborar dicha política, incluida la política común de seguridad y defensa (PCSD). Todo ello incluye estructuras y mecanismos diplomáticos, militares y de inteligencia, en particular la Capacidad Única de Análisis de Inteligencia (SIAC) —punto de entrada único para la inteligencia de los Estados miembros—, el Estado Mayor de la UE (EMUE) —fuente de conocimientos especializados en materia militar—, el conjunto de instrumentos de ciberdiplomacia de la UE, así como la red de Delegaciones de la UE, que pueden contribuir a la gestión de crisis desde una dimensión exterior. El SEAE también elabora con la Comisión los informes ISAA.

22) En el anexo II se describen las funciones y competencias de los agentes pertinentes a nivel de la Unión en relación con la gestión de crisis de ciberseguridad y se incluyen las principales redes y agentes.

V: Prepararse para incidentes de ciberseguridad a gran escala y crisis de ciberseguridad

Panorama de amenazas

23) Los Estados miembros y las entidades pertinentes de la Unión deben tomar las medidas necesarias para mejorar la conciencia situacional, reconociendo que el panorama de amenazas y la conciencia situacional específica sobre incidentes exigen modos de operación diferenciados. Los Estados miembros y las entidades pertinentes de la Unión deben trabajar juntos a partir de datos verificados y fiables, que incluyan las tendencias de los incidentes, las tácticas, las técnicas, los procedimientos y las vulnerabilidades aprovechadas activamente.

24) A la hora de compartir información a nivel de la UE, 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 EU-CyCLONe.

25) A fin de mejorar la conciencia situacional común y facilitar la evaluación del impacto en la UE, EU-CyCLONe y la red de CSIRT, con el apoyo de ENISA, deben utilizar mecanismos de información acordados internamente para crear una visión de conjunto de las actividades técnicas y operativas a partir de la información recopilada a escala nacional.

26) EU-CyCLONe y la red de CSIRT deben:

a) cooperar para mejorar la puesta en común de información entre los niveles técnico y operativo, así como la conciencia situacional en su conjunto;

b) seguir creando un clima de confianza entre sus miembros y entre las redes;

c) hacer pleno uso de las herramientas disponibles para la puesta en común de información, con el apoyo de ENISA, y reflexionar sobre la manera en que se pueden mejorar estas herramientas y velar por la interoperabilidad entre las redes.

27) EU-CyCLONe, la red de CSIRT y el CIIC deben cooperar para velar por el intercambio eficaz de la información pertinente.

28) ENISA, como secretaría de la red de CSIRT y EU-CyCLONe, desempeña un papel central de apoyo a los Estados miembros y las instituciones, los órganos y los organismos de la Unión para lograr una conciencia situacional común de la UE desde el punto de vista técnico y operativo a fin de contribuir a la preparación para incidentes y crisis de ciberseguridad a gran escala.

29) De conformidad con la Directiva (UE) 2022/2555 y el Reglamento (UE) 2019/881, los Estados miembros y las entidades pertinentes de la Unión deben coordinarse con el sector privado, lo que incluye a los fabricantes y las comunidades de código abierto, a fin de mejorar la puesta en común de información. En particular, ENISA debe utilizar su programa de asociación a este respecto. Además, los Estados miembros y las entidades pertinentes de la Unión también podrían basarse en los centros de puesta en común y análisis de la información existentes a escala nacional y de la UE para mejorar la capacidad de ciberseguridad y responder a los incidentes de ciberseguridad, en particular mediante la celebración de reuniones conjuntas del sector privado con EU-CyCLONe y la red de CSIRT.

30) A fin de mejorar la puesta en común de información en el seno de las redes y entre ellas y de aclarar las expectativas mutuas relativas a dicha puesta en común, EU-CyCLONe, con el apoyo de ENISA como secretaría y previa consulta a la red de CSIRT y el Grupo de Cooperación SRI, debe acordar una taxonomía común adaptada de los niveles de gravedad de los incidentes en el plazo de 24 meses a partir de la adopción de la presente Recomendación. Dicha taxonomía debe permitir comparar la gravedad de los incidentes en todos los Estados miembros examinando las repercusiones en la prestación de servicios, el número de entidades afectadas y su respectiva relevancia, las repercusiones en otros servicios e infraestructuras, así como el perjuicio económico, el daño a la reputación y el daño político causado. Debe basarse en las escalas o taxonomías pertinentes que ya existan, como la taxonomía de referencia para la clasificación de incidentes.

En el nivel técnico

31) La red de CSIRT es la plataforma para la cooperación técnica y la puesta en común de información entre todos los Estados miembros y, a través del CERT-EU, con las entidades de la Unión.

32) De conformidad con la Directiva (UE) 2022/2555, cada CSIRT tiene el cometido de realizar un seguimiento y analizar las ciberamenazas, las vulnerabilidades y los incidentes a escala nacional. Los CSIRT, tanto en el marco de la red de CSIRT como de forma bilateral, deben intercambiar la información pertinente sobre incidentes, cuasiincidentes, ciberamenazas, riesgos y vulnerabilidades a fin de lograr una conciencia situacional común.

33) Con vistas a reforzar la cooperación operativa en el ámbito de la Unión, la red de CSIRT debe considerar la posibilidad de invitar a que participen en sus actividades los órganos y organismos de la Unión implicados en la política de ciberseguridad, como Europol.

34) De conformidad con el Reglamento 2023/2841, el CERT-EU debe recopilar, gestionar, analizar y compartir con las instituciones, órganos y organismos de la Unión información sobre las ciberamenazas, las vulnerabilidades y los incidentes relacionados con infraestructuras de TIC no clasificadas y, cuando sea necesario, hacer propuestas específicas al CIIC de directrices y recomendaciones dirigidas a instituciones, órganos y organismos de la Unión. El CERT-EU debe cooperar e intercambiar información con homólogos de los Estados miembros, en particular a través de la red de CSIRT.

En el nivel operativo

35) De conformidad con la Directiva (UE) 2022/2555, EU-CyCLONe debe servir de plataforma de cooperación entre las autoridades de gestión de crisis de ciberseguridad de los Estados miembros y a través de la Comisión y con las entidades pertinentes de la Unión, con el objetivo de incrementar el nivel de preparación para la gestión de incidentes de ciberseguridad a gran escala y crisis de ciberseguridad y desarrollar una conciencia situacional común de los incidentes de ciberseguridad a gran escala y crisis de ciberseguridad.

36) De conformidad con la Directiva (UE) 2022/2555 y el Reglamento (UE) 2024/2847, ENISA recibe información sobre incidentes transfronterizos significativos, vulnerabilidades aprovechadas activamente e incidentes que afectan a productos digitales. ENISA, en calidad de secretaría, debe asesorar a la red de CSIRT y EU-CyCLONe con el objetivo de apoyar las redes a la hora de determinar si deben realizarse otras actuaciones y para contribuir a la conciencia situacional común.

En el nivel político

37) Los Estados miembros y las entidades pertinentes de la Unión deben realizar un seguimiento de los acontecimientos internacionales que afecten a la ciberseguridad (en particular las ciberamenazas, las amenazas híbridas y la manipulación de información e injerencia por parte de agentes extranjeros, incluida la desinformación, cuando proceda). Deben tenerse en cuenta iniciativas como los informes sobre la situación técnica de la ciberseguridad, los análisis de la Capacidad Única de Análisis e Inteligencia y otros productos pertinentes que facilitan información especializada.

38) El Alto Representante debe seguir informando a los Estados miembros y fomentando su participación en las iniciativas diplomáticas de la Unión relacionadas con las ciberamenazas —en especial las que atañen a agentes estatales— su diálogo con terceros países y organizaciones internacionales —en particular la OTAN— y la aplicación de medidas diplomáticas, incluidas las medidas restrictivas.

39) La Presidencia del Consejo de la Unión Europea puede iniciar una página de seguimiento en la plataforma web de la IRPC en la que los Estados miembros y las instituciones y organismos de la UE puedan intercambiar información sobre una posible crisis.

Ejercicios comunes

40) La Comisión, en coordinación con el Alto Representante y con el apoyo de ENISA, previa consulta a EU-CyCLONe y la red de CSIRT, debe elaborar un programa continuo de ejercicios de ciberseguridad de carácter anual con el fin de prepararse para las crisis de ciberseguridad y reforzar la eficiencia organizativa. El programa continuo de ejercicios de ciberseguridad debe tener en cuenta los ejercicios del Mecanismo de Protección Civil de la Unión y otros mecanismos de la Unión de respuesta a las crisis, en particular el ejercicio que se expone en el Plan Director de la UE de Infraestructuras Críticas. El primer programa continuo debe desarrollarse en un plazo de 12 meses después de la adopción de Plan Director de Ciberseguridad, y los programas ulteriores deben completarse antes del 31 de marzo de cada año. El programa continuo debe remitirse al Consejo con fines informativos.

41) El programa continuo también debe abarcar ejercicios elaborados a partir de las hipótesis derivadas de las evaluaciones de riesgos coordinadas a nivel de la UE. Asimismo, debe incluir ejercicios en los que participen todos los agentes pertinentes, en particular el sector privado y la OTAN.

42) ENISA, en su función de secretaría de la red de CSIRT y EU-CyCLONe, debe velar por la recopilación sistemática de las enseñanzas extraídas de los ejercicios, así como la identificación de las consiguientes medidas y la modalidad propuesta para su aplicación, a fin de garantizar su ejecución efectiva y los efectos positivos en la resiliencia común de la UE, incluidos los respectivos procedimientos operativos normalizados comunes.

43) Todos los agentes y las redes deben mejorar la coordinación en caso de incidentes de ciberseguridad a gran escala y crisis de ciberseguridad a partir de las enseñanzas extraídas de los ejercicios. En particular, EU-CyCLONe y la red de CSIRT deben abordar los retos detectados durante los ejercicios a fin de mejorar la coordinación, especialmente los relativos a la cooperación entre las redes y, en caso necesario, deben adaptar rápidamente los procedimientos operativos normalizados comunes.

44) El Grupo de Cooperación SRI debe invitar a la red de CSIRT, EU-CyCLONe y ENISA a presentar las enseñanzas extraídas de los ejercicios, así como la identificación de las consiguientes medidas y la modalidad propuesta para su aplicación.

45) El Consejo puede invitar a las presidencias de la red CSIRT, EU-CyCLONe, el Grupo de Cooperación SRI y ENISA a que presenten la manera en que se hayan aplicado las enseñanzas extraídas de los ejercicios.

46) Se invita a ENISA, en cooperación con la Comisión y el Alto Representante, a que organice un ejercicio para poner a prueba el Plan Director de Ciberseguridad durante el próximo ejercicio CyberEurope. En el ejercicio deben participar todos los agentes pertinentes, también del ámbito político. Se invita a ENISA a que coordine con la Presidencia del Consejo de la Unión Europea la participación de las instancias del ámbito político. El ejercicio también puede incluir al sector privado y a la OTAN.

VI: Detectar un incidente que podría convertirse en un incidente de ciberseguridad a gran escala o una crisis de ciberseguridad

47) De conformidad con sus respectivos mandatos y con arreglo a un enfoque que contemple todos los riesgos, todos los agentes deben aportar a las redes pertinentes la información que indique un posible incidente de ciberseguridad a gran escala o crisis de ciberseguridad.

48) De conformidad con el Reglamento (UE) 2025/38 del Parlamento Europeo y del Consejo ([13]), cuando los centros de ciberseguridad transfronterizos obtengan información relativa a un incidente de ciberseguridad a gran escala potencial o en curso, deben garantizar, a efectos de conciencia situacional común, que se facilite a las autoridades de los Estados miembros y a la Comisión la información pertinente a través de EU-CyCLONe y de la red de CSIRT, sin demora indebida.

([13]) 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).

49) Cuando se observe un incidente significativo, en particular que cause repercusiones inmediatas, puede ser notificado a un CSIRT, o detectado por este, así como por las autoridades de gestión de crisis de ciberseguridad de los Estados miembros u otras autoridades sectoriales. Se anima a los Estados miembros a que compartan la información relacionada con incidentes de esta índole en el seno de las redes, que deben estudiar la posibilidad de tomar las medidas adecuadas. La activación de la red de CSIRT y EU-CyCLONe puede ser independiente, en función de la naturaleza del incidente y de la respuesta que requiera. No obstante, se anima a ambas redes a que prosigan la cooperación mutua con arreglo a disposiciones de procedimiento acordadas. La decisión de activación corresponde a la red respectiva con carácter exclusivo y autónomo.

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

51) Como indica la Directiva (UE) 2022/2555, la red de CSIRT y EU-CyCLONe deben acordar sin demora 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.

VII: Responder en el ámbito de la Unión a un incidente de ciberseguridad a gran escala o una crisis de ciberseguridad

Respuesta a un incidente de ciberseguridad a gran escala o una crisis de ciberseguridad para los que la IRPC no esté activada en modo de activación plena

52) La respuesta eficaz en el ámbito de la UE a los incidentes de ciberseguridad a gran escala o crisis de ciberseguridad depende de una cooperación técnica, operativa y política eficaz con un enfoque que abarque al Gobierno en su conjunto, incluidos, cuando sea posible, los servicios policiales.

53) En cada ámbito, los agentes implicados deben llevar a cabo actividades específicas para lograr una conciencia situacional común y una respuesta coordinada. Estas medidas asegurarán la difusión ordenada y eficaz de la información.

54) La respuesta debe ser adecuada a las repercusiones del incidente de ciberseguridad a gran escala o crisis de ciberseguridad. De conformidad con la Directiva (UE) 2022/2555, las autoridades de gestión de crisis de ciberseguridad de los Estados miembros deben garantizar la coherencia nacional y la coordinación de las respuestas sectoriales a la crisis de ciberseguridad.

55) En el caso de un incidente de ciberseguridad a gran escala o una crisis de ciberseguridad, todos los agentes y redes deben responder en estrecha coordinación de la siguiente manera:

a) en el nivel técnico:

i. los Estados miembros afectados y sus CSIRT deben cooperar con las entidades afectadas para responder a los incidentes y prestar asistencia, cuando proceda;

ii. los CSIRT deben cooperar a través de la red de CSIRT para intercambiar información técnica pertinente sobre el incidente; los CSIRT cooperan en sus esfuerzos por analizar los artefactos técnicos disponibles y demás información técnica relacionada con el incidente, con el fin de determinar la causa y las posibles medidas técnicas de mitigación;

iii. cuando un CSIRT o una autoridad de gestión de crisis de ciberseguridad de un Estado miembro tenga conocimiento de un incidente significativo, se les anima a que compartan la información en el marco de la red CSIRT o EU-CyCLONe;

iv. la red CSIRT, con el apoyo de ENISA, debe preparar una agrupación de los informes nacionales proporcionados por los CSIRT, que debe presentarse a EU-CyCLONe;

v. cuando un incidente de ciberseguridad tenga el potencial de convertirse en un incidente o una crisis de ciberseguridad a gran escala, la red de CSIRT debe compartir la información procedente con EU-CyCLONe. EU-CyCLONe debe emplear dicha información para informar al Consejo;

vi. La red de CSIRT debe mantener un estrecho contacto con Europol para velar por el intercambio de la información técnica pertinente. La red de CSIRT y Europol deben establecer puntos de contacto para mejorar la puesta en común de información cuando proceda en el caso de un incidente de ciberseguridad a gran escala;

b) en el nivel operativo:

i. los Estados miembros deben mitigar las repercusiones del incidente a escala nacional mediante el empleo de las medidas adecuadas;

ii. la red de CSIRT debe facilitar a EU-CyCLONe evaluaciones técnicas de los incidentes en curso, que EU-CyCLONe pueda utilizar;

iii. EU-CyCLONe debe evaluar las consecuencias y repercusiones de los incidentes de ciberseguridad a gran escala y crisis de ciberseguridad pertinentes y proponer posibles medidas de mitigación, apoyar la gestión coordinada de incidentes de ciberseguridad a gran escala y crisis de ciberseguridad y respaldar la toma de decisiones en el nivel político;

iv. en el caso de que un incidente de ciberseguridad a gran escala con repercusiones intersectoriales requiera la activación de acciones de respuesta a nivel de la Unión, en particular de los correspondientes mecanismos horizontales y sectoriales de gestión de crisis de la Unión mencionados en el anexo II,

(a) los agentes pertinentes pueden, en función del tipo de mecanismo sectorial de gestión de crisis de la Unión, pedir la activación de dicho mecanismo;

(b) en el caso de que se active dicho mecanismo sectorial, las entidades pertinentes apoyan a las entidades sectoriales a la hora de mitigar las repercusiones del incidente;

(c) 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 nivel de la Unión mencionados en el anexo II y EU-CyCLONe, y debe perseguir un análisis intersectorial y proponer opciones para un plan de respuesta integrada adecuado;

(d) la Comisión, a través de EU-CyCLONe, y cuando proceda, en colaboración con el Alto Representante, debe velar por la coherencia y la coordinación de las medidas operativas de la Unión en el ámbito cibernético con acciones de respuesta conexas a nivel de la Unión, en particular en relación con las solicitudes de ayuda realizadas a través del Mecanismo de Protección Civil de la Unión;

(e) si ya se ha iniciado una página de seguimiento de la IRPC sobre el incidente, sus repercusiones y las medidas adoptadas también deben compartirse con los Estados miembros y las entidades de la Unión a través de la plataforma web del dispositivo IRPC;

v. Los Estados miembros pueden solicitar los servicios de la Reserva de Ciberseguridad de la UE de conformidad con el artículo 15 del Reglamento (UE) 2025/38. Sin perjuicio de lo que se prevea en futuros actos de ejecución adoptados con arreglo a dicho Reglamento, los servicios de la Reserva de Ciberseguridad de la UE deben prestarse en un plazo de veinticuatro horas a partir de la solicitud;

c) en el nivel político:

i. a fin de dar una respuesta política y estratégica adecuada, el Consejo puede solicitar información de las principales partes interesadas, en particular la Comisión, el Alto Representante y EU-CyCLONe;

ii. el Consejo, con el apoyo de la Comisión y el Alto Representante, puede decidir las medidas adecuadas para responder al incidente de ciberseguridad a gran escala, incluidas las posibles respuestas diplomáticas en consonancia con el Capítulo IX;

iii. los Estados miembros pueden activar instrumentos o mecanismos de gestión de crisis de ciberseguridad adicionales en función de la naturaleza y las repercusiones del incidente;

iv. la activación del dispositivo IRPC en el modo de puesta en común de información desencadena la capacidad de apoyo al conocimiento y análisis integrados de la situación, lo que incrementa el intercambio de información a través de la plataforma web del dispositivo IRPC y garantiza una visión general común de la situación. Los informes de situación de EU-CyCLONe y la red de CSIRT deben seguir siendo los principales instrumentos que presenten una conciencia situacional común desde el punto de vista operativo y técnico, respectivamente. Estos informes pueden servir de base a los informes ISAA;

v. en el caso de un incidente que requiera la activación de acciones de respuesta a nivel de la Unión, en particular de los mecanismos horizontales y sectoriales de gestión de crisis pertinentes de la Unión mencionados en el anexo II, el Consejo, en cooperación con la Comisión y el Alto Representante, debe velar por la coherencia y coordinación de las respuestas a la crisis de ciberseguridad y las acciones de respuesta conexas en el ámbito de la Unión;

vi. Cuando se soliciten los mecanismos pertinentes, en particular los servicios de la Reserva de Ciberseguridad, los servicios de la Comisión y, cuando proceda, el SEAE, así como los órganos pertinentes del Consejo, en particular el Grupo Horizontal «Cuestiones Cibernéticas» y el Grupo Horizontal «Aumento de la Resiliencia y Lucha contra las Amenazas Híbridas», según proceda, deben coordinar el diseño y la aplicación de medidas y el proceso de toma de decisiones adecuado con medidas adicionales, en consonancia con el conjunto de instrumentos de la UE contra las amenazas híbridas ([14]), en el caso de una actividad informática malintencionada que forme parte de una campaña híbrida más amplia.

Respuesta a un incidente de ciberseguridad a gran escala o una crisis de ciberseguridad para los que la IRPC esté activada en modo de activación plena

56) Deben aplicarse los pasos mencionados en la sección anterior «*Respuesta a un incidente de ciberseguridad a gran escala o una crisis de ciberseguridad para los que el Dispositivo IRPC no esté activado en modo de activación plena*».

57) Cuando la IRPC esté activada en modo de activación plena, los informes ISAA sirven para garantizar una conciencia situacional común desde el punto de vista político. Los informes de situación de EU-CyCLONe y la red de CSIRT deben seguir siendo los principales instrumentos que presenten una conciencia situacional común desde el punto de vista operativo y técnico, respectivamente. Estos informes pueden servir de base a los informes ISAA.

58) En el caso de un incidente ciberseguridad a gran escala o una crisis de ciberseguridad que dé lugar a la activación de la IRPC en modo de activación plena, todos los agentes deben responder en estrecha coordinación con un enfoque que abarque al Gobierno en su conjunto de la siguiente manera:

a) el Consejo coordina la respuesta de la Unión desde el punto de vista político, por medio del Dispositivo IRPC;

b) EU-CyCLONe, en colaboración con la red de CSIRT, debe proporcionar información clara a las instancias políticas sobre el impacto, las posibles consecuencias y las medidas de respuesta y reparación del incidente, en particular contribuyendo a los informes ISAA;

c) además de la capacidad de conocimiento y análisis integrados de la situación, la Presidencia del Consejo de la Unión Europea puede convocar mesas redondas de la RPIC a fin de posibilitar la coordinación política y estratégica de la respuesta de la UE, con la contribución de las actuaciones en el marco del Plan Director de Ciberseguridad y las actividades de los mecanismos sectoriales pertinentes a la labor de la RPIC. Asimismo, las mesas redondas pueden detectar lagunas específicas en la respuesta e invitar a agentes concretos de la UE a que las aborden e informen a las mesas redondas ulteriores, a fin de apoyar la coordinación política y estratégica en la RPIC;

d) la Presidencia del Consejo de la Unión Europea debe considerar la posibilidad de invitar a EU-CyCLONe a las reuniones pertinentes, en particular las mesas redondas en el marco del Dispositivo RPIC y otras reuniones del Consejo pertinentes;

e) las autoridades de gestión de crisis de los Estados miembros deben garantizar la coherencia y la coordinación de las respuestas sectoriales a la crisis de ciberseguridad con el apoyo de las autoridades de gestión de crisis de ciberseguridad;

f) las posibles respuestas diplomáticas deben considerarse y aplicarse en consonancia con el Capítulo IX.

VIII: Actividades de comunicación pública

59) Cuando realicen actividades de comunicación destinadas a la población de un Estado miembro acerca de un incidente de ciberseguridad a gran escala o crisis de ciberseguridad en curso, en particular en el marco de la labor de sensibilización, que es una competencia nacional, los Estados miembros, la Comisión y el Alto Representante deben aspirar a coordinar su comunicación pública en la medida de lo posible. Según el caso, podrá participar en estas actividades la red informal de comunicadores de crisis de la RPIC.

60) A efectos de prepararse para los incidentes de ciberseguridad a gran escala o las crisis de ciberseguridad, se invita a los Estados miembros y, según proceda, a la Comisión y el CERT-EU a que dialoguen sobre sus actividades de comunicación en el marco de EU-CyCLONe y la red de CSIRT, en particular sobre las mejores prácticas, como anuncios o campañas de sensibilización. ENISA debe facilitar herramientas para apoyar dicho diálogo y garantizar el fácil acceso.

([14]) 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.

61) En caso de incidente de ciberseguridad a gran escala o crisis de ciberseguridad, se invita a los Estados miembros a que, en el marco de EU-CyCLONe, compartan información sobre sus actividades de comunicación pública a fin de construir un conocimiento común y coordinar las actuaciones. Por iniciativa propia o previa solicitud del Consejo, EU-CyCLONe puede transmitir al Consejo una visión general de estos planteamientos.

IX: Respuesta diplomática y cooperación con los socios estratégicos

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

a) apoyar la toma de decisiones en el Consejo, en particular mediante análisis, informes y propuestas, sobre el uso de posibles medidas en el marco del conjunto de instrumentos de ciberdiplomacia de la UE. Esto permitirá el uso de todo el espectro de herramientas de que dispone la Unión para prevenir e impedir las actividades informáticas malintencionadas y responder a ellas, reforzando su sólida postura de ciberseguridad y promoviendo la paz, la seguridad y la estabilidad internacionales en el ciberespacio;

b) facilitar el flujo de la información necesaria con los socios estratégicos, incluida la OTAN, en su caso, cuando se detecte un incidente relevante;

c) mejorar la coordinación con los socios estratégicos, incluida la OTAN, cuando proceda, 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 de la UE, en consonancia con sus directrices de aplicación.

63) Los Estados miembros, el Alto Representante, la Comisión y otras entidades pertinentes de la Unión deben cooperar 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 incidentes de ciberseguridad potenciales o a gran escala.

64) La cooperación entre la Unión Europea y la OTAN debe llevarse a cabo de conformidad con los principios rectores acordados de inclusividad, reciprocidad y transparencia, y respetando plenamente la autonomía decisoria de la Unión.

65) La Comisión y el Alto Representante, teniendo en cuenta los acuerdos existentes, como el acuerdo técnico CERT-EU/OTAN de 2016, deben establecer puntos de contacto para la coordinación con la OTAN en caso de crisis ciberseguridad con el objetivo de intercambiar la información necesaria sobre la situación y el uso de los mecanismos de respuesta a las crisis, a fin de mejorar la cooperación y la eficacia de la respuesta. Con este propósito, la Unión debe explorar cómo mejorar la puesta en común de información con la OTAN, de forma inclusiva, recíproca y no discriminatoria, en particular garantizando la existencia de herramientas para una comunicación segura al tiempo que se tienen en cuenta las normas relativas a la puesta en común de información de los distintos Estados miembros.

66) En el marco del programa continuo de ejercicios de ciberseguridad de la Unión a que se refiere el Capítulo V, los servicios de la Comisión y el SEAE deben considerar la posibilidad de organizar un ejercicio del personal con la OTAN destinado a poner a prueba la cooperación entre las entidades civiles y militares en caso de incidente de ciberseguridad a gran escala o crisis de ciberseguridad en el que los Estados miembros o la OTAN busquen respuestas para un ciberataque que afecte a su seguridad. El ejercicio debe llevarse a cabo de forma inclusiva y no discriminatoria y respetando plenamente los principios acordados en relación con los parámetros de cooperación UE-OTAN. El ejercicio debe realizarse en el marco del ejercicio «EU Integrated Resolve» (ejercicios paralelos y coordinados). Deben tomarse todas las medidas necesarias para garantizar la participación de todos los agentes a que se refiere el Plan Director de Ciberseguridad.

67) También debe considerarse, en consulta con el Consejo, la Comisión y el Alto Representante, la posibilidad de realizar ejercicios de ciberseguridad conjuntos a nivel de la Unión con los países de los Balcanes Occidentales, la República de Moldavia, Ucrania y otros socios estratégicos y terceros países afines.

X: Coordinación de la gestión de crisis de ciberseguridad con agentes militares a nivel de la UE

68) Los Estados miembros deben seguir reforzando la cooperación entre los ciberagentes civiles y militares a escala nacional.

69) EU-CyCLONe y la red de CSIRT deben determinar las modalidades y procedimientos posibles para cooperar con los agentes militares pertinentes de la UE, como la Conferencia de Cibermandos de la UE y la Red Operativa de Equipos Militares de Respuesta a Emergencias Informáticas, a fin de beneficiarse de una perspectiva militar y civil conjunta, en particular mediante reuniones conjuntas. EU-CyCLONe y la red de CSIRT deben informar al Consejo del progreso alcanzado con respecto a esta cooperación.

70) Se invita al Estado miembro afectado a que informe a EU-CyCLONe, así como al SEAE, si se emplean capacidades de respuesta militares nacionales o multinacionales pertinentes en el contexto de un incidente de ciberseguridad a gran escala o una crisis de ciberseguridad y se acuerda la transmisión de esta información entre el usuario y el proveedor de dicha capacidad de respuesta.

71) En el marco del programa continuo de ejercicios de ciberseguridad de la Unión a que se refiere el Capítulo V, la Comisión y el Alto Representante deben considerar la posibilidad de organizar un ejercicio conjunto destinado a poner a prueba la cooperación entre ciberagentes tanto civiles como militares en caso de incidente de ciberseguridad a gran escala que afecte a los Estados miembros.

XI: Recuperación y enseñanzas extraídas de una crisis de ciberseguridad

72) Los Estados miembros y las entidades y redes pertinentes de la Unión deben colaborar durante la fase de recuperación tras una crisis de ciberseguridad a fin de velar por el rápido restablecimiento de las funcionalidades esenciales. Los servicios policiales también deben participar en dicha cooperación, cuando proceda. En esta fase, la cooperación con el sector privado es crucial, en particular a la hora de facilitar la recuperación de datos y el restablecimiento de los sistemas. La coordinación eficaz entre las partes interesadas debe consistir principalmente en minimizar las perturbaciones y garantizar la continuidad de la actividad.

73) Los Estados miembros y las entidades y redes pertinentes de la Unión deben colaborar en la fase de recuperación basándose en las enseñanzas extraídas de las crisis de ciberseguridad o los incidentes de ciberseguridad gestionados en el pasado, así como en los informes de incidentes, en particular en el contexto del Mecanismo Europeo de Revisión de Incidentes de Ciberseguridad establecido por el Reglamento (UE) 2025/38.

74) EU-CyCLONe debe facilitar a la red de CSIRT, al Grupo de Cooperación SRI y al Consejo una lista exhaustiva de las enseñanzas extraídas de las crisis de ciberseguridad o los incidentes de ciberseguridad gestionados en el pasado y de las mejores prácticas. ENISA debe velar por que estas enseñanzas se reflejen adecuadamente en las futuras actividades de preparación y cuando se esté considerando la planificación de futuros ejercicios.

XII: Comunicación segura

75) Partiendo del inventario de herramientas de comunicación segura existentes ([15]), la Comisión debe proponer un conjunto interoperable de soluciones de comunicación seguras. El Consejo, la Comisión, el Alto Representante, EU-CyCLONe y la red de CSIRT deben acordar dicho conjunto antes del final de 2027. Estas soluciones deben aprovechar las actuaciones en el ámbito de las comunicaciones seguras que las instituciones de la UE pueden llevar a cabo con arreglo a la Estrategia de Preparación de la Unión y han de abarcar toda la gama de modos de comunicación necesarios (voz, datos, videoconferencia, mensajería, colaboración, puesta en común de documentos y consulta). Las soluciones deben cumplir los requisitos comúnmente definidos para la protección de la información delicada no clasificada. Deben emplearse soluciones basadas en un protocolo abierto con programas de código abierto adecuadas para la comunicación en tiempo real gestionadas por una entidad residente en la UE.

76) A los efectos del intercambio de información clasificada RESTREINT UE/EU RESTRICTED, EU-CyCLONe y la red de CSIRT deben poder utilizar, en caso necesario, canales de comunicación segura garantizados para las instituciones, los órganos y los organismos de la UE a fin de intercambiar información entre sí y con los Estados miembros.

77) El Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad, creado en virtud del Reglamento (UE) 2021/887 del Parlamento Europeo y del Consejo ([16]), 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 herramientas de comunicación segura. Debe evitarse toda duplicación de inversiones en sistemas seguros interoperables.

78) En particular, las entidades de la UE y los Estados miembros deben elaborar planes de contingencia para 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.

([15]) WK 862/2023.

([16]) 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).

79) Para dar una respuesta eficaz a las crisis de ciberseguridad, deben establecerse mecanismos de comunicación y puesta en común de información entre los servicios policiales y las redes de ciberseguridad, en particular en el ámbito técnico. Estos mecanismos deben respetar el papel de cada parte, evitar interferir en las operaciones en curso y garantizar la redundancia de las comunicaciones. El sistema europeo de comunicación crítica que se está desarrollando en la actualidad puede ser beneficioso para la respuesta conjunta con las comunidades cibernéticas pertinentes.

XIII: Disposiciones finales

80) EU-CyCLONe, en cooperación con la red de CSIRT y otros agentes principales del ecosistema de gestión de crisis de ciberseguridad de la UE y con el apoyo de ENISA, debe elaborar, en el plazo de un año tras la publicación de la presente Recomendación, diagramas detallados de flujo de procesos que describan los flujos de información entre los agentes pertinentes, los procesos decisorios y los informes elaborados durante la gestión de los incidentes de ciberseguridad a gran escala o crisis de ciberseguridad que se describen en la presente Recomendación. Los diagramas de flujo deben abarcar diferentes modalidades y capas de cooperación y deben actualizarse cuando sea necesario.

81) Para fomentar la aplicación eficaz del Plan Director de Ciberseguridad revisado y sobre la base de experiencia adquirida a través de los ejercicios de ciberseguridad conjuntos realizados con arreglo al Plan, en caso necesario el Consejo puede elaborar un conjunto de directrices de aplicación. Dichas directrices podrían abordar los retos detectados durante los ejercicios, así como colmar las lagunas y los elementos de enlace que faltan en la coordinación, la comunicación y la interacción operativa.

82) La Comisión debe revisar la presente Recomendación en cooperación con los Estados miembros, como mínimo cada cuatro años tras su publicación. Tras cada revisión, la Comisión debe publicar un informe y presentarlo al Consejo. La Comisión y los Estados miembros deben tener en cuenta, en particular, las repercusiones del panorama de amenazas cambiante, los resultados de los ejercicios conjuntos y los cambios legislativos, en especial cualquier posible cambio derivado de la revisión del Reglamento (UE) 2019/881.

Hecho en Bruselas, el 6 de junio de 2025.

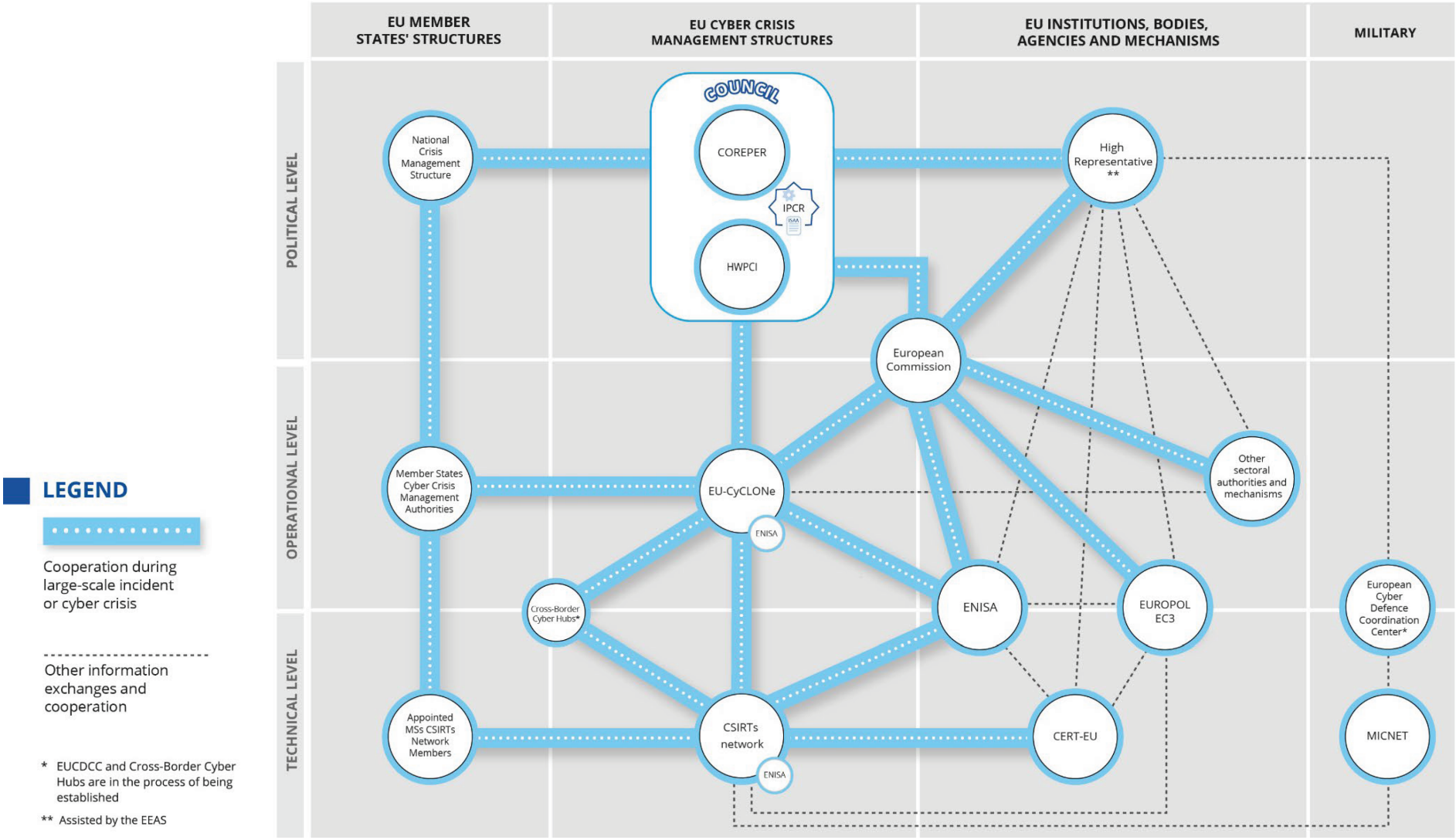
Por el Consejo

El Presidente

D. KLIMCZAK

ANEXO I

PLAN DIRECTOR DE LA UNIÓN PARA RESPONDER A UNA CRISIS DE CIBERSEGURIDAD



ANEXO II

AGENTES PERTINENTES DE LA UNIÓN (ENTIDADES Y REDES) Y MECANISMOS DE GESTIÓN DE CRISIS

(1) **Participación de los agentes principales en todo el ciclo de vida de la gestión de crisis de ciberseguridad (incidentes de ciberseguridad a gran escala y crisis de ciberseguridad)**

	Preparación	Detección	Respuesta a incidentes de ciberseguridad a gran escala o crisis de ciberseguridad			Comunicación pública	Recuperación y enseñanzas extraídas
			en el nivel técnico	en el nivel operativo	en el nivel político		
Estados miembros	X	X	X	X	X	X	X
Comisión	X			X	X	X	
Alto Representante, con la asistencia del SEAE	X			X	X	X	
Consejo	X				X	X	X
ENISA	X		X	X			
CERT-EU	X	X	X	X		X	X
Red de CSIRT	X	X	X				X
EU-CyCLONe	X			X	X		X

(2) **Funciones y competencias de los agentes y mecanismos pertinentes de la Unión (por orden alfabético del inglés) en relación con la gestión de crisis de ciberseguridad**

Agente	Nivel	Función y competencia	Referencia
CERT-EU	Técnico / operativo	Coordina la respuesta a las crisis en el nivel técnico y la gestión de los incidentes graves que afecten a las entidades de la Unión. Lleva un inventario de los conocimientos técnicos disponibles que serían necesarios para la respuesta a incidentes en caso de incidentes graves y asiste al CIIC en la coordinación de los planes de gestión de crisis de ciberseguridad de las entidades de la Unión para los incidentes graves. Miembro de la red de CSIRT. Presta apoyo a la Comisión en EU-CyCLONe con respecto a la gestión coordinada de los incidentes y crisis de ciberseguridad a gran escala. Actúa como centro de intercambio de información sobre ciberseguridad y de coordinación de la respuesta a incidentes, facilitando el intercambio de información sobre incidentes, ciberamenazas, vulnerabilidades y cuasiincidentes entre entidades y contrapartes de la Unión. Solicita la utilización de la Reserva de Ciberseguridad de la UE en nombre de las entidades de la Unión. Coopera con el Centro de Ciberseguridad de la OTAN con arreglo a su acuerdo técnico.	Reglamento (UE, Euratom) 2023/2841 Reglamento (UE) 2025/38
Consejo de la Unión Europea	Político	Ejerce funciones de definición de políticas y de coordinación. Tiene a su cargo la RPIC, que está relacionada con la coordinación y la respuesta en el nivel político de la Unión.	Artículo 16 del Tratado de la Unión Europea
Presidencia del Consejo de la Unión Europea	Político	Decide (excepto cuando se invoca la cláusula de solidaridad en virtud del artículo 222 del Tratado de Funcionamiento de la Unión Europea) si procede activar la RPIC previa consulta a los Estados miembros afectados, según proceda, así como a la Comisión y al Alto Representante.	Artículo 16 del Tratado de la Unión Europea Decisión de Ejecución (UE) 2018/1993 del Consejo

Agente	Nivel	Función y competencia	Referencia
Centros cibernéticos transfronterizos	Técnico	Un centro cibernético transfronterizo es una plataforma plurinacional creada mediante un acuerdo de consorcio escrito que reúne en una estructura de red coordinada a los centros cibernéticos nacionales de al menos tres Estados miembros, y que se ha concebido para mejorar el seguimiento, la detección y el análisis de las ciberamenazas, prevenir los incidentes y fomentar la producción de inteligencia sobre ciberamenazas, en particular mediante el intercambio de datos e información pertinentes, en su caso anonimizados, así como mediante la puesta en común de herramientas de vanguardia y el desarrollo conjunto de capacidades de detección, análisis, prevención y protección cibernéticos en un entorno de confianza; Cooperan estrechamente con la red de CSIRT para compartir información. Facilitan información relativa a un incidente de ciberseguridad a gran escala, potencial o en curso, a las autoridades de los Estados miembros y a la Comisión a través de EU-CyCLONe y la red de CSIRT.	Reglamento (UE) 2025/38
Red de CSIRT	Técnico	Contribuye al refuerzo de la confianza y la seguridad y fomenta una cooperación operativa rápida entre los Estados miembros. Es la principal red para intercambiar información pertinente sobre los incidentes, los cuasiincidentes, las ciberamenazas, los riesgos y las vulnerabilidades. A petición de un miembro potencialmente afectado por un incidente, la red intercambia y debate información relacionada con dicho incidente y las ciberamenazas asociadas. La red también puede facilitar la respuesta coordinada a un incidente que se haya detectado dentro del ámbito de competencia de un miembro solicitante. Presta asistencia a los Estados miembros a la hora de gestionar incidentes transfronterizos y explora otras formas de cooperación, entre ellas, la asistencia mutua. Recibe información de los Estados miembros sobre sus solicitudes a la Reserva de Ciberseguridad de la UE.	Directiva (UE) 2022/2555 Reglamento (UE) 2025/38

Agente	Nivel	Función y competencia	Referencia
Conferencia de Cibermandos		Un foro para que los cibermandos nacionales de los Estados miembros colaboren e intercambien información vital sobre las operaciones y estrategias en curso en el ciberespacio con el fin de mitigar los incidentes de ciberseguridad a gran escala. Lo organiza la Presidencia rotatoria del Consejo de la Unión Europea con el apoyo de la Agencia Europea de Defensa (AED) y del Servicio Europeo de Acción Exterior (SEAE), incluido el Estado Mayor de la UE (EMUE).	Comunicación conjunta sobre la política de ciberdefensa de la UE (2022)
Comisión	Operativo / político	Órgano ejecutivo de la Unión Europea. Garantiza el buen funcionamiento del mercado interior. Facilita la coherencia y la coordinación entre las acciones conexas de respuesta a las crisis a nivel de la Unión. Determinadas acciones generales de preparación a nivel de la Unión en virtud de la Decisión MPCU, incluida la gestión del Centro de Coordinación de la Respuesta a Emergencias y del Sistema Común de Comunicación e Información de Emergencia. Observador en EU-CyCLONe y miembro cuando un incidente a gran escala, potencial o en curso, tenga o pueda tener repercusiones significativas en los servicios y actividades incluidos en el ámbito de aplicación de la Directiva (UE) 2022/2555. Observador en la red de CSIRT. Responsabilidad general de la implementación de la Reserva de Ciberseguridad de la UE. Punto de contacto en el Consejo Interinstitucional de Ciberseguridad para la puesta en común de información pertinente relativa a incidentes graves con EU-CyCLONe. La Presidencia del Consejo le consulta sobre las decisiones de activar o desactivar la RPIC (excepto cuando se invoca la cláusula de solidaridad en virtud del artículo 222 del TFUE). Los servicios de la Comisión elaboran, junto con el SEAE, los informes ISAA.	Artículo 17 del Tratado de la Unión Europea Decisión de Ejecución (UE) 2018/1993 Decisión n.º 1313/2013/UE Directiva (UE) 2022/2555 Reglamento (UE) 2025/38 Reglamento (UE, Euratom) 2023/2841

Agente	Nivel	Función y competencia	Referencia
Agencia de la Unión Europea para la Ciberseguridad (ENISA)	Técnico / operativo	Desempeña su cometido con el fin de lograr un elevado nivel de ciberseguridad en toda la Unión, especialmente mediante el apoyo activo a los Estados miembros y a las instituciones de la Unión. Se encarga de la secretaría de la red de CSIRT y EU-CyCLONe. Prepara un informe periódico y detallado sobre la situación técnica de la ciberseguridad en la UE relativo a incidentes y ciberamenazas (con EC3 y el CERT-EU y en estrecha colaboración con los Estados miembros). Contribuye a la preparación de una respuesta común a crisis o incidentes transfronterizos a gran escala, en particular, mediante: — la agregación y el análisis de informes de fuentes nacionales; — la garantía del flujo de información entre los niveles técnico, operativo y político; — la facilitación de la gestión de incidentes, previa solicitud; — el apoyo a las entidades de la Unión en lo que respecta a la comunicación pública; — el apoyo a los Estados miembros en lo que respecta a la comunicación pública, previa solicitud; — la puesta a prueba de las capacidades de respuesta a incidentes y la organización periódica de ejercicios de ciberseguridad. Asume las funciones de órgano de contratación cuando se le hayan encomendado el funcionamiento y la administración de la Reserva de Ciberseguridad de la UE, parcialmente o por completo. Organiza, en el ámbito de la Unión y con frecuencia bienal, un ejercicio exhaustivo de ciberseguridad a gran escala con elementos técnicos, operativos o estratégicos. Elabora informes de revisión de incidentes en colaboración con el Estado miembro afectado y otras partes interesadas pertinentes, para evaluar las causas, las consecuencias y la medidas paliativas de los incidentes (a petición de la Comisión o de EU-CyCLONe y con la aprobación del Estado miembro afectado). Informa a EU-CyCLONe si la información facilitada en virtud de las obligaciones de información del Reglamento de Ciberresiliencia son pertinentes para la gestión coordinada de incidentes de ciberseguridad a gran escala y crisis a nivel operativo.	Directiva (UE) 2022/2555 Reglamento (UE) 2019/881 Reglamento (UE) 2025/38 Reglamento (UE) 2024/2847

Agente	Nivel	Función y competencia	Referencia
Red Europea de Organizaciones de Enlace Nacionales para las Crisis de Ciberseguridad (EU-CyCLONe)	Operativo	Apoya la gestión coordinada de crisis e incidentes de ciberseguridad a gran escala a nivel operativo. Garantiza el intercambio regular de información pertinente entre los Estados miembros y las instituciones, los órganos y los organismos de la Unión. Coordina la gestión de incidentes y crisis de ciberseguridad a gran escala y apoya la toma de decisiones a nivel político en relación con tales incidentes y crisis. Evalúa las consecuencias y las repercusiones de los incidentes y crisis de ciberseguridad a gran escala pertinentes y propone posibles medidas de mitigación. Examina, a petición de un Estado miembro afectado, los planes nacionales de respuesta a incidentes y crisis de ciberseguridad a gran escala. Elabora, junto con ENISA y la Comisión, el modelo para facilitar la presentación de solicitudes de apoyo de la Reserva de Ciberseguridad de la UE. Recibe información de los Estados miembros sobre sus solicitudes a la Reserva de Ciberseguridad de la UE. Recibe información relativa a un incidente de ciberseguridad a gran escala, potencial o en curso, de los centros cibernéticos transfronterizos o de la red de CSIRT.	Directiva (UE) 2022/2555 Reglamento (UE) 2025/38

Agente	Nivel	Función y competencia	Referencia
Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad, con el apoyo del Servicio Europeo de Acción Exterior	Político	Dirige y coordina los esfuerzos de la Unión para hacer frente a las amenazas a la seguridad exterior en los ámbitos de amenazas híbridas y de ciberseguridad. Responsable de los instrumentos de ciberdiplomacia y ciberdefensa de la Unión para disuadir y responder a las amenazas externas, entre otros medios, utilizando los instrumentos contra las amenazas híbridas y de ciberdiplomacia de la Unión. Colabora con socios externos, también a través de la participación de la PCSD. Proporciona preparación de cara a la conciencia situacional y la capacidad de la Unión y de los Estados miembros para reaccionar ante las amenazas híbridas y de ciberseguridad, por ejemplo, mediante ejercicios prácticos, formación y redes. Se ocupa de las implicaciones en materia de seguridad y defensa de los activos espaciales de la Unión, especialmente en el marco de la política común de seguridad y defensa (PCSD) de la Unión. Presta apoyo a la Conferencia de Cibermandos de la UE. Presta apoyo a la Red Operativa de Equipos Militares de Respuesta a Emergencias Informáticas (MICNET). La Presidencia del Consejo le consulta sobre las decisiones de activar o desactivar la RPIC (excepto cuando se invoca la cláusula de solidaridad en virtud del artículo 222 del TFUE). El SEAE elabora junto con los servicios de la Comisión los informes ISAA.	Decisión 2010/427/UE del Consejo
Centro de Coordinación de la Ciberdefensa de la UE	Horizontal	Su objetivo inicial es, en primer lugar, mejorar principalmente una conciencia situacional común de la Unión y sus Estados miembros sobre las actividades malintencionadas en el ciberespacio, en particular en lo que respecta a las misiones y operaciones militares de la PCSD.	Comunicación conjunta sobre la política de ciberdefensa de la UE (2022)
Europol	Operativo	Presta apoyo operativo y técnico a las autoridades competentes de los Estados miembros para la prevención y disuasión de la ciberdelincuencia. Ayuda a las autoridades competentes de los Estados miembros, a petición de estas, a responder a ciberataques de presunto origen delictivo.	Reglamento (UE) 2016/794, con todas sus modificaciones

ELI: http://data.europa.eu/eli/C/2025/3445/oj

Agente	Nivel	Función y competencia	Referencia
Consejo Interinstitucional de Ciberseguridad		Establece un plan de gestión de crisis de ciberseguridad para apoyar, desde el punto de vista operativo, la gestión coordinada de los incidentes graves que afecten a las entidades de la Unión y contribuir al intercambio periódico de información pertinente. Coordina la adopción de los planes de gestión de crisis de ciberseguridad de las distintas entidades de la Unión. Adopta, sobre la base de una propuesta del CERT-EU, directrices o recomendaciones sobre la cooperación en materia de respuesta a incidentes en caso de incidentes significativos que afecten a entidades de la Unión.	Reglamento (UE, Euratom) 2023/2841
Red Operativa de Equipos Militares de Respuesta a Emergencias Informáticas (MICNET)	Técnico	Fomenta una respuesta más sólida y coordinada a las ciberamenazas que afectan a los sistemas de defensa de la Unión, incluidos los utilizados en misiones y operaciones militares de la PCSD; recibe el apoyo de la Agencia Europea de Defensa.	Comunicación conjunta sobre ciberdefensa de 2022
Capacidad Única de Análisis de Inteligencia (SIAC)		Compuesta por 1) el Centro de Inteligencia y de Situación de la Unión Europea (INTCEN) y 2) la Dirección de Información del Estado Mayor de la Unión Europea (EMUE INT). Proporciona inteligencia estratégica sobre política exterior, terrorismo y amenazas híbridas, y Se ocupa de la inteligencia militar para las misiones de la PCSD y apoya las operaciones de defensa y gestión de crisis de la Unión. Bajo la autoridad del Alto Representante.	Artículos 38 y 42 a 46 del Tratado de la Unión Europea

(3) **Mecanismos y plataformas de gestión de crisis pertinentes a nivel de la Unión**

Mecanismo	Horizontal / sectorial / ámbito cibernético	Descripción	Referencia
ARGUS	Horizontal	Proceso de coordinación y sistema general de alerta de la Comisión para dar una respuesta coherente en casos de crisis transfronterizas graves que requieran una actuación a nivel de la UE. Reúne a todos los servicios y gabinetes pertinentes para tomar decisiones sobre las medidas y coordinarlas. Permite a la Comisión intercambiar información pertinente sobre crisis multisectoriales emergentes o amenazas previsibles o inminentes que requieran la actuación de la Unión.	Comunicación COM(2005) 662 final de la Comisión

Mecanismo	Horizontal / sectorial / ámbito cibernético	Descripción	Referencia
Centro de Respuesta a las Crisis (CRC) del SEAE	Horizontal	Punto de entrada único para todas las cuestiones relacionadas con crisis en el SEAE y la capacidad permanente de respuesta a las crisis 24/7 para emergencias que amenacen la seguridad del personal de las delegaciones de la UE o en respuesta a crisis que afecten a ciudadanos de la Unión en el extranjero. Reúne a expertos en seguridad, conciencia situacional y asuntos consulares al tiempo que se apoya en profesionales destacados sobre el terreno en las delegaciones de la Unión.	Una Brújula Estratégica para la Seguridad y la Defensa – Por una Unión Europea que proteja a sus ciudadanos, defienda sus valores e intereses y contribuya a la paz y la seguridad internacionales (21 de marzo de 2022)
Plan Director de Infraestructuras Críticas	Horizontal	Coordina la respuesta de la Unión a las perturbaciones de infraestructuras críticas con importancia transfronteriza significativa.	Recomendación C/2024/4371 del Consejo
Sistema de Alerta de Ciberseguridad	Ámbito cibernético	Garantiza capacidades avanzadas de la Unión para mejorar las capacidades de detección, análisis y tratamiento de datos en relación con las ciberamenazas y la prevención de incidentes en la Unión.	Reglamento (UE) 2025/38
Conjunto de instrumentos de ciberdiplomacia (marco para una respuesta diplomática conjunta de la UE a las actividades informáticas malintencionadas)	Ámbito cibernético	Facilita la respuesta diplomática conjunta de la Unión a las actividades informáticas malintencionadas, que contribuye a la prevención de conflictos, la mitigación de las amenazas de ciberseguridad y una mayor estabilidad en las relaciones internacionales.	Conclusiones del Consejo de 19 de junio de 2017 Directrices de aplicación revisadas 10289/23, 8 de junio de 2023
Reserva de Ciberseguridad de la UE	Ámbito cibernético	Moviliza recursos y a expertos en ciberseguridad durante las crisis para apoyar los esfuerzos de respuesta en los Estados miembros y en las instituciones, órganos u organismos de la Unión	Reglamento (UE) 2025/38
Código de red sobre normas sectoriales específicas para los aspectos de ciberseguridad de los flujos transfronterizos de electricidad	Sectorial	Establece un proceso recurrente de evaluaciones de riesgos de ciberseguridad en el sector de la electricidad a nivel de la Unión, de los Estados miembros, regional y de las entidades. Contiene disposiciones específicas para la gestión de crisis y la cooperación con los CSIRT y EU-CyCLONe en caso de que un incidente de ciberseguridad a gran escala repercuta en otros sectores dependientes de la seguridad del suministro de electricidad.	Reglamento Delegado (UE) 2024/1366 de la Comisión

ELI: http://data.europa.eu/eli/C/2025/3445/oj

Mecanismo	Horizontal / sectorial / ámbito cibernético	Descripción	Referencia
Conjunto de instrumentos contra las amenazas híbridas	Horizontal	Incluye un conjunto de disposiciones para garantizar una visión general de lo que está disponible en la UE para responder a todo tipo de amenazas híbridas y su uso coordinado, garantizando la coherencia de nuestras acciones en todos los ámbitos. El conjunto de instrumentos contra las amenazas híbridas ayuda a garantizar que la toma de decisiones se base en una conciencia situacional global y en las lecciones extraídas.	Conclusiones del Consejo sobre un marco para una respuesta coordinada de la UE a las campañas híbridas, de 22 de junio de 2022 Directrices de aplicación para el marco para una respuesta coordinada de la UE a las campañas híbridas, 14 de diciembre de 2022
Equipos de respuesta rápida de la UE contra amenazas híbridas	Horizontal	Dentro del conjunto de instrumentos de la UE contra las amenazas híbridas, los equipos de respuesta rápida de la UE contra amenazas híbridas se basan en los conocimientos especializados sectoriales nacionales y de la UE en materia civil y militar para proporcionar asistencia a corto plazo, adaptada y específica a los Estados miembros, a las misiones y operaciones de la política común de seguridad y defensa y a los países socios en la lucha contra las amenazas y campañas híbridas.	Marco orientativo para los aspectos prácticos del establecimiento de equipos de respuesta rápida de la UE contra amenazas híbridas (21 de mayo de 2024) Orientaciones operativas para el despliegue de equipos de respuesta rápida contra amenazas híbridas, aprobadas por el Coreper el 4 de diciembre de 2024
RPIC	Horizontal	Apoya la toma de decisiones rápida y coordinada en el nivel político de la Unión en caso de crisis graves y complejas. La decisión de activación y desactivación la adopta 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. La SGC, los servicios de la Comisión y el SEAE también podrán acordar, en consulta con la Presidencia, activar la RPIC en modo de puesta en común de información. La labor de la RPIC se basa en los informes ISAA elaborados por los servicios de la Comisión y el SEAE. Dichos informes se basan en la información y los análisis pertinentes aportados por los Estados miembros (por ejemplo, a través de los correspondientes centros nacionales de crisis) y por los órganos y organismos pertinentes de la Unión.	Decisión de Ejecución (UE) 2018/1993 del Consejo
Protocolo de Respuesta Policial ante Emergencias de la UE	Horizontal	Herramienta para ayudar a los servicios policiales de la Unión a dar una respuesta inmediata a los ciberataques transfronterizos importantes mediante una evaluación rápida, la puesta en común segura y oportuna de información crítica y la coordinación eficaz de los aspectos internacionales de sus investigaciones.	Conclusiones del Consejo (26 de junio de 2018) sobre la respuesta coordinada de la UE a los incidentes y crisis de ciberseguridad a gran escala.

Mecanismo	Horizontal / sectorial / ámbito cibernético	Descripción	Referencia
Equipos de Respuesta Telemática Rápida de la CEP	Ámbito cibernético	Los Equipos de Respuesta Telemática Rápida de la CEP representan una capacidad de ciberdefensa de ámbito civil-militar creada en común para responder rápidamente a los incidentes y crisis de ciberseguridad, así como para llevar a cabo acciones preventivas, como evaluaciones de la vulnerabilidad y observación electoral. Su cometido es facilitar apoyo cibernético, previa solicitud, a los Estados miembros de la UE, las instituciones, órganos y organismos de la UE, las misiones y operaciones militares de la PCSD de la UE, así como a los países socios.	Artículo 42, apartado 6, artículo 46 y Protocolo n.º 10 del Tratado de la Unión Europea.
Arquitectura de respuesta a amenazas espaciales	Sectorial (Amenazas espaciales, incluidas las relacionadas con la ciberseguridad)	Arquitectura de respuesta a las amenazas espaciales sobre las responsabilidades que deben ejercer el Consejo y el Alto Representante para evitar una amenaza derivada de la instalación, funcionamiento o utilización de los sistemas creados y de los servicios prestados en el marco del Programa Espacial de la Unión	Decisión (PESC) 2021/698 del Consejo
Marco de coordinación de ciberincidentes sistémicos (EU-SCICF)	Sectorial	Marco que se está creando para la comunicación y la coordinación que aborda y gestiona posibles sucesos sistémicos de ciberseguridad en el sector financiero. Se basará en una de las funciones previstas de las Autoridades Europeas de Supervisión en virtud del Reglamento (UE) 2022/2554 de facilitar de forma gradual una respuesta coordinada eficaz a nivel de la Unión en caso de que se produzca un incidente transfronterizo grave relacionado con las tecnologías de la información y la comunicación (TIC) o una amenaza conexa que tenga un impacto sistémico en el sector financiero de la Unión en su conjunto.	Recomendación de la Junta Europea de Riesgo Sistémico, de 2 de diciembre de 2021, sobre un marco paneuropeo de coordinación de ciberincidentes sistémicos para las autoridades pertinentes (JERS/2021/17)
Mecanismo de Protección Civil de la Unión	Horizontal	Garantiza la cooperación en materia de protección civil para mejorar la prevención, la preparación y la respuesta ante catástrofes.	Decisión n.º 1313/2013
ECII - Entorno Común de Intercambio de Información	Ámbito marítimo específico que abarca siete sectores.	ECII es una red que conecta sistemas de autoridades de la UE/EEE responsables de la vigilancia marítima. El ECII permite el intercambio de información pertinente a través de las fronteras y de diferentes sectores de manera fluida y automatizada.	Una Brújula Estratégica para la Seguridad y la Defensa – Por una Unión Europea que proteja a sus ciudadanos, defienda sus valores e intereses y contribuya a la paz y la seguridad internacionales (21 de marzo de 2022)

(4) **Sectores de alta criticidad y otros sectores críticos con arreglo a la Directiva (UE) 2022/2555 y mecanismos de crisis sectoriales a nivel de la Unión (cuando proceda)**

Sectores	Subsector	Mecanismos de gestión de crisis sectoriales aplicables
Energía	Electricidad	Grupo de Coordinación de la Electricidad
	Sistemas urbanos de calefacción y de refrigeración	n. p.
	Crudo	Grupo de Coordinación del Petróleo Grupo de Autoridades de la Unión Europea para las Actividades en Alta Mar del Sector del Petróleo y el Gas (EUOAG)
	Gas	Grupo de Coordinación del Gas
	Hidrógeno	n. p.
Transporte	Transporte aéreo	Célula de Coordinación de Crisis de la Aviación Europea (CCCAE)
	Transporte por ferrocarril	n. p.
	Transporte marítimo y fluvial	Agencia Europea de Control de la Pesca (AECP) SafeSeaNet (SSN) Servicios Marítimos Integrados (IMS) Centro de datos de identificación y seguimiento de largo alcance (LRIT) Servicios de Apoyo Marítimo de la AESM
	Transporte por carretera	n. p.
	Horizontal	La Red de Puntos de Contacto para el Transporte, establecida por el Plan de Contingencia para el Transporte [COM (2022) 211]
Banca		EU-SCICF
Infraestructuras de los mercados financieros		EU-SCICF Mecanismo Europeo de Estabilización Financiera

Sectores	Subsector	Mecanismos de gestión de crisis sectoriales aplicables
Sector sanitario		Sistema de Alerta Precoz y Respuesta (SAPR) Centro de Operaciones de Emergencia Sanitaria (HEOF), sistema de alerta rápida para componentes tisulares, celulares y sanguíneos (RATC/RAB) Marco de emergencia de salud pública Sistema de alerta rápida para incidentes químicos (RASCHEM) Portal Europeo de Vigilancia de Enfermedades Infecciosas Autoridad de Preparación y Respuesta ante Emergencias Sanitarias (HERA) Sistema de información médica y sanitaria (MediSys) Grupo Director Ejecutivo sobre la Escasez de Productos Sanitarios (MDSSG) Alerta Rápida de Farmacovigilancia Grupo de Trabajo sobre Salud de la UE (EUHTF) Comité de Seguridad Sanitaria
Agua potable		n. p.
Aguas residuales		n. p.
Infraestructura digital		n. p.
Gestión de Servicios de TIC		n. p.
Entidades de la Administración pública, con exclusión del poder judicial, los parlamentos y los bancos centrales		n. p.
Espacio		Arquitectura de respuesta a amenazas espaciales
Servicios postales y de mensajería		n. p.
Gestión de residuos		n. p.
Fabricación, producción y distribución de sustancias y mezclas químicas		Sistema de alerta rápida para incidentes químicos (RASCHEM)

Sectores	Subsector	Mecanismos de gestión de crisis sectoriales aplicables
Producción, transformación y distribución de alimentos		Sistema europeo de seguimiento de cultivos Detección de puntos críticos de anomalías en la producción agrícola mundial (ASAP) Red Europea de Información Fitosanitaria (Europhyt) Equipo de Emergencia Veterinaria de la UE (EUVET) Sistema de Alerta Rápida para Alimentos y Piensos (RASFF) Mecanismo Europeo de Preparación y Respuesta ante las Crisis de Seguridad Alimentaria (MEPRCSA) Reglamento de Emergencia y Resiliencia del Mercado Interior
Fabricación	Productos sanitarios	n. p.
	Productos informáticos, electrónicos y ópticos	n. p.
	Maquinaria y equipos	n. p.
	Fabricación de vehículos de motor, remolques y semirremolques	n. p.
	Fabricación de otros equipos de transporte	n. p.
Proveedores de servicios digitales		n. p.
Investigación		n. p.

ANEXO III

MARCO DE GESTIÓN DE CRISIS DE CIBERSEGURIDAD DE LA UE E INSTRUMENTOS RELACIONADOS

Desde 2017, la Unión ha creado su marco de ciberseguridad a través de varios instrumentos que contienen disposiciones pertinentes para la gestión de las crisis de ciberseguridad:

— Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo ([1]);

— Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo ([2]);

— Reglamento de Ejecución (UE) 2024/2690 de la Comisión ([3]), Reglamento (UE, Euratom) 2023/2841 del Parlamento Europeo y del Consejo ([4]);

— Reglamento (UE) 2021/887 del Parlamento Europeo y del Consejo ([5]);

— Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo ([6]), y

— Reglamento (UE) 2025/38 del Parlamento Europeo y del Consejo ([7]).

Entre las medidas sectoriales específicas en materia de crisis de ciberseguridad figuran el Reglamento Delegado (UE) 2024/1366 de la Comisión ([8]) y el futuro marco de coordinación de ciberincidentes sistémicos (EU-SCICF) en el contexto del Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo ([9]).

([1]) 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).

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

([3]) 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 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).

([4]) 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).

([5]) 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).

([6]) 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).

([7]) 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).

([8]) 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).

([9]) 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).

La Directiva 2013/40 ([10]) 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 ([11]), cuando sea aplicable, facilitará considerablemente las medidas policiales en este ámbito.

La política de ciberdefensa de la UE ([12]) esboza las funciones de la Red Operativa de Equipos 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 nivel de la Unión en caso de perturbaciones de infraestructuras críticas con importancia transfronteriza significativa» ([13]) prevé la cooperación entre los agentes pertinentes cuando un incidente afecte tanto a aspectos físicos como a la ciberseguridad de las infraestructuras críticas.

([10]) 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).

([11]) 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).

([12]) JOIN(2022) 49 final.

([13]) DO C, C/2024/4371, 5.7.2024.