Consejo de la Unión Europea

Bruselas, 7 de septiembre de 2023
(OR. en)

12485/23
ADD 1

Expediente interinstitucional: 2023/0318(NLE)

PROCIV 57
ENV 925
JAI 1084
SAN 494
COSI 140
CHIMIE 85
ENFOPOL 356
RECH 380
CT 133
DENLEG 38
COTER 153
RELEX 987
ENER 467
HYBRID 53
TRANS 329
CYBER 203
TELECOM 251
ESPACE 45
ATO 48
CSC 408
ECOFIN 839
CSCI 149
DATAPROTECT 216
MI 698
CODEC 1500
COPS 418
JAIEX 46
COPEN 292
IND 441
POLMIL 221
IPCR 55
DIGIT 160
DISINFO 62
CSDP/PSDC 608
MARE 18
POLMAR 47

NOTA DE TRANSMISIÓN

De:	Por la secretaria general de la Comisión Europea, D.ª Martine DEPREZ, directora
Fecha de recepción:	6 de septiembre de 2023
A:	D.ª Thérèse BLANCHET, secretaria general del Consejo de la Unión Europea
N.° doc. Ción.:	COM(2023) 526 final - ANEXO
Asunto:	ANEXO de la Propuesta de RECOMENDACIÓN DEL CONSEJO sobre un Plan director para coordinar la respuesta a escala de la Unión en caso de perturbaciones de infraestructuras críticas con importancia transfronteriza significativa

Adjunto se remite a las Delegaciones el documento – COM(2023) 526 final - ANEXO.

Adj.: COM(2023) 526 final - ANEXO

COMISIÓN
EUROPEA

Bruselas, 6.9.2023
COM(2023) 526 final

ANNEX

ANEXO

de la

Propuesta de RECOMENDACIÓN DEL CONSEJO

sobre un Plan director para coordinar la respuesta a escala de la Unión en caso de perturbaciones de infraestructuras críticas con importancia transfronteriza significativa

ANEXO

El presente anexo describe los principios, los objetivos, los principales agentes, la interacción con los mecanismos existentes de respuesta a las crisis y el funcionamiento de un Plan director para coordinar la respuesta a incidentes significativos que afecten a infraestructuras críticas («Plan director de infraestructuras críticas») y mejorar la cooperación entre los Estados miembros y las instituciones, órganos y organismos pertinentes de la Unión en relación con tales incidentes, de conformidad con las normas y procedimientos aplicables. El Plan no afecta en modo alguno al papel ni al funcionamiento de otras disposiciones.

PARTE I: OBJETIVOS, PRINCIPIOS, AGENTES Y OTROS INSTRUMENTOS

1. Objetivos

El Plan director de infraestructuras críticas tiene por objeto alcanzar los tres objetivos principales siguientes en respuesta a un incidente significativo de infraestructura crítica:

a) **Conocimiento compartido de la situación**, ya que una buena comprensión del incidente en una infraestructura crítica en los Estados miembros, su origen y sus posibles consecuencias para todas las partes interesadas pertinentes a nivel operativo, estratégico y político es esencial para una respuesta coordinada adecuada.

b) **Comunicación pública coordinada**, pues contribuye a mitigar los efectos negativos del incidente y a minimizar las discrepancias en los mensajes transmitidos al público en los Estados miembros y entre ellos. Una comunicación pública clara también es importante para mitigar las consecuencias de la desinformación.

c) **Una respuesta eficaz**, dado que el refuerzo de la respuesta de los Estados miembros y de la cooperación entre ellos y con las instituciones, órganos y organismos pertinentes de la Unión contribuye a mitigar los efectos del incidente y permite el rápido restablecimiento de los servicios esenciales de forma que se reduzca al mínimo la vulnerabilidad frente a nuevos incidentes significativos.

2. Principios

Proporcionalidad

Los incidentes que perturban infraestructuras críticas o la prestación de servicios esenciales a menudo se sitúan por debajo del umbral de un incidente significativo de infraestructura crítica, tal como se especifica en el punto 2 de la presente Recomendación. Como tales, pueden abordarse, en principio, de forma eficaz a nivel nacional. Por lo tanto, la aplicación del Plan director de infraestructuras críticas se limita a los incidentes significativos de infraestructuras críticas.

Subsidiariedad

Los Estados miembros tienen la responsabilidad principal de responder a las perturbaciones de una infraestructura crítica o de los servicios esenciales prestados por entidades críticas, de conformidad con el Derecho de la Unión. No obstante, las instituciones, órganos y organismos pertinentes de la Unión, así como el Servicio Europeo de Acción Exterior («SEAE»), desempeñan un importante papel complementario en caso de un incidente significativo en infraestructuras críticas con gran importancia transfronteriza, ya que puede afectar a varios o incluso a todos los sectores de la actividad económica del mercado interior, la vida de los ciudadanos de la Unión, la seguridad y las relaciones internacionales de la Unión.

Complementariedad

El Plan tiene en cuenta y refleja el funcionamiento de los mecanismos de gestión de crisis existentes a escala de la Unión, a saber, el Dispositivo de Respuesta Política Integrada a las Crisis («DIRPC») del Consejo, el proceso de coordinación interna de crisis de la Comisión ARGUS, el Mecanismo de Protección Civil de la Unión («MPCU»), apoyado por el Centro de Coordinación de la Respuesta a Emergencias («CECRE»), y el Mecanismo de Respuesta a las Crisis del SEAE. También se basa en disposiciones sectoriales, incluidas las relativas a la gestión coordinada de los incidentes de ciberseguridad a gran escala previstas en la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo[1] y el marco establecido en el Plan director para la respuesta coordinada a incidentes y crisis de ciberseguridad transfronterizos a gran escala («Plan director cibernético»)[2], la Red de puntos de contacto para el transporte[3] y la Célula de Coordinación de Crisis de la Aviación Europea[4].

Además, el Plan se basa en las estructuras y mecanismos establecidos por la Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo[5], en particular en lo que respecta a la cooperación entre las autoridades competentes y con la Comisión y con el Grupo de Resiliencia de las Entidades Críticas, y debe aplicarse de conformidad con ellas. También tiene en cuenta las responsabilidades de las instituciones, órganos y organismos de la Unión pertinentes en virtud del marco jurídico que les es aplicable. Las actividades de respuesta a las crisis de infraestructuras críticas son complementarias de otros mecanismos de gestión de crisis a escala de la Unión, nacional y sectorial que apoyan la coordinación multisectorial.

Confidencialidad de la información

El Plan tiene en cuenta la importancia de salvaguardar la confidencialidad de la información clasificada y sensible no clasificada relacionada con las infraestructuras y las entidades críticas.

3. Agentes pertinentes

Cada Estado miembro y las instituciones, órganos y organismos pertinentes de la Unión a que se refieren las letras a) a e) siguientes decidirán, de conformidad con las normas y el procedimiento que les sean aplicables, los agentes pertinentes para cada incidente significativo de infraestructura crítica, en función del sector afectado y del tipo de incidente.

a) Estados miembros

- Autoridades competentes (por ejemplo, las encargadas de las infraestructuras críticas; autoridades sectoriales pertinentes; puntos de contacto únicos designados o establecidos de conformidad con el artículo 9, apartado 2, de la Directiva (UE) 2022/2557; autoridades

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

[2] 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).

[3] Comunicación de la Comisión - Plan de contingencia para el transporte, COM(2022) 211 final.

[4] Creada en virtud del artículo 19 del Reglamento de Ejecución (UE) 2019/123 de la Comisión, de 24 de enero de 2019, por el que se establecen disposiciones de aplicación de las funciones de la red de gestión del tránsito aéreo (ATM).

[5] Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo (DO L 333 de 27.12.2022, p. 164).

designadas o establecidas de conformidad con el artículo 9, apartado 1, de la Directiva (UE) 2022/2557);

- Cuando proceda, la red europea de organizaciones de enlace para crisis cibernéticas («EU-CyCLONe») a que se refiere el artículo 16 de la Directiva (UE) 2022/2555;

- Grupo de cooperación mencionado en el artículo 14 de la Directiva (UE) 2022/2555;

- Cuando proceda, otras partes interesadas, incluidas entidades o personas privadas, como los operadores de infraestructuras críticas, incluidas las identificadas como entidades críticas;

- Los ministros responsables de la resiliencia de las infraestructuras críticas o de los sectores más afectados por el incidente.

b) Consejo

- La Presidencia rotatoria;

- Grupos de trabajo pertinentes, como el Grupo «Protección Civil», incluido el subgrupo sobre resiliencia de las entidades críticas PROCIV-CER y los presidentes de los grupos de trabajo pertinentes en función de los sectores afectados y de la naturaleza del incidente, como el Grupo Horizontal «Cuestiones Cibernéticas» y el Grupo Horizontal «Aumento de la Resiliencia y Lucha contra las Amenazas Híbridas»;

- El Coreper, el Comité Político y de Seguridad y el DIRPC, todos ellos con el apoyo de la Secretaría General del Consejo.

c) Comisión, incluidos sus grupos de expertos

- Servicio responsable designado (dependiendo del sector afectado) con el apoyo del CECRE como centro operativo permanente que gestiona las respuestas a las crisis y la Dirección General de Migración y Asuntos de Interior como servicio responsable en este ámbito y, en caso de incidente intersectorial, dicha Dirección General y otros servicios pertinentes de la Comisión;

- Dirección General de Comunicación y servicios del portavoz;

- Dirección General HERA - Autoridad de Preparación y Respuesta ante Emergencias Sanitarias;

- Grupo de Resiliencia de las Entidades Críticas presidido por un representante de la Comisión (DG de Migración y Asuntos de Interior), establecido por la Directiva (UE) 2022/2557, y, en su caso, otros grupos de expertos y comités pertinentes;

- CECRE creado en virtud del MPCU mediante la Decisión 1313/2013/UE del Parlamento Europeo y del Consejo[6] (centro operativo permanente de gestión de emergencias en el marco del MPCU, ubicado en la DG de Protección Civil y Operaciones de Ayuda Humanitaria Europeas);

- Grupo de cooperación mencionado en el artículo 14 de la Directiva (UE) 2022/2555;

- Centro de Conocimiento y Análisis de la Situación Cibernética;

[6] 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).

- Grupo de cooperación mencionado en el artículo 4 de la Directiva (UE) 2022/2371[7];

- Secretaría General de la Comisión (Secretaría de ARGUS) y el secretario general (adjunto) (proceso ARGUS), DG de Recursos Humanos (Dirección de Seguridad);

- Otros grupos de expertos pertinentes de la Comisión que la asistan en la coordinación de medidas en situaciones de emergencia o crisis;

- Otras redes de gestión de crisis, incluidas las sectoriales (por ejemplo, la red de puntos de contacto de transporte gestionada por la DG de Movilidad y Transportes, el grupo de trabajo interinstitucional sobre cibercrisis[8], la célula de coordinación de crisis de la aviación europea);

- El presidente, vicepresidente o comisario responsable.

d) SEAE

- Capacidad Única de Análisis de Inteligencia («SIAC»), compuesta por el Centro de Inteligencia y de Situación («IntCen») y la Dirección de Inteligencia del Estado Mayor de la Unión Europea («EMUE Int»);

- Centro de Respuesta a las Crisis («CRC»);

- Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad y Vicepresidente de la Comisión.

e) Organismos y órganos pertinentes de la Unión, como Europol, en función del sector afectado[9].

4. Interacción con otros mecanismos e instrumentos pertinentes de gestión de crisis

El Plan director de infraestructuras críticas es una herramienta flexible que describe diversas medidas que podrían adoptarse parcial o totalmente utilizando diferentes disposiciones existentes, dependiendo de la naturaleza y gravedad del incidente significativo de infraestructuras críticas y de la necesidad de coordinación operativa, estratégica y política.

a) Protocolo de la UE sobre la lucha contra las amenazas híbridas[10] («Protocolo de la UE»)

El Protocolo de la UE se aplica en el caso de amenazas híbridas[11] y esboza los procesos e instrumentos aplicables en caso de tales amenazas o campañas.

---

7 Reglamento (UE) 2022/2371 del Parlamento Europeo y del Consejo de 23 de noviembre de 2022 sobre las amenazas transfronterizas graves para la salud y por el que se deroga la Decisión n.º 1082/2013/UE (DO L 314 de 6.12.2022, p. 26).

8 Grupo informal que incluye los servicios pertinentes de la Comisión, el SEAE, la Agencia de la Unión Europea para la Ciberseguridad (ENISA), el CERT-UE y Europol, copresidido por la DG de Redes de Comunicación, Contenido y Tecnologías y el SEAE.

9 Como Europol; en el caso del transporte: Agencia de la Unión Europea para la Seguridad Aérea (AESA), Agencia Europea de Seguridad Marítima (AESM) y Agencia Ferroviaria Europea (AFE); en el de la salud: Centro Europeo para la Prevención y el Control de las Enfermedades (CEPCE) y Agencia Europea de Medicamentos (EMA); en el de la energía: Agencia de Cooperación de los Reguladores de la Energía (ACER); en el del espacio: Agencia del Programa Espacial de la UE (EUSPA); en el sector alimentario: Autoridad Europea de Seguridad Alimentaria (EFSA); en el ámbito marítimo: Agencia Europea de Control de la Pesca (AECP); para ciberincidentes: Agencia de la Unión Europea para la Ciberseguridad (ENISA), equipos de respuesta a incidentes de seguridad informática (CSIRT) y Equipo de respuesta a emergencias informáticas de las instituciones, órganos y organismos de la UE (CERT-UE).

10 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].

En caso de incidente significativo de infraestructura crítica con una dimensión híbrida, el Protocolo de la UE se aplicará de forma complementaria con el Plan director de infraestructuras críticas, cuando proceda, por ejemplo a efectos de información, análisis o comunicación específicos sobre aspectos híbridos del incidente y de cooperación con socios externos.

b) Plan director de respuesta coordinada a incidentes y crisis de ciberseguridad transfronterizos a gran escala

El Plan director cibernético se aplica a los incidentes de ciberseguridad que causen perturbaciones demasiado fuertes como para que el Estado miembro afectado los resuelva por sí mismo o cuando afecten a dos o más Estados miembros o instituciones de la UE y tengan un impacto tan grande y de tanta relevancia técnica o política que requieran una coordinación y una respuesta oportuna a nivel político de la Unión.

En caso de incidente significativo de infraestructuras críticas que coincida con un incidente de ciberseguridad a gran escala o que parezca estar relacionado con él, los grupos de trabajo pertinentes del Consejo establecerán una coordinación adecuada a nivel operativo, también con EU-CyCLONe o mediante una reunión conjunta del Grupo de Resiliencia de las Entidades Críticas con el Grupo de Cooperación. El objetivo de la coordinación es determinar qué agente, herramientas o mecanismos podrían contribuir con mayor eficacia a responder al incidente significativo de infraestructuras críticas, evitando al mismo tiempo la duplicación y las líneas de trabajo paralelas.

c) ***Mecanismo de Protección Civil de la Unión y Centro de Coordinación de la Respuesta a Emergencias***

De conformidad con la Decisión 1313/2013/UE relativa a un Mecanismo de Protección Civil de la Unión, las respuestas operativas en el marco del MPCU a catástrofes naturales o provocadas por el ser humano reales o inminentes (incluidas las que impliquen perturbaciones en las infraestructuras críticas) dentro y fuera de la Unión están dirigidas por el CECRE, el centro operativo único permanente de la Comisión gestiona las respuestas a las crisis. En tales casos, el CECRE puede facilitar alerta rápida, notificación, análisis y apoyo para el intercambio de información y, en caso de activación del MPCU por parte de un Estado miembro, el despliegue de asistencia operativa y expertos en las zonas afectadas. Además, el CECRE puede facilitar la coordinación sectorial e intersectorial tanto a escala de la Unión como entre la Unión y las autoridades nacionales pertinentes, incluidas las responsables de la protección civil y la resiliencia de las infraestructuras críticas.

d) Otros mecanismos e instrumentos sectoriales o intersectoriales

El Plan director de infraestructuras críticas no duplica otros instrumentos o mecanismos de coordinación sectoriales o intersectoriales de gestión de crisis. Cuando ya existan tales instrumentos o mecanismos en el sector afectado, el Plan, dentro de su ámbito de aplicación, puede utilizarse como herramienta complementaria a los instrumentos o mecanismos sectoriales o intersectoriales, pero no los sustituye. Habría que garantizar la necesaria coordinación entre los distintos agentes para evitar esta duplicación. Esto podría lograrse, por ejemplo, en el proceso de coordinación interna de crisis de la Comisión, ARGUS, con el apoyo del CECRE o en reuniones de coordinación del DIRPC.

---

[11] Las amenazas híbridas pueden caracterizarse como una combinación de actividades coercitivas y subversivas, y métodos convencionales y no convencionales, que pueden ser utilizados de forma coordinada por agentes estatales o no estatales para alcanzar objetivos específicos, al tiempo que se mantienen por debajo del umbral de guerra oficialmente declarada (véase el Protocolo de la UE sobre las amenazas híbridas).

PARTE II: INTERCAMBIO DE INFORMACIÓN Y RESPUESTA COORDINADA

Las acciones descritas a continuación consisten en modos de cooperación, especialmente intercambio de información, comunicación coordinada y respuesta. Esta estructura corresponde a los modos del DIRPC y tiene en cuenta, más generalmente, el posible uso de los mecanismos de coordinación de crisis ya existentes a escala de la UE. Esta estructura muestra cómo se integrarían estos modos de cooperación si se utilizaran. Sin embargo, la mayoría de estas medidas también pueden adoptarse de forma autónoma: no dependen de la utilización de este mecanismo, sino que lo complementan. Las acciones se presentan en orden cronológico, teniendo en cuenta que, en caso de crisis a gran escala que constituya un incidente significativo en infraestructuras críticas, pueden emprenderse varias acciones de forma simultánea y continua.

1. INTERCAMBIO DE INFORMACIÓN

a) A nivel operativo

Los Estados miembros afectados por el incidente significativo de infraestructuras críticas aplicarán sus propias medidas de contingencia, garantizando la coordinación con los mecanismos nacionales pertinentes de gestión de crisis y la participación de todos los agentes nacionales, regionales y locales pertinentes, según proceda.

Cuando proceda por lo que se refiere a la asistencia en materia de protección civil, la coordinación entre los Estados miembros y con la Comisión se encauzará a través del CECRE en el marco del MPCU.

i) Intercambio de información y notificación por parte de las autoridades nacionales competentes

Además de las obligaciones de notificación e información con arreglo al artículo 15 de la Directiva (UE) 2022/2557, las autoridades nacionales competentes responsables de las infraestructuras críticas en los Estados miembros afectados por el incidente significativo de infraestructuras críticas comparten con la Presidencia rotatoria del Consejo y la Comisión, a través de sus puntos de contacto únicos y sin demora indebida, la información pertinente recibida de los operadores de infraestructuras críticas, las entidades críticas u otras fuentes, así como información relativa a los mecanismos de gestión de crisis activados. En el caso de la Comisión, el CECRE garantizará un contacto operativo y una capacidad permanentes y coordinará, supervisará y apoyará instantáneamente la respuesta a las emergencias a escala de la Unión, al tiempo que servirá a los Estados miembros y a la Comisión como centro operativo para dar respuesta a las crisis al promover un enfoque intersectorial de la gestión de catástrofes.

Este intercambio de información se refiere a la naturaleza del incidente significativo de infraestructuras críticas, su causa, el impacto observado o estimado de la perturbación en las infraestructuras críticas y la prestación de servicios esenciales, las consecuencias del incidente a través de sectores y fronteras y las medidas de mitigación ya adoptadas o previstas, a nivel nacional o con otros Estados miembros pertinentes y la Comisión, a través de acuerdos existentes, por ejemplo, acuerdos de intercambio de información en virtud de los artículos 9 y 15 de la Directiva (UE) 2022/2557. Esta notificación se realiza sin desviar recursos de las infraestructuras críticas o, en algunos casos, de la entidad crítica o del Estado miembro de las actividades relacionadas con la gestión de incidentes, que debe priorizarse.

A fin de garantizar el seguimiento, el CECRE o los servicios de la Comisión notificados responsables del sector en el que se haya producido el incidente informarán al punto de

contacto de la DG de Migración y Asuntos de Interior así como a la Secretaría General de la Comisión. Mientras tanto, si no se ha iniciado ya, el CECRE comenzará a hacer un seguimiento de los acontecimientos, especialmente en caso de activación del MPCU por uno o varios de los Estados miembros afectados.

Si la información puede ser pertinente para abordar una dimensión de ciberseguridad o estar relacionada con un incidente de ciberseguridad, la Comisión compartirá la información pertinente con EU-CyCLONe.

Las autoridades nacionales competentes en virtud de la Directiva (UE) 2022/2557 deberán cooperar e intercambiar información con las autoridades competentes en virtud de la Directiva (UE) 2022/2555, sin demora indebida, en relación con incidentes e incidentes cibernéticos que afecten a entidades críticas, incluidas las medidas físicas y de ciberseguridad adoptadas por las entidades críticas.

En el ámbito marítimo, las autoridades nacionales competentes deberán considerar la posibilidad de utilizar el Entorno Común de Intercambio de Información («ECII») para compartir información sin demora indebida.

ii) Organización de reuniones de expertos

La Comisión convocará lo antes posible al Grupo de Resiliencia de las Entidades Críticas para facilitar el intercambio de información pertinente entre las autoridades nacionales competentes responsables de las infraestructuras críticas y las instituciones, órganos y organismos de la Unión pertinentes sobre el incidente (naturaleza, causa, impacto y consecuencias para los sectores y entre fronteras) y sobre las medidas a adoptar, incluidas medidas de mitigación y el apoyo técnico a los Estados miembros afectados. En función del centro de gravedad del incidente, los servicios pertinentes de la Comisión estarán estrechamente asociados a la reunión del Grupo de Resiliencia de las Entidades Críticas con vistas a compartir la información recopilada a través de los instrumentos sectoriales existentes. En caso de incidentes con una combinación de ciberseguridad y aspectos físicos no cibernéticos, los servicios pertinentes de la Comisión, el CERT-UE y el SEAE, cuando proceda, notificarán y consultarán lo antes posible en el seno del grupo de trabajo sobre cibercrisis, así como a los respectivos presidentes del grupo de cooperación a que se refiere el artículo 14 de la Directiva (UE) 2022/2555, y EU-CyCLONe, según proceda, sobre la necesidad de actividades de coordinación. De acuerdo con los respectivos presidentes, la Comisión (DG de Migración y Asuntos de Interior y DG de Redes de Comunicación, Contenido y Tecnologías) podrá proponer una reunión conjunta del Grupo de Resiliencia de las Entidades Críticas con el grupo de cooperación con vistas a compartir datos sobre la situación y a coordinar las respuestas respectivas.

En caso de incidente significativo intersectorial de infraestructuras críticas que requiera o pueda requerir una gestión de las consecuencias a escala de la Unión, la Comisión podrá convocar reuniones de coordinación intersectorial en las que participen todas las partes interesadas pertinentes.

En caso de que un incidente significativo de infraestructuras críticas afecte también a un tercer país, la Comisión consultará a la autoridad competente del tercer país afectado y podrá invitarla a una reunión del Grupo de Resiliencia de las Entidades Críticas.

iii) Apoyo de la Comisión y de las agencias de la Unión

Cuando proceda y actuando de conformidad con su mandato, Europol presentará a la Unión un informe sobre el incidente. Otras agencias de la Unión, cuando proceda y de conformidad con sus respectivos mandatos, comunicarán información pertinente que contribuya a conocer la situación o a responder coordinadamente al incidente significativo de infraestructuras

críticas a las respectivas direcciones generales de las que dependen, que, a su vez, informarán a la Comisión (DG de Migración y Asuntos de Interior, en su calidad de presidenta del Grupo de Resiliencia de las Entidades Críticas).

La Comisión podrá contribuir al conocimiento de la situación utilizando los activos del Programa Espacial de la Unión[12], como Copernicus, Galileo y EGNOS, cuando proceda y de conformidad con el marco jurídico aplicable.

b) Nivel estratégico

i) Elaboración de informes sobre la situación

Sobre la base de la información compartida por las autoridades nacionales competentes en una reunión del Grupo de Resiliencia de las Entidades Críticas, o de reuniones conjuntas con los servicios, grupos de expertos o redes pertinentes, la Comisión elaborará un informe sobre la situación basado en las contribuciones de las autoridades nacionales competentes y otra información disponible.

Dicho informe deberá tener en cuenta, cuando proceda, los resultados de las evaluaciones de riesgos, evaluaciones e hipótesis pertinentes a escala de la UE desde la perspectiva de la ciberseguridad, incluidas las realizadas por la Comisión, el Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad y el Grupo de Cooperación.

En caso de activación del DIRPC, este informe puede contribuir al análisis integrado de conocimiento de la situación («ISAA») elaborado por los servicios de la Comisión y el SEAE.

La SIAC presentará una evaluación actualizada del incidente basada en la información, cuando proceda.

ii) Activación de los mecanismos de coordinación de crisis de la Unión y uso de los instrumentos de la Unión

El CECRE comenzará a prestar apoyo al conocimiento de la situación en torno al incidente, cuando proceda, en particular si el suceso da lugar a una activación del MPCU[13]. Además, los Estados miembros afectados podrán solicitar imágenes por satélite de su territorio a través del servicio de gestión de emergencias de Copernicus.

Cuando se considere oportuno compartir información entre la Comisión y el SEAE y las agencias pertinentes de la Unión, la Dirección General responsable o la DG de Migración y Asuntos de Interior, en coordinación con la Secretaría General, activará el proceso interno de coordinación de crisis de la Comisión ARGUS-Fase I mediante la apertura de un acto en la herramienta informática Argus.

La Presidencia rotatoria del Consejo de la Unión podrá activar el DIRPC para la puesta en común de información, lo que implica la elaboración de informes ISAA por la Comisión y el SEAE con contribuciones de las autoridades nacionales competentes y otras fuentes, cuando proceda. Incluso sin activar el DIRPC, la Presidencia rotatoria del Consejo o la Comisión podrán iniciar una página de seguimiento en la plataforma web del DIRPC en determinadas condiciones.

---

[12] Reglamento (UE) 2021/696 del Parlamento Europeo y del Consejo de 28 de abril de 2021 por el que se crean el Programa Espacial de la Unión y la Agencia de la Unión Europea para el Programa Espacial y por el que se derogan los Reglamentos (UE) n.º 912/2010, (UE) n.º 1285/2013 y (UE) n.º 377/2014 y la Decisión n.º 541/2014/UE (DO L 170 de 12.5.2021, p. 69).

[13] Como la publicación de productos de seguimiento de los medios de comunicación, mensajes de protección civil, notas analíticas, mapas e indicadores diarios de ECHO y otros productos a medida.

Podrán activarse otros mecanismos e instrumentos (sectoriales) de gestión de crisis de la Unión siguiendo los procedimientos respectivos, según proceda. La Comisión garantizará la coordinación entre estos mecanismos e instrumentos.

Si el incidente físico coincide o parece estar relacionado con un incidente de ciberseguridad a gran escala, tal como se define en el artículo 6, apartado 7, de la Directiva (UE) 2022/2555, la Presidencia rotatoria del Consejo podrá utilizar el Plan director cibernético para determinar la coordinación adecuada a nivel operativo, en la que participen, entre otros, el CyCLONe de la UE y el Grupo de Resiliencia de las Entidades Críticas.

iii) Coordinación de la comunicación pública

Los Estados miembros afectados por la infraestructura crítica significativa coordinarán en la medida de lo posible su comunicación pública sobre la crisis, respetando al mismo tiempo las competencias nacionales a este respecto. La Red de Comunicación de Crisis del DIRPC podrá participar, según proceda.

Sobre la base del conocimiento compartido de la situación, el Grupo de Resiliencia de las Entidades Críticas y los Estados miembros afectados apoyarán la formulación de líneas de comunicación pública acordadas, cuando proceda.

Europol y otras agencias pertinentes de la Unión coordinarán sus actividades de comunicación pública con el servicio del portavoz de la Comisión, sobre la base de un conocimiento compartido de la situación.

Si el incidente significativo de infraestructuras críticas conlleva una dimensión exterior, híbrida o de política común de seguridad y defensa, la comunicación pública se coordinará con el SEAE y el servicio de portavoz de la Comisión de conformidad con el Protocolo de la UE para la lucha contra las amenazas híbridas[14].

2. RESPUESTA (MEDIANTE LAS ACCIONES CONTINUAS DESCRITAS EN EL APARTADO «INTERCAMBIO DE INFORMACIÓN Y ACCIONES ADICIONALES A NIVEL ESTRATÉGICO Y POLÍTICO»)

a) Nivel estratégico

i) Elaboración continua de informes de situación

Se informará al Grupo Protección Civil-Resiliencia de las Entidades Críticas (PROCIV-REC) del Consejo de la elaboración de un informe de situación política y estratégico (por ejemplo, ISAA en caso de activación del DIRPC o informe de conocimiento de la situación compartido elaborado por la Comisión) y se advertirá al Coreper, en caso de que no hubiera sido convocado todavía, o a la reunión del Comité Político y de Seguridad, según proceda.

La SIAC intensificará su colaboración con los servicios de inteligencia de los Estados miembros, recopilará la información procedente de todas las fuentes y preparará un análisis y una evaluación del incidente, así como actualizaciones periódicas, en caso necesario.

ii) Plena activación de los mecanismos de coordinación de crisis de la Unión y uso de los instrumentos de la Unión

En caso de que el presidente de la Comisión active el proceso interno de coordinación de crisis de la Comisión ARGUS-Fase II, las reuniones del Comité de Coordinación de Crisis en

[14] 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].

las que participen los servicios pertinentes de la Comisión, las agencias y el SEAE, cuando proceda, se convocarán con poca antelación para coordinar todos los aspectos del incidente significativo de infraestructuras críticas.

En caso de que la Presidencia del Consejo active plenamente el DIRPC:

- La Presidencia rotatoria del Consejo pedirá rápidamente una reunión informal de los agentes nacionales, europeos e internacionales pertinentes, en la que el representante de la Comisión que actúe como presidente del Grupo de Resiliencia de las Entidades Críticas (DG de Migración y Asuntos de Interior) pueda informar sobre las reuniones del grupo convocadas previamente, complementadas por otros servicios de la Comisión y el SEAE, según proceda.

- Durante la reunión, la SIAC y las agencias pertinentes de la Unión podrán ser invitadas a presentar información actualizada sobre la situación del incidente.

El servicio responsable del ISAA (el servicio principal de la Comisión o el SEAE) preparará el informe ISAA con las contribuciones de los servicios pertinentes de la Comisión, las instituciones, órganos y organismos pertinentes de la Unión y las autoridades nacionales competentes. Se invita a los Estados miembros a aportar información, a través de la plataforma web del DIRPC, para la elaboración de los informes ISAA.

En caso de que se produzca un incidente significativo de infraestructuras críticas de importancia para la seguridad internacional, los servicios de la Comisión y el SEAE podrán convocar una reunión de diálogo estructurado UE-OTAN sobre resiliencia para analizar conjuntamente la situación e intercambiar información sobre las medidas adoptadas por la Unión y la OTAN, respectivamente.

iii) Comunicación pública

El Consejo preparará mensajes comunes destinados a la opinión pública. La red informal de comunicadores de crisis establecida a través del DIRPC puede apoyar esta labor. El servicio del portavoz de la Comisión también preparará nota dirigidas al público, según proceda.

Si el incidente significativo de infraestructuras críticas conlleva una dimensión exterior, híbrida o de política común de seguridad y defensa, la comunicación pública será coordinada con el SEAE y el servicio de portavoz de la Comisión de conformidad con el Protocolo de la UE para la lucha contra las amenazas híbridas.

iv) Apoyo a los Estados miembros y respuesta eficaz

La Presidencia rotatoria podrá convocar una reunión de PROCIV-CER para apoyar las actividades en el marco del DIRPC, si se activa.

Los Estados miembros afectados por el incidente podrán solicitar el apoyo técnico de otros Estados miembros o de las instituciones, órganos y organismos pertinentes de la Unión a través del Grupo de Resiliencia de las Entidades Críticas, por ejemplo, asesoramiento específico para mitigar los efectos adversos del incidente.

Los Estados miembros afectados por el incidente críticas también podrán solicitar el apoyo técnico o financiero de la Comisión o de las agencias pertinentes de la Unión. La Comisión, en coordinación con las agencias pertinentes de la Unión, evaluará su posible apoyo y activará, cuando proceda, medidas técnicas de mitigación a escala de la Unión de conformidad con sus respectivos procedimientos y coordinará las capacidades técnicas necesarias para detener o reducir el impacto del incidente.

En el contexto específico del MPCU, los países afectados podrían solicitar asistencia a través del Sistema Común de Comunicación e Información de Emergencia («SCCIE»), tras lo cual

el CECRE coordinaría la prestación de asistencia de los Estados miembros y de los Estados participantes en el MPCU, así como a través de rescEU.

En el marco de sus respectivos mandatos y previa solicitud, Europol y otras agencias pertinentes de la Unión apoyarán a los Estados miembros afectados por un incidente significativo de infraestructura crítica en la investigación del mismo.

b) Nivel político

La Presidencia del Consejo podría considerar la necesidad de convocar mesas redondas del DIRPC, reuniones de los grupos de trabajo del Consejo, Coreper, Consejo de Ministros o cumbres para intercambiar impresiones sobre el posible origen y las consecuencias previstas del incidente significativo de infraestructuras críticas para los Estados miembros y para la Unión, acordar directrices comunes, y adoptar las medidas necesarias para apoyar a los Estados miembros afectados por el incidente significativo de infraestructura crítica y mitigar sus efectos.

Gráfico 1: Esquema general del Plan director de infraestructuras críticas

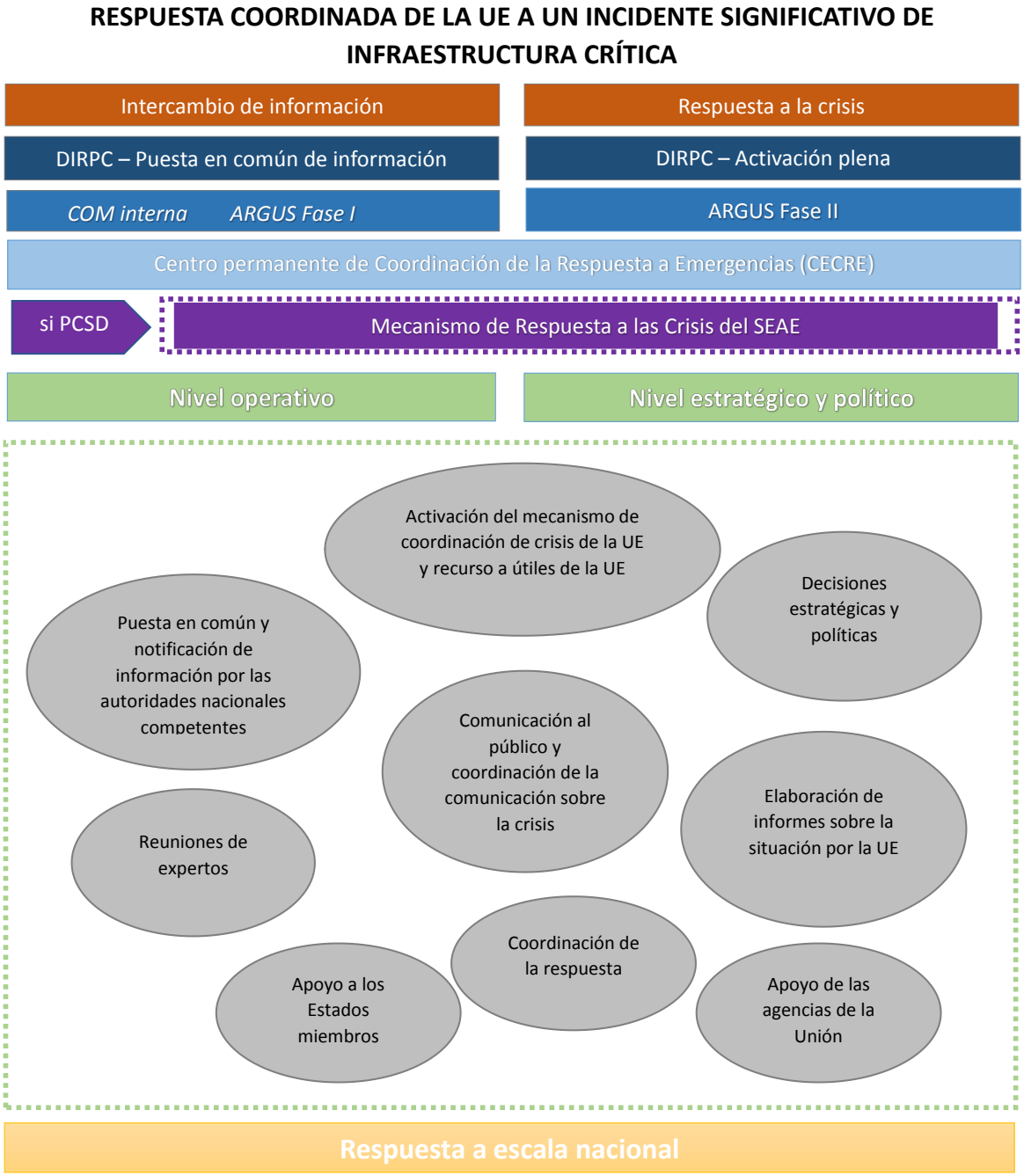

Gráfico 2: Decisión sobre el Plan director de infraestructuras críticas