Consejo de la Unión Europea

Bruselas, 20 de octubre de 2021
(OR. en)

13048/21

CYBER 263
JAI 1117
TELECOM 384
CSC 362
CIS 116
RELEX 874
ENFOPOL 370
COPS 373
COSI 190
HYBRID 62
CSCI 133
POLGEN 177
DATAPROTECT 244

RESULTADO DE LOS TRABAJOS

De:	Secretaría General del Consejo
Fecha:	19 de octubre de 2021
A:	Delegaciones
N.º doc. prec.:	12534/21
Asunto:	Conclusiones del Consejo sobre la exploración del potencial de la iniciativa relativa a una Unidad Cibernética Conjunta como complemento de la respuesta coordinada de la UE a los incidentes y crisis de ciberseguridad a gran escala - Conclusiones del Consejo (19 de octubre de 2021)

Adjunto se remite a las delegaciones las Conclusiones del Consejo sobre la exploración del potencial de la iniciativa relativa a una Unidad Cibernética Conjunta como complemento de la respuesta coordinada de la UE a los incidentes y crisis de ciberseguridad a gran escala, adoptadas por el Consejo en su sesión del 19 de octubre de 2021.

ANEXO

Conclusiones del Consejo sobre la exploración del potencial de la iniciativa relativa a una Unidad Cibernética Conjunta como complemento de la respuesta coordinada de la UE a los incidentes y crisis de ciberseguridad a gran escala

THE COUNCIL OF THE EUROPEAN UNION,

RECORDANDO sus Conclusiones sobre:

– la Estrategia de Ciberseguridad de la UE para la Década Digital[1],

– la respuesta coordinada de la UE a los incidentes y crisis de ciberseguridad a gran escala[2],

– la ciberdiplomacia[3],

– un marco para una respuesta diplomática conjunta de la UE a las actividades informáticas malintencionadas («conjunto de instrumentos de ciberdiplomacia»)[4],

– seguridad y defensa[5],

– el marco político de ciberdefensa de la UE[6],

– la configuración del futuro digital de Europa[7],

– la 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,

---

1 7290/21.
2 10086/18.
3 6122/15 + COR 1.
4 10474/17.
5 8396/21.
6 15585/14.
7 8711/20.

– la Comunicación conjunta al Parlamento Europeo y al Consejo titulada «Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE»[8],

– el desarrollo de capacidades y competencias en materia de ciberseguridad en la UE[9],

1. HACE HINCAPIÉ en la importancia de la ciberseguridad para construir una Europa resiliente, digital y ecológica. SUBRAYA que la ciberseguridad es indispensable para la prosperidad y la seguridad de la Unión y sus Estados miembros y de sus ciudadanos, empresas e instituciones, así como para defender la integridad de nuestras sociedades libres y democráticas.

2. TOMA CONSTANCIA del carácter transfronterizo e intersectorial de numerosas amenazas de ciberseguridad, así como de los riesgos y las posibles repercusiones de las campañas continuadas de actividades informáticas malintencionadas más eficaces, sofisticadas, selectivas, complejas, persistentes o generalizadas[10]. La pandemia de COVID-19 ha hecho más patentes las vulnerabilidades de nuestras sociedades, así como el riesgo que entrañan los incidentes de ciberseguridad a gran escala de perjudicar la economía, la democracia, los servicios esenciales y las infraestructuras críticas, especialmente en el sector sanitario. Además, ha aumentado la importancia de la conectividad y ha acentuado la dependencia de la sociedad respecto de redes y sistemas de información fiables, solventes y seguros. En definitiva, ha subrayado la necesidad de contar con una internet mundial, abierta, libre, estable y segura, y de poder confiar en los productos, procesos y servicios de las tecnologías de la información y la comunicación (TIC) y en la seguridad de estos, con especial atención al imperativo de garantizar una cadena de suministro resiliente.

---

8 14435/17 + COR 1.
9 7737/19.
10 Informe «Panorama de amenazas 2020» de ENISA.

3. REITERA la importancia de la ciberresiliencia y de seguir desarrollando el marco de la UE para la gestión de crisis de ciberseguridad[11] con el fin de dar una respuesta eficiente y oportuna en el ámbito de la UE a los incidentes y crisis de ciberseguridad a gran escala, y de integrar dicho marco en mayor medida en los mecanismos de la UE de respuesta a las crisis, horizontales y sectoriales, ya existentes. DESTACA el papel del Consejo y del Dispositivo de la UE de Respuesta Política Integrada a las Crisis a la hora de garantizar una coordinación y una respuesta oportunas en el nivel político de la Unión ante crisis que tengan gran repercusión o importancia política, independientemente de que se generen dentro o fuera de la Unión. PONE DE RELIEVE la importancia de someter a prueba estos marcos y mecanismos en ejercicios periódicos.

4. RECUERDA que las actividades realizadas en el ámbito de la UE en relación con incidentes y crisis de ciberseguridad a gran escala se rigen por los principios de subsidiariedad, proporcionalidad, complementariedad, no duplicación y confidencialidad. REITERA que los Estados miembros son los principales responsables de la respuesta a aquellos incidentes y crisis de ciberseguridad a gran escala que les afecten. RECUERDA la importancia de respetar las competencias de los Estados miembros y su responsabilidad exclusiva en materia de seguridad nacional, de conformidad con el artículo 4, apartado 2, del Tratado de la Unión Europea, también en el ámbito de la ciberseguridad.

5. RECUERDA al mismo tiempo la importancia de respetar las competencias y los mandatos de las instituciones, órganos y organismos de la UE. El Alto Representante, la Comisión y otras instituciones, órganos y organismos de la UE también han de desempeñar un papel esencial, derivado del Derecho de la Unión, en particular debido a las repercusiones que pueden tener los incidentes y crisis de ciberseguridad a gran escala en el mercado único, así como en el funcionamiento de las propias instituciones, órganos y organismos de la UE.

[11] 10086/18.

6. SUBRAYA la necesidad de evitar duplicaciones innecesarias y buscar la complementariedad y un valor añadido a la hora de seguir desarrollando el marco de la UE para la gestión de crisis de ciberseguridad, además de garantizar la armonización con los mecanismos, iniciativas, redes, procesos y procedimientos existentes a escalas nacional y europea. HACE HINCAPIÉ en la importancia de racionalizar los procesos y estructuras existentes para reducir su complejidad, y en aras de la cohesión dentro de la Unión, a fin de mejorar su accesibilidad y la capacidad de dar respuesta a quienes buscan asistencia y solidaridad.

7. RECONOCE la aplicabilidad del Derecho internacional, en particular de la Carta de las Naciones Unidas en su totalidad, el Derecho internacional humanitario y la legislación de derechos humanos en el ciberespacio, y PROMUEVE la adhesión a las normas, reglas y principios, voluntarios y no vinculantes, sobre la conducta responsable de los Estados en el ciberespacio, refrendados por todos los Estados miembros de las Naciones Unidas.

8. CELEBRA los avances logrados en los últimos años en el Consejo, en particular en el Grupo Horizontal «Cuestiones Cibernéticas» y otros grupos de trabajo pertinentes del Consejo, así como en la puesta en marcha de otras iniciativas, redes y mecanismos de cooperación e intercambio de información entre Estados miembros, entre otros el Grupo de Cooperación SRI y la Red de CSIRT de la UE establecidos por la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, la Red de Organizaciones de Enlace Nacionales para la Gestión de Cibercrisis (CyCLONe), los proyectos relacionados con la ciberdefensa emprendidos en el marco de la Cooperación Estructurada Permanente (CEP)[12], el Grupo Especial Conjunto de Acción contra los Delitos Cibernéticos (J-CAT), la Red Judicial Europea sobre Ciberdelincuencia (RJEC), las contribuciones voluntarias de los Estados miembros al Centro de Inteligencia y de Situación de la Unión Europea (INTCEN) y la coordinación y cooperación en el contexto del conjunto de instrumentos de ciberdiplomacia.

[12] En particular, los Equipos de Respuesta Telemática Rápida y de Asistencia Mutua en el ámbito de la Ciberseguridad coordinados por Lituania, el Centro de Coordinación del Ámbito del Ciberespacio y de la Información coordinado por Alemania y la Plataforma de Intercambio de Información sobre Respuestas a Ciberamenazas e Incidentes de Ciberseguridad coordinada por Grecia.

9. RECUERDA los marcos existentes para la cooperación entre las instituciones, órganos y organismos de la UE, como la cooperación estructurada entre ENISA y el CERT-UE, y el memorando de acuerdo entre ENISA, la Agencia Europea de Defensa (AED), el Centro Europeo de Ciberdelincuencia de Europol (EC3) y el CERT-UE. INSISTE en la importancia de mantener un intercambio periódico de información con el Consejo sobre las novedades relativas a estos marcos de cooperación.

10. DESTACA la importancia de mejorar la cooperación y el intercambio de información entre las diversas comunidades cibernéticas de la UE y sus Estados miembros a todos los niveles necesarios —técnico, operativo y estratégico/político— y de vincular los mecanismos, redes, estructuras, procesos y procedimientos de gestión de crisis existentes cuando ello apoye y mejore la gestión de los incidentes y crisis de ciberseguridad a gran escala.

11. RECONOCE los avances logrados por un grupo de Estados miembros en la creación de una cibercapacidad operativa conjunta denominada «Equipos de Respuesta Telemática Rápida» en el marco de la CEP, con el objetivo de intensificar la cooperación voluntaria en el ámbito cibernético mediante la asistencia mutua, también como respuesta a incidentes y crisis de ciberseguridad a gran escala.

12. RECONOCE la experiencia y la capacidad de respuesta ininterrumpida (24 horas al día, 7 días a la semana) de la comunidad policial en el ámbito de la cooperación operativa y el intercambio seguro de información contra los ciberataques transfronterizos importantes a través del Protocolo de Respuesta Policial ante Emergencias de la UE.

13. RECONOCE la aplicación constante del marco para una respuesta diplomática conjunta de la UE a las actividades informáticas malintencionadas («conjunto de instrumentos de ciberdiplomacia»). RECUERDA que cada Estado miembro es libre de decidir de manera soberana con respecto a la atribución de una actividad cibernética malintencionada, caso por caso. RECUERDA que las medidas adoptadas en el marco de una respuesta diplomática conjunta de la UE a las actividades informáticas malintencionadas deben basarse en una conciencia situacional común acordada entre los Estados miembros. El INTCEN desempeña un papel central como plataforma de conciencia situacional y evaluación de amenazas sobre cuestiones cibernéticas para la UE, a partir de contribuciones voluntarias de inteligencia de los Estados miembros y sin perjuicio de las competencias de estos.

14. REITERA la importancia de la asistencia mutua y la solidaridad, en consonancia con el artículo 42, apartado 7, del Tratado de la Unión Europea y el artículo 222 del Tratado de Funcionamiento de la Unión Europea, y PIDE que se realicen más ejercicios con una dimensión cibernética. RECUERDA la necesidad de reflexionar sobre la articulación entre el marco de gestión de crisis de ciberseguridad de la UE, el conjunto de instrumentos de ciberdiplomacia y las disposiciones de los artículos antes mencionados en caso de incidente o crisis de ciberseguridad a gran escala. RECUERDA que las obligaciones que se derivan del artículo 42, apartado 7, del Tratado de la Unión Europea para los Estados miembros se entienden sin perjuicio de la especificidad de la política de seguridad y defensa de determinados Estados miembros. RECUERDA que la OTAN sigue siendo el fundamento de la defensa colectiva de los Estados que son miembros de ella.

15. RECONOCE la cooperación entre la UE y la OTAN en materia de ciberseguridad y ciberdefensa, que incluye el intercambio de información entre el CERT-UE y el equipo de capacidad de respuesta ante incidentes informáticos de la OTAN (NCIRC), dentro del respeto íntegro de los principios de transparencia, reciprocidad e inclusividad, así como de la autonomía decisoria de ambas organizaciones.

16. RECONOCE la importancia de la cooperación, en su caso, con el sector privado en lo que respecta a los ejercicios de intercambio de información y la aportación de la pericia pertinente, así como de soluciones y servicios de confianza, incluido, por ejemplo, el apoyo a la respuesta ante incidentes y el refuerzo de la conciencia situacional entre las distintas comunidades cibernéticas.

17. INSISTE en la importancia de disponer de vías de comunicación seguras para el intercambio de información clasificada y sensible. DESTACA la necesidad de seguir avanzando.

A este respecto, y teniendo en cuenta lo que antecede,

18. RECONOCE en la Recomendación de la Comisión sobre la creación de una Unidad Cibernética Conjunta una iniciativa que debe tenerse en cuenta a la hora de seguir desarrollando el marco de gestión de crisis de ciberseguridad de la UE[13].

19. INSTA a la UE y a sus Estados miembros a que prosigan sus esfuerzos por crear un marco de gestión de crisis de ciberseguridad de la UE más completo y eficaz, sobre la base de los mecanismos existentes y de los progresos ya realizados, y a que tengan en cuenta el potencial de la iniciativa relativa a una Unidad Cibernética Conjunta para complementar estos mecanismos aplicando un planteamiento gradual. HACE HINCAPIÉ en que un proceso gradual, transparente e inclusivo es esencial para reforzar la confianza y, por tanto, vital para para seguir desarrollando un marco de gestión de crisis de ciberseguridad de la UE. Este proceso debe respetar las funciones, competencias y mandatos existentes de los Estados miembros y de las instituciones, órganos y organismos de la UE, así como los principios enunciados en las presentes Conclusiones, como la proporcionalidad, la subsidiariedad, la inclusividad, la complementariedad, la no duplicación y la confidencialidad de la información. INSISTE, al mismo tiempo, en que cualquier posible participación o contribución de los Estados miembros a una posible Unidad Cibernética Conjunta será voluntaria.

---

13 C(2021) 4520 final (11155/21 y 11155/21 ADD1).

20. HACE HINCAPIE en la necesidad de establecer unos métodos de trabajo y gobernanza adecuados, con vistas a permitir la intervención y la participación de todos los Estados miembros en los procesos deliberativos, de desarrollo y de decisión efectiva sobre el marco de gestión de crisis de ciberseguridad de la UE, incluida la posible iniciativa relativa a una Unidad Cibernética Conjunta. PIDE que se respeten las prerrogativas que los Tratados atribuyen al Consejo, así como el principio de cooperación leal.

21. SUBRAYA la importancia de reconocer a todas las comunidades cibernéticas pertinentes dentro de la UE y sus Estados miembros y de fomentar su participación, teniendo en cuenta al mismo tiempo sus diferentes funciones y responsabilidades en los distintos tipos de incidentes y crisis de ciberseguridad a gran escala. SUBRAYA el papel decisivo del Consejo, en particular por medio del Grupo Horizontal «Cuestiones Cibernéticas», en la función de elaboración de políticas y coordinación con vistas a seguir desarrollando el marco de gestión de crisis de ciberseguridad de la UE. RUEGA, por tanto, a los Estados miembros, a la Comisión, al Servicio Europeo de Acción Exterior, al INTCEN, al CERT-UE, a ENISA, a Europol (EC3), a Eurojust (RJEC), al Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad, así como a los representantes de la Red de CSIRT, de la Red CyCLONe, del Grupo de Cooperación SRI, de la AED y de los proyectos pertinentes de la CEP, y a otros posibles interesados, que participen en este proceso. Podría estudiarse con mayor profundidad la posibilidad de crear un grupo de trabajo, tal como propone la Recomendación de la Comisión, que garantice una representación suficiente de todos los Estados miembros, actúe bajo la orientación política del Consejo y sirva de foro temporal que reúna a representantes de todas las comunidades cibernéticas pertinentes en los Estados miembros y dentro de la UE. Dicho grupo de trabajo debe informar periódicamente sobre sus actividades y presentar sugerencias al Consejo para su debate y aprobación y la formulación de orientaciones adicionales. Además, podrían establecerse otras formas de diálogo dentro de las comunidades y entre estas, en particular a través de talleres, seminarios y formación y ejercicios conjuntos.

22. SUBRAYA el papel del Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y de la Red de Centros Nacionales de Coordinación en relación con la posible Unidad Cibernética Conjunta, especialmente teniendo en cuenta su función de aumentar sustancialmente las capacidades y las soluciones tecnológicas, así como los medios y las competencias de la Unión en el ámbito de la ciberseguridad.

23. RUEGA a la UE y a sus Estados miembros que se comprometan a seguir desarrollando el marco de gestión de crisis de ciberseguridad de la UE, en particular explorando el potencial de la iniciativa relativa a una Unidad Cibernética Conjunta, estableciendo y definiendo el proceso, incluidos unos hitos y un calendario, y aclarando los objetivos y las posibles funciones y responsabilidades. INSISTE en la necesidad de consolidar, con carácter prioritario, las redes e interacciones existentes dentro de cada comunidad, así como de establecer un inventario exhaustivo de las posibles carencias y necesidades en materia de intercambio de información dentro de las comunidades cibernéticas y entre ellas, así como dentro de las instituciones, órganos y organismos europeos y entre ellos, y posteriormente acordar los posibles objetivos y prioridades principales de una posible Unidad Cibernética Conjunta. Sin anticipar el resultado, DESTACA la necesidad de centrarse en detectar las necesidades de intercambio de información para crear una conciencia situacional común a todas las comunidades pertinentes. A la hora de detectar las carencias y necesidades en materia de intercambio de información, como el posible uso de plataformas virtuales, debe seguir prestándose la debida atención a la seguridad de los canales de comunicación para el intercambio de información clasificada y sensible, DESTACANDO al mismo tiempo la importancia de utilizar las infraestructuras ya existentes. La adopción de un planteamiento gradual tiene por objeto generar confianza y sentar las bases de posibles nuevas medidas relacionadas con el refuerzo de la preparación y la cooperación operativa. RECONOCE que los diferentes objetivos podrían justificar soluciones diferentes y la participación de un grupo diferente de representantes de las comunidades cibernéticas pertinentes dentro de la UE y sus Estados miembros.

24. PIDE que se siga estudiando una base jurídica para la posible Unidad Cibernética Conjunta a lo largo de todo el proceso, incluida una evaluación de las tareas y los cometidos asignados a ENISA en la Recomendación a la luz del artículo 7 del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019. PIDE que se siga reflexionando acerca de cada uno de los elementos de la Recomendación sobre la creación de una Unidad Cibernética Conjunta, también en lo que se refiere a la idea de los equipos de reacción rápida de la UE en materia de ciberseguridad y al Plan de la UE de Respuesta a Incidentes y Crisis de Ciberseguridad. HACE HINCAPIÉ en que la posible Unidad Cibernética Conjunta debe respetar las competencias, los mandatos y los poderes legales de sus posibles participantes futuros.

25. INSTA a la UE y a sus Estados miembros a que consideren el potencial de la iniciativa relativa a una Unidad Cibernética Conjunta, también desde la perspectiva de las instituciones, órganos y organismos de la UE, a fin de complementar los esfuerzos en curso a nivel de los Estados miembros. CELEBRA la intención de la Comisión de reforzar la resiliencia de las instituciones, órganos y organismos pertinentes de la UE por medio de su futura propuesta de Reglamento sobre normas comunes vinculantes en materia de ciberseguridad para las instituciones, órganos y organismos de la UE.

26. Como conclusión, REITERA su compromiso de reforzar la ciberresiliencia y seguir desarrollando el marco de gestión de crisis de ciberseguridad de la UE, y OBSERVARÁ PERIÓDICAMENTE los avances y proporcionará nuevas orientaciones para complementar el marco de gestión de crisis de ciberseguridad de la UE.