



Bruselas, 20 de marzo de 2019
(OR. en)

7737/19

CYBER 101	RELEX 287
COPEN 118	TELECOM 141
COPS 92	DAPIX 109
COSI 52	CATS 43
DATAPROTECT 98	CSC 111
IND 102	CSCI 47
JAI 313	IA 106
JAIEX 44	EJUSTICE 44
POLMIL 31	

RESULTADO DE LOS TRABAJOS

De: Secretaría General del Consejo

Fecha: 19 de marzo de 2019

A: Delegaciones

N.º doc. prec.: 6866/19

Asunto: Conclusiones del Consejo sobre el desarrollo de capacidades y competencias en materia de ciberseguridad en la UE

Adjunto se remite a las delegaciones la Conclusiones del Consejo sobre el desarrollo de capacidades y competencias en materia de ciberseguridad en la UE adoptadas por el Consejo de Asuntos Generales del 19 de marzo de 2019.

Conclusiones del Consejo sobre el desarrollo de capacidades y competencias en materia de ciberseguridad en la UE

El Consejo de la Unión Europea,

1. RECORDANDO sus Conclusiones sobre «Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE»¹;
2. RECORDANDO sus Conclusiones sobre la respuesta coordinada de la UE a los incidentes y crisis de ciberseguridad a gran escala²;
3. RECORDANDO sus Conclusiones sobre el desarrollo de la capacidad cibernética exterior³;
4. REITERANDO que es posible proporcionar un elevado nivel de seguridad de las redes y sistemas de información mediante el refuerzo de las capacidades y competencias de los Estados miembros y las instituciones, órganos y organismos de la UE en materia de ciberseguridad y el consiguiente fortalecimiento de su ciberresiliencia;
5. ACOGIENDO CON SATISFACCIÓN los progresos logrados por los Estados miembros en el refuerzo de los equipos de respuesta a incidentes de seguridad informática (CSIRT);
6. ENCOMIANDO la creación de la red de CSIRT por los Estados miembros con el apoyo activo de la Comisión y la ENISA, así como la cooperación reforzada a nivel estratégico a través del Grupo de cooperación para la seguridad de las redes y sistemas de información (SRI), compuesto por los Estados miembros, la Comisión y la ENISA;

¹ Doc. 14435/17 (Conclusiones del Consejo sobre la Comunicación conjunta al Parlamento Europeo y al Consejo titulada «Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE», de noviembre de 2017)

² Doc. 10086/18 (Conclusiones del Consejo sobre la respuesta coordinada de la UE a los incidentes y crisis de ciberseguridad a gran escala, de 26 de junio de 2018).

³ Doc. 10496/18 (Conclusiones del Consejo sobre las directrices para el desarrollo de la capacidad cibernética exterior de la UE, de 26 de junio de 2018).

7. HACIENDO HINCAPIÉ en el papel fundamental del Grupo de cooperación SRI a la hora de proporcionar la orientación necesaria para armonizar lo máximo posible los planteamientos en la transposición de la Directiva SRI⁴ en toda la UE, así como a la hora de abordar cuestiones importantes de ciberseguridad;
8. RECONOCIENDO el apoyo que presta la Comisión a los Estados miembros para el desarrollo de capacidades de los CSIRT a través del Mecanismo «Conectar Europa»;
9. RECONOCIENDO el apoyo prestado a las autoridades policiales para el desarrollo de capacidades en la lucha contra la ciberdelincuencia a través del Fondo de Seguridad Interior y la CEPOL;
10. ACOGIENDO CON SATISFACCIÓN la actualización del marco político de ciberdefensa de la UE con el fin de apoyar en mayor medida el desarrollo de las capacidades de los Estados miembros de la UE en ciberdefensa;
11. ELOGIANDO los progresos logrados en la aplicación de la Directiva SRI por los Estados miembros;
12. OBSERVANDO que la ciberseguridad es un ámbito complejo, interdependiente y en continuo cambio que requiere la adaptación del marco político y jurídico a las nuevas tendencias tecnológicas y las tecnologías emergentes, tales como la inteligencia artificial, la cadena de bloques y la informática cuántica;

⁴ Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (DO L 194 de 19.7.2016).

13. HACIENDO HINCAPIÉ en que los programas de enseñanza y formación profesional relacionados con la ciberseguridad y las campañas de información y sensibilización sobre las amenazas de seguridad para los usuarios finales son cruciales para reducir los riesgos para la ciberseguridad;
14. SUBRAYANDO que los ciberejercicios son herramientas eficaces para evaluar y seguir mejorando el grado de preparación de la UE y sus Estados miembros a la hora de hacer frente a los incidentes y crisis de ciberseguridad a gran escala;
15. REITERANDO que el ciberespacio no tiene fronteras, lo que implica que las perspectivas y la cooperación transfronterizas e intersectoriales son un principio ineludible de las actividades e iniciativas de desarrollo de capacidades en materia de ciberseguridad;
16. DESTACANDO la importancia de la cooperación entre el sector público, el sector privado y el mundo académico, en particular a través de proyectos de colaboración;
17. DESTACANDO la importancia de la cooperación cívico-militar, en pos de metas comunes en el ámbito cibernético para garantizar una respuesta coherente y eficaz a las ciberamenazas;
18. OBSERVA los progresos logrados por un grupo de Estados miembros en la creación de equipos de respuesta telemática rápida para intensificar la cooperación voluntaria en el ámbito cibernético mediante la asistencia mutua;

19. ACOGE CON SATISFACCIÓN el debate que mantiene actualmente el Consejo sobre la propuesta de la Comisión de Reglamento del Parlamento Europeo y del Consejo 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;
20. ANIMA a la participación activa en los trabajos en curso del Grupo de cooperación SRI, especialmente en lo que atañe al desarrollo de la capacidad cibernética;
21. APOYA los trabajos en curso del Grupo de cooperación SRI sobre la respuesta coordinada de la UE a los incidentes y crisis de seguridad a gran escala;
22. INVITA a los Estados miembros a avanzar a partir de sus estrategias nacionales de ciberseguridad y a integrar la ciberseguridad teniendo en cuenta los requisitos específicos del sector;
23. INVITA a los Estados miembros a que realicen un seguimiento y una evaluación y valoración continuos de los efectos de las medidas adoptadas para reforzar la ciberresiliencia y mejorar las competencias y capacidades cibernéticas a nivel nacional;
24. INVITA a los Estados miembros a que integren la ciberseguridad y la alfabetización digital en los programas de todos los niveles de enseñanza (primaria, secundaria, terciaria y aprendizaje permanente), sobre la base, cuando sea pertinente, de perfiles profesionales existentes y futuros;
25. INVITA a los Estados miembros a emprender iniciativas de sensibilización sobre ciberseguridad y de ciberhigiene destinadas al público y a los usuarios finales, y específicamente al personal del sector público;
26. ANIMA a los Estados miembros a que dirijan ejercicios de ciberseguridad a nivel nacional y a que los dirijan también o participen en ellos a nivel de la UE, con el fin de poner a prueba los aspectos estratégicos y tecnológicos y formarse al respecto, así como de desarrollar eficazmente las habilidades necesarias y de índole práctica;

27. INVITA a los Estados miembros a que sigan desarrollando las capacidades técnicas y operativas de ciberseguridad de sus CSIRT en prevención, atenuación y respuesta a incidentes;
28. PIDE a la Comisión y a la ENISA que sigan respaldando el desarrollo de las capacidades y competencias de la red de CSIRT por parte de los Estados miembros con el fin de cooperar mejor, compartir información sobre incidentes y responder eficazmente a los incidentes transfronterizos a gran escala;
29. INVITA a los Estados miembros a que sigan ayudando a las autoridades policiales a desarrollar competencias específicas en coordinación con las autoridades europeas pertinentes, al objeto de luchar eficazmente contra la ciberdelincuencia a escala de la UE;
30. INVITA a los Estados miembros a que aumenten su inversión en el desarrollo de cibercapacidades;
31. PIDE a la Comisión y a la ENISA que emprendan programas de sensibilización sobre ciberseguridad y formación conexas destinados al personal de las instituciones, órganos y organismos de la UE;
32. PIDE a la UE y a sus Estados miembros que compartan información y las mejores prácticas de forma voluntaria para contribuir a detectar y abordar las principales necesidades en materia de desarrollo de cibercapacidades en los ámbitos nacional y de la UE;
33. INVITA a la UE y a sus Estados miembros a que apoyen la investigación en ciberseguridad y a que promuevan la ciberseguridad en otros ámbitos de estudio, de modo que reúnan diversas ramas de investigación y desarrollo relacionados con la ciberseguridad en un conjunto integrado, y a que fomenten la excelencia en la investigación sobre ciberseguridad;
34. INVITA a la UE y a sus Estados miembros a que emprendan labores de investigación sobre ciberseguridad que reflejen las necesidades de la sociedad e integren los resultados de la investigación en el mercado;
35. PIDE a la UE y a sus Estados miembros que tomen en consideración las cuestiones de ciberseguridad en sus licitaciones de contratación pública de tecnologías de la información y de las comunicaciones, según corresponda.