Consejo de la Unión Europea

Bruselas, 12 de diciembre de 2017
(OR. en)

15748/17

CYBER 215
TELECOM 362
ENFOPOL 618
JAI 1206
MI 959
COSI 333
JAIEX 117
RELEX 1122
IND 377
CSDP/PSDC 720
COPS 400
POLMIL 167

RESULTADO DE LOS TRABAJOS

De:	Secretaría General del Consejo
Fecha:	12 de diciembre de 2017
A:	Delegaciones
N.º doc. prec.:	14435/17 + COR 1
Asunto:	Plan de acción para la aplicación de las Conclusiones del Consejo sobre la Comunicación conjunta al Parlamento Europeo y al Consejo titulada «Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE» - Plan de acción (12 de diciembre de 2017)

Adjunto se remite a las delegaciones el Plan de acción para la aplicación de las Conclusiones del Consejo sobre la Comunicación conjunta al Parlamento Europeo y al Consejo titulada «Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE», adoptadas por el Consejo de Asuntos Generales el 12 de diciembre de 2017.

ANEXO

El presente Plan de acción para la aplicación de las Conclusiones del Consejo sobre la Comunicación conjunta al Parlamento Europeo y al Consejo titulada «Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE» es un documento de nivel estratégico, producto del encargo del Consejo Europeo del 19 de octubre de 2017 y del Consejo del 24 de octubre de 2017. Tal como se indica en las mencionadas Conclusiones del Consejo de 20 de noviembre de 2017, el Plan de acción es un documento vivo, por lo que el Consejo lo revisará y actualizará periódicamente. Está pensado como una herramienta de supervisión horizontal y de seguimiento estratégico de la aplicación de las Conclusiones del Consejo y de las acciones que se detallan a continuación.

Actuación[1]	**Líder / principal responsable**	**Partes interesadas u otras partes implicadas**	**Plazo**	**Avances**	**Notas / observaciones**
Garantizar la transposición y la aplicación plenas y efectivas de la Directiva SRI					
Transposición y aplicación de la Directiva SRI	Estados miembros; Comisión Europea		Mayo de 2018	La Comisión hará un resumen de los avances, que se debatirá en el Grupo de cooperación	
Garantizar una cooperación estratégica eficaz entre los Estados miembros en el Grupo de cooperación	Estados miembros / Presidencia del Consejo	Comisión Europea, ENISA		Resumen de los avances en el informe periódico del Grupo de cooperación	El programa bienal de trabajo del Grupo de cooperación contendrá más detalles sobre los trabajos del Grupo

[1] Cuando procede, la aplicación de las acciones tiene en cuenta los recursos en el marco financiero plurianual.

Alcanzar la plena capacidad operativa de la red de CSIRT	Estados miembros / Presidencia del Consejo	ENISA, Comisión Europea		Resumen de los avances logrados en el informe periódico de la Red al Grupo de cooperación	
Reforzar la respuesta a escala de la UE a los ciberincidentes a gran escala mediante la organización periódica de ejercicios paneuropeos de ciberseguridad					
Llevar a cabo ejercicios de ciberdiplomacia sobre el uso del marco para una respuesta diplomática conjunta a las actividades cibernéticas maliciosas	SEAE	Estados miembros, Comisión Europea y ENISA		Las sucesivas Presidencias del Consejo; los debates sobre los ejercicios en relación con el marco han empezado durante la Presidencia estonia	
Organizar periódicamente ejercicios CyberEurope	Presidencia junto con los Estados miembros	Estados miembros, en particular la red de CSIRT, ENISA, SEAE, Comisión Europea			Frecuencia definida en el encargo dentro del mandato de ENISA y en el transcurso de los debates del Consejo de Administración de ENISA

Llevar a cabo de manera periódica ejercicios estratégicos de ciberseguridad en las distintas formaciones del Consejo	Presidencia	con el apoyo del SEAE o de la Comisión Europea		EU CYBRID 2017 fue llevado a cabo durante la Presidencia estonia para el Consejo de Asuntos Exteriores (Defensa)	Los Estados miembros en el seno del Consejo definirán la periodicidad
Adopción por los colegisladores del REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a ENISA, la «Agencia de Ciberseguridad de la UE», y por el que se deroga el Reglamento (UE) n.º 526/2013, y relativo a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación («Reglamento de Ciberseguridad»)[2]					
Celebrar en el Grupo Horizontal «Cuestiones Cibernéticas» debates en profundidad sobre la propuesta legislativa que den lugar a una orientación general	Presidencia búlgara		Junio de 2018	Estudio de la propuesta por la Presidencia estonia	
Conclusión de las negociaciones entre los colegisladores	Presidencia austriaca		Diciembre de 2018		Plazo indicativo

[2] La aplicación se lleva a cabo sin perjuicio de las competencias del Parlamento Europeo.

Crear la red de centros de competencia en ciberseguridad con un Centro Europeo de Competencia e Investigación en Ciberseguridad					
Presentar una evaluación de impacto, una previsión presupuestaria y los instrumentos jurídicos correspondientes para la creación de la red de centros de competencia en ciberseguridad con un Centro Europeo de Competencia e Investigación en Ciberseguridad	Comisión Europea	Estados miembros, SEAE, AED	Junio de 2018		Los Estados miembros reunidos en el Consejo decidirán nuevas medidas relativas a los instrumentos entregados
Poner en marcha una fase piloto en el marco del programa Horizonte 2020	Comisión Europea	Estados miembros, Grupo de cooperación SRI	Finales de 2018 / principios de 2019		

Desarrollar una capacidad europea para evaluar el grado de seguridad de la criptografía empleada en productos y servicios a disposición de los ciudadanos, las empresas y los Gobiernos en el marco del mercado único digital	Estados miembros		2019		
Garantizar una financiación suficiente para apoyar el refuerzo de la ciberresiliencia y de los esfuerzos de investigación y desarrollo en materia de ciberseguridad en toda la UE					
Garantizar una financiación suficiente para la ciberseguridad, respetando los recursos disponibles	Estados miembros, Comisión Europea		2020		

Aumentar las contribuciones del sector público para reforzar la ciberresiliencia e intensificar los esfuerzos de investigación y desarrollo en materia de ciberseguridad	Estados miembros		2020		
Incentivar las inversiones del sector privado para reforzar la ciberresiliencia e intensificar los esfuerzos de investigación y desarrollo en materia de ciberseguridad	Comisión Europea	con el apoyo de la Organización de Ciberseguridad Europea	2018		
Aumentar las inversiones para la aplicación de las nuevas tecnologías al ámbito de la ciberseguridad	Comisión Europea, Estados miembros	con el apoyo de la Organización de Ciberseguridad Europea	2020		

Estudiar una posible propuesta para la creación de un Fondo de respuesta a emergencias en materia de ciberseguridad	Consejo[3]				Solo se procede al estudio si la propuesta es presentada por la Comisión Europea
Mantener una financiación suficiente para las iniciativas de ciberseguridad dentro de los instrumentos existentes y los programas acordados	Estados miembros, Comisión Europea	BEI	2020		

[3] Sin perjuicio de las competencias del Parlamento Europeo, cuando proceda.

Proporcionar servicios de ciberseguridad coordinados y dignos de crédito y confianza, así como su gobernanza, a las instituciones de la UE					
Aclarar y armonizar la gobernanza de ciberseguridad de las instituciones, órganos y organismos de la UE	Consejo, Comisión Europea y SEAE	Instituciones, organismos y agencias de la UE	2020	Debe presentarse al Grupo Horizontal «Cuestiones Cibernéticas» un informe sobre la gobernanza y los avances logrados en ese ámbito	
Garantizar recursos y apoyo adecuados para el desarrollo del CERT-UE	Instituciones, organismos y agencias de la UE		2020	El CERT-UE presenta periódicamente informes al Grupo Horizontal «Cuestiones Cibernéticas» sobre las ciberamenazas que pesan contra las entidades que la componen Puede aumentarse la asignación de recursos al CERT-UE en el marco de los debates pertinentes en el Grupo Horizontal «Cuestiones Cibernéticas»	
Hacer más hincapié en la sensibilización cibernética y en las aptitudes, la educación y la formación digitales					
Reforzar las campañas de sensibilización cibernética en los Estados miembros	Estados miembros	ENISA	2020		

Reforzar la ciberseguridad en los planes de estudios académicos, educativos y de formación profesional	Estados miembros	Comisión Europea, Organización de Ciberseguridad Europea	2020	Seguimiento de los avances por los Estados miembros y la Comisión Europea	
Crear una red de cooperación de puntos de contacto educativos	Estados miembros	ENISA	2020		
Incorporar y reforzar los programas de prácticas en el ámbito de la ciberseguridad	Estados miembros	Comisión Europea, Organización de Ciberseguridad Europea	2020		
Fomentar la sensibilización relacionada con la ciberseguridad en las administraciones públicas que participan en actividades sociales o económicas fundamentales	Estados miembros		2020	Compromiso de ciberhigiene firmado por seis Estados miembros, el SEAE y la AED en mayo de 2015	

Desarrollar las capacidades de la UE para prevenir, disuadir, detectar y responder a las actividades cibernéticas malintencionadas					
Integrar la ciberseguridad en los mecanismos de gestión de crisis ya existentes a nivel de la UE	Comisión Europea, Consejo	SEAE, agencias de la UE	2018		
Abordar de manera adecuada la respuesta a los incidentes de ciberseguridad en los mecanismos de gestión de crisis nacionales y proponer procedimientos necesarios para la cooperación a escala de la UE	Estados miembros		2018		
Actualizar el Marco político de ciberdefensa de la UE	Estados miembros, SEAE, AED, Comisión Europea		2018		
Fomentar la cooperación entre las comunidades civil y militar dedicadas a la respuesta a incidentes cibernéticos	Estados miembros				

Crear una plataforma de formación y educación en materia de ciberdefensa	Comisión Europea	SEAE, AED, EESD	Finales de 2018		
Aprovechar plenamente las iniciativas de defensa propuestas para acelerar el desarrollo de las capacidades de ciberdefensa en la UE	Estados miembros	SEAE, AED, Comisión Europea			Se pueden elaborar los proyectos de ciberdefensa en el marco de la cooperación estructurada permanente, si lo estiman necesario los Estados miembros que participan en ella. El FED puede financiar proyectos en el ámbito cibernético, si están previstos en los programas de trabajo

Apoyar la lucha contra la delincuencia y suprimir los obstáculos a una justicia penal efectiva en el ciberespacio					
Elaborar una hoja de ruta para luchar contra la evolución de la delincuencia en la red oscura	Europol	Estados miembros	Principios de 2018	El COSI deberá refrendar la hoja de ruta y supervisar su aplicación	
Aplicar las medidas prácticas propuestas por la Comisión para hacer frente al desafío que plantea el cifrado en el contexto de los procesos penales, garantizando a la vez el respeto de los derechos humanos y las libertades fundamentales	Comisión Europea	Estados miembros, Europol	En curso	Supervisión de los avances por el CATS	

Mejorar la capacidad de las servicios policiales y las autoridades judiciales para investigar y enjuiciar los delitos	Estados miembros	Comisión Europea		El COSI supervisará los avances y se propondrán códigos de conducta voluntarios a los proveedores de servicios de Internet para limitar el número de abonados detrás de cada IPv4 mediante el despliegue de tecnologías alternativas al NAT a gran escala (Estados miembros) La Comisión Europea planteará la cuestión del registro del número de puerto de origen a los proveedores de contenidos de Internet en el Foro de Internet de la UE	Teniendo en cuenta las recomendaciones del informe final del Grupo «Cuestiones Generales, incluida la Evaluación» sobre la séptima ronda de la evaluación mutua sobre la lucha contra la ciberdelincuencia

Incentivar el despliegue del IPv6 por parte del sector privado, por ejemplo mediante la posible incorporación de requisitos a las contrataciones públicas	Estados miembros	Comisión Europea	En curso	Los órganos preparatorios del Consejo pertinentes (Grupo Horizontal «Cuestiones Cibernéticas», COSI) supervisarán los avances	
Desarrollar y aprobar un protocolo de respuesta ante emergencias para una respuesta policial coordinada de la UE a los incidentes cibernéticos de gran envergadura	Europol	Estados miembros, Comisión Europea, SEAE, Consejo	Principios de 2018	El COSI deberá refrendar el protocolo y supervisar su aplicación	
Presentar una propuesta legislativa destinada a facilitar el acceso transfronterizo a las pruebas electrónicas por parte de los servicios policiales	Comisión Europea	Consejo, Parlamento Europeo	Principios de 2018	Supervisión de los avances por el CATS	

Presentar un informe de situación sobre la aplicación de las medidas prácticas para mejorar el acceso transfronterizo a las pruebas electrónicas (incluida la cooperación entre los servicios policiales y los proveedores de servicios privados)	Comisión Europea	Estados miembros	Finales de 2017	Supervisión de los avances por el CATS	
Crear una plataforma plenamente operativa para que los Estados miembros puedan intercambiar de manera segura pruebas electrónicas y formularios electrónicos de órdenes europeas de investigación	Comisión Europea	Estados miembros	Mediados de 2019	Supervisión de los avances por el CATS	

Reforzar la cooperación internacional en favor de un ciberespacio mundial abierto, libre, pacífico y seguro					
Mantener el diálogo con los socios internacionales para influir en favor del apoyo mundial a un ciberespacio abierto, libre, pacífico y seguro	SEAE, Consejo, Comisión Europea	Estados miembros	Mediados de 2019	Supervisión de los avances por el Grupo Horizontal «Cuestiones Cibernéticas»	
Crear una red dedicada al desarrollo de las competencias cibernéticas de la UE y unas directrices para el desarrollo de la capacidad cibernética de la UE	SEAE, Comisión Europea, con el apoyo de los Estados miembros				Cooperación posible con el Foro mundial sobre conocimientos cibernéticos
Desarrollar la cooperación UE-OTAN en el ámbito de la formación y la educación	SEAE, Consejo, AED	Estados miembros			
Mantener la cooperación UE-OTAN en el ámbito de los ejercicios de ciberdefensa y poner en común buenas prácticas en la gestión de crisis	SEAE, Consejo	Estados miembros, AED, Comisión Europea			

Tener en cuenta, en los regímenes internacionales pertinentes de control de las exportaciones, las aplicaciones fundamentales de las nuevas tecnologías en el ámbito de la ciberseguridad	Estados miembros, Comisión Europea				
Desarrollar y comunicar una posición consolidada de la UE en los debates sobre la gobernanza mundial de Internet	Consejo, Comisión Europea, SEAE	Estados miembros	2018 y en curso	El COSI deberá facilitar la adopción de una posición común de la UE sobre un sistema WHOIS compatible con el Reglamento general de protección de datos, que garantizará un acceso rápido y oportuno a información de registro exacta sobre nombres de dominio y propietarios de direcciones IP (datos WHOIS) con fines legítimos, en particular a efectos de cumplimiento de la ley, protección del consumidor, protección de los derechos de propiedad intelectual y actividades de ciberseguridad	