TRIBUNAL DE CUENTAS EUROPEO

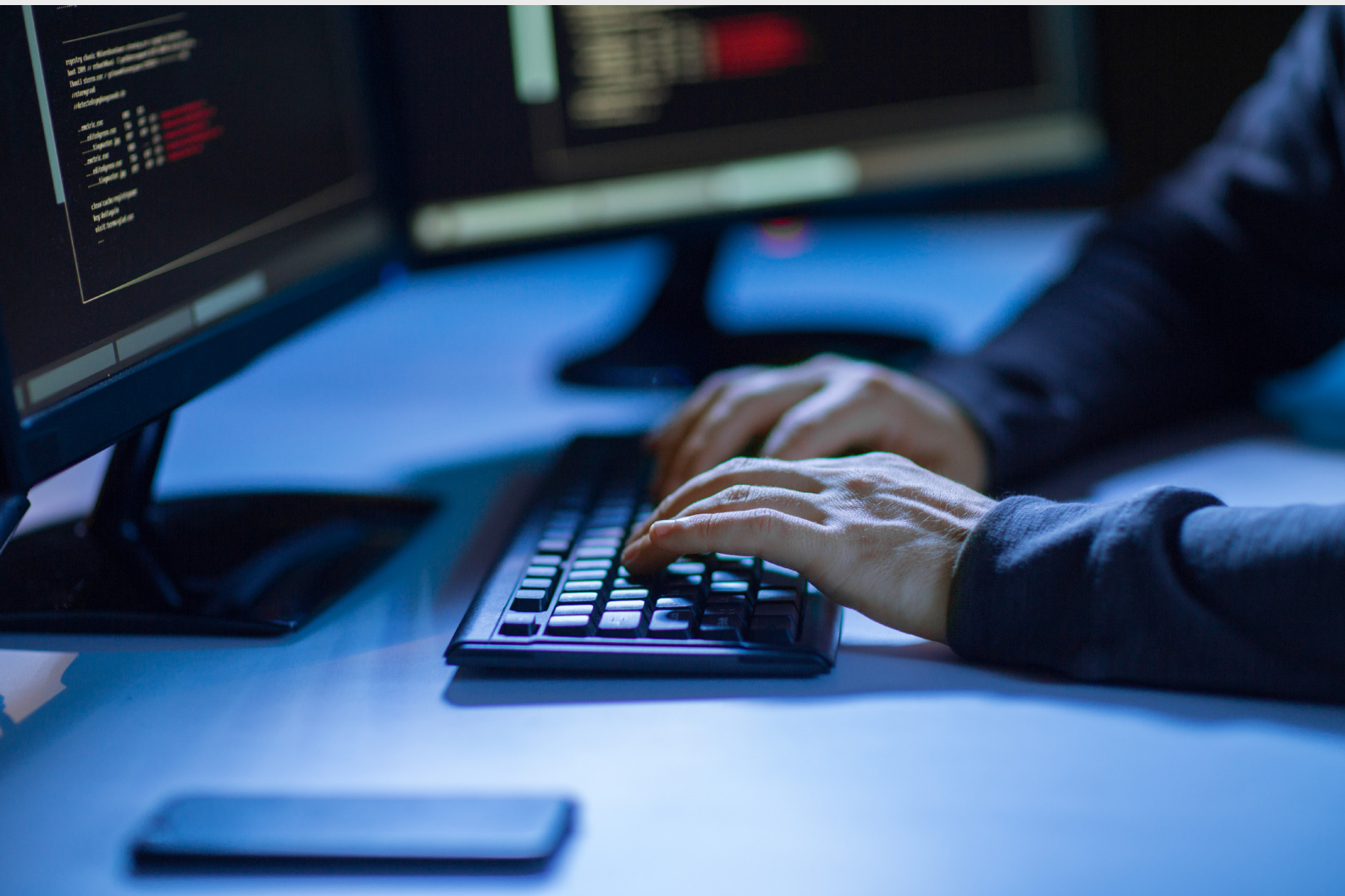
ES

2019

Desafíos de una política eficaz de ciberseguridad en la UE

Documento informativo

Marzo de 2019



Acerca del documento:

En el presente documento informativo, que no es un informe de auditoría, se presenta una visión general de la compleja política de ciberseguridad de la UE y se determinan los principales desafíos que plantea su aplicación eficaz. Trata sobre la seguridad de las redes y de la información, la ciberdelincuencia, la ciberdefensa, y la desinformación. También servirá para preparar futuros trabajo de auditoría sobre esta cuestión.

El Tribunal realizó un análisis documental de información publicada en documentos oficiales, documentos de posición y estudios de terceros. Realizó el trabajo de campo entre abril y septiembre de 2018, y tuvo en cuenta la evolución hasta diciembre de 2018. Completó su trabajo con una encuesta a las oficinas nacionales de auditoría de los Estados miembros y entrevistas con partes interesadas clave de instituciones de la UE y representantes del sector privado.

Los desafíos identificados se dividen en cuatro amplios grupos: i) marco político; ii) financiación y gasto; iii) refuerzo de la ciberresiliencia, y iv) respuesta eficaz a los ciberincidentes. Puesto que lograr un mayor nivel de ciberseguridad en la UE sigue siendo imprescindible, cada capítulo termina con una serie de ideas que sirvan de materia de reflexión a responsables políticos, legisladores y profesionales.

El Tribunal desea reconocer las contribuciones constructivas que ha recibido de la Comisión, el Servicio Europeo de Acción Exterior, el Consejo de la Unión Europea, ENISA, Europol, la Organización Europea de Ciberseguridad y las oficinas nacionales de auditoría de los Estados miembros.

Índice

Resumen

I La tecnología abre todo un mundo nuevo de oportunidades, de nuevos productos y servicios que han pasado a ser elementos fundamentales de nuestra vida cotidiana. Pero, en contrapartida, aumenta el riesgo de sufrir ciberdelincuencia o ciberataques, cuyo impacto económico y social sigue aumentando. El reciente impulso de la Unión Europea que, desde 2017, ha acelerado las iniciativas de refuerzo de la ciberseguridad y de su autonomía digital, llega por tanto en un momento crítico.

II El objetivo del presente documento informativo, que no es un informe de auditoría y está basado en información pública, es presentar una visión general de un panorama político complejo y desigual, e identificar los principales desafíos que plantea la aplicación de políticas eficaces. Este documento abarca la política de ciberseguridad de la UE, la ciberdelincuencia y la ciberdefensa, y los esfuerzos en la lucha contra la desinformación. Los desafíos identificados se dividen en cuatro amplios grupos: i) marco político y legislativo; ii) financiación y gasto; iii) refuerzo de la ciberresiliencia; y iv) respuesta eficaz a los ciberincidentes. Cada capítulo contiene algunas reflexiones sobre los desafíos presentados.

Marco político y legislativo

III Desarrollar medidas que se ajusten a los amplios objetivos de la estrategia de ciberseguridad de la UE de convertirse en el entorno digital más seguro del mundo plantea un desafío ante la falta de objetivos cuantificables y de datos fiables, que son escasos. Rara vez se cuantifican los resultados y pocas políticas han sido evaluadas. Por tanto, un desafío clave es **garantizar una rendición de cuentas y una evaluación significativa**s mediante la transición hacia una cultura del rendimiento con prácticas de evaluación integradas.

IV El marco legislativo sigue estando incompleto. **Las carencias de la legislación de la UE y la falta de coherencia en su transposición** impiden aprovechar plenamente su potencial.

Financiación y gasto

V **Ajustar los niveles de inversión a los objetivos** es complicado: exige incrementar no solo la inversión global en ciberseguridad, que en la UE ha sido limitada y fragmentada, sino también su impacto, en especial aprovechando mejor los resultados del gasto en investigación y garantizando la selección y financiación eficaz de empresas emergentes.

VI **Tener una visión general clara del gasto de la UE** es fundamental para que tanto la UE como sus Estados miembros conozcan las carencias que deben subsanar para cumplir los objetivos que se han fijado. Como no hay un presupuesto específico de la UE para financiar la estrategia de ciberseguridad, tampoco existe una idea clara de cuánto y cómo se invierte y se asigna.

VII En una época de prioridades políticas cada vez más centradas en la seguridad, **las restricciones en la dotación de recursos a las agencias de la UE relacionadas con la cibernética** puede impedir el logro de las ambiciones de la UE. Una forma de abordar este desafío es encontrar maneras de atraer y retener el talento.

Refuerzo de la ciberresiliencia

VIII En los sectores público y privado de la UE, así como en el ámbito internacional, existen numerosas deficiencias en la gobernanza de la ciberseguridad. Esto afecta a la capacidad de la comunidad mundial para responder a los ciberataques y limitarlos, e impide la aplicación de un enfoque coherente en toda la UE. Por tanto, el desafío consiste en **reforzar la gobernanza de la ciberseguridad**.

IX Es fundamental **mejorar las capacidades y la sensibilización** en todos los sectores y niveles de la sociedad, teniendo en cuenta el creciente déficit de cualificaciones en ciberseguridad en el mundo. Actualmente, en la UE existen pocas normas de formación, titulación o evaluación de riesgos cibernéticos.

X Es fundamental crear un clima de confianza para reforzar la ciberresiliencia global. La propia Comisión ha valorado que la coordinación general sigue siendo insuficiente. **Mejorar el intercambio de información y la coordinación** entre los sectores público y privado sigue siendo un desafío.

Respuesta eficaz a los ciberincidentes

XI Los sistemas digitales son actualmente tan complejos que es imposible prevenir todos los ataques. La respuesta a este desafío es una **detección y una respuesta rápidas**. Sin embargo, la ciberseguridad todavía no está totalmente integrada en los mecanismos existentes en la UE de coordinación de respuestas ante crisis, lo que puede limitar la capacidad de la Unión de responder a los ciberincidentes transfronterizos a gran escala.

XII La **protección de las infraestructuras críticas y las funciones sociales** es fundamental. La posible interferencia en procesos electorales y las campañas de desinformación son desafíos críticos.

XIII Los actuales desafíos que plantean las amenazas cibernéticas a las que se enfrenta la UE y el mundo en general requieren un compromiso continuo y una garantía firme de respeto de los valores fundamentales de la UE.

Introducción

01 La tecnología ha abierto un mundo nuevo de posibilidades. A medida que aparecen, los nuevos productos y servicios pasan a formar parte de nuestra vida cotidiana. No obstante, con cada nuevo avance, crece nuestra dependencia tecnológica y, por tanto, también la importancia de la ciberseguridad. Cuantos más datos personales introducimos en Internet y cuanto más conectados estamos, más probable es que seamos víctimas de alguna forma de ciberdelincuencia o de ciberataque.

¿Qué es la ciberseguridad?

02 No existe ninguna definición normalizada y universalmente aceptada de ciberseguridad[1], pero, en líneas generales, se puede describir como el conjunto de garantías y medidas adoptadas para defender los sistemas de información y a sus usuarios frente a accesos no autorizados, ataques y daños para garantizar la confidencialidad, la integridad y la disponibilidad de los datos.

03 La ciberseguridad consiste en prevenir y detectar ciberincidentes, así como responder ante los mismos y recuperarse de estos. Los incidentes pueden ser o no intencionados y consisten, por ejemplo, en acciones que van desde la divulgación accidental de información hasta los ataques a empresas e infraestructuras críticas, o el robo de datos personales, e incluso la interferencia en procesos democráticos. Pueden tener efectos nocivos de amplio alcance sobre las personas, las organizaciones y las comunidades.

04 Tal y como se entiende en los círculos políticos de la UE, la ciberseguridad no se limita a la seguridad de la información y de las redes, sino que abarca cualquier actividad ilícita que implique el uso de tecnologías digitales en el ciberespacio, o sea, actos de ciberdelincuencia tales como el lanzamiento de ataques de virus informáticos y el fraude de medios de pago distintos del efectivo, pero también otros delitos relacionados con el contenido más que con los sistemas, como la difusión en línea de pornografía infantil. También se ocupa de las campañas de desinformación para influir en debates en línea y de las presuntas interferencias electorales. Asimismo, Europol considera que existe una convergencia entre la ciberdelincuencia y el terrorismo[2].

05 Diversos actores, entre los que se cuentan Estados, organizaciones delictivas y hacktivistas, instigan los ciberincidentes movidos por distintos motivos. Estos

incidentes tienen repercusiones de alcance nacional, europeo e incluso mundial. Sin embargo, la naturaleza intangible y en buena medida transfronteriza de internet, y de las herramientas y tácticas empleadas, dificultan a menudo la identificación del autor de un ataque (el denominado «problema de atribución»).

06 Los múltiples tipos de amenazas a la ciberseguridad se pueden clasificar en función de lo que hacen a los datos (divulgación, modificación, destrucción o negación de acceso) o de los principios fundamentales de seguridad de la información que vulneran, como se muestra en la ***ilustración 1*** *infra*. En el ***recuadro 1*** se describen algunos ejemplos de ataques. Cuanto más aumenta la sofisticación de los sistemas de información, menos eficaces se vuelven nuestros mecanismos de defensa[3].

Ilustración 1 – Tipos de amenazas y principios de seguridad que ponen en peligro

Fuente: Tribunal de Cuentas Europeo, modificado a partir de un estudio del Parlamento Europeo[4].
Candado = no afecta a la seguridad; Signo de exclamación = pone en peligro la seguridad

Recuadro 1

Tipos de ciberataques

Cada vez que un nuevo dispositivo se conecta a internet o a otros dispositivos, aumenta la denominada «superficie de ataque» de la ciberseguridad. El crecimiento exponencial del internet de las cosas, la nube, los macrodatos y la digitalización de la industria viene acompañado de un crecimiento de la exposición a las vulnerabilidades, lo que facilita a los agentes maliciosos llegar cada vez a más víctimas. La variedad de tipos de ataques y su creciente sofisticación hacen que sea verdaderamente difícil mantener el ritmo[5].

Los **programas maliciosos** (programas informáticos malintencionados) están diseñados para dañar a los dispositivos o redes. Pueden contener virus, troyanos, programas de secuestro, gusanos, *adware* y programas espía. Los **programas de secuestro** encriptan datos e impiden a los usuarios acceder a sus archivos hasta que paguen un rescate, generalmente en criptomoneda, o lleven a cabo una determinada acción. Según Europol, los ataques de los programas de secuestro son los más frecuentes y en los últimos años se han multiplicado exponencialmente los distintos tipos de estos programas. Aumentan asimismo los ataques de **denegación de servicio distribuido** (DDoS), que impiden el acceso a los servicios o recursos al inundarlos de más solicitudes de las que pueden gestionar, y un tercio de las organizaciones se enfrentaron a este tipo de ataque en 2017[6].

Los usuarios pueden ser manipulados para que realicen una acción o desvelen información confidencial sin darse cuenta. Esta artimaña se pueden utilizar para el robo de datos o para el ciberespionaje, y se conoce como **ingeniería social**. Hay distintas formas de conseguirlo, pero un método común es la **suplantación de identidad**, que consiste en engañar a los usuarios a través de correos que parezcan procedentes de fuentes fiables para que revelen información o para que pulsen enlaces que infectarán los dispositivos con programas maliciosos descargados. Más de la mitad de los Estados miembros informaron d investigaciones de ataques de redes[7].

Probablemente, los tipos de amenaza más perversos son las **amenazas persistentes avanzadas** (APT). Se trata de atacantes sofisticados que realizan una vigilancia a largo plazo, roban datos y, en ocasiones, también tienen fines destructivos. Su objetivo es pasar desapercibidos sin ser detectados durante el mayor tiempo posible. Las APT a menudo están relacionadas con los Estados y se tienen como objetivo sectores especialmente delicados, como la tecnología, la defensa y las infraestructuras críticas. Se considera que el ciberespionaje representa al menos una cuarta parte de los ciberincidentes y la mayoría de los gastos[8].

Gravedad del problema

07 Es difícil calcular el impacto de no estar bien preparados para un ciberataque debido a la falta de datos fiables. El impacto económico de la ciberdelincuencia se quintuplicó entre 2013 y 2017[9], y afectó a gobiernos y a empresas, tanto grandes como pequeños por igual. El crecimiento previsto de las primas de seguros cibernéticos, que pasaron de 3 000 millones en 2018 a 8 900 millones en 2020, refleja esta tendencia.

08 Aunque el impacto financiero de los ciberataques sigue creciendo, hay una disparidad alarmante entre el coste del lanzamiento de un ataque y el coste de la prevención, la investigación y la reparación. Por ejemplo, llevar a cabo un ataque de DDoS puede costar tan solo 15 euros al mes, pero las pérdidas sufridas por la empresa atacada, incluidos los daños a su reputación, son mucho más elevados[10].

09 A pesar de que el 80 % de las empresas de la UE experimentaron al menos un incidente de ciberseguridad en 2016[11], el conocimiento de los riesgos sigue siendo alarmantemente bajo. El 69 % de las empresas de la UE tiene un conocimiento nulo o limitado de su exposición a las amenazas cibernéticas[12], y el 60 % no ha calculado nunca las potenciales pérdidas financieras[13]. Además, según una encuesta mundial, un tercio de las organizaciones preferirían pagar el rescate al *hacker* en vez de invertir en seguridad de la información[14].

10 Los ataques mundiales de los programas de secuestro *Wannacry* y del programa malicioso escoba *NotPetya* de 2017 afectaron en conjunto a más de 320 000 víctimas en unos 150 países[15]. Estos incidentes sirvieron para concienciar al mundo de la amenaza que suponen los ciberataques e impulsar la integración de la ciberseguridad en el pensamiento político general. Además, actualmente el 86 % de los ciudadanos de la UE cree que el riesgo de ser víctima de la ciberdelincuencia va en aumento[16].

Acción de la UE en materia de ciberseguridad

11 La UE participó como organización observadora en el Comité del Convenio sobre la Ciberdelincuencia del Consejo de Europa en 2001[17] (el Convenio de Budapest) y, desde entonces, ha utilizado las políticas, la legislación y el gasto para mejorar su ciberresiliencia. Desde 2013, en el contexto del aumento de los ciberataques e incidentes graves, la actividad se ha acelerado, como muestra la ***ilustración 2***. Paralelamente, los Estados miembros han adoptado (y en algunos casos ya han actualizado) sus primeras estrategias nacionales de ciberseguridad.

12 En el ***recuadro 2*** y en el ***anexo I*** se describen los principales actores de la UE con responsabilidades en materia de ciberseguridad.

Recuadro 2

¿Quién participa?

El objetivo de la **Comisión Europea** es aumentar las capacidades y la cooperación en materia de ciberseguridad, reforzar el papel de la UE en el ámbito de la ciberseguridad e integrar este aspecto en otras políticas de la UE. Las principales direcciones generales responsables de la política de ciberseguridad son la DG **Redes de Comunicación, Contenido y Tecnologías** (ciberseguridad) y la DG **Migración y Asuntos de Interior** (ciberdelincuencia), responsables del Mercado Único Digital y de la Unión de la Seguridad, respectivamente. La DG **Informática** es responsable de la seguridad informática de los propios sistemas de la Comisión.

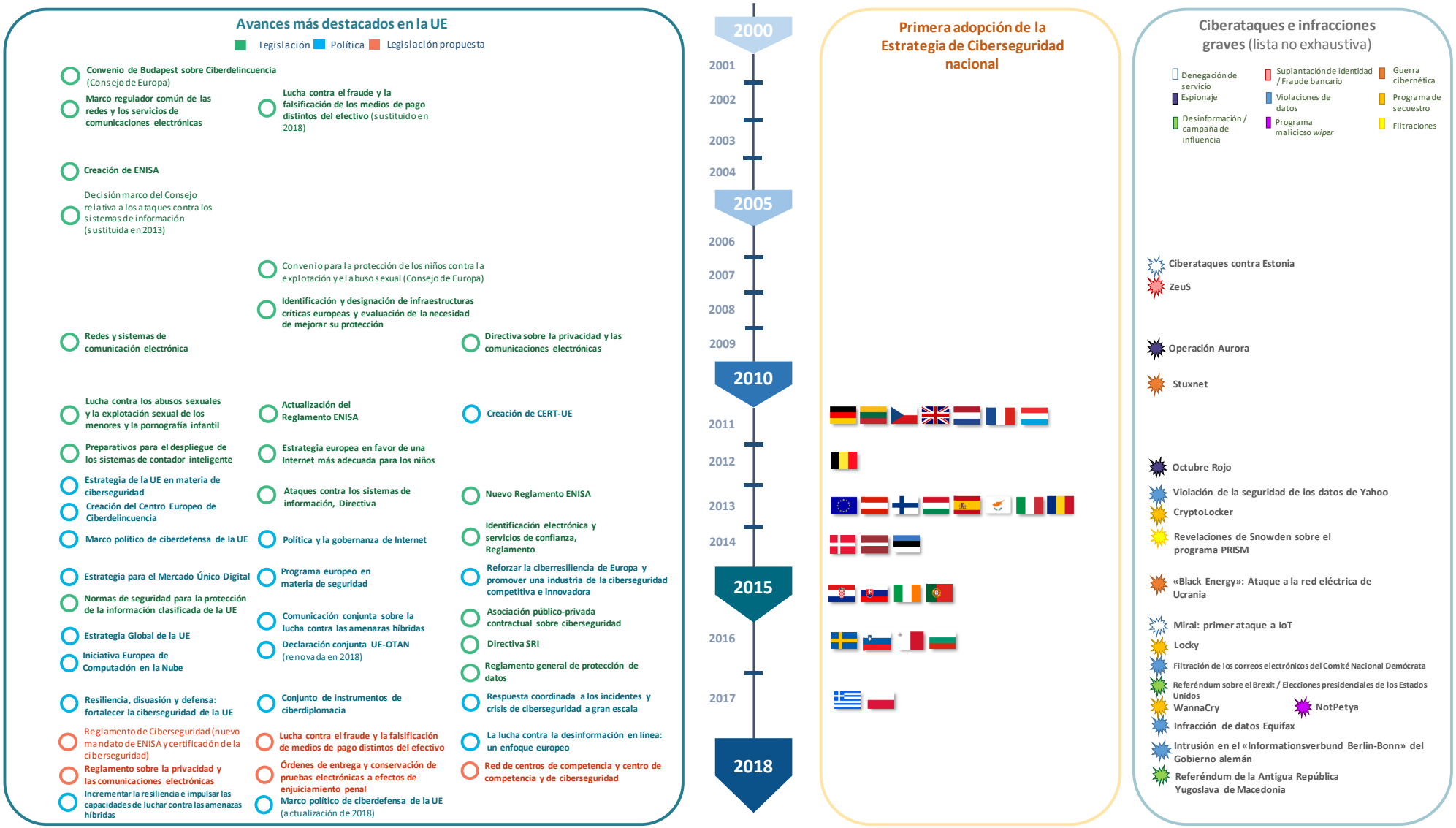
Numerosas agencias de la UE prestan apoyo a la Comisión, en particular **ENISA** (Agencia de Seguridad de las Redes y de la Información de la Unión Europea), la agencia de ciberseguridad de la UE: organismo principalmente asesor que apoya el desarrollo de políticas, la creación de capacidad y la sensibilización. El Centro Europeo de Ciberdelincuencia (**EC3**) de Europol se creó para reforzar la respuesta policial de la UE ante la ciberdelincuencia. La Comisión cuenta con un Equipo de respuesta a emergencias informáticas (**CERT-UE**), que da apoyo a todas las instituciones, órganos y organismos de la UE.

El **Servicio Europeo de Acción Exterior** (SEAE) está al frente de la ciberdefensa, la ciberdiplomacia y la comunicación estratégica, y alberga centros de análisis e inteligencia. La **Agencia Europea de Defensa** (AED) tiene por objeto desarrollar capacidades de ciberdefensa.

Los **Estados miembros** son responsables principalmente de su propia ciberseguridad y, en el contexto de la UE, actúan a través del **Consejo**, que dispone de numerosos organismos de coordinación y para compartir información (entre los cuales se encuentra el Grupo Horizontal «Cuestiones Cibernéticas»). El **Parlamento Europeo** actúa como colegislador.

Las **organizaciones del sector privado** tales como la industria, los organismos de gobernanza de internet y las instituciones académicas, son socios y a la vez participantes en el desarrollo y la aplicación de las políticas, también a través de una asociación público-privada contractual (**APPc**).

Ilustración 2 – Aceleración en el desarrollo de políticas y en la legislación (a 31 de diciembre de 2018)



Fuente: Tribunal de Cuentas Europeo.

Política

13 El ecosistema cibernético de la UE es complejo, multidimensional y afecta a varios ámbitos políticos internos, como Justicia y Asuntos de Interior, Mercado Único Digital y Políticas de Investigación. En política exterior, la ciberseguridad afecta a la diplomacia y cada vez está más integrada en la emergente política de defensa de la UE.

14 La piedra angular de la política de la UE es la **Estrategia de Ciberseguridad de 2013**[18]. El objetivo de la Estrategia es lograr que el entorno digital de la UE sea el más seguro del mundo, defendiendo al mismo tiempo los valores y las libertades fundamentales. Tiene cinco objetivos principales: i) aumentar la ciberresiliencia; ii) reducir la ciberdelincuencia; iii) desarrollar estrategias y capacidades de ciberdefensa; iv) desarrollar recursos tecnológicos e industriales de ciberseguridad; y v) crear una política internacional del ciberespacio de acuerdo con los valores esenciales de la UE.

15 La Estrategia de Ciberseguridad está interrelacionada con tres estrategias adoptadas posteriormente:

— La **Agenda Europea de Seguridad** (2015), cuyo objetivo es mejorar la aplicación de la Ley y la respuesta judicial ante la ciberdelincuencia, principalmente mediante la renovación y actualización de la legislación y de las políticas existentes[19]. Otro de sus objetivos es identificar los obstáculos a las investigaciones penales sobre la ciberdelincuencia y mejorar las acciones de desarrollo de la capacidad informática.

— La **Estrategia para el Mercado Único Digital**[20] (2015), cuyo objetivo es mejorar el acceso a los bienes y servicios digitales mediante la creación de las condiciones adecuadas para aprovechar al máximo el potencial de crecimiento de la economía digital. Para ello, resulta fundamental reforzar la seguridad en línea, la confianza y la inclusión.

— La **Estrategia Global**[21], cuyo objetivo es impulsar el papel de la UE en el mundo. La ciberseguridad constituye un pilar básico que surge de un compromiso renovado sobre cuestiones cibernéticas, de la cooperación con socios clave y de la determinación de abordarlas desde todos los ámbitos políticos,además de ofrecer refutaciones de desinformación a través de la comunicación estratégica.

16 En los últimos años, el ciberespacio, cada vez más militarizado[22] y armado[23], ha llegado a considerarse como el quinto escenario bélico[24]. La ciberdefensa protege los sistemas del ciberespacio, las redes y la infraestructura crítica frente a los ataques

militares o de otro tipo. En 2014 se adoptó un **marco político de ciberdefensa de la UE**, que fue actualizado en 2018[25]. Las actualizaciones de 2018 identifican seis prioridades, entre las que figura el desarrollo de capacidades en ciberdefensa, así como la protección de las redes de comunicación e información de la política común de seguridad y defensa de la UE (PCSD). La ciberdefensa también forma parte del marco de Cooperación Estructurada Permanente (CEP) y de la cooperación UE-OTAN.

17 El **Marco común de lucha contra las amenazas híbridas** (2016) de la UE aborda las amenazas cibernéticas para las infraestructuras críticas y para los usuarios privados y subraya que los ciberataques se pueden llevar a cabo a través de campañas de desinformación en las redes sociales[26]. También señala la necesidad de mejorar la sensibilización y la cooperación entre la UE y la OTAN, que se plasmó en las declaraciones conjuntas UE-OTAN de 2016 y 2018[27].

18 En 2017, la Comisión presentó un nuevo paquete de ciberseguridad que refleja la creciente urgencia de protección digital. Incluía una nueva comunicación de la Comisión que actualizaba la estrategia de ciberseguridad de 2013[28], un plan rector para una respuesta rápida y coordinada ante un ataque importante, y para la rápida aplicación de la Directiva sobre seguridad de las redes y sistemas de información (Directiva SRI)[29]. Además, el paquete contenía varias propuestas legislativas (véase el apartado ***22***).

Legislación

19 Desde 2002, se ha adoptado legislación más o menos relacionada con la ciberseguridad.

20 La pieza clave jurídica, pilar principal de la estrategia de ciberseguridad de 2013, es la **Directiva sobre seguridad de las redes y sistemas de información (Directiva SRI)**[30] de 2016, el primer acto legislativo de la UE sobre ciberseguridad. El objeto de la Directiva, que se debía transponer a más tardar en mayo de 2018, es conseguir un nivel mínimo de capacidades armonizadas mediante la obligación impuesta a los Estados miembros de adoptar estrategias nacionales de SRI y crear puntos de contacto únicos y equipos de respuesta a incidentes de seguridad informática (CSIRT)[31]. Asimismo, establece requisitos en materia de seguridad y notificación para los operadores de servicios esenciales en sectores críticos y para los proveedores de servicios digitales.

21 Paralelamente, el **Reglamento general de protección de datos**[32] entró en vigor en 2016 y se aplicó a partir de mayo de 2018. Su objetivo es proteger los datos personales de los ciudadanos europeos estableciendo normas sobre su tratamiento y difusión. Concede determinados derechos a los interesados e impone obligaciones a los responsables del tratamiento (proveedores de servicios digitales) en relación con el uso y la transferencia de información. Asimismo, establece requisitos de notificación en caso de incumplimiento y, en algunos casos, puede imponer multas. La ***ilustración 3*** muestra cómo se complementan los objetivos de la Directiva SRI y del Reglamento general de protección de datos de reforzar la ciberseguridad y garantizar la protección de datos.

22 Actualmente se están debatiendo varios proyectos legislativos: la propuesta de Reglamento de Ciberseguridad para reforzar ENISA y establecer un mecanismo de certificación de la UE[33], la propuesta de Reglamento sobre las órdenes europeas de entrega y conservación de pruebas electrónicas[34] y la propuesta de Directiva sobre pruebas electrónicas[35]. La propuesta de 2018 de creación de un Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y una Red de Centros Nacionales de Coordinación (denominados en lo sucesivo «red de centros de competencia en ciberseguridad y un centro de competencia de investigación») forma parte del paquete de ciberseguridad de 2017[36].

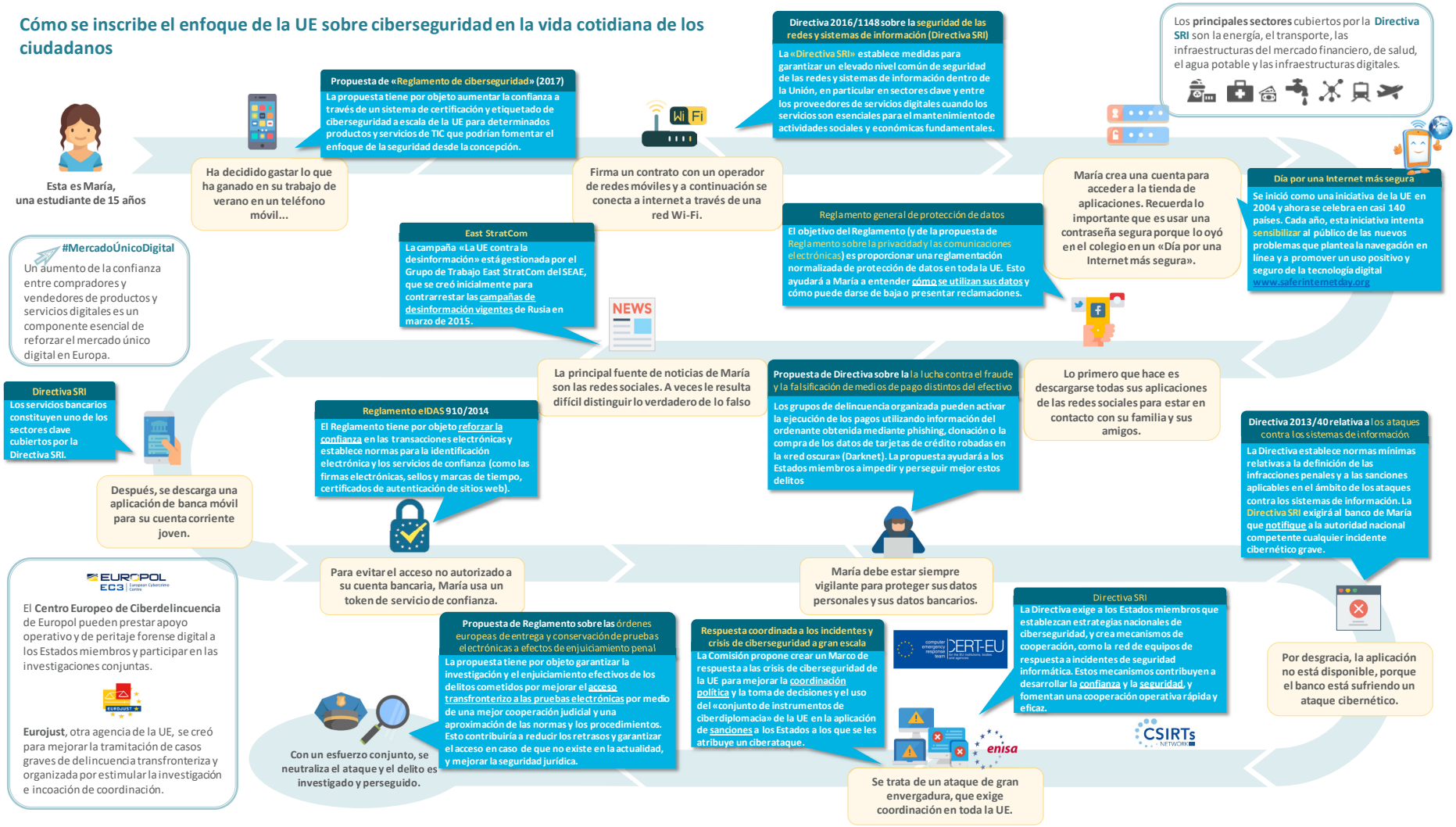
23 Puede resultar difícil percibir la amplitud del marco político y legislativo sobre ciberseguridad y cómo afecta a nuestra vida cotidiana.

24 La ***ilustración 4*** intenta reflejar las interacciones de varios actos legislativos y otras actividades con la vida de un ciudadano europeo ficticio.

Ilustración 3 – Cómo se complementan entre sí la Directiva SRI y el Reglamento general de protección de datos

Fuente: Tribunal de Cuentas Europeo.

Ilustración 4 – Cómo se inscribe el enfoque de la UE sobre ciberseguridad en la vida cotidiana de los ciudadanos



Fuente: Tribunal de Cuentas Europeo.

Construcción de un marco político y legislativo

25 El ecosistema cibernético de la UE es complejo y multidimensional, e implica a muchas partes interesadas (véase el ***anexo I***). Agrupar todas las piezas que lo conforman constituye todo un desafío. Desde 2013 se realiza un esfuerzo concertado para dotar de coherencia al ámbito de la ciberseguridad en la UE[37].

Desafío 1: Una evaluación y una rendición de cuentas verdaderamente significativas

26 Como ha señalado la Comisión, es difícil establecer una relación causal entre la estrategia de 2013 y los cambios observados. Los objetivos de la estrategia de 2013 se formularon en términos muy generales, lo que expresa más bien una visión y no una meta cuantificable[38]. Sin objetivos cuantificables, desarrollar medidas que se ajusten a estos fines generales constituye un desafío. La finalidad del marco político actualizado de ciberdefensa (2018) será desarrollar objetivos que fijen el nivel mínimo de ciberseguridad y confianza que se debe alcanzar, aunque limitándose exclusivamente a la ciberdefensa, pues no se han fijado objetivos que definan el nivel deseado de resiliencia de la Unión en su conjunto.

27 Rara vez se cuantifican los resultados y pocas políticas han sido evaluadas[39]. Esto se debe, en parte, a la reciente aplicación de muchas de las medidas (legislativas o de otro tipo), lo que impide una evaluación completa de su impacto. El desafío consiste en definir criterios de evaluación significativos que puedan ayudar a medir el impacto. Además todavía no se aplica por norma la evaluación rigurosa en materia de ciberseguridad. Por tanto, es necesario adoptar una cultura basada en los resultados que incorpore prácticas de evaluación y normalización de los informes. Actualmente, ENISA no es competente en materia de evaluación y seguimiento del estado de la ciberseguridad de la UE y de su preparación.

28 La elaboración de políticas basadas en pruebas depende de la disponibilidad de estadísticas y datos fiables suficientes que permitan supervisar y analizar tendencias y necesidades. Debido a la ausencia de un sistema de supervisión común y obligatorio, los datos fiables sean escasos. Con frecuencia no resulta fácil disponer de indicadores ni definirlos[40]. Sin embargo, se han desarrollado parámetros específicos en algunos ámbitos, como el ciclo de actuación de la UE, empleado, en la lucha contra la delincuencia grave y organizada.

29 Pocos Estados miembros recopilan regularmente datos oficiales sobre cuestiones relacionadas con el ámbito cibernético, por lo que es difícil compararlos. Hasta ahora, la UE apenas ha hecho alusión a la necesidad de consolidar las estadísticas a escala europea[41]. Asimismo, existen pocos análisis independientes disponibles de la UE que abarquen cuestiones como las siguientes[42]: la economía de la ciberseguridad, incluidos los aspectos conductuales (desajuste de incentivos o asimetrías de información); la comprensión del impacto de los fallos cibernéticos y la ciberdelincuencia; macroestadísticas sobre tendencias cibernéticas y desafíos esperados, y las mejores soluciones para hacer frente a las amenazas.

30 Debido a la falta de objetivos específicos y a la escasez de datos fiables e indicadores bien definidos, la evaluación de los logros de la estrategia ha sido en gran medida cualitativa hasta la fecha. Los informes de situación con frecuencia describen las actividades realizadas o los logros conseguidos pero no miden exhaustivamente los resultados. Además, todavía no se han establecido los valores de referencia para la evaluación de la resiliencia de los sistemas. Por otro lado, a falta de una definición codificada de ciberdelincuencia, es prácticamente imposible encontrar indicadores europeos pertinentes que sirvan de ayuda en la supervisión y evaluación.

31 La supervisión independiente de la aplicación de la política de ciberseguridad difiere entre los distintos Estados miembros. El Tribunal realizó encuestas a las oficinas nacionales de auditoría acerca de su experiencia en la auditoría de este ámbito. La mitad de ellas[43] no habían auditado nunca esta cuestión, y los que sí lo habían hecho se habían centrado principalmente en los siguientes aspectos: gobernanza de la información, protección de infraestructuras críticas, intercambio de información y coordinación entre partes interesadas clave, y preparación, notificación y respuesta con respecto a los incidentes. Dos de los aspectos menos tratados eran las medidas de sensibilización y el déficit de capacidades digitales. Los resultados de estas auditorías o evaluaciones no siempre se hacen públicos por motivos de seguridad nacional. En el ***anexo III*** figura una lista de informes de auditoría publicados por oficinas nacionales de auditoría.

32 Según la percepción de los encuestados, las limitaciones en las capacidades cibernéticas (véanse también los apartados ***82 a 90***) y las dificultades para evaluar los avances en ciberseguridad constituían los principales desafíos de la auditoría de las medidas gubernamentales en este ámbito.

Desafío 2: Colmar las carencias de la legislación de la UE y corregir su desigual transposición

33 La velocidad de aparición de tecnologías y amenazas nuevas supera con creces a la de desarrollo y aplicación de legislación de la UE. Los procedimientos de la Unión no se concibieron para la era digital: desarrollar procedimientos flexibles e innovadores que proporcionen un marco jurídico y político idóneo[44] para mejorar la capacidad de prever y configurar el futuro es una prioridad crítica[45].

34 Pese a fomentar la coherencia, el marco legislativo de la ciberseguridad aun está incompleto (véanse algunos ejemplos en el ***cuadro 1***). La fragmentación y las carencias dificultan el logro de los objetivos políticos generales y dan lugar a ineficiencias. La Comisión identificó en su evaluación de la estrategia, entre otras, las siguientes carencias i: el internet de las cosas, el equilibrio de responsabilidades entre los usuarios y los proveedores de productos digitales, y algunos aspectos no previstos en la Directiva SRI. La propuesta de Reglamento de Ciberseguridad trata de resolver parcialmente estas carencias fomentando la seguridad desde el diseño a través de un programa de certificación para toda la UE. Algunas partes interesadas creen que todavía es patente la falta de una ciberpolítica industrial bien definida y de un enfoque común del ciberespionaje[46].

Cuadro 1 – Carencias y transposición desigual del marco legislativo (lista no exhaustiva)

Ámbito político	Ejemplos
Mercado Único Digital	o La presente Directiva sobre venta de bienes de consumo no abarca la ciberseguridad. Las propuestas de Directivas sobre contenidos digitales[47] y compraventa en línea[48] intentan colmar este vacío. o Los marcos jurídicos de los deberes de diligencia en los Estados miembros de la UE son limitados y diversos, lo que genera inseguridad jurídica y dificultades para recurrir[49]. o Las políticas sobre divulgaciones de vulnerabilidad de software se están desarrollando a distintas velocidades en los Estados miembros, y en la UE no existe un marco jurídico global que permita la adopción de un enfoque coordinado[50].
Refuerzo de la seguridad de las redes y de la información	o Los Estados miembros pueden incluir sectores que no figuren en la Directiva SRI[51]. La industria hotelera, que no está cubierta, puede ser la vía de acceso de otros delitos, como el tráfico de drogas, la trata de personas y la inmigración ilegal[52].
Lucha contra la ciberdelincuencia	o Muchos Estados miembros no han definido las pruebas electrónicas en su legislación nacional[53] (véase también el apartado ***22***). o La actual Decisión marco sobre el fraude de medios de pago distintos del efectivo no prevé explícitamente instrumentos de pago inmateriales como las monedas virtuales, el dinero electrónico y el dinero a través del móvil, ni actos como la suplantación de identidad, el robo de datos para la clonación de tarjetas y la posesión y divulgación de información sobre el pagador[54]. o La Directiva relativa a los ataques contra los sistemas de información no aborda directamente la adquisición ilegal de datos desde dentro (por ejemplo, el ciberespionaje), lo que plantea dificultades para la aplicación de la Ley[55]. o A raíz de la sentencia del Tribunal de Justicia de la Unión Europea sobre conservación de datos[56], las diferencias en la aplicación del marco jurídico entre los Estados miembros han obstaculizado el cumplimiento de la ley, lo cual puede haber provocado la pérdida de pistas de investigación y afectado al enjuiciamiento efectivo de la actividad delictiva en línea[57].

Fuente: Tribunal de Cuentas Europeo.

35 La aplicación de algunos aspectos de la legislación sigue siendo voluntario tanto para las autoridades nacionales como para los operadores privados. Por ejemplo, en el marco del Grupo de cooperación, la evaluación de las estrategias nacionales sobre seguridad de las redes y los sistemas de información y la eficacia de los CSIRT es voluntaria. Asimismo, con arreglo al régimen de certificación propuesto en el Reglamento de Ciberseguridad, la aplicación de la certificación para los productos y servicios de TIC será voluntaria.

36 Aunque la ciberseguridad sea una prerrogativa de los Estados miembros en la UE, esta desempeña una función esencial en la creación de las condiciones para que mejoren las capacidades de sus Estados miembros y trabajen conjuntamente y generen confianza. Teniendo en cuenta las enormes diferencias entre los Estados miembros en términos de capacidad y compromiso[58], el suministro de información delicada para la seguridad nacional seguirá siendo voluntario.

37 El hecho de que la transposición de la legislación de la UE no sea sistemática en todos los Estados miembros puede dar lugar a incoherencias jurídicas y operativas, además de limitar su potencial. Por ejemplo, los Estados miembros entienden de manera diferente cómo han de aplicarse los controles de las exportaciones de productos de doble uso[59], por lo que es posible que algunas empresas ubicadas en la UE exporten tecnologías y servicios que se pueden utilizar para cibervigilancia y violaciones de los derechos humanos mediante la censura o la interceptación. El Parlamento Europeo ha manifestado su preocupación al respecto[60].

38 Por otro lado, la protección de la privacidad y la libertad de expresión requieren una respuesta legislativa adaptada para mantener el justo equilibrio entre la protección de los valores fundamentales y el respeto de las exigencias de seguridad de la UE. Por ejemplo, ¿cómo se puede garantizar el cifrado de extremo a extremo favoreciendo al mismo tiempo la aplicación de la ley? O ¿cómo cumplir los objetivos del Reglamento general de protección de datos sabiendo cómo repercute en la información pública sobre los titulares de nombres de dominio y los propietarios de bloques de direcciones IP? Y ¿cómo puede esto afectar negativamente a las investigaciones policiales[61]?

39 La legislación por sí sola no garantiza la resiliencia. Aunque el objetivo de la Directiva SRI sea alcanzar un elevado nivel de seguridad en toda la UE, se centra explícitamente en lograr la mínima, que no la máxima, armonización[62]. Con la evolución del panorama cibernético seguirán apareciendo lagunas.

Puntos de reflexión — Marco político

- ¿Qué medidas esenciales hay que tomar para lograr que responsables políticos y legisladores por igual adopten una cultura más sólida, basada en los resultados, con respeto a la ciberseguridad y la definición de la resiliencia general?

- ¿Cómo puede mejorar la investigación su contribución a la generación de los datos y las estadísticas necesarios para permitir una evaluación significativa?

- ¿Cómo pueden adaptarse los procesos legislativos de la UE para que sean más flexibles y tengan más en cuenta la rapidez de los avances tecnológicos y de las amenazas?

- ¿Cómo se puede lograr que el proceso de desarrollo de parámetros (indicadores, objetivos, etc.) del ciclo de actuación de la UE se adapte y se amplíe al ámbito de la ciberseguridad en su conjunto y se reproduzca en este?

- ¿Qué pueden aprender las oficinas nacionales de auditoría de sus respectivos enfoques sobre la auditoría de las medidas y las políticas de ciberseguridad?

- ¿Qué incoherencias en la transposición y aplicación del marco jurídico de la UE restan eficacia a la respuesta frente a las carencias en ciberseguridad y frente a la ciberdelincuencia, y cómo podrían encontrar los Estados miembros y las instituciones de la UE mejores maneras de solucionarlas?

- ¿Qué eficacia tienen los controles de la UE a las exportaciones de bienes y servicios cibernéticos en la prevención de violaciones de los derechos humanos fuera de la UE?

Financiación y gasto

40 El objetivo de la UE es convertirse en el entorno en línea más seguro del mundo. Lograrlo requiere esfuerzos significativos por parte de todas las partes interesadas, así como una base financiera sólida y bien gestionada.

Desafío 3: Adecuar los niveles de inversión a los objetivos

Aumentar la inversión

41 Se estima que el gasto total en ciberseguridad en todo el mundo asciende al 0,1 % del PIB. En los Estados Unidos[63], este porcentaje representa aproximadamente el 0,35 % (con inclusión del sector privado). El gasto presupuestado para 2019 del Gobierno federal de los Estados Unidos supone aproximadamente el 0,1 % del PIB, aproximadamente 21 000 millones de dólares estadounidenses[64].

42 En comparación, el gasto en la UE ha sido reducido, ha estado fragmentado y a menudo no se ha visto respaldado por programas promovidos por el Estado. Es difícil encontrar cifras, pero se estima que el gasto público de la UE en ciberseguridad oscila entre uno y dos millones de euros al año[65]. El gasto de algunos Estados miembros en porcentaje del PIB supone la décima parte de los niveles de los Estados Unidos, o incluso menos[66]. La UE y sus Estados miembros necesitan saber a cuánto ascienden todas sus inversiones para determinar los déficits que deben colmar.

43 Es difícil componer una imagen exhaustiva sin contar con datos claros debido a la naturaleza transversal de la ciberseguridad y a que a menudo no se puede distinguir el gasto informático general del de ciberseguridad[67]. La encuesta del Tribunal ha confirmado que es difícil obtener estadísticas fiables sobre el gasto en los sectores público y privado. Tres cuartas partes de las oficinas nacionales de auditoría notificaron que no tenían una visión centralizada del gasto público relacionado con el ámbito cibernético, y en ningún Estado miembro era obligatorio para las entidades públicas notificar el gasto en ciberseguridad por separado en sus planes financieros.

44 Ampliar la inversión pública y privada en las empresas de ciberseguridad de Europa supone un desafío especial. A menudo se dispone de capital público para las fases iniciales, pero este se reduce para las fases de crecimiento y expansión[68]. Existen numerosas iniciativas de financiación de la UE, pero no se aprovechan debido, en gran medida, a la burocracia[69]. En general, las empresas especializadas en ciberseguridad de

la UE presentan peores resultados que sus homólogos internacionales: son menos numerosas y el importe medio de recursos que obtienen es significativamente más bajo[70]. Por tanto, es crucial garantizar la financiación y una orientación eficaz de las empresas emergentes para lograr los objetivos de las políticas digitales de la UE.

Incrementar el impacto

45 Es necesario que al colmar el déficit de inversión en el ámbito cibernético se obtengan resultados útiles. Por ejemplo, a pesar de la fortaleza del sector de la investigación y la innovación de la UE, los resultados no se patentando, comercializan o amplían lo suficiente como para reforzar la resiliencia, la competitividad y la autonomía digital[71], especialmente en comparación con los competidores mundiales de la UE. La escasez de resultados debidamente aprovechados se debe a varios factores[72], entre los que cabe citar:

- la falta de una estrategia transnacional coherente que amplíe el enfoque para ajustarse a las necesidades digitales más amplias de competitividad y mayor autonomía;
- la duración del ciclo de la cadena de valor, que implica que las herramientas se queden obsoletas rápidamente;
- la falta de sostenibilidad, puesto que los proyectos suelen terminar con la disolución del equipo del proyecto y con la suspensión de las ayudas, las actualizaciones y los parches.

46 La propuesta de la Comisión de establecer una red de centros de competencia en ciberseguridad y un centro de competencia de investigación es un intento de superar la fragmentación en el ámbito de la investigación en ciberseguridad, así como de estimular la inversión a gran escala[73]. En total, hay unos 665 centros especializados en la UE.

Desafío 4: Una visión clara del gasto presupuestario de la UE

47 Es importante tener una visión centralizada del gasto por motivos de transparencia y para mejorar la coordinación. De lo contrario, los responsables políticos difícilmente pueden comprender cómo se ajusta el gasto a las necesidades para cumplir los objetivos prioritarios.

48 No hay fondos presupuestarios específicos para financiar la estrategia de ciberseguridad. A escala de la UE, el gasto en ciberseguridad procede, en cambio, del presupuesto general de la UE y de la cofinanciación de los Estados miembros. En su análisis, el Tribunal halló una compleja estructura de al menos diez instrumentos distintos dentro del presupuesto general de la UE, pero no encontró una descripción clara de la cuantía ni del destino de los fondos (véase el ***anexo II***).

49 Trazar un esquema claro de los gastos en una materia que afecta a muchos ámbitos políticos constituye todo un desafío. Los programas de gasto son gestionados por distintos servicios de la Comisión que tienen sus propios objetivos, normas y calendarios. El panorama se complica más aún cuando se incorpora la cofinanciación de los Estados miembros, como sucede con el Fondo de Seguridad Interior (Policía)[74].

Gasto identificable en ciberseguridad

50 En el período 2014 – 2018, la Comisión gastó al menos 1 400 millones de euros en la aplicación de la Estrategia[75],y destinó la mayor parte a Horizonte 2020[76]. La financiación de Horizonte 2020 se canaliza principalmente a través del reto «Sociedades seguras» y del objetivo específico «Liderazgo en las tecnologías industriales y de capacitación»[77]. El Tribunal identificó 279 proyectos contratados relacionados con la ciberseguridad hasta septiembre de 2018, con una financiación total de la UE de 786 millones de euros[78]. En la ***ilustración 5*** se muestra la tipología de estos proyectos a partir de este análisis.

Ilustración 5 – Proyectos contratados de investigación en ciberseguridad de Horizonte 2020 (millones de euros)

Fuente: Tribunal de Cuentas Europeo.

51 En 2016 se creó una asociación público-privada contractual para incentivar la industria europea de ciberseguridad. El objetivo era canalizar 450 millones de euros del programa Horizonte 2020 a la asociación público-privada contractual y atraer 1 800 millones de euros adicionales del sector privado para 2020. En el período de 18 meses transcurrido hasta el 31 de diciembre de 2017, se canalizaron 67,5 millones de euros de Horizonte 2020 a la asociación público-privada contractual, y el sector privado invirtió 1 000 millones de euros[79].

52 La lucha contra la ciberdelincuencia recibe apoyo también del Fondo de Seguridad Interior – Policía (FSI-Policía), que financia estudios, reuniones de expertos y actividades de comunicación que ascendieron a cerca de 62 millones de euros entre 2014 y 2017. Los Estados miembros también pueden recibir subvenciones para equipos, formación, investigación y recogida de datos en régimen de gestión compartida. Diecinueve Estados miembros han recibido estas subvenciones por valor de 42 millones de euros.

53 Los fondos destinados a la cooperación judicial y al funcionamiento de los tratados de asistencia jurídica mutua, y especialmente al intercambio de datos

electrónicos e información financiera, ascendieron a 9 millones de euros en el marco del programa Justicia gestionado por la DG Justicia y Consumidores.

54 La Directiva SRI prevé explícitamente que los CSIRT deben disponer de recursos adecuados para desempeñar eficazmente sus funciones[80]. Entre 2016 y 2018, había 13 millones de euros disponibles anualmente del Mecanismo «Conectar Europa», que los Estados miembros podían solicitar como ayuda para aplicar los requisitos de la Directiva. No se ha realizado ningún estudio para determinar cuáles son las necesidades financieras reales para que la red de los CSIRT y el Grupo de cooperación surtan efecto.

55 Varios de los costes operativos de las agencias se han destinado específicamente a actividades relacionadas con la ciberdelincuencia o la ciberseguridad. Sin embargo, es difícil extraer cifras exactas a partir de la información pública disponible.

56 El Convenio de Budapest (véase el apartado ***11***) ha representado el pilar del gasto externo de la UE en relación con el ámbito cibernético. La UE gastó aproximadamente 50 millones de euros en reforzar la ciberseguridad más allá de sus fronteras en el período 2014-2018. Prácticamente la mitad de este gasto se realizó a través del Instrumento en pro de la Estabilidad y la Paz, con un proyecto principal (GLACY+, de 13,5 millones de euros) destinado a reforzar las capacidades en todo el mundo para desarrollar y aplicar legislación en materia de ciberdelincuencia y aumentar la cooperación internacional[81]. Por otro lado, el gasto de otros instrumentos financieros de la UE se centró en gran medida en los Balcanes Occidentales[82], así como en la vecindad europea: por ejemplo, el proyecto Cybercrime@EaP con los países de la Asociación Oriental se destina a mejorar la cooperación internacional sobre la ciberdelincuencia y las pruebas electrónicas.

Otros gastos en ciberseguridad

57 No siempre es posible identificar el gasto específico de ciberseguridad dentro de los programas de la UE:

- La financiación de Horizonte 2020 se ha canalizado también a través de la Empresa Común Componentes y Sistemas Electrónicos para el Liderazgo Europeo (ECSEL) para los sistemas ciberfísicos. Sin embargo, el Tribunal no ha podido determinar qué se destinaba específicamente a la ciberseguridad en los 27 proyectos por un valor total de 437 millones de euros entre 2015 y 2016.

- Los Fondos Estructurales y de Inversión Europeos han puesto a disposición hasta 400 millones de euros para gastos en ciberseguridad y servicios de confianza. Esto abarca las inversiones en seguridad y protección de datos para mejorar la interoperabilidad y la interconexión de las infraestructuras digitales, la identificación electrónica y los servicios de confianza y privacidad.

58 En su plan de operaciones de 2018, el Banco Europeo de Inversiones ha anunciado su intención de aumentar la financiación de la tecnología de doble uso, la ciberseguridad y la seguridad civil hasta 6 000 millones de euros en un plazo de tres años[83].

Perspectivas de futuro

59 El componente de ciberseguridad de 2 000 millones de euros del nuevo programa Europa Digital[84] (PED) propuesto para el período 2021-2027 está concebido para reforzar la industria de ciberseguridad de la UE y la protección social general, ayudando también a aplicar la Directiva SRI. Se espera que la red de centros de competencia en ciberseguridad y un centro de competencia de investigación que se ha propuesto, cuyo objeto es racionalizar el enfoque, conforme el mecanismo de aplicación principal para el gasto de la UE en el marco del PED.

60 El gasto en defensa del presupuesto de la UE ha aumentado recientemente a través del Programa Europeo de Desarrollo Industrial en materia de Defensa, y en 2019 y 2020 se asignarán 500 millones de euros[85]. Se centrará en mejorar la coordinación y la eficacia del gasto en defensa de los Estados miembros a través de incentivos para el desarrollo conjunto. Su objetivo es generar un total de 13 000 millones de euros de inversión en capacidades de defensa, entre las que se cuenta la ciberdefensa, a partir de 2020 a través del Fondo Europeo de Defensa[86].

Desafío 5: Dotar de recursos suficientes a las agencias de la UE

61 Los tres organismos esenciales de la política de ciberseguridad de la UE – ENISA, el EC3 de Europol y CERT-UE (véase el ***recuadro 2***) —afrontan dificultades para obtener recursos en un momento en el que las prioridades políticas se centran cada vez en la seguridad. La actual asignación de recursos humanos y financieros en las agencias de la UE sigue siendo un desafío que deben superar para satisfacer las expectativas[87].

62 No se han satisfecho plenamente las solicitudes de recursos adicionales de las agencias para poder atender la creciente demanda, lo que podría poner en peligro el cumplimiento (oportuno) de los objetivos de las políticas. Por ejemplo:

- La limitación de recursos contribuyó a impedir que ENISA cumpliera plenamente sus objetivos en 2017[88]. En el paquete de 2017 se propusieron recursos adicionales adecuados al nuevo mandato de ENISA.

- El suministro de analistas y la inversión en capacidades TIC en el Centro Europeo de Ciberdelincuencia de Europol no han evolucionado al mismo ritmo que la demanda[89]. Asimismo, el personal del Grupo especial conjunto de acción contra los delitos cibernéticos (J-CAT) de la Comisión Europea está compuesto por expertos de los Estados miembros y de terceros países que prestan apoyo a las investigaciones basadas en la inteligencia, pero los correspondientes costes son asumidos en gran medida por los países emisores, lo que desincentiva la movilización de un mayor número de expertos. Se ha desarrollado una movilización temporal, caso por caso, financiada parcialmente por Europol o por el ciclo de actuación de la UE para permitir la participación de más países.

63 Algunas limitaciones son autoinfligidas. Buena parte del personal de CERT-UE y ENISA son agentes contractuales, cuyos procedimientos de selección suelen ser lentos. Otras, como la atracción y retención de talento, surgen de la incapacidad de las agencias para competir con los salarios del sector privado o por las malas perspectivas de evolución de la carrera profesional. Por tanto, entre 2014 y 2016, ENISA subcontrató buena parte de su trabajo[90].

64 Los recortes de personal y herramientas necesarias pueden implicar riesgos significativos, especialmente para la recopilación de información sobre amenazas. El volumen de datos de fuentes abiertas y cerradas sigue aumentando y los riesgos superan la capacidad de los analistas de realizar análisis adecuados de las amenazas. Si no se cuenta con las capacidades y herramientas adecuadas para integrar e interconectar satisfactoriamente estos datos, no se logrará obtener de ellos información útil sobre amenazas que se pueda compartir y analizar en toda la UE[91].

Puntos de reflexión – Financiación y gasto

- ¿Qué pueden hacer la Comisión y los legisladores para racionalizar el gasto en ciberseguridad de la UE y, más concretamente, adaptarlo a objetivos claramente definidos?
- ¿Cómo se pueden corregir globalmente las carencias de recursos de las agencias de la UE teniendo en cuenta las necesidades y objetivos de la Unión?
- ¿Qué medidas se aplican en la UE y los Estados miembros para reducir los obstáculos que impiden a las pymes acceder a capital de inversión para expandir sus actividades?
- ¿Qué resultados concretos y duraderos se obtienen con los fondos de Horizonte 2020 en la búsqueda de soluciones de ciberseguridad?
- ¿Cómo refuerzan los ejercicios de desarrollo de capacidades de la UE las capacidades de países terceros de acuerdo con los valores de la UE?

Consolidación de una cultura ciberresiliente

65 La gobernanza de la ciberseguridad consiste en la gestión de las amenazas y los riesgos, el refuerzo de las capacidades y la sensibilización, y la coordinación y el intercambio de información en un clima de confianza.

Desafío 6: Reforzar la gobernanza y las normas

Gobernanza de la seguridad de la información

66 La gobernanza de la seguridad de la información consiste en la creación de estructuras y políticas para garantizar la confidencialidad, integridad y disponibilidad de los datos. Es más que una mera cuestión técnica, por lo que exige un liderazgo efectivo, procesos sólidos, y estrategias en consonancia con los objetivos de la organización[92]. Dentro de esta gobernanza, a modo de subconjunto, la gobernanza de la ciberseguridad se ocupa de las amenazas cibernéticas de todo tipo, tales como ataques avanzados selectivos, infracciones o incidentes difíciles de detectar o de gestionar.

67 Los modelos de gobernanza de la ciberseguridad difieren entre los Estados miembros, y dentro de estos, las competencias en materia de ciberseguridad a menudo se reparten entre numerosas entidades. Estas diferencias podrían obstruir la cooperación necesaria para responder a incidentes transfronterizos de gran envergadura y el intercambio de conocimientos en el ámbito nacional, y, sobre todo, en el ámbito de la UE. Según la encuesta realizada por el Tribunal a las oficinas nacionales de auditoría, estas consideran que los mayores riesgos radican en las insuficiencias de las disposiciones adoptadas por los poderes públicos en materia de gobernanza y gestión del riesgo.

68 Pese a las graves consecuencias que pueden acarrear a las organizaciones del sector privado, las deficiencias en materia de cibergobernanza son muy frecuentes. Prácticamente nueve de cada diez organizaciones afirman que su función de ciberseguridad no cubre completamente sus necesidades[93], y los encargados de la ciberseguridad suelen estar por lo menos dos niveles por debajo del consejo de administración[94].

69 Las Directivas sobre Derecho de sociedades de la UE no establecen requisitos específicos sobre la divulgación de los riesgos cibernéticos. En los Estados Unidos, la Securities and Exchange Commission (comisión de valores y bolsa) ha publicado recientemente orientaciones no vinculantes para ayudar a las empresas públicas en la preparación de información sobre los riesgos en materia de ciberseguridad e incidentes[95]. El Comité Mixto de las Autoridades Europeas de Supervisión (AES)[96] advirtió del aumento de los riesgos cibernéticos e instó a las entidades financieras a mejorar los frágiles sistemas informáticos y a estudiar los riesgos inherentes para la seguridad de la información, la conectividad y la externalización[97].

70 Reforzar la gobernanza de la seguridad de la información de las pymes es especialmente difícil, ya que, con frecuencia, no pueden aplicar los sistemas adecuados. Las pymes no cuentan con directrices adecuadas sobre la aplicación de los requisitos de seguridad de la información y de privacidad y sobre la mitigación de los riesgos tecnológicos[98]. Los principales retos son, por tanto, comprender mejor sus necesidades y ofrecer los incentivos y el apoyo necesarios.

71 La falta de un marco de gobernanza coherente e internacional en materia de ciberseguridad reduce la capacidad de la comunidad internacional para responder a los ciberataques y limitarlos. Por lo tanto, es importante llegar a un consenso sobre el marco de gobernanza que mejor refleje los intereses y los valores de la UE[99]. Los intentos de establecer normas internacionales vinculantes para el ciberespacio resultan cada vez más difíciles, como se ha visto en la falta de consenso en el grupo de expertos gubernamentales de la ONU en 2017 sobre cómo debe aplicarse el Derecho internacional a las respuestas a los incidentes.

72 Para reforzar su programa en materia de gobernanza del ciberespacio, la UE también ha formalizado seis ciberasociaciones para establecer diálogos políticos periódicos destinados a consolidar confianza y ámbitos comunes de cooperación[100]. Los resultados son variables, pero, en general, en el ámbito internacional, la UE todavía no es considerada como un agente de ciberseguridad importante, aunque ha reforzado su imagen[101].

La seguridad de la información en las instituciones de la UE

73 Cada institución de la UE tiene sus propias normas de gobernanza sobre seguridad de la información. En un acuerdo interinstitucional se establece que la Comisión prestará asistencia a otras instituciones y agencias en materia de seguridad de la información. Las instituciones y los organismos de la Unión han reconocido la

necesidad de desarrollar sus cibercapacidades y sus enfoques de gestión de riesgo de manera coherente. La Comisión, el Consejo y el SEAE presentarán un informe en 2020 al Grupo Horizontal «Cuestiones Cibernéticas» sobre la gobernanza y los avances logrados en la clarificación y armonización de la gobernanza de la ciberseguridad en las instituciones y agencias de la UE[102].

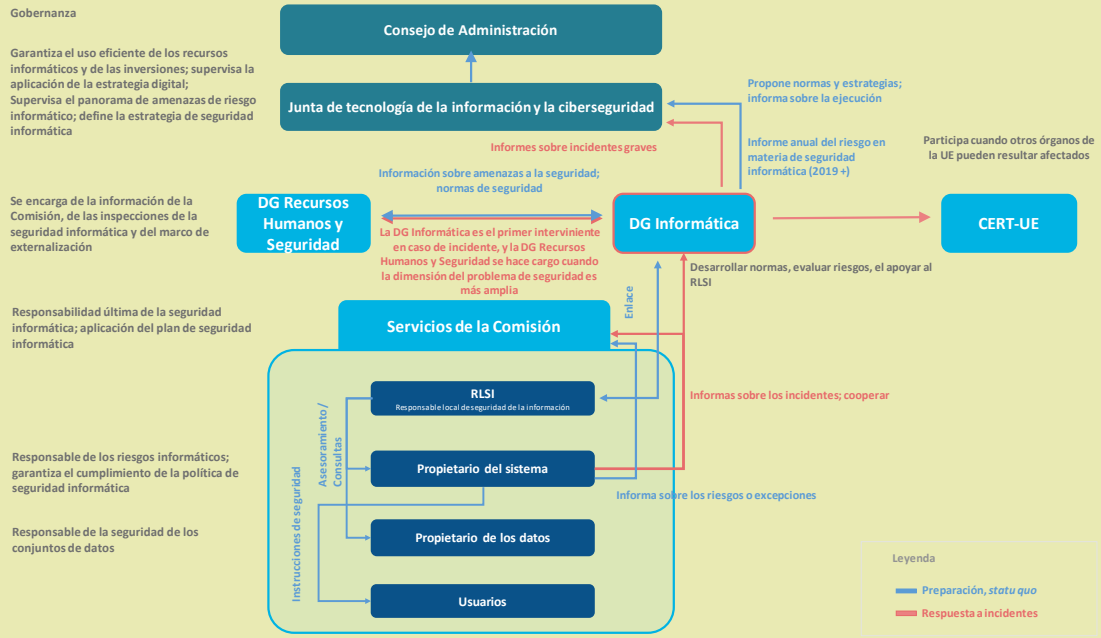
74 Dentro de la Comisión, la Dirección General de Informática (DG Informática) es responsable de la seguridad de la infraestructura y los servicios informáticos (véase el ***recuadro 3***). Los principales objetivos en materia de seguridad informática de la estrategia digital de la Comisión son: la integración de la seguridad informática en los procesos de gestión, el suministro de infraestructura y resiliencia eficaz (y rentable), la ampliación del alcance de la detección de incidentes y de la respuesta, y la integración de la gobernanza de la informática y de la seguridad[103]. La Comisión, en el marco de su contrato de prestación, garantiza el mantenimiento activo de casi todos los programas informáticos y que únicamente se utilicen programas informáticos que cuenten con servicio posventa del proveedor[104].

75 La importancia de la protección de las instituciones también afecta a las misiones y operaciones de la PCSD con que cuenta la UE en todo el mundo. Una de las prioridades del marco político de ciberdefensa de la UE (actualización de 2018) es mejorar la protección de los sistemas de información y comunicación de la CSDP utilizados por las entidades de la UE. Ya se ha creado la Junta de Cibergobernanza del SEAE, que se reunió por primera vez en junio de 2017[105].

Recuadro 3

Protección de los sistemas de información de la Comisión

Los aproximadamente 1 300 sistemas y 50 000 dispositivos con que cuenta la Comisión son blanco continuo de ciberataques. Las competencias en materia de informática están descentralizadas, como se muestra a continuación en el gráfico. La información y la seguridad informática se basan en un plan de seguridad informática establecido por la DG Informática. El Information Technology and Cybersecurity Board (consejo de tecnologías de la información y ciberseguridad) actúa de facto como responsable principal de Seguridad de los Sistemas de Información y constituye el vínculo entre la vertiente operativa de la seguridad informática y la alta dirección de la Comisión, representada por el Consejo de Administración.



Fuente: Tribunal de Cuentas Europeo, a partir de Decisiones de la Comisión[106].

El principal cometido de la DG Recursos Humanos y Seguridad es brindar protección a los agentes, la información y los activos de la Comisión. También realiza investigaciones de seguridad sobre incidentes con una dimensión de seguridad superior a la de las tecnologías de información por sí solas, contribuyendo así a sus actividades de contrainteligencia y de lucha contra el terrorismo.

La DG Informática es responsable de la seguridad y alberga el CERT-UE (Equipo de Respuesta a Emergencias Informáticas). Creado en 2011, el CERT-UE funciona con un presupuesto anual de unos 2,5 millones de euros y cuenta aproximadamente con 30 empleados. Es el primer interviniente en cualquier incidente de seguridad de la información que afecte a varias instituciones, aunque todavía no funciona permanentemente. Alberga una plataforma de intercambio de información. En 2018, el CERT-UE firmó un memorando de entendimiento no vinculante con ENISA, el EC3 y la Agencia Europea de Defensa para reforzar la cooperación y la coordinación. Tiene además un acuerdo técnico con el equipo de capacidad de respuesta ante incidentes informáticos de la OTAN (NCIRC).

Evaluación de amenazas y riesgos

76 Las evaluaciones de amenazas y riesgos continuas y bien fundadas constituyen herramientas importantes para las organizaciones públicas y privadas por igual. Sin embargo, no hay un planteamiento común para clasificar y cartografiar las amenazas cibernéticas o para realizar evaluaciones de riesgos, ya que el contenido de las evaluaciones varía considerablemente, lo cual dificulta la aplicación de un enfoque coherente a la ciberseguridad en el ámbito de la UE[107]. Por otra parte, suelen basarse en las mismas fuentes, o incluso otras evaluaciones de amenazas, lo que se traduce en

una caja de resonancia que repite las conclusiones[108], con el consiguiente riesgo de no prestar suficiente atención a otras amenazas. Esta situación se agrava por la continua reticencia a compartir información y a la notificación incompleta de los incidentes.

77 La Célula de Fusión de la UE contra las Amenazas Híbridas[109], integrada en el SEAE, fue creada con el fin de mejorar la conciencia situacional y prestar apoyo en la toma de decisiones mediante el intercambio de análisis, pero necesita ampliar sus conocimientos especializados, en particular sobre ciberseguridad. Paralelamente, el CERT-UE aporta a las instituciones, los órganos y los organismos de la Unión Europea informes y sesiones informativas sobre las amenazas cibernéticas dirigidas contra ellos.

78 ENISA ya ha constatado anteriormente que muchos Estados miembros tienen una comprensión cualitativa de las amenazas, y que es necesario realizar una mayor modelización de las ciberamenazas[110]. Una capacidad de supervisión que facilite el análisis estratégico reforzará la comprensión global. No obstante, las evaluaciones de las amenazas podrían abarcar no solo las amenazas tecnológicas, sino también las económicas y sociopolíticas para garantizar una visión más global de la amenaza y de los motivos sus impulsores y de sus agentes.

Incentivos

79 Todavía existen muy pocos incentivos legales y económicos para que las organizaciones notifiquen y compartan información sobre los incidentes. Por temor a dañar su reputación, muchas organizaciones todavía prefieren tratar los ciberataques con toda discreción o pagar a los autores. Aún está por ver la eficacia de la Directiva sobre ciberseguridad para elevar el nivel de notificaciones de incidentes. La Comisión espera que las mejoras se materialicen principalmente en el ámbito nacional, pero el Reglamento de Ciberseguridad aportará una dimensión para toda la UE[111].

80 Incorporando ciertas normas en las adjudicaciones, los poderes públicos ejercen una influencia significativa en los proveedores como compradores de productos y servicios digitales mediante la contratación pública y la financiación de investigación y programas (por ejemplo, exigiendo la adopción de algunas normas técnicas como el Protocolo Internet IPv6 para contribuir a la lucha contra la ciberdelincuencia), aunque actualmente no exista un marco de contratación conjunta para la infraestructuras de ciberseguridad[112]. La Comisión puede hacer mucho en este sentido. La propuesta de programa Europa Digital para el próximo marco financiero plurianual tiene por objeto mejorar la hasta ahora limitada inversión del sector público en la compra de las últimas tecnologías de ciberseguridad.

81 Gracias a su capacidad reguladora, la Comisión garantiza el desarrollo de normas adecuadas cuya adopción general permita mejorar la seguridad. La Comisión y Europol trabajan con organismos de gobernanza de Internet como ICANN (véase el apartado ***38***) y RIPE-NCC[113], lo cual es esencial para establecer la estructura adecuada de lucha contra la ciberdelincuencia para apoyar a las autoridades judiciales y respaldar la aplicación de la Ley.

Desafío 7: Potenciar la capacidad y la concienciación

82 ENISA ha señalado que los usuarios desempeñan un papel fundamental en la lucha contra los ciberataques y que el refuerzo de la capacidad, la educación y la concienciación es fundamental para construir una sociedad ciberresiliente[114]. Tanto en el entorno laboral como en el doméstico, las personas preparadas para detectar señales de alerta y conocedoras de las técnicas adecuadas pueden frenar o prevenir los ataques.

83 Un motivo de especial preocupación es la creciente desproporción entre los conocimientos técnicos necesarios para cometer un acto de ciberdelincuencia o lanzar un ciberataque, y las competencias necesarias para defenderse de él. El modelo del «delito como servicio» ha eliminado barreras de entrada al mercado de la ciberdelincuencia: personas sin conocimientos técnicos para construirlos pueden ahora alquilar redes infectadas, o explotar equipos o programas de secuestro.

Formación, competencias y desarrollo de capacidades

84 El mundo se enfrenta a un creciente déficit de competencias en ciberseguridad: el déficit de mano de obra ha aumentado en un 20 % desde 2015[115]. Los canales tradicionales de contratación no alcanzan a satisfacer la demanda de personal cualificado ni a cubrir los puestos interdisciplinares y de gestión[116]. Casi el 90 % de las personas que trabajan en ciberseguridad son hombres: esta persistente falta de diversidad de género limita aún más la reserva de talento[117]. Por otra parte, en las universidades, las materias relacionadas con la cibernética apenas se estudian en los programas que no son de carácter técnico.

85 La educación y la formación en materia cibernética son necesarias en todos los ámbitos: funcionarios, agentes de los cuerpos de seguridad, autoridades judiciales, fuerzas armadas y educadores. Por ejemplo, es necesario que los tribunales judiciales puedan hacer frente a la rápida evolución de las especificidades técnicas de la

ciberdelincuencia y de sus víctimas[118], pero actualmente no existen una normativa europea de formación y certificación[119]. Es importante que las instituciones de la UE posean la combinación de capacidades adecuada, ya que, si no cuentan con los conocimientos y las competencias adecuados, quizás no sean capaces de definir correctamente el alcance de los problemas, ni de determinar cuáles son los socios y las prestaciones de seguridad que necesitan, ni de gestionar programas. Esto también restaría eficacia al desarrollo de programas o políticas por parte de la UE.

86 Aunque los Estados miembros son responsables de las políticas de educación de la UE, ya se están llevando a cabo numerosas actividades (véase el ***cuadro 2***) y ejercicios (véase el ***recuadro 4***) formativos. La UE puede contribuir a la introducción de normas europeas en los programas lectivos de todas las disciplinas pertinentes[120]. En el ámbito de la informática forense, por ejemplo, se necesitan normas comunes de formación para facilitar la admisibilidad de pruebas en los Estados miembros. Debido a su naturaleza transfronteriza, la ciberdelincuencia implica a múltiples jurisdicciones, lo cual requiere una formación a escala de la UE. Sin embargo, la CEPOL, agencia europea para la formación policial, ha observado que más de dos terceras partes de los Estados miembros no proporcionan periódicamente formación en cuestiones cibernéticas a los funcionarios policiales[121]. La UE también puede buscar sinergias educativas y formativas entre los ámbitos civil y militar[122]. Dicho esto, en ENISA se ha constatado que las oportunidades de formación existentes en sectores críticos son amplias, pero que no se orientan suficientemente a la resiliencia de las infraestructuras críticas[123].

Cuadro 2 – Algunas las iniciativas de la UE de formación cibernética

Proyectos de la Agencia Europea de Defensa, como, por ejemplo, ejercicios en ciberdefensa por el sector privado y el proyecto sobre ciberrangos.	Red de la Escuela Europea de Seguridad y Defensa (que ofrece formación civil y militar), y plataforma de educación, formación, evaluación y ejercicio en materia de cibernética.	Formación de ENISA, que ofrece programas de formación cuando el mercado comercial no los puede facilitar.
Programas de formación de la Europol, la CEPOL, ECTEG[124], incluido el curso «Training Governance Model and Training Competency Framework» (con certificación).	Red de centros de competencia y centro de competencia y de investigación (propuesta)	Medidas sobre cifrado propuestas en el undécimo informe de situación relativo a una Unión de la Seguridad.
Cooperación entre la UE y la OTAN sobre ciberdefensa, formación y educación.	Programa «Erasmus militar».	Red Europea de Formación Judicial.

Fuente: Tribunal de Cuentas Europeo.

87 La Unión Europea ha destinado a una serie expertos en seguridad y lucha contra el terrorismo a diecisiete delegaciones de la UE para reforzar el vínculo entre la

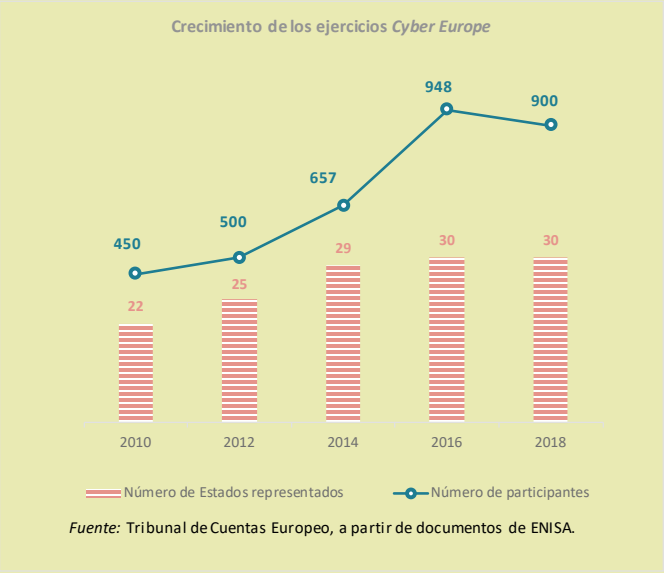
seguridad interior y exterior de la UE[125]. Pese a las limitaciones de recursos, con mayores conocimientos especializados en cibernética podrían ponerse en marcha proyectos adecuados, y encontrar sinergias con otros programas o fuentes de financiación[126]. También mejoraría la visibilidad de la ciberseguridad en el diálogo político, pese a competir con muchas otras prioridades, como la migración, la delincuencia organizada o los combatientes extranjeros que regresan.

Recuadro 4

Ejercicios

Los ejercicios son aspectos importantes de la educación y la formación cibernéticas, porque brindan oportunidades excelentes de impulsar la preparación poniendo a prueba las capacidades, ofreciendo respuestas a situaciones reales y estableciendo relaciones de trabajo en red. Desde 2010, se realizan con mucha mayor frecuencia.

Los participantes intervienen *in situ* o a distancia. Hay evaluaciones posteriores a los ejercicios para determinar las lecciones aprendidas, aunque estas no se transmitan plenamente entre los estratos estratégico/político, operativo y técnico[127].



Fuente: Tribunal de Cuentas Europeo, a partir de documentos de ENISA.

Las maniobras emblemáticas de ciberdefensa de la UE y la OTAN —ejercicios bienales *Cyber Europe* (operativos) y anuales *Locked Shields* (técnicos)— reúnen a más de mil participantes procedentes de unos treinta Estados. Ambos ejercicios consisten en la protección y el mantenimiento de infraestructuras críticas en situaciones simuladas de ataque. Estos ejercicios han adquirido mucha más profundidad, y ambos cuentan ahora con elementos de los medios de comunicación y de la política jurídica y financiera para que las personas que practican tengan un mejor conocimiento de la situación. La ejercicios paralelos y coordinados de la APCE (estratégicos) ponen a prueba la interacción UE-OTAN en un escenario de crisis híbrida.

Estos no son los únicos ejercicios internacionales. ENISA organiza un reto cibernético anual en el que varios equipos compiten para solucionar problemas de seguridad tales como seguridad de aplicaciones web y móviles, rompecabezas criptográficos, ingeniería inversa, ética y ciencia forense. El primer ejercicio realizado en ministerios, EU CYBRID, tuvo lugar en septiembre de 2017, y se dedicó a la adopción de decisiones estratégicas. En 2018 se lanzó el ejercicio *Crossed Swords,* asociado a la OTAN, con el objetivo de mejorar los elementos ofensivos de su ejercicio *Locked Shields*. La OTAN también organiza los ejercicios *Cyber Coalition*.

Un reto clave es garantizar la participación activa de todas las partes interesadas importantes y la coordinación de todos los ejercicios para evitar duplicaciones y que las lecciones aprendidas puedan compartirse eficazmente.

Concienciación

88 Los ciudadanos suelen ser vectores de ataque y de propagación de desinformación, ya que, sin saberlo, están expuestos a las vulnerabilidades de dispositivos y programas informáticos baratos y ampliamente distribuidos distribución o son víctimas de la ingeniería social. La sensibilización es, por tanto, esencial para lograr una ciberresiliencia efectiva, pero no es en absoluto tarea fácil, ya que es difícil que personas sin conocimientos especializados comprendan la complejidad de la ciberseguridad y los riesgos que existen.

89 La campaña anual de sensibilización «*Mes Europeo de la Ciberseguridad*» y el «*Día por una Internet más segura*» constituyen ejemplos de concienciación. Actualmente, se han sumado al *Mes Europeo de la Ciberseguridad* siete países no pertenecientes a la UE[128]. La campaña *¡Di no!* de Europol tiene por objeto reducir el riesgo de extorsión y coacción sexual en línea de menores. Reducir el riesgo es importante porque pocas víctimas de ataques denuncian actualmente estos delitos a la policía[129]. La Comisión reconoce que la estrategia de ciberseguridad solo ha sido «parcialmente eficaz» para concienciar a los ciudadanos y las empresas[130]. Esto es debido a la magnitud de la tarea, la limitación de los recursos, el desigual compromiso de los Estados miembros, y la falta de pruebas científicas sobre la mejor manera de incrementar y medir la sensibilización.

90 La Comisión y las agencias pertinentes se enfrentan al desafío de garantizar que las medidas de sensibilización: están bien orientadas y publicitadas, son integradoras, se adaptan al panorama de las amenazas, evitan efectos indeseables como la «fatiga de seguridad»[131], y desarrollan métodos de evaluación e indicadores para evaluar su eficacia. Esto debe aplicarse en igual medida en las propias instituciones de la UE, que necesitan mejorar la cultura de sensibilización[132].

Desafío 8: Mejor intercambio de información y coordinación

91 La ciberseguridad requiere la cooperación entre los sectores público y privado, sobre todo en el intercambio de información y de buenas prácticas. La confianza es esencial en todos los niveles para crear el entorno adecuado para el intercambio de información delicada a través de las fronteras. La descoordinación conduce a la fragmentación, la duplicación de esfuerzos y la dispersión de competencias. Una coordinación eficaz puede traducirse en logros tangibles, como el cierre de mercados de la web oscura[133]. A pesar de los avances logrados en los últimos años, los niveles de

confianza siguen siendo «insuficientes»[134] en el ámbito de la UE y en algunos Estados miembros[135].

Coordinación entre las instituciones de la UE y con los Estados miembros

92 Uno de los objetivos de la estrategia de ciberseguridad y de las estructuras de cooperación establecidas por la Directiva SRI ha sido reforzar la confianza entre las partes interesadas. En la evaluación de la estrategia se reconocía que se habían sentado las bases para la cooperación estratégica y operativa en el ámbito de la UE[136]. A pesar de ello, la coordinación en general es «insuficiente»[137]. El reto radica en garantizar que el intercambio de información no solo sea significativo, sino que también ofrezca una visión global de la cuestión. Un factor importante en este sentido es alcanzar una visión común basada en una terminología aceptada (véase el ***recuadro 5***).

93 En su evaluación, ENISA señaló, no obstante, que el enfoque de la UE con respecto a la ciberseguridad no estaba suficientemente coordinado, con la consiguiente falta de sinergias entre las actividades de ENISA y las de otras partes interesadas. Los mecanismos de cooperación todavía son relativamente inmaduros[138]; la finalidad del Reglamento de Ciberseguridad es resolver este problema mediante el refuerzo de la función coordinadora de ENISA. La voluntad de mejorar la cooperación es la razón de ser del memorando de entendimiento firmado en 2018 entre la AED, ENISA, Europol EC3 y el CERT-UE[139]. Será prioritario para la Comisión en los próximos años garantizar la adecuada armonización entre las iniciativas políticas, las necesidades y programas de inversión a fin de superar la fragmentación y crear sinergias[140].

94 Las funciones de coordinación están integradas en diferentes organismos institucionales. El Grupo de Trabajo sobre la Unión de la Seguridad se creó para desempeñar un papel fundamental en la coordinación de las diferentes direcciones generales de la Comisión con el fin de apoyar el programa de actuación de la Unión de la Seguridad[141]. La DG Redes de Comunicación, Contenido y Tecnologías preside el subgrupo de trabajo sobre ciberseguridad.

95 En el Consejo, la ciberseguridad es gestionado por el Grupo Horizontal «Cuestiones Cibernéticas», que coordina cuestiones cibernéticas estratégicas y horizontales, y contribuye a la preparación de ejercicios y a la evaluación de sus resultados. La UE colabora estrechamente con el Comité Político y de Seguridad, que desempeña papel decisorio fundamental en las medidas diplomáticas de carácter cibernético (véase el ***recuadro 6*** del siguiente capítulo). Puesto que la ciberseguridad

es una cuestión transversal, la coordinación de todos los intereses pertinentes no es sencilla: recientemente se han dedicado a cuestiones cibernéticas más de veinticuatro grupos de trabajo y órganos preparatorios[142].

96 Las dos últimas propuestas legislativas sobre el refuerzo de ENISA y (2017) y el establecimiento de una red de centros de competencia en ciberseguridad y un centro de competencia en investigación (2018) tienen el objetivo específico de hacer frente a la fragmentación y a la duplicación de esfuerzos. Un factor determinante que inspiró la creación de la red de centros de competencia en materia de ciberseguridad y del centro de competencia en investigación ha sido la necesidad de colmar el vacío que la estructuras cooperativas de la Directiva SRI no llenaban al no estar concebidas para apoyar el desarrollo de soluciones «de vanguardia».

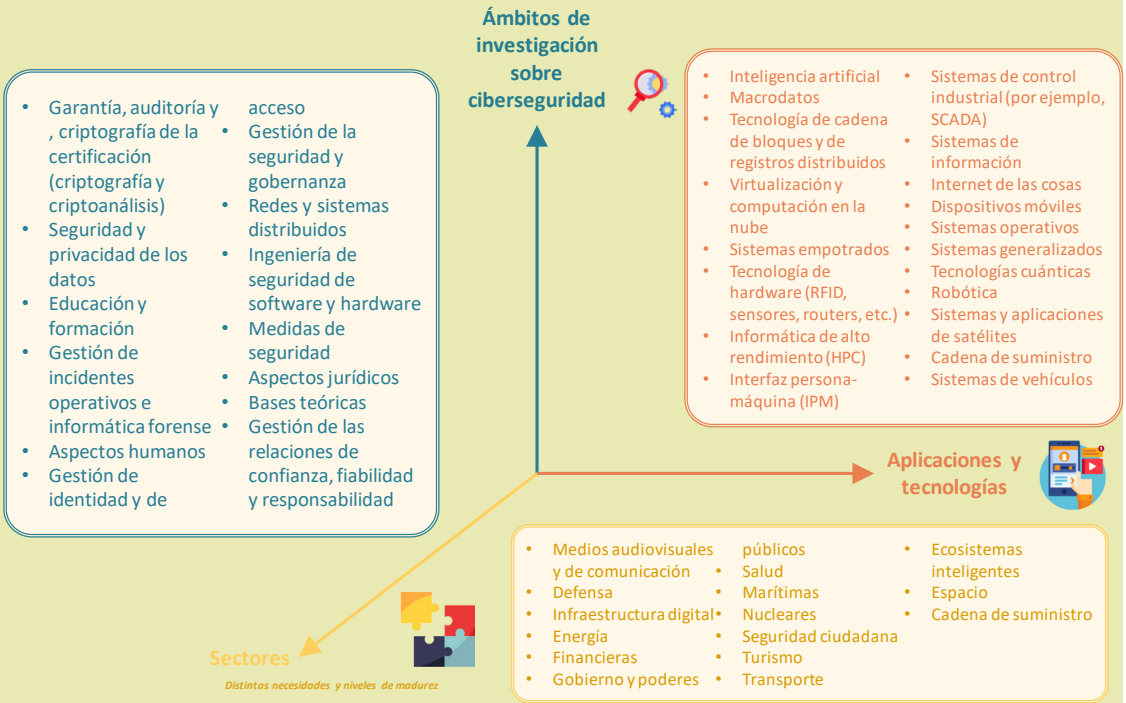
Recuadro 5

Un intento de hablar el mismo ciberlenguaje: coherencia tecnológica

La claridad terminológica mejora el conocimiento de la situación y la coordinación[143], y ayuda a establecer con precisión lo que constituye una amenaza y un riesgo.

El Centro Común de Investigación de la Comisión (CCI) ha desarrollado recientemente una taxonomía de la investigación revisada a partir de diferentes normas internacionales[144]. Su objetivo es servir de referencia para su uso como índice por las entidades de investigación en toda Europa.

Taxonomía de la ciberseguridad



Fuente: Tribunal de Cuentas Europeo, a partir de datos adaptados de la Comisión Europea.

Hasta hace poco, las instituciones y organismos de la UE no tenían definiciones comunes. Esta situación está cambiando. En el marco de su programa, el Grupo de cooperación elaboró una taxonomíade los incidentes con el objetivo de facilitar la colaboración transfronteriza eficaz.

La cooperación y el intercambio de información con el sector privado

97 La cooperación entre las autoridades públicas y el sector privado es fundamental para fortalecer el nivel global de ciberseguridad. No obstante, en su evaluación de 2017 sobre la estrategia de ciberseguridad, la Comisión llegó a la conclusión de que el intercambio de información entre partes interesadas privadas y los sectores público y privado aún no era óptimo debido a una falta de mecanismos de notificación e incentivos para compartir información[145], lo que dificulta la consecución de los objetivos estratégicos. La Comisión también ha constatado la ausencia de un mecanismo de colaboración eficiente que permita a los Estados miembros trabajar juntos para mejorar estratégicamente las capacidades industriales duraderas a escala[146].

98 Los centros de puesta en común y análisis de la información son organismos establecidos para suministrar plataformas y recursos que faciliten el intercambio de información entre los sectores público y privado, así como para recabar información sobre las amenazas cibernéticas. Su objetivo es generar confianza a través del intercambio de experiencias, conocimiento y análisis, especialmente sobre las causas profundas, incidentes y amenazas. Los centros de puesta en común y análisis de la información nacionales y sectoriales ya existen en muchos Estados miembros, pero en el ámbito europeo todavía son relativamente limitados[147]. No obstante, presentan una serie de problemas (limitación de recursos y dificultades para evaluar si sus resultados son satisfactorios, crear estructuras adecuadas, conseguir la participación de los sectores público y privado, y conseguir la participación de la policía) que deben resolverse para que puedan contribuir a la aplicación de la Directiva SRI y a la creación de capacidades de seguridad en el ámbito europeo[148].

99 En la lucha contra la ciberdelincuencia compleja, es particularmente importante una estrecha cooperación con el sector privado, pero su eficiencia es desigual según los Estados miembros y depende del nivel de confianza[149]. El Centro Europeo de Ciberdelincuencia de Europol, sin embargo, ha establecido una serie de grupos consultivos con operadores del sector privado, instituciones y organismos de la UE y otras organizaciones internacionales para mejorar la colaboración a través de redes de cooperación y del intercambio de información estratégica. Trabajan en planes adaptados a los objetivos del ciclo de actuación de la UE[150]. El abuso del cifrado es otro ámbito muy problemático que requiere una mayor cooperación con el sector privado. El Centro Europeo de Ciberdelincuencia de Europol está estudiando actualmente opciones de acogida a casos específicos el J-CAT anexos a corto plazo (véase el apartado ***62***) de expertos del sector privado y del mundo académico.

100 La falta de mecanismos de cooperación eficientes (públicos o privados) afecta a las comunidades civil y militar. Entre los ámbitos que plantean un reto común cabe citar la criptografía, los sistemas empotrados seguros, la detección de programas maliciosos, las técnicas de simulación, la protección de las redes y los sistemas de comunicación y la tecnología de la autenticación. El fomento de la cooperación civil-militar y el apoyo a la investigación y a la tecnología (en particular mediante el apoyo a las pymes) son dos de las prioridades del marco político de ciberdefensa de la UE actualizado (actualización de 2018).

Puntos de reflexión — Aumento de la resiliencia

- ¿Cómo puede alcanzarse un equilibrio adecuado entre la necesidad de integrar la política de ciberseguridad y garantizar una coordinación eficiente entre los distintos actores y la dispersión de responsabilidades?
- ¿Hasta qué punto están preparadas las instituciones y organismos de la UE para afrontar el próximo gran ataque que se lance directamente contra ellos?
- ¿Cómo conseguir que los organismos de la UE relacionados con la cibernética resulten más atractivos para captar talento?
- ¿Qué nuevas medidas son necesarias para garantizar que las instituciones y los organismos de la UE tengan la capacidad adecuada para contar con un marco coherente de evaluación de riesgos y amenazas?
- ¿Cómo afrontan las Autoridades Europeas de Supervisión (Autoridad Bancaria Europea, Autoridad Europea de Valores y Mercados y Autoridad Europea de Seguros y Pensiones de Jubilación) las vulnerabilidades de ciberseguridad inherentes al sector financiero, y qué lecciones pueden extraerse de ello en otros sectores?
- Dada la escasez generalizada de conocimientos especializados, ¿cómo pueden aprovecharse la asistencia técnica de la UE a las autoridades públicas para que tenga la mayor repercusión posible en la mejora de la resiliencia cibernética?
- ¿Cómo lograr la presencia significativa de la UE y de los Estados miembros en los debates internacionales para configurar la gobernanza y las normas del ciberespacio y fomentar los valores de la UE?
- ¿Qué medidas de sensibilización (y acciones preventivas) de la UE y de los Estados miembros logran realmente cambiar las cosas, y qué puede hacer la UE para potenciarlas?
- ¿Cómo contribuye la UE a la diversidad de género en el ámbito de la ciberseguridad?
- ¿Cómo pueden la UE y los Estados miembros reforzar las sinergias entre las comunidades civil y militar en el marco político de ciberdefensa (actualizado en 2018)?

Respuesta eficaz a los ciberincidentes

101 Diseñar una respuesta eficaz a los ciberataques es fundamental para atajarlos cuanto antes. Es especialmente importante que los sectores críticos, los Estados miembros y las instituciones de la UE ofrezcan una respuesta rápida y coordinada. Para ello, es esencial la detección precoz.

Desafío 9: Detección y respuesta eficaces

Detección y notificación

102 Los instrumentos comunes de detección permiten neutralizar diariamente la gran mayoría de los ataques[151]. No obstante, los sistemas digitales se son ahora tan complejos que evitar todos y cada uno de los ataques es imposible. Por su complejidad, con frecuencia los ataques escapan a la detección durante durante mucho tiempo, por lo que, según los expertos, habría que centrarse en la rapidez de detección y de defensa[152], aunque también es cierto que algunos instrumentos de detección como la automatización, el aprendizaje automático y el análisis comportamental, destinados a la reducción de riesgos y al análisis y el aprendizaje del comportamiento del sistema tienen un bajo índice de aceptación en las empresas[153]. Esto se debe a la generación de falsos positivos, que llevan a que actividades que no constituyen una amenaza se tomen por maliciosas.

103 Una vez detectada y analizada la infracción, es necesario notificarla y elaborar informes para que otras entidades públicas y privadas pueden adoptar medidas preventivas y que las autoridades puedan prestar apoyo a los afectados. Muchas organizaciones se resisten a reconocer y notificar los ciberincidentes[154]. También es esencial la pronta intervención de la policía en la respuesta inicial a la presuntos delitos informáticos y el intercambio proactivo de información con los CSIRT.

104 La anterior falta de requisitos comunes para la UE sobre notificación de incidentes, que la introducción de la Directiva NIS trataba de subsanar, podía retrasar la comunicación de infracciones y dificultar la respuesta (véase el apartado ***20***). A raíz de los ataque *Wannacry* de 2017, la Comisión llegó a la conclusión de que el sistema de la red CSIRT «todavía no era plenamente operativo»[155]. Más adelante se verá si, cuando se aplique la Directiva, las orientaciones elaboradas por el Grupo de Cooperación sirven para vencer la resistencia a notificar incidentes[156].

105 Con arreglo a la reglamentación vigente en la UE, los operadores de servicios esenciales en determinados sectores tienen múltiples obligaciones de notificación (también a los consumidores), que pueden restar eficiencia al proceso. Por ejemplo, los operadores de los sectores bancario y financiero están sujetos a diferentes criterios, normas, umbrales y plazos de notificación en virtud del Reglamento general de protección de datos, la Directiva NIS, la Directiva sobre servicios de pago, el BCE / MUS, TARGET2 y el Reglamento eIDAS[157]. Por este motivo es importante racionalizar estas obligaciones ya que, además de constituir una carga administrativa innecesaria, su heterogeneidad puedes dar lugar a información fragmentaria.

Respuesta coordinada

106 Todavía se está desarrollando el marco de cooperación europea en caso de crisis. El correspondiente «plan director»[158] (véase el apartado ***18***) se introdujo por tanto para dotar de una perspectiva cibernética al Dispositivo Integrado de Respuesta Política a las Crisis (DIRPC), mejorar el conocimiento de la situación y garantizar una mejor integración con otros mecanismos de gestión de crisis de la UE[159]. El plan director afecta a instituciones, organismos y Estados miembros de la UE. La integración sin fisuras de todos estos mecanismos de respuesta a las crisis constituye un desafío[160]. La actual falta de una red común de comunicaciones segura entre las instituciones de la UE constituye asimismo una deficiencia importante[161].

107 La capacidad de la UE para responder a los ciberataques operativos y políticos en caso de incidentes transfronterizos de gran envergadura ha sido calificada de «limitada» debido, en parte, a que la ciberseguridad todavía no está integrada en los mecanismos existentes en la UE de coordinación de la respuesta frente a las crisis[162]. La Directiva NIS no trataba este problema.

108 La reciente propuesta para reformar ENISA, en la que se preveía la atribución a la agencia de un mayor protagonismo operativo en la gestión de los incidentes de ciberseguridad a gran escala, no recibió el apoyo de los Estados miembros, que preferían que la función de la agencia apoyara y complementara la propia acción operativa de estos[163]. En los Estados miembros ya existen muchos CERT / CSIRT, pero sus capacidades varían considerablemente. Esto representa un obstáculo a la eficaz cooperación transfronteriza necesaria para responder a los incidentes a gran escala[164].

109 El Tribunal trató de esbozar el mapa de las funciones asignadas a los distintos actores que figuran en el plan, pero había lagunas que deberán colmarse a medida que se avance en la aplicación. Uno de los ámbitos que no había recibido atención

suficiente era el de aplicación de las leyes, aunque el protocolo de la UE de respuesta policial ante emergencias entró en vigor en diciembre de 2018[165]. Para que el plan director sea eficaz, es fundamental que sea práctico y que todas las partes sepan qué deben hacer, lo cual requerirá la realización de muchas pruebas en los próximos años.

110 Una respuesta eficaz va más allá de la contención de daños: la atribución de la responsabilidad del ataque es también decisiva. La localización e identificación de los autores, sobre todo en los ataques híbridos, puede ser muy difícil debido al creciente abuso de las herramientas de anonimización, las criptomonedas, y el cifrado. Es el denominado problema de atribución. Ponerle remedio no es solo una cuestión técnica, sino también de justicia penal. Las diferencias legales y de procedimiento entre países pueden obstaculizar las investigaciones penales y la imputación de los sospechosos. Para resolver el problema de atribución será necesario un intercambio operativo de información más formalizado a través de procedimientos más claros con Europol o con Red Judicial Europea sobre Ciberdelincuencia de Eurojust.

111 En el plano político, se ha creado el conjunto de instrumentos de ciberdiplomacia (véase el ***recuadro 6***) para prestar apoyo a la resolución pacífica de conflictos internacionales en el ciberespacio. La creación de equipos de respuesta telemática rápida y de una iniciativa de asistencia mutua en el ámbito de la ciberseguridad son dos proyectos que fomentan un mejor intercambio de información y que se desarrollan en el marco de la CEP[166].

Recuadro 6

Instrumentos de ciberdiplomacia

La respuesta diplomática conjunta de la UE a las actividades informáticas malintencionadas[167] o «conjunto de instrumentos de ciberdiplomacia» surgió de las conclusiones del Consejo sobre la ciberdiplomacia[168]. El objetivo de la ciberdiplomacia es desarrollar y aplicar un enfoque común y global del ciberespacio basado en los valores de la UE, en el Estado de Derecho, en el desarrollo de capacidades, la creación de asociaciones, el fomento del modelo multilateral de la gobernanza de internet, la reducción de las amenazas a la ciberseguridad y la mayor estabilidad de las relaciones internacionales.

El conjunto de instrumentos permite a la UE y a sus Estados miembros organizar una respuesta diplomática conjunta de la UE a las actividades informáticas malintencionadas haciendo pleno uso de las medidas de la política exterior y de seguridad común. Entre ellas figuran medidas preventivas (sensibilización, desarrollo de capacidades), de cooperación, estabilizadoras y restrictivas (prohibición de viajar, embargo de armas, congelación de fondos) o apoyo a las respuestas de los Estados

miembros[169]. La idea central es que una mayor cooperación para mitigar las amenazas y la indicación clara de las posibles consecuencias de una respuesta conjunta puede disuadir (en potencia) de comportamientos agresivos.

Esta respuesta conjunta a las actividades informáticas malintencionadas sería proporcionada al alcance, escala, duración, intensidad, complejidad, sofisticación e impacto de dichas actividades.

Para el funcionamiento satisfactorio del conjunto de instrumentos, será esencial cómo se realice su integración en el plan director y en el Dispositivo de la UE de Respuesta Política Integrada a las Crisis (véase el apartado ***106***), cómo se establezca una adecuada conciencia situacional mediante el intercambio de información rápido y continuo (también de elementos de atribución)[170] y, por último, la cooperación eficaz. Otro elemento clave para la aplicación satisfactoria del conjunto de instrumentos es la comunicación eficaz y coordinada. Hasta el momento, el conjunto de instrumentos se ha utilizado en dos ocasiones: para entablar un diálogo con los Estados Unidos tras el ataque*Wannacry*[171], y para elaborar conclusiones de la Comisión para condenar el uso malintencionado de las tecnologías de la información y de las comunicaciones[172]. Ya está en marcha la aplicación del conjunto de instrumentos, aunque aún queda por ver si cumple eficazmente sus objetivos.

Desafío 10: Protección de las infraestructuras críticas y las funciones sociales

Protección de la infraestructura

112 Gran parte de la infraestructura crítica de la UE se gestiona a través de sistemas de control industrial[173]. Muchos de ellos están concebidos como sistemas independientes, con limitada conectividad al mundo exterior. Como algunos componentes de los sistemas de control industrial se han conectado a internet, ahora son más vulnerables a interferencias externas. Puede que ya no sea posible mantener y parchear los sistemas existentes, pero su actualización tampoco es rápida ni barata. Por tanto, las medidas encaminadas a mejorar la seguridad de las infraestructuras críticas deben empezar por la mejora de las sistemas de control industrial.

113 A medida que la industria se digitaliza (lo que se conoce comúnmente como «Industria 4.0»), el impacto de un incidente a gran escala en un sector industrial puede tener efectos colaterales en los demás. ENISA ha señalado la importancia de trazar de un mapa de la repercusión de las dependencias mutuas en los sectores críticos[174], que

es esencial para comprender la potencial propagación de un incidente y constituye la base de la coordinación en las respuestas.

114 La Directiva SRI tiene por objeto mejorar la preparación de sectores clave de los que dependen infraestructuras críticas. Sin embargo, no todos los sectores están cubiertos (véase el ***cuadro 1***)[175], lo cual reduce la eficacia de la estrategia[176]: en este sentido, una de las mayores preocupaciones es proteger la integridad democrática de las elecciones de la interferencia en la infraestructura electoral y de la desinformación (véase el ***recuadro 7***). Por tanto, además de revisar la legislación vigente, un desafío fundamental consistirá en encontrar el modo de que estos sectores participen en la respuesta eficaz a incidentes de gran envergadura.

115 Las vulnerabilidades de las infraestructuras críticas no se detienen en las fronteras de Europa. Un reto particular que afronta la Comisión es impulsar a los países candidatos a adoptar las mismas normas que los Estados miembros, por ejemplo, en ámbitos como la legislación relacionada con la cibernética o la protección de infraestructuras críticas.

Recuadro 7

Protección de las funciones sociales básicas: lucha contra la injerencia en las elecciones

En mayo de 2019, unos 400 millones de votantes acudirán a las urnas en las elecciones al Parlamento Europeo, las primeras que se celebrarán en el marco del Reglamento General de Protección de Datos. Se producen justo después de los escándalos de abuso de datos personales para la microsegmentación política y de las campañas sin precedentes de desinformación («noticias falsas»). La Comisión ha advertido de que pueden producirse ciberinjerencias similares en estas elecciones[177]; para evitarlas, es necesario abordar el problema desde la Administración y la sociedad en su conjunto.

Infraestructura electoral

La organización de elecciones es compleja, y garantizar su protección e integridad es responsabilidad de los Estados miembros. El objetivo de las injerencias en las elecciones y en la infraestructura electoral puede ser influir en las preferencias de los votantes, en su participación o en el propio proceso electoral, en la votación real, el recuento de los votos y la comunicación de los resultados. En las elecciones al Parlamento Europeo, la protección del «último kilómetro» (la comunicación de los resultados de las capitales nacionales a Bruselas) es un reto fundamental, dado que

no existe un enfoque común en materia de seguridad o ha sido sometido a ensayo para ello[178].

El reciente paquete de elecciones de la Comisión contenía medidas para reforzar la ciberseguridad electoral, como la designación de puntos de contacto nacionales para coordinar e intercambiar información en la fase previa a las elecciones. Es muy importante intercambiar buenas prácticas y conclusiones extraídas[179].

No se considera que los sistemas electorales formen parte de las infraestructuras críticas[180], ni tampoco están cubiertos por la Directiva SRI. Pese a ello, el Grupo de Cooperación ha desarrollado orientaciones prácticas sobre la seguridad de la tecnología electoral para prestar apoyo a los poderes públicos. Se espera que los puntos de contacto nacionales se reúnan al principio de 2019[181]. También se insta a los Estados miembros a efectuar evaluaciones de riesgo sobre ciberamenazas a sus procesos electorales.

Desinformación

La desinformación es un aspecto de creciente importancia en los ataques híbridos, que consiste en ciberataques y en intrusión en las redes. Puede utilizarse para dividir a las sociedades, sembrar la desconfianza y minar la confianza en los procesos democráticos o en otras cuestiones (como la reticencia a la vacunación o el cambio climático). Ha crecido en escala, velocidad e intervalo, y supone una auténtica amenaza para la seguridad de la Unión.

La UE ha puesto en marcha recientemente una serie de medidas para combatir este problema. A partir de 2015, se estableció el Grupo de Trabajo East StratCom, basado en el SEAE, para contrarrestar las campañas de desinformación de Rusia[182]. Los expertos han alabado su trabajo para promocionar las políticas de la UE, apoyar los medios de comunicación independientes de la Vecindad, y prever, detectar y combatir la desinformación[183]. Sin embargo, los recursos del Grupo de Trabajo de la Comisión son limitados frente a la magnitud y la complejidad de las campañas de desinformación[184]. Es necesaria una interacción más sistemática la con las estructuras existentes de la UE y la mejora de la cooperación en materia de comunicación estratégica[185]. En diciembre de 2018, el Consejo aprobó un nuevo plan de acción[186].

Más recientemente, la Comisión, en su comunicación de abril de 2018 sobre la lucha contra la desinformación en línea[187], ha desarrollado un código de buenas prácticas voluntario y autorregulado[188], basado en instrumentos políticos ya existentes, al que se han adherido plataformas en línea y la industria publicitaria[189]. Entre otras medidas cabe citar las destinadas a aumentar la fiabilidad de los contenido y el apoyo a las iniciativas para mayor alfabetización mediática y de las noticias. También se ha creado una red europea de verificadores de datos.

La Comisión ha declarado que, de no cumplirse el código de buenas prácticas, aplicará medidas reguladoras adicionales. Determinar la eficacia de las medidas será

fundamental, especialmente al decidir cómo medir las mejoras en la confianza, la transparencia y la rendición de cuentas.

Otro desafío será encontrar formas de mejorar la detección, el análisis y la revelación de la desinformación[190]. También es necesario el seguimiento activo y estratégico, y el análisis de fuentes de datos abiertas[191]. Los intentos de comprender mejor el contexto de amenazas deben abarcar también las tendencias emergentes, como las falsedades profundas («deep fakes»: falsos vídeos creados con la asistencia de la inteligencia artificial y el aprendizaje automático), así como las herramientas necesarias para su detección.

Mejorar la autonomía

116 La UE es un importador neto de productos y servicios de ciberseguridad, lo cual incrementa el riesgo de dependencia tecnológica y la vulnerabilidad frente a los operadores de terceros países[192]. En particular, este hecho es perjudicial para la seguridad de la infraestructura crítica de la UE, que también se apoya en cadenas de suministro mundiales complejas. El riesgo aumenta todavía más cuando los operadores de países terceros adquieren empresas de ciberseguridad europeas. El control de la inversión extranjera directa (IED) compete a los Estados miembros, y, en la actualidad, no existe ningún mecanismo de control a escala de la UE[193].

117 Mayor autonomía estratégica es un objetivo en la Estrategia Global de la UE y la de 2017 titulada «*Resiliencia, disuasión y defensa*»[194]. Hacer frente a los múltiples retos que se presentan en el presente informe contribuirá a incrementar la deseada autonomía. Una única medida no logrará este objetivo por sí sola.

Puntos de reflexión: Respuesta eficaz

- ¿Cómo ha contribuido la Directiva SRI a mejorar la notificación de los ciberincidentes en los sectores críticos y en otros ámbitos?
- ¿Cómo integran las instituciones de la UE la coordinación de respuestas ante crisis frente a un incidente cibernético grave?
- ¿Cómo puede desempeñar un papel más destacado la ciberdiplomacia en las acciones exteriores de la UE?
- ¿Son las actuales estructuras y acciones de la UE para hacer frente a la desinformación proporcionales a la magnitud y complejidad del problema?

Observaciones finales

118 En los últimos años, la UE y sus Estados miembros han concedido mayor prioridad a la ciberseguridad para mejorar globalmente su ciberresiliencia. Sin embargo, lograr un mayor nivel de ciberseguridad en la Unión sigue siendo una empresa enorme. En este documento informativo hemos querido destacar algunos de los principales retos que plantea la aspiración de la UE de convertirse en el entorno digital más seguro del mundo.

119 En este documento se muestra que es necesario avanzar hacia una cultura del rendimiento con prácticas de evaluación integrada para garantizar una **rendición de cuentas y una evaluación**significativas. Quedan **lagunas en la legislación, y la transposición de las reglamentaciones por los Estados miembros no se realiza de manera sistemática**. Esto puede hacer más difícil que la legislación alcance su pleno potencial. Otro desafío radica en **ajustar los niveles de inversión a los objetivos estratégicos**, que exige incrementar los niveles de inversión y su impacto. Esto es más complicado si la UE y sus Estados miembros carecen de **una visión general clara del gasto de la UE** en ciberseguridad. También se habla de **las restricciones en la asignación de recursos suficientes a las agencias pertinentes de la UE relacionadas con el ámbito cibernético,** y de dificultades para atraer y mantener el talento.

120 Los estudios realizados llegan a la conclusión de que la **gobernanza de la ciberseguridad puede reforzarse** para impulsar la capacidad de la comunidad mundial de responder a los ciberataque y a los incidentes. Al mismo tiempo, es imposible prevenir todos los ataques. Por tanto, **la detección y respuesta rápidas** y la **protección de las infraestructuras críticas y las funciones sociales**, junto con una **mejora del intercambio de información y la coordinación** entre los sectores público y privado son desafíos clave que hay que afrontar. Por último, es fundamental **aumentar las capacidades y la sensibilización** en todos los sectores y niveles de la sociedad, teniendo en cuenta el creciente déficit de ciberseguridad mundial.

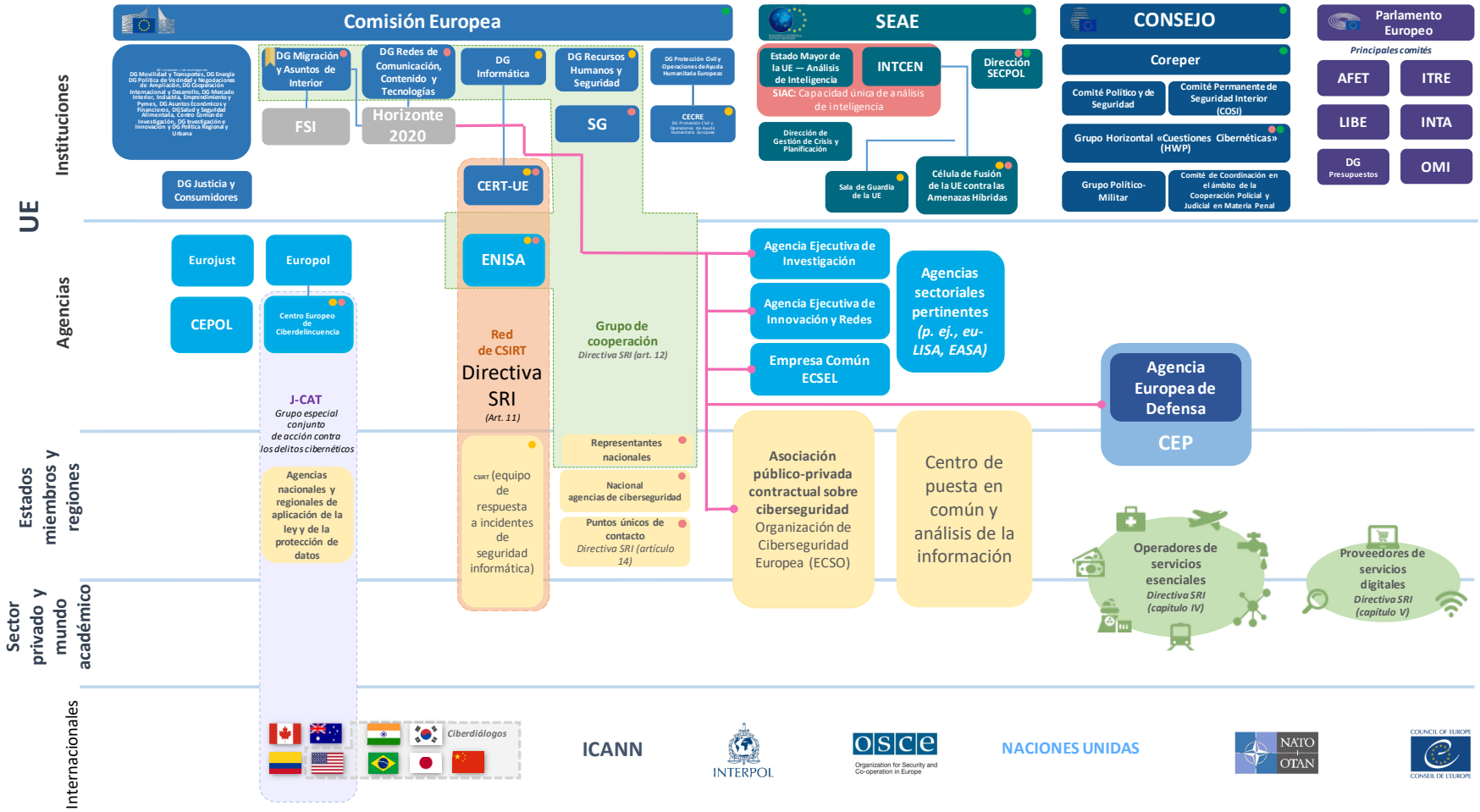
121 Estos desafíos que plantean las amenazas cibernéticas a las que se enfrenta la UE y el mundo en general requieren un compromiso continuo y una garantía firme de respeto de los valores fundamentales de la UE.

El presente documento informativo han sido aprobadas por la Sala III en su reunión del día 22 de febrero de 2019.

Por el Tribunal de Cuentas

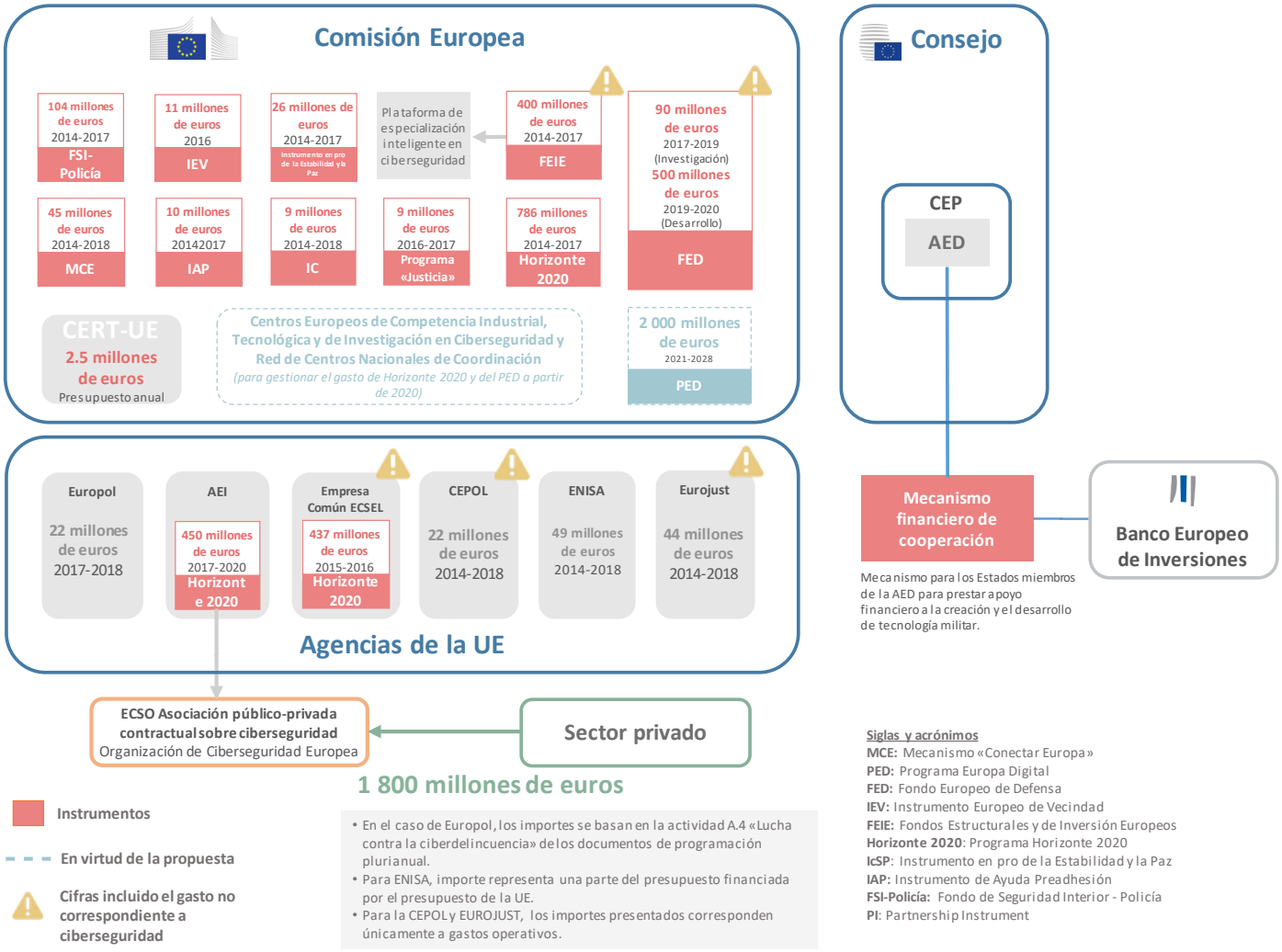
Klaus-Heiner Lehne
Presidente

Anexo I — Un panorama multidimensional y complejo con muchos agentes



Fuente: Tribunal de Cuentas Europeo.

Anexo II — Gasto de la UE en ciberseguridad desde 2014



Fuente: Tribunal de Cuentas Europeo, a partir de los datos de la Comisión Europea y de los organismos de la Unión Europea.

Anexo III — Informes de auditoría de los Estados miembros de la UE

Tipo	Título (con hiperlink)	Año	EM
Auditorías de conformidad	Nota de evaluación de control interno	2014	FR
	Informe de certificación de las cuentas del Régimen de la Seguridad Social(defensa, asuntos exteriores)	2016	FR
	Certificación de las cuentas del Estado	2016	FR
	Garantizar la seguridad y la protección de las bases de datos nacionales de importancia crítica en Estonia	Fin. 2018 / todavía no se ha publicado	EE
	Eficacia de los controles internos para la protección de los datos personales en las bases de datos nacionales	2008	EE
Auditorías de gestión/optimización de recursos	Informe sobre la mitigación de los efectos de los ciberataques	2013	DK
	RiR 2014:23 Seguridad de la información el la Administración Pública civil	2014	SE
	Informe sobre el tratamiento de datos confidenciales de personas y empresas por las Administraciones Públicas	2014	DK
	Programa nacional de ciberseguridad	2014	UK
	Informe a la comisión presupuestaria del Parlamento Federal alemán con arreglo al artículo 88, apartado 2, del Código presupuestario federal (BHO) – Consolidación IT, Gobierno Federal	2015	DE
	Informe sobre el acceso a los sistemas informáticos que apoyan la prestación de servicios esenciales a la sociedad danesa	2015	DK
	Autoridad de Planificación Pública Plaine de Francia	2015	FR
	Entorno de ciberseguridad en Lituania Versión lituana resumen traducido al inglés	2015	LT
	Actuación de los organismos públicos en relación con la ciberseguridad en Polonia (en polaco)	2015	PL
	RiR 2015:21 Ciberdelincuencia: policías y fiscales pueden ser más eficiente.	2015	SE
	Deficiencias de las Administraciones Públicas en materia de cibercapacidades (encuesta)	2015	UK
	Informe al Parlamento Federal: Finanzas federales: recaudación del impuesto de sucesiones	2016	BE
	Informe sobre la gestión de la seguridad informática de los sistemas contratada a proveedores externos	2016	DK
	Informe de fiscalización de la actividad crediticia del Instituto de Crédito Oficial (ICO), ejercicio 2016	2016	ES
	Dirección de la red de seguridad pública	2016	FI
	Garantizar la seguridad de los sistemas informáticos empleados en las actividades públicas	2016	PL
	Prevención y lucha contra el ciberacoso a niños y jóvenes	2016	PL
	Trabajo en seguridad de la información en nueve agencias	2016	SE

Tipo	Título (con hiperlink)	Año	EM
	- Nueva auditoría sobre la seguridad de la información en las Administraciones Públicas. RIR 2016:		
	Protección de la información en las Administraciones Públicas	2016	UK
	Informe sobre la protección de los sistemas informáticos y los datos sanitarios en tres regiones de Dinamarca	2017	DK
	Nota sobre los resultados de la auditoría paralela internacional sobre la eficacia de los controles internos en la protección de los datos personales de las bases de datos nacionales.	2017	EE
	Medidas de ciberprotección	2017	FI
	Dirección de la fiabilidad operativa de los servicios electrónicos	2017	FI
	Red de Cámaras Agrarias (síntesis)	2017	FR
	Vaucluse Cámara de Comercio e Industria (por la Cámara Regional de Cuentas PACA)	2017	FR
	Garantizar la seguridad y protección de las bases de datos nacionales de Estonia de importancia crítica	Fin. 2018 / todavía no se ha publicado	EE
	Desarrollo de la infraestructura de comunicaciones electrónicas públicas Versión lituana resumen traducido al inglés)	2017	LT
	Auditoría de la tecnología de la información: La ciberseguridad en las entidades estatales	2017	EE
	El sistema de los registros nacionales: seguridad, rendimiento y manejabilidad	2017	PL
	El incidente *WannaCry*	2017	UK
	Fraude online	2017	UK
	Informe sobre la protección contra los ataques de los programas de secuestro	2018	DK
	Hospital de Arpajon (por la Cámara Regional de Île-de-France)	2018	RF
	Gestión de los recursos informativos críticos del Estado	2018	LT
	Delitos electrónicos	2019	LT
	Seguridad de la información en Polonia	2019	PL
Otros	Bases de datos de organismos públicos	s.o.	BE
	Cuestionario pobre la política de seguridad y de análisis de riesgos (en curso)	s.o.	BE

Siglas y acrónimos

AED: Agencia Europea de Defensa

AES: Autoridad Europea de Supervisión

CEP: Marco de cooperación estructurada permanente

CERT - UE: Equipo de respuesta a emergencias informáticas de las instituciones, órganos y organismos de la Unión Europea

cPPP: Asociación público-privada contractual

CSIRT: Equipo de respuesta a incidentes de seguridad informática

DDoS: Denegación de servicio distribuido

DG Informática: Dirección General de Informática

DG Justicia y Consumidores: Dirección General de Justicia y Consumidores

DG Migración y Asuntos de Interior: Dirección General de Migración y Asuntos de Interior

DG Redes de Comunicación, Contenido y Tecnologías: Dirección General de Redes de Comunicación, Contenido y Tecnologías

Directiva SRI: Directiva sobre seguridad de las redes y de la información

EC3: Centro Europeo de Ciberdelincuencia de Europol

ECSEL: Empresa Común Componentes y Sistemas Electrónicos para el Liderazgo Europeo

ECSO: Organización de Ciberseguridad Europea

ENISA: Agencia de Seguridad de las Redes y de la Información de la Unión Europea

Fondos EIE: Fondos Estructurales y de Inversión Europeos

FSI - P: Fondo de Seguridad Interior - Policía

HWPCI: Grupo Horizontal «Cuestiones Cibernéticas»

IED: Inversión extranjera directa

ISSB: Consejo Director de Seguridad de la Información

JRC: Centro Común de Investigación

MESC: Mes europeo de sensibilización en materia de ciberseguridad

NCIRC: Equipo de capacidad de respuesta ante incidentes informáticos de la OTAN

ONA: Oficina Nacional de Auditoría

PCSD: Política común de seguridad y defensa

PED: Programa Europa Digital

Pyme: Pequeña y mediana empresa

RGPD: Reglamento general de protección de datos

RLSI: Responsable local de seguridad de la información

SCI: Sistema de control industrial

SEAE: Servicio Europeo de Acción Exterior

Tribunal: Tribunal de Cuentas Europeo

UE: Unión Europea

Glosario

***Adware*:** Programa informático malicioso que muestra anuncios publicitarios o ventanas desplegables con código para rastrear el comportamiento en línea de las víctimas.

Amenaza híbrida: Expresión de intento hostil que realizan los adversarios utilizando una combinación de técnicas de guerra convencionales y no convencionales (es decir, métodos militares, políticos, económicos y tecnológicos) en la persecución de sus objetivos.

Ciberataque: Intento de socavar o destruir la confidencialidad, la integridad y la disponibilidad de datos o de un sistema informático a través del ciberespacio.

Ciberdefensa: Subconjunto de la ciberseguridad destinado a defender el ciberespacio con medios militares u otros medios adecuados para lograr objetivos militares estratégicos.

Ciberdelincuencia: Distintas actividades delictivas en las que están implicados ordenadores y sistemas informáticos como herramienta u objetivo principal y que comprenden las siguientes: delitos tradicionales (por ejemplo, fraude, falsificación y usurpación de identidad), delitos relacionados con los contenidos (por ejemplo, distribución en línea de pornografía infantil o incitación al odio racial) y delitos exclusivos de ordenadores y sistemas de información (por ejemplo, ataques contra los sistemas de información, ataques de denegación de servicio o programas maliciosos).

Ciberespacio: Entorno global intangible en el que se produce la comunicación en línea entre las personas, el software y los servicios a través de redes informáticas y dispositivos tecnológicos.

Ciberincidente: Incidente que perjudica o daña directa o indirectamente la resiliencia y la seguridad de un sistema informático y los datos que este procesa, almacena o transmite.

Ciberresiliencia: Capacidad de prevenir los ciberataques e incidentes, de prepararse para los mismos, de resistir y de recuperarse ante estos.

Ciberseguridad: Conjunto de salvaguardias y medidas adoptadas para defender los sistemas informáticos y sus datos frente a accesos no autorizados, ataques y daños para garantizar su disponibilidad, confidencialidad e integridad.

Cifrado: Transformación de información legible en código ilegible para su protección. Para leer la información, el usuario debe tener acceso a una clave secreta o contraseña.

Computación en la nube: Provisión de recursos informáticos a demanda, como el almacenamiento, la potencia de computación o la capacidad de intercambio de datos, en internet a través de un alojamiento en servidores remotos.

Confidencialidad: Protección de información, datos o activos frente a un acceso no autorizado o su divulgación.

Contenido digital: Datos, como texto, sonido, imágenes o vídeo, almacenados en un formato digital.

Criptomoneda: Activo digital que se emite e intercambia utilizando técnicas de encriptación con independencia de un banco central y que es aceptada como medio de pago entre los miembros de una comunidad virtual.

Datos de acceso: Información sobre la actividad de inicio y cierre de sesión de un usuario para acceder a un servicio como la hora, la fecha y la dirección IP.

Datos personales: Información relativa a un individuo identificable.

Delito facilitado por internet: Delito tradicional cometido a una escala mayor mediante la utilización de sistemas informáticos.

Delito relacionado con el ciberespacio: Delito que solo puede ser cometido utilizando dispositivos informáticos.

Denegación de servicio distribuido (DDoS): Ciberataque para impedir que los usuarios legítimos accedan a servicios o recursos en línea inundándolos de más solicitudes de las que pueden gestionar.

Desinformación: Información verificablemente falsa o engañosa que se crea, presenta y divulga con fines lucrativos o para engañar deliberadamente a la población, y que puede causar un perjuicio público.

Disponibilidad: Garantizar el acceso oportuno y fiable a la información, así como su utilización.

Ecosistema cibernético: Comunidad compleja de dispositivos, datos, redes, personas, procesos y organizaciones en interacción, así como el entorno de procesos y tecnologías que influyen y apoyan estas interacciones.

Gestión de la vulnerabilidad: Parte integrante de la seguridad de un ordenador y red para mitigar o evitar proactivamente la explotación de las vulnerabilidades del sistema y del software a través de su identificación, clasificación y reparación.

Hacktivista: Personas o grupos que obtienen acceso no autorizado a sistemas o redes de información con fines de promoción de fines sociales o políticos.

Infraestructura electoral: Abarca las bases de datos y los sistemas informáticos de campaña, la información sensible sobre los candidatos, el registro de los votantes y los sistemas de gestión.

Infraestructuras críticas: Recursos físicos, servicios e instalaciones cuya perturbación o destrucción tendría un grave impacto sobre el funcionamiento de la economía y la sociedad.

Ingeniería social: En seguridad de la información, manipulación psicológica para engañar a una persona para que realice una acción o divulgue información confidencial.

Integridad: Protección frente a la modificación inapropiada o la destrucción de información y garantía de su autenticidad.

Internet de las cosas: Red de objetos cotidianos equipados con electrónica, software y sensores para que puedan comunicar e intercambiar datos a través de internet.

Kit de explotación: Tipo de herramienta que emplean los ciberdelincuentes para atacar las vulnerabilidades en las redes y los sistemas de información para que puedan distribuir programas maliciosos o llevar a cabo otras actividades malintencionadas.

Modelo de «delito como servicio»: Modelo de negocio delictivo que impulsa la economía digital sumergida proporcionando una amplia gama de herramientas y servicios comerciales que permiten a ciberdelincuentes que se están iniciando practicar la ciberdelincuencia.

Parcheado: Introducción de un conjunto de cambios al software o para actualizar, reparar o mejorar el software, incluida la reparación de vulnerabilidades de seguridad.

Programa de secuestro: Software malicioso que impide que las víctimas puedan acceder a un sistema informático o que hace ilegibles los archivos, generalmente mediante encriptación. Posteriormente, el atacante suele chantajear a la víctima negándose a restaurar el acceso hasta que no se pague un rescate.

Programa malicioso *wiper*: Tipo de programa malicioso cuya intención es borrar el disco duro del ordenador que infecta.

Programa malicioso: Software malicioso. Programa informático diseñado para dañar ordenadores, servidores o redes.

Red infectada: Red de ordenadores infectados con programas informáticos maliciosos y controlados de forma remota, sin el conocimiento de los usuarios, para enviar correos electrónicos no deseados, robar información o lanzar ciberataques coordinados.

Robo de datos para la clonación de tarjetas: Robo de datos de tarjetas de débito o de crédito al introducirlos en internet.

Seguridad de la información: Conjunto de procesos y herramientas que protegen los datos físicos y digitales del acceso no autorizado, el uso, la divulgación, la perturbación, la modificación, el registro o la destrucción.

Seguridad de la red: Subconjunto de datos de protección de la ciberseguridad enviados a través de dispositivos en la misma red para garantizar que no se intercepta o modifica la información.

Servicios de confianza: Servicios que mejoran la validez jurídica de una transacción electrónica, como las firmas electrónicas, los sellos de tiempo, las entregas certificadas y las autenticaciones de sitio web.

Sistema heredado: Sistema informático, aplicación o lenguaje de programación obsoleto o desactualizado que sigue operativo pero para el que es posible que ya no haya actualizaciones ni soporte del fabricante, incluido soporte de seguridad.

Suplantación de identidad: Práctica de enviar correos electrónicos supuestamente procedentes de una fuente fiable para engañar a sus destinatarios para que pulsen enlaces maliciosos o compartan información personal.

Vectorización de texto: Proceso de conversión de palabras, frases o documentos enteros en vectores numéricos para que los algoritmos de aprendizaje automático puedan utilizarlos.

[1] En el proyecto de Reglamento de Ciberseguridad de la UE se define como «todas las actividades necesarias para la protección de las redes y sistemas de información, de sus usuarios y de las personas afectadas por las ciberamenazas». Su aprobación por el Parlamento Europeo y el Consejo está prevista para principios de 2019.

[2] Europol, *Internet Organised Crime Threat Assessment 2017*.

[3] Organización de Ciberseguridad Europea (ECSO), *European Cybersecurity Industry Proposal for a contractual Public-Private Partnership*, junio de 2016.

[4] Parlamento Europeo, *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses*, estudio para la Comisión de Libertades Civiles, Justicia y Asuntos de Interior, septiembre de 2015.

[5] ENISA, *ENISA Threat Landscape Report 2017*, 18 de enero de 2018.

[6] Europol, *Internet Organised Crime Threat Assessment 2018*.

[7] Europol, *ibid.*, 2018.

[8] Centro Europeo de Economía Política Internacional, *Stealing Thunder: Will cyber espionage be allowed to hold Europe back in the global race for industrial competitiveness?*, Occasional Paper n.º 2/18, febrero de 2018.

[9] Comisión Europea, Estado de la Unión 2017 del Presidente.

[10] Europol, *World's Biggest Marketplace selling internet paralysing DDoS attacks taken down*, comunicado de prensa, 25 de abril de 2018.

[11] Europol, *Internet Organised Crime Threat Assessment 2017*.

[12] Ficha informativa de la Comisión Europea sobre la ciberseguridad, septiembre de 2017.

[13] Entre los costes cabe citar pérdida de ingresos, gastos de reparación de sistemas dañados, posibles responsabilidades por activos o información robados, incentivos de retención de clientes, primas de seguros más altas, incremento de los costes de protección (nuevos sistemas, trabajadores, formación, etc.) y posibles liquidaciones de gastos de cumplimiento o litigios.

[14] NTT Security, *Risk: Value 2018 Report*.

[15] El programa de secuestro *Wannacry* explotó las vulnerabilidades de un protocolo de Microsoft Windows que permite el control remoto de cualquier ordenador. Microsoft lanzó un parche cuando descubrió la vulnerabilidad, pero como cientos de miles de ordenadores no habían sido actualizados todavía, muchos fueron infectados posteriormente. Fuente: A. Greenberg, *Hold North Korea Accountable For Wannacry—and the NSA, too*, WIRED, 19 de diciembre de 2017.

[16] Comisión Europea, *Europeans' attitudes towards cybersecurity*, Eurobarómetro especial 464a, septiembre de 2017. La publicación de una encuesta de seguimiento está prevista para principios de 2019.

[17] El Convenio de Budapest es una directriz internacional vinculante para países que desarrollan legislación contra la ciberdelincuencia. Ofrece un marco para la cooperación internacional entre los Estados parte. La Comisión, el Consejo de la Unión Europea, Europol, ENISA y Eurojust representan actualmente a la UE.

[18] Comisión Europea, *Estrategia de ciberseguridad de la Unión Europea:Un ciberespacio abierto, protegido y seguro*, JOIN(2013) 1 final, 7 de febrero de 2013.

[19] Comisión Europea, *Agenda de Seguridad de la Unión Europea*, COM (2015) 185 final, 28 de abril de 2015.

[20] Comisión Europea, *Una Estrategia para el Mercado Único Digital de Europa*, COM (2015) 192 final, 6 de mayo de 2015.

[21] SEAE *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy*, junio de 2016.

[22] Centro de Estudios Políticos Europeos, *Strengthening the EU's Cyber Defence Capabilities – Report of a CEPS Task Force*, noviembre de 2018.

[23] El programa malicioso utilizado para el ataque con programas de secuestro *Wannacry* que los Estados Unidos, el Reino Unido y Australia atribuyeron a Corea del Norte, , fue desarrollado y almacenado inicialmente por la Agencia de Seguridad Nacional de los Estados Unidos para explotar vulnerabilidades de Windows. Fuente: A. Greenberg, *ibid*., WIRED, 19 de diciembre de 2017. A raíz de los ataques, Microsoft condenó el almacenamiento de vulnerabilidades de software por los Gobiernos y reiteró su llamamiento en favor de un Convenio de Ginebra Digital.

[24] Además de los escenarios terrestre, marítimo, aéreo y espacial.

[25] Marco político de ciberdefensa de la UE (actualización de 2018), 14413/18, 19 de noviembre de 2018.

[26] Comisión Europea/Servicio Europeo de Acción Exterior, *Comunicación conjunta sobre la lucha contra las amenazas híbridas: Una respuesta de la Unión Europea*, JOIN (2016) 18 final, 6 de abril de 2016.

[27] Declaración conjunta del Presidente del Consejo Europeo, el Presidente de la Comisión Europea y el Secretario General de la Organización del Tratado del Atlántico Norte, 8 de julio de 2016 y 10 de julio de 2018.

[28] Comisión Europea/Servicio Europeo de Acción Exterior, *Resiliencia, disuasión y defensa:fortalecer la ciberseguridad de la UE*, JOIN (2017) 450 final, 13 de septiembre de 2017.

[29] 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, p. 1).

[30] 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.

[31] Estos están integrados en estructuras cooperativas establecidas por la Directiva, la red de CSIRT (integrada por CSIRT designados de los Estados miembros de la UE y el CERT-UE y cuya Secretaría es asumida por ENISA) y el Grupo de cooperación (apoya y facilita la cooperación estratégica y el intercambio de información entre los Estados miembros, y la Comisión asumen su Secretaría).

[32] Reglamento (UE) 2016/679del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DO L 119 de 4.5.2016, p. 1).

[33] Comisión Europea, *Propuesta de 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»*, COM (2017) 477 final, 13 de septiembre de 2017.

[34] Comisión Europea, *Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal*, COM (2018) 225 final, 17 de abril de 2018.

[35] Comisión Europea, *Propuesta de Directiva del Parlamento Europeo y del Consejo por la que se establecen normas armonizadas para la designación de representantes legales a efectos de recabar pruebas para procesos penales*. COM (2018) 226 final, 17 de abril de 2018.

[36] Comisión Europea, *Propuesta 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,* COM (2018) 630 final, 12 de septiembre de 2018.

[37] H. Carrapico y A. Barrinha, *The EU as a Coherent (Cyber)Security Actor?*, Journal of Common Market Studies, vol. 55, n.º 6, 2017.

[38] Comisión Europea, *ibid*., SWD(2017) 295 final, 13 de septiembre de 2017.

[39] Servicio de Estudios del Parlamento Europeo, *Transatlantic cyber-insecurity and cybercrime. Economic impact and future prospects*, PE 603.948, diciembre de 2017.

[40] ENISA, *An evaluation framework for Cyber Security Strategies*, 27 de noviembre de 2014.

[41] Una excepción es el artículo 14 («Seguimiento y estadísticas») de la 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.

[42] Comité Económico y Social Europeo, *Cybersecurity: ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks*, marzo de 2018. CEPS-ECRI Task Force, Cybersecurity in Finance: Getting the policy mix right!, junio de 2018.

[43] Respondieron a la encuesta del Tribunal veinticuatro de las veintiocho oficinas nacionales de auditoría.

[44] Es decir, basado en principios y, en lo posible, tecnológicamente neutro.

[45] Comisión Europea, Mecanismo de Asesoramiento Científico, Scientific Opinion 2/2017, 24 de marzo de 2017.

[46] L. Rebuffi, *EU Digital Autonomy: A possible approach*, Digma Zeitschrift für Datenrecht und Informationssicherheit, septiembre de 2018. Centro Europeo de Economía Política Internacional, *ibid*., Occasional Paper No 2/18, febrero de 2018.

[47] Comisión Europea, *Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a determinados aspectos de los contratos de suministro de contenidos digitales*, COM(2015) 634 final, 9 de diciembre de 2015.

[48] Comisión Europea, *Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a determinados aspectos de los contratos de compraventa en línea y otras ventas a distancia de bienes*, COM(2017) 635 final, 9 de diciembre de 2015.

[49] Consejo Neerlandés de Ciberseguridad, *European Foresight Cyber Security Meeting 2016: Public private academic recommendations to the European Commission about Internet of Things and Harmonization of duties of care*, 2016.

[50] Centro de Estudios Políticos Europeos, *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges – Report of a CEPS Task Force*, junio de 2018.

[51] Comisión Europea, *Aprovechar al máximo la SRI - hacia la aplicación efectiva de la Directiva (UE) 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión*, COM(2017) 476 final/2, 4 de octubre de 2017.

[52] Europol, *ibid*., 2017.

[53] Consejo de la Unión Europea, *Informe definitivo de la séptima ronda de evaluaciones mutuas sobre «Aplicación práctica y funcionamiento de las políticas europeas de prevención y lucha contra la ciberdelincuencia»*, 12711/1/17 REV 1, 9 de octubre de 2017.

[54] Comisión Europea, *Impact assessment accompanying the document Proposal for a Directive on combating fraud and counterfeiting of non-cash means of payment*, SWD/2017/0298 final, 13 de septiembre de 2017. El acuerdo político sobre la nueva legislación se alcanzó en diciembre de 2018 y su adopción está prevista para el principio de 2019.

[55] Europol, *ibid*., 2017.

[56] C-362/14: Maximillian Schrems v. Data Protection Commissioner (Irlanda), 6 de octubre de 2015.

[57] Europol/Eurojust, *Common challenges in combatting cybercrime*, 7021/17, 13 de marzo de 2017.

[58] Comisión Europea, *Assessment of the EU 2013 Cybersecurity Strategy*, SWD (2017) 295 final, 13 de septiembre de 2017.

[59] Servicio de Estudios del Parlamento Europeo, *Briefing: EU Legislation in Progress – Review of dual-use export controls*, *PE589.832*.

[60] Resolución del Parlamento Europeo, *Derechos humanos y tecnología: el impacto de los sistemas de intrusión y vigilancia en los derechos humanos en terceros países*, (2014/2232(INI)), 8 de septiembre de 2015. Los bienes y servicios de doble uso, entre los que figuran el software y la tecnología, pueden tener aplicaciones civiles y militares.

[61] La información pública disponible se almacena en la base de datos WHOIS, gestionada por ICANN (Corporación para la Asignación de Nombres y Números en Internet). ICANN mantiene el sistema de nombres de dominio. El uso indebido de nombres de dominio facilita la ciberdelincuencia.

[62] Artículo 3, Directiva SRI, *ibid*.

[63] Consejo Atlántico, *Risk Nexus: Overcome by cyber risks? Economic benefits and costs of alternate cyber futures*, 10 de septiembre de 2015.

[64] La Casa Blanca, *Cybersecurity spending fiscal year 2019*.

[65] Comisión Europea, *Documento de trabajo de los servicios de la Comisión:«Impact Assessment Accompanying the document "Proposal for a Regulation of the European Parliament and of the Council establishing the Digital Europe programme for the period 2021-2027"»*, SWD(2018) 305 final, 6 de junio de 2018.

[66] Centro de Estudios Estratégicos de La Haya, *Dutch investments in ICT and cybersecurity: putting it in perspective*, diciembre de 2016.

[67] Comisión Europea, *ibid*., COM (2018) 630 final, 12 de septiembre de 2018.

[68] Unidad de Prospectiva Científica del Servicio de Estudios del Parlamento Europeo, *Achieving a sovereign and trustworthy ICT industry in the EU*, diciembre de 2017.

[69] European Digital SME Alliance, *Position Paper on European Cybersecurity Strategy: Fostering the SME ecosystem*, 31 de julio de 2017.

[70] Unidad de Prospectiva Científica del Servicio de Estudios del Parlamento Europeo, *ibid*., diciembre de 2017.

[71] *Ibid*.

[72] Comisión Europea, *Impact assessment on the proposed research competence centre and network of national coordination centres*, SWD(2018) 403 final (parte 1/4), 12 de septiembre de 2018.

[73] Comisión Europea, *ibid*., COM (2018) 630 final, 12 de septiembre de 2018.

[74] Informe Especial n.º 13/2018 del Tribunal de Cuentas Europeo: «Hacer frente a la radicalización que conduce al terrorismo».

[75] Las ilustraciones citadas en esta sección proceden de documentos publicados de la Comisión, salvo la relativa a los 42 millones de euros del apartado ***51***, que el Tribunal obtuvo directamente de la Comisión.

[76] Horizonte 2020 es el programa de investigación e innovación de 80 000 millones de euros de la UE que presta apoyo a la Unión por la Innovación, destinada a garantizar la competitividad global de la UE.

[77] Horizonte 2020, desafío de la sociedad 7: «Sociedades seguras - Proteger la libertad y la seguridad de Europa y sus ciudadanos».

[78] El Tribunal analizó proyectos de Horizonte 2020 procedentes del conjunto de datos de CORDIS y realizó una vectorización de texto de todas las descripciones de proyectos, utilizando la taxonomía de ciberseguridad del JRC (véase el ***recuadro 5*** en el siguiente capítulo), para identificar aquellos proyectos que puedan estar relacionados con la ciberseguridad. Posteriormente, comprobó y analizó manualmente los resultados.

[79] Organización de Ciberseguridad Europea, *ECS cPPP Progress Monitoring Report 2016-2017*, 29 de octubre de 2018.

[80] Artículo 9, apartado 2, Directiva SRI, *ibid*.

[81] GLACY+ (Acción Mundial contra la Ciberdelincuencia) es un proyecto conjunto con el Consejo de Europa que presta apoyo a doce países de África, Asia-Pacífico, y América Latina y la región del Caribe, los cuales a su vez pueden servir como plataformas para compartir su experiencia en sus respectivas regiones.

[82] El Centro Europeo de Estrategia Política (EPSC), grupo de reflexión de la Comisión, se ha referido al riesgo de que se produzca un «punto ciego digital» si sigue creciendo la brecha entre la UE y sus vecinos de los Balcanes Occidentales. Países como China y Rusia están invirtiendo importantes cantidades en la región, con el consiguiente riesgo de que la UE quede marginada como actor cibernético en la región. Fuente: EPSC, *Engaging with the Western Balkans: an investment in Europe's security*, 17 de mayo de 2018.

[83] Banco Europeo de Inversiones, *The EIB Group Operating Framework and Operational Plan 2018*, 12 de diciembre de 2017. No había más información disponible cuando se redactó este documento.

[84] Comisión Europea, *Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establece el programa Europa Digital para el período 2021-2027*, COM(2018) 434 final, 6 de junio de 2018.

[85] Comisión Europea, *Reglamento (UE) 2018/1092 del Parlamento Europeo y del Consejo, de 18 de julio de 2018, por el que se establece el Programa Europeo de Desarrollo Industrial en materia de Defensa con el objetivo de apoyar la competitividad y la capacidad de innovación de la industria de la defensa de la Unión* (DO L 200, 7.8.2018, p. 30). Asimismo, en 2017 se estableció una Acción preparatoria sobre investigación en materia de defensa, financiada por Horizonte 2020, que ascendió a 90 millones de euros para 2017-2019. No está claro si abarca el gasto relacionado con el ámbito cibernético.

[86] En 2019 está prevista la publicación de otro documento informativo del Tribunal de Cuentas Europeo sobre defensa de la UE.

[87] El EC3 de Europol, ENISA, el SEAE, la Agencia Europea de Defensa y CERT-UE cuentan con 159 trabajadores en total. Esta cifra no incluye el personal relacionado con el ámbito cibernético de la Comisión Europea o de los Estados miembros. Fuente: Centro de Estudios Políticos Europeos, *ibid*., noviembre de 2018.

[88] *ENISA evaluation*, 2017.

[89] Europol solicitó un incremento anual de personal de 70 agentes temporales en su plan plurianual 2018-2020, pero solo se aprobó un incremento de 26 para 2018. En el próximo proyecto de plan plurianual para 2019-2021, Europol incluyó un incremento modesto dando por hecho que no se cubriría la demanda de mayores recursos. Fuente: Consulta del proyecto de plan plurianual para 2019-2021, entregado al Grupo Conjunto de Control Parlamentario, A 000834, 1 de febrero de 2018.

[90] *ENISA evaluation*, 2017. Entre 2014 y 2016, alrededor del 80 % del presupuesto operativo de ENISA se empleó en la contratación externa de estudios.

[91] ENISA, *Exploring the opportunities and limitations of current Threat Intelligence Platforms*, diciembre de 2017.

[92] ISACA (antes denominada «Information Systems Audit and Control Association»), *Information Security Governance: Guidance for Boards of Directors and Executive Management*, 2nd ed., 2006.

[93] EY, *Cybersecurity regained: preparing to face cyber attacks. 20th Global Information Security Survey 2017*, p. 16.

[94] McKinsey (J. Choi, J. Kaplan, C. Krishnamurthy and H. Lung), *Hit or myth? Understanding the true costs and impact of cybersecurity programs*, Julio de 2017.

[95] Securities and Exchange Commission, *Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures*, 21 de febrero de 2018.

[96] Foro de cooperación entre la Autoridad Bancaria Europea , la Autoridad Europea de Valores y Mercados y la Autoridad Europea de Seguros y Pensiones de Jubilación.

[97] Autoridad Europea de Valores y Mercados, *Joint Committee report on risks and vulnerabilities in the EU financial system*, abril de 2018.

[98] ENISA, *Information security and privacy standards for SMEs: Recommendations to improve the adoption of information security and privacy standards in SMEs*, diciembre de 2015.

[99] En referencia a los Estados miembros de la UE, el Mecanismo de Asesoramiento Científico de la Comisión ha observado el nivel sustancial y único de acuerdo sobre los principios y valores fundamentales, así como un interés estratégico que puede ser esencial para la gobernanza de ciberseguridad de la UE. Fuente: Scientific Opinion 2/2017, 24 de marzo de 2017.

[100] Estados Unidos, China, Japón, Corea del Sur, India y Brasil.

[101] Escuela Europea de Seguridad y Defensa (T. Renard and A. Barrinha), *Handbook on cyber security, chapter 3.4 The EU as a partner in cyber diplomacy and defence*, 23 de noviembre de 2018.

[102] Consejo de la Unión Europea, *Plan de acción para la aplicación de las Conclusiones del Consejo sobre la Comunicación conjunta al Parlamento Europeo y al Consejo: «Resiliencia, disuasión y defensa: Fortalecer la ciberseguridad de la UE*, 15748/17, 12 de diciembre de 2017.

[103] Comisión Europea, *European Commission Digital Strategy: A digitally transformed, user-focused and data-driven Commission*, C(2018) 7118 final, 21 de noviembre de 2018.

[104] Respuesta de la comisaria Gabriel a la pregunta parlamentaria escrita (E-004294-17) de 28 de junio de 2017.

[105] Consejo de la Unión Europea, *Annual Report on the Implementation of the Cyber Defence Policy Framework*, 15870/17, 19 de diciembre de 2017.

[106] Las Decisiones 2015/443, 2015/444 y 2017/46 regulan la seguridad de las comunicaciones y los sistemas de información de la Comisión. En la Decisión de la Comisión C(2018) 7706, de 21 de noviembre de 2018, se establece un Consejo de Tecnología de la Información y de ciberseguridad, que fusiona la anterior Junta de tecnología de la información y el antiguo comité de dirección de la seguridad de los sistemas de información.

[107] Comité Económico y Social Europeo , *ibid.*, marzo de 2018.

[108] Parlamento Europeo, *ibid*., septiembre de 2015.

[109] La Célula de Fusión de la UE contra las Amenazas Híbridas se creó en 2016 dentro del Centro de Inteligencia y de Situación de la Unión Europea del SEAE. Recibe y analiza información clasificada y de dominio público relativa a amenazas híbridas, procedente de diferentes partes interesadas.

[110] ENISA, *National-level Risk Assessments: An Analysis Report*, noviembre de 2013.

[111] European Commission, *Impact assessment on the EU Cybersecurity Agency and Cybersecurity Act*, SWD(2017) 500 final (parte 1/6), 13 de septiembre de 2017.

[112] Comisión Europea, *ibid*., SWD(2018) 403 final, 12 de septiembre de 2018.

[113] El Centro de Coordinación de la Red RIPE, registro regional de internet para Europa, que supervisa la asignación y el registro de números de registro en internet.

[114] ENISA, *EISAS Large-Scale Pilot Collaborative Awareness Raising for EU Citizens & SMEs*, noviembre de 2012.

[115] The Centre for Cyber Safety and Education, in partnership with Booz Allen Hamilton, Alta Associates and Frost & Sullivan, *2017 Global Information Security Workforce Study – Benchmarking Workforce Capacity and Response to Cyber Risk*.

[116] Comité Económico y Social Europeo , *ibid.*, marzo de 2018.

[117] House of Lords, *House of Commons Joint Committee on the National Security Strategy, Cyber Security Skills and the UK's Critical National Infrastructure, Second Report of Session 2017–19*, 16 de julio de 2018.

[118] Europol/Eurojust, *Common challenges in combatting cybercrime*, 7021/17, 13 de marzo de 2017.

[119] Europol/Eurojust, *ibid*., 7021/17, 13 de marzo de 2017.

[120] Comisión Europea, *ibid*., SWD(2018) 403 final, 12 de septiembre de 2018.

[121] CEPOL, *Decision of the Management Board 33/2018/MB on the CEPOL Single Programming Document 2020-2022*, 20 de noviembre de 2018.

[122] Por ejemplo, la cooperación entre el SEAE, los Estados miembros, las agencias y organismos tales como CEPOL, ECTEG o EESD.

[123] ENISA, *Stock-taking of information security training needs in critical sectors*, diciembre de 2017.

[124] Grupo Europeo de Formación y Educación en Ciberdelincuencia.

[125] Comisión Europea, Decimotercer informe de situación relativo a una Unión de la Seguridad genuina y efectiva, COM(2018) 46 final de 24 de enero 2018.

[126] Sobre la base de las observaciones delInforme Especial n.º 14/2018, *ibid*.

[127] Resolución del Parlamento Europeo, de 13 de junio de 2018, sobre ciberdefensa 2018/2004(INI). Consejo de la Unión Europea, *ibid*., 15870/17, 19 de diciembre de 2017.

[128] Suiza, Antigua República Yugoslava de Macedonia, Ucrania, Bosnia y Herzegovina, Kosovo (la denominación «Kosovo» se entiende sin perjuicio de las posiciones sobre su estatuto y está en consonancia con la Resolución 1244 (1999) del Consejo de Seguridad de las Naciones Unidas y con la Opinión de la Corte Internacional de Justicia sobre la declaración de independencia de Kosovo), Turquía y los Estados Unidos.

[129] Europol, *Internet Organised Crime Threat Assessment 2018*.

[130] Comisión Europea, *ibid*., SWD(2017) 295 final, 13 de septiembre de 2017.

[131] B. Stanton, M. F. Theofanos, S. S. Prettyman and S. Furman, *Security Fatigue*, "IT Professional", vol. 18, n.º 5, 2016, pp. 26 a 32. Véase asimismo NIST.

[132] Comisión Europea/Servicio Europeo de Acción Exterior, *Increasing resilience and bolstering capabilities to address hybrid threats*, JOIN (2018) 16 final, 13 de junio de 2018.

[133] Por ejemplo, el cierre de AlphaBay y Hansa en operaciones conjuntas dirigidas por el FBI y la policía nacional de los Países Bajos, con el apoyo de Europol. Estas son dos de los mayores mercados para el comercio de mercancías ilícitas como drogas, armas de fuego e instrumentos de ciberdelincuencia tales como programas maliciosos. Fuente: Europol, *Crime on the Dark Web: Law Enforcement coordination is the only cure*, Press Release, 29 de mayo de 2018.

[134] Comisión Europea, *ibid*., SWD(2018) 403 final, 12 de septiembre de 2018.

[135] Consejo de la Unión Europea, *ibid*., 12711/1/17 REV 1, 9 de octubre de 2017.

[136] Comisión Europea, *ibid*., SWD(2017) 295 final, 13 de septiembre de 2017.

[137] Comisión Europea/ Servicio Europeo de Acción Exterior, *ibid*., JOIN(2018) 16, 13 de junio de 2018.

[138] Comisión Europea, SWD(2017) 500 final, 13 de septiembre de 2017.

[139] *Memorandum of Understanding (AED, ENISA, Europol EC3 y CERT-UE)*; 23 de mayo de 2018.

[140] Comisión Europea, convocatoria de licitación: *Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap*, 27 de octubre de 2017.

[141] Jean-Claude Juncker, Mission letter for the Commissioner for the Security Union, 2 de agosto de 2016. La defensa no entra dentro del mandato del grupo.

[142] Consejo de la Unión Europea, *EU cybersecurity roadmap*, 8901/17, 11 de mayo 2017.

[143] Friends of Europe, *Debating Security Plus: Crowdsourcing solutions to the world's security issues, 5th ed.*, noviembre de 2017.

[144] JRC Technical Reports, European Cybersecurity Centres of Expertise Map: *Definitions and Taxonomy.* Impact Assessment on the proposed Research Competence Centre and the Network of National Coordination Centres, SWD(2018) 403 final, 12 de septiembre de 2018.

[145] Comisión Europea, *ibid*., SWD(2017) 295 final, 13 de septiembre de 2017.

[146] Comisión Europea, *ibid*., SWD(2018) 403 final, 12 de septiembre de 2018.

[147] Por ejemplo, el centro de puesta en común y análisis de la información de las instituciones financieras europeas cuenta con representantes del sector financiero, los CERT nacionales, la policía, ENISA, la Europol, el Banco Central Europeo, el Consejo Europeo de Pagos y la Comisión Europea.

[148] ENISA, *Information Sharing and Analysis Centres (ISACs) Cooperative models*, 14 de febrero de 2018.

[149] Consejo de la Unión Europea, *ibid*., 12711/1/17 REV 1, 9 de octubre de 2017.

[150] https://www.europol.europa.eu/empact.

[151] En un estudio realizado en 2018 por Accenture en 15 países se observó que el 87 % de los ciberataques se evitaban: *2018 State of Cyber Resilience*, 10 de abril de 2018.

[152] P. Timmers, *Cybersecurity is Forcing a Rethink of Strategic Autonomy*, Oxford University Politics Blog, 14 de septiembre de 2018.

[153] Caroline Preece, *Three reasons why cyber threat detection is still ineffective*, IT Pro, 14 de julio de 2017.

[154] Comité Económico y Social Europeo, *Ibid.*, marzo de 2018.

[155] Comisión Europea, *Octavo informe de situación relativo a una Unión de la Seguridad genuina y efectiva*, COM(2017) 354 final de 29 de junio de 2017.

[156] Véanse las distintas publicaciones del Grupo de Cooperación.

[157] Segunda Directiva sobre servicios de pago: Segunda Directiva sobre servicios de pago; BCE / MUS: Banco Central Europeo / Mecanismo Único de Supervisión; TARGET2 Sistema automatizado transeuropeo de transferencia urgente para la liquidación bruta en tiempo real (segunda generación), Reglamento 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior. Fuente: Grupo de trabajo CEPS-ECRI, *ibid*., junio de 2018.

[158] Comisión Europea, *Respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala*, C(2017) 6100 final de 13 de septiembre de 2017.

[159] Comisión Europea, *ibid*., SWD(2017) 295 final, 13 de septiembre de 2017. Existen varios mecanismos de gestión de crisis entre los que se cuenta el Dispositivo de la UE de Respuesta Política Integrada a las Crisis, ARGUS (sistema general y seguro de alerta rápida de la Comisión), el mecanismo de respuesta ante situaciones de crisis del SEAE, el Mecanismo de Protección Civil de la Unión y el Protocolo de la UE de respuesta policial ante emergencias.

[160] Además, esto puede propiciar que se invoque el artículo 42, apartado 7 del Tratado de la Unión Europea (cláusula de Asistencia Mutua) o el artículo 222 del Tratado de Funcionamiento de la Unión Europea (cláusula de solidaridad) .

[161] Comisión Europea/Servicio Europeo de Acción Exterior,, *ibid*., JOIN(2018) 16, 13 de junio de 2018. En diciembre de 2018, algunos medios de comunicación publicaron que se habían producido presentas intrusiones informáticas en la red diplomática de comunicaciones del SEAE, COREU, (fuente: *New York Times, Hacked European Cables Reveal a World of Anxiety About Trump, Russia and Iran*; 18 de diciembre de 2018). Actualmente este asunto está siendo investigado.

[162] También se necesario desarrollar más la cooperación sobre alertas tempranas y asistencia mutua: *Council Conclusions on EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises*, 10085/18, 26 de junio de 2018.

[163] Servicio de Estudios del Parlamento Europeo , *Briefing EU Legislation in Progress: ENISA and a new cybersecurity act*, PE 614.643, septiembre de 2018.

[164] Comité Económico y Social Europeo , *ibid.*, marzo de 2018.

[165] Consejo de la Unión Europea, *EU Law Enforcement Emergency Response Protocol (LE ERP) for Major Cross-Border Cyber-Attacks*, 14893/18, diciembre de 2018.

[166] Equipos de Respuesta Telemática Rápida y de Asistencia Mutua en el ámbito de la Ciberseguridad y Plataforma de Intercambio de Información sobre Respuestas a Ciberamenazas e Incidentes de Ciberseguridad. Fuente: Consejo de la Unión Europea, *Permanent Structured Cooperation (PESCO) updated list of PESCO projects – Overview*, 19 de noviembre de 2018.

[167] Consejo de la Unión Europea, Conclusiones del Consejo sobre un marco para una respuesta diplomática conjunta de la UE a las actividades informáticas malintencionada, 9916/17, 7 de junio de 2017.

[168] Consejo de la Unión Europea, *Conclusiones del Consejo sobre la ciberdiplomacia*, 6122/55, 11 de febrero de 2015.

[169] Consejo de la Unión Europea, *Draft implementing guidelines for the Framework on a Joint Diplomatic Response to Malicious Cyber Activities*, 13007/17.

[170] La atribución de responsabilidades por los incidentes sigue siendo una decisión política soberana de los Estados miembros y no todas las medidas del conjunto de instrumentos requieren atribución.

[171] El conjunto de instrumentos no llevó a una acción conjunta, sino que los Estados miembros adoptaron individualmente la posición de los Estados Unidos.

[172] Consejo de la Unión Europea, *Conclusiones del Consejo sobre la ciberdiplomacia*, 7925/18, 11 de febrero de 2015.

[173] Sistemas informáticos utilizados para los procesos de control en diversos sectores, como servicios públicos, fabricación industrial y de productos químicos, transformación alimentaria, sistemas y nudos de transporte y servicios logísticos.

[174] ENISA, *ibid*., diciembre de 2017.

[175] Por ejemplo, Administraciones Públicas, industrias química y nuclear, la fabricación, transformación alimentaria, turismo, logística y protección civil.

[176] Comisión Europea, *ibid*., SWD(2017) 295 final, 13 de septiembre de 2017.

[177] Discurso pronunciado por el comisario Jourová ante el Pleno del Parlamento Europeo *Increasing EU resilience against the influence of foreign actors on the upcoming EP election campaign*, 14 de noviembre de 2018.

[178] Carnegie Endowment for International Peace, *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks*, 23 de mayo de 2018.

[179] Centro Europeo de Estrategia Política (L. Past), Cybersecurity of Election Technology: Inevitable Attacks and Variety of Responses, in: "Election Interference in the Digital Age – Building Resilience to Cyber-Enabled Threats: A collection of think pieces of 35 leading practitioners and experts", 2018.

[180] Según la Directiva 2008/114/CE del Consejo , sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección.

[181] Comisión Europea, Recomendación sobre las redes de cooperación electoral, la transparencia en línea, la protección contra los incidentes de seguridad informática y la lucha contra las campañas de desinformación en el contexto de las elecciones al Parlamento Europeo, C(2018) 5949 final, 12 de septiembre de 2018.

[182] Conclusiones del Consejo Europeo EUCO 11/15, 20 de marzo de 2015. Desde entonces, se han añadido dos Grupos de Trabajo adicionales para los Balcanes Occidentales y la vecindad meridional de la UE.

[183] En un informe, el Consejo Atlántico pedía a la UE que pidiese a todos los Estados miembros que enviaran expertos nacionales al Grupo Operativo. Véase: D. Fried and A. Polyakova, *Democratic Defense Against Disinformation*, 5 de marzo de 2018.

[184] Aunque inicialmente carecía de presupuesto propio, en 2018 el Parlamento Europeo le concedió 1,1 millones de euros para una acción preparatoria «StratCom Plus».

[185] Carnegie Endowment for International Peace (E. Brattberg, T. Maurer), *ibid*., 23 de mayo de 2018.

[186] Comisión Europea y de la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad, *Action Plan against Disinformation*, JOIN(2018) 36 final. El plan consiste en: mejorar las capacidades de las instituciones de la UE para detectar, analizar y sacar a la luz la desinformación; reformar las respuestas coordinadas y conjuntas; movilizar al sector privado, sensibilizar y mejorar la resiliencia social.

[187] Comisión Europea, *La lucha contra la desinformación en línea: un enfoque europeo*, COM(2018) 236 final, 26 de abril de 2018.

[188] No debe confundirse con el código de conducta para luchar contra la incitación al odio ilegal en línea.

[189] JRC, *The digital transformation of news media and the rise of disinformation and fake news*, JRC Technical Reports, JRC Digital Economy Working Paper 2018-02, abril de 2018.

[190] ENISA, *Strengthening Network & Information Security & Protecting Against Online Disinformation ("Fake News"),* abril de 2018

[191] Centro Europeo de Estrategia Política Europea (C. Frutos López), *A Responsibility to Support Electoral Organisations in Anticipating and Countering Cyber Threats*, en: *ibid*, 2018.

[192] Comisión Europea, *ibid*., SWD(2018) 403 final, 12 de septiembre de 2018.

[193] La propuesta de Reglamento (COM(2017) 487 final, de 13 de septiembre de 2018) de control de la IED, presentado en septiembre de 2017, actualmente se encuentra en el proceso legislativo. En concreto, abarca las tecnologías críticas, que incluyen la inteligencia artificial, la ciberseguridad y las aplicaciones de doble uso.

[194] Comisión Europea/Servicio Europeo de Acción Exterior, *ibid*., JOIN(2017) 450 final, 13 de septiembre de 2018.

Equipo del Tribunal de Cuentas Europeo

El presente documento informativo *Desafíos de una política eficaz de ciberseguridad en la UE* fue aprobado por la Sala III, encargada de la auditoría de los ámbitos de gastos de acciones exteriores, seguridad y justicia, y presidida por Bettina Jakobsen, Miembro del Tribunal. El trabajo fue dirigido por Baudilio Tomé Muguruza, Miembro del Tribunal, con el apoyo de Daniel Costa de Magalhaes, Jefe de Gabinete, e Ignacio García de Parada, Agregado de Gabinete; Alejandro Ballester-Gallardo, Gerente Principal; Michiel Sweerts, Jefe de Tarea; Simon Dennett, Aurelia Petliza, Mirko Iaconisi, Michele Scardone y Silvia Monteiro Da Cunha, auditores, y Johannes Bolkart, becario. Hannah Critoph prestó apoyo lingüístico.

De izquierda a derecha: Ignacio García de Parada, Silvia Monteiro Da Cunha, Michele Scardone, Michiel Sweerts, Mirko Iaconisi, Baudilio Tomé Muguruza, Simon Dennett, Hannah Critoph y Daniel Costa de Magalhaes.

TRIBUNAL
DE CUENTAS
EUROPEO

Oficina de Publicaciones

TRIBUNAL DE CUENTAS EUROPEO
12, rue Alcide De Gasperi
L-1615 Luxemburgo
LUXEMBURGO

Tel. +352 4398-1

Preguntas: eca.europa.eu/es/Pages/ContactForm.aspx
Sitio web: eca.europa.eu
Twitter: @EUAuditors