COMISIÓN
EUROPEA

ALTA REPRESENTANTE DE LA
UNIÓN EUROPEA PARA
ASUNTOS EXTERIORES Y
POLÍTICA DE SEGURIDAD

Bruselas, 7.2.2013
JOIN(2013) 1 final

COMUNICACIÓN CONJUNTA AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES

Estrategia de ciberseguridad de la Unión Europea:

Un ciberespacio abierto, protegido y seguro

COMUNICACIÓN CONJUNTA AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES

Estrategia de ciberseguridad de la Unión Europea:

Un ciberespacio abierto, protegido y seguro

1. INTRODUCCIÓN

1.1. Contexto

En las dos últimas décadas, Internet y, más en general, el ciberespacio han ejercido un poderoso influjo en todos los segmentos de la sociedad. Nuestra vida cotidiana, los derechos fundamentales, las interacciones sociales y las economías dependen de tecnologías de la información y la comunicación que prestan servicios ininterrumpidos. Ha sido este ciberespacio abierto y libre el que ha promovido la integración política y social en todo el mundo; el que ha hecho caer fronteras entre países, comunidades y ciudadanos, potenciando la interacción y el intercambio de información e ideas en todo el planeta; el que se ha convertido en foro para defender la libertad de expresión y los derechos fundamentales, y el que ha permitido tomar la palabra y actuar a los ciudadanos en su lucha en pro de unas sociedades democráticas y más justas, como ocurrió, de forma espectacular, durante la Primavera Árabe.

Para que el ciberespacio siga siendo abierto y libre, deben aplicarse en línea los mismos principios, valores y normas que la UE promueve fuera de línea. Los derechos fundamentales, la democracia y el Estado de Derecho deben ser protegidos en el ciberespacio. Nuestra libertad y nuestra prosperidad dependen cada vez más de una Internet sólida e innovadora, que seguirá progresando si la innovación procedente del sector privado y la sociedad civil impulsan su crecimiento. Pero la libertad en línea requiere también protección y seguridad. El ciberespacio ha de ser protegido de incidentes, actividades malintencionadas y utilizaciones abusivas. A las administraciones públicas les corresponde un papel destacado en la custodia de un ciberespacio libre y seguro. Entre sus tareas figuran las de salvaguardar el acceso y la apertura, respetar y proteger los derechos fundamentales en línea y mantener la fiabilidad e interoperabilidad de Internet. Con todo, el sector privado posee y explota cuotas significativas de ciberespacio, por lo que toda iniciativa que pretenda alcanzar el éxito en este ámbito debe reconocer su liderazgo.

Las tecnologías de la información y la comunicación se han convertido en la piedra angular de nuestro crecimiento económico y constituyen un recurso crítico del que dependen todos los sectores económicos. Actualmente reposan en ellas los complejos sistemas que permiten funcionar a nuestras economías en sectores clave tales como las finanzas, la sanidad, la energía y los transportes. Muchos modelos empresariales se basan en la disponibilidad ininterrumpida de Internet y el buen funcionamiento de los sistemas de información.

Si se llegara a implantar el mercado único digital, Europa podría aumentar su PIB casi 500 000 millones EUR anuales[1], lo que supone una media de 1 000 EUR por persona. Para que las nuevas tecnologías conectadas —entre ellas, los pagos electrónicos, la computación en

[1] http://www.epc.eu/dsm/2/Study_by_Copenhagen.pdf

nube o la comunicación de máquina a máquina[2]—, puedan florecer, es preciso que inspiren confianza a los ciudadanos. Desafortunadamente, una encuesta del Eurobarómetro de 2012[3] mostraba que casi una tercera parte de los europeos dudaba de su capacidad para utilizar Internet en sus trámites bancarios o sus compras. Una mayoría abrumadora indicó asimismo que evitaba divulgar información personal en línea por motivos de seguridad. En toda la UE, más de uno de cada diez usuarios de Internet ha sido ya víctima de un fraude en línea.

En los últimos años se ha comprobado que el mundo digital aporta grandes beneficios, pero que también es vulnerable. Los incidentes de ciberseguridad[4], tanto deliberados como accidentales, están incrementándose a un ritmo alarmante y podrían llegar a perturbar el suministro de servicios esenciales que damos por descontados como el agua, la asistencia sanitaria, la electricidad o los servicios móviles. Las amenazas pueden tener varios orígenes, entre ellos los ataques delictivos, por motivos políticos, terroristas o patrocinados por los Estados, así como catástrofes naturales o errores no intencionados.

La economía de la UE se ve ya afectada por actividades de ciberdelincuencia[5] contra el sector privado y las personas. Los ciberdelincuentes recurren a métodos cada vez más complejos para introducirse en los sistemas de información, sustraer datos críticos o exigir rescates a las empresas. El aumento del espionaje económico y de las actividades alentadas por los Estados en el ciberespacio representa una nueva categoría de amenaza para las administraciones públicas y empresas de la UE.

Asimismo, las autoridades de terceros países pueden emplear abusivamente el ciberespacio para ejercer vigilancia y control sobre sus propios ciudadanos. La UE puede contrarrestar esta situación fomentando la libertad en línea y velando por el respeto de los derechos fundamentales en la red.

Todos estos factores explican que los Gobiernos de todo el mundo hayan comenzado a desarrollar estrategias de ciberseguridad y a considerar el ciberespacio un asunto internacional cada vez más importante. Ha llegado el momento de que la UE intensifique su intervención en este ámbito. La estrategia de ciberseguridad de la Unión Europea que se propone, presentada por la Comisión y la Alta Representante de la Unión Europea para Asuntos Exteriores y Política de Seguridad (Alta Representante), expone la visión de la UE en este campo, aclara funciones y responsabilidades y establece las medidas necesarias, basadas en una protección y una promoción amplias y efectivas de los derechos de los ciudadanos con el fin de que el entorno en línea de la UE llegue a ser el más seguro del mundo.

---

2 Por ejemplo, plantas en las que se han insertado sensores que indican al sistema de aspersión cuándo hay que regar.

3 Eurobarómetro especial 390 sobre ciberseguridad, 2012.

4 La ciberseguridad abarca por lo general las salvaguardias y medidas que pueden utilizarse para proteger el ciberespacio, en los ámbitos tanto civil como militar, de las amenazas inherentes a sus redes interdependientes e infraestructuras de información, o que pueden dañarlas. La ciberseguridad tiene como objetivo mantener la disponibilidad e integridad de las redes e infraestructuras y la confidencialidad de la información que contienen.

5 La ciberdelincuencia abarca por lo general una amplia gama de actividades delictivas en las que los ordenadores y los sistemas de información se utilizan como principales herramientas para delinquir o son objeto principal del delito. La ciberdelincuencia comprende delitos tradicionales (por ejemplo, fraude, falsificación o 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, denegación de servicio o programas maliciosos).

1.2. Principios de ciberseguridad

La Internet sin fronteras y con múltiples niveles se ha convertido en uno de los instrumentos más poderosos del progreso mundial, sin la tutela ni la reglamentación de los Estados. El sector privado debería seguir liderando la construcción y la gestión cotidiana de Internet, pero también hay que tener en cuenta que los requisitos en materia de transparencia, rendición de cuentas y seguridad están adquiriendo cada vez mayor importancia. La presente estrategia aclara los principios que han de presidir la política de ciberseguridad tanto en la UE como a escala internacional.

Los valores esenciales de UE lo son tanto en el mundo físico como en el digital

Las leyes y normas aplicables en otros ámbitos de nuestras vidas cotidianas lo son también en el ciberespacio.

Protección de los derechos fundamentales, la libertad de expresión, los datos personales y la intimidad

La ciberseguridad solo puede resultar positiva y eficaz si se basa en los derechos fundamentales y las libertades enunciados en la Carta de los Derechos Fundamentales de la Unión Europea y en los valores esenciales de la UE. Por su parte, los derechos individuales no pueden protegerse sin redes y sistemas seguros. Todo intercambio de información a efectos de ciberseguridad en que se manejen datos personales debe cumplir la normativa de protección de datos de la UE y tomar plenamente en consideración los derechos de las personas en este ámbito.

Acceso para todos

Un acceso limitado o nulo a Internet y el analfabetismo digital constituyen una desventaja para los ciudadanos, dada la omnipresencia del mundo digital en las actividades que se desarrollan en nuestra sociedad. Todos los ciudadanos deberían poder acceder a Internet y a un flujo de información libre de trabas. Deben garantizarse la integridad y la seguridad de Internet para así hacer posible un acceso seguro para todos.

Gobernanza multilateral democrática y eficaz

El mundo digital no está controlado por una sola entidad. Actualmente intervienen en él varias partes, muchas de las cuales son entidades comerciales y no gubernamentales que participan en la gestión diaria de los recursos, protocolos y normas de Internet y en su futuro desarrollo. La UE reafirma la importancia de todas las partes interesadas en el actual modelo de gobernanza de Internet y respalda este planteamiento de gobernanza multilateral[6].

Garantizar la seguridad: una responsabilidad compartida

La creciente dependencia de las tecnologías de la información y de las comunicaciones en todas las esferas de la vida humana ha hecho surgir una serie de puntos vulnerables que es preciso delimitar debidamente, analizar exhaustivamente, subsanar o atenuar. Todas las partes interesadas, ya sean las administraciones públicas, el sector privado o los ciudadanos, han de reconocer esta responsabilidad compartida, tomar medidas para protegerse y, en caso necesario, ofrecer una respuesta coordinada para reforzar la ciberseguridad.

[6] Véase asimismo COM(2009) 277, Comunicación de la Comisión al Parlamento Europeo y al Consejo, *La gobernanza de Internet: los próximos pasos.*

2. PRIORIDADES Y MEDIDAS ESTRATÉGICAS

La UE debería defender un entorno en línea que ofreciese el mayor grado posible de libertad y seguridad en beneficio de todos. Aun reconociendo que corresponde ante todo a los Estados miembros hacerse cargo de los problemas de seguridad del ciberespacio, la presente estrategia propone medidas concretas que pueden mejorar los resultados generales de la UE en este campo. Se trata de medidas a corto y largo plazo que recurren a diversos instrumentos de actuación[7] y requieren la participación de diversos tipos de agentes, entre ellos las instituciones de la UE, los Estados miembros o las empresas.

La visión de la UE que se presenta en esta estrategia se articula en torno a cinco prioridades estratégicas para resolver los problemas antes esbozados:

- Lograr la ciberresiliencia
- Reducir drásticamente la ciberdelincuencia
- Desarrollar estrategias y capacidades de ciberdefensa vinculadas a la Política Común de Seguridad y Defensa (PCSD)
- Desarrollar recursos industriales y tecnológicos de ciberseguridad
- Establecer una política internacional coherente del ciberespacio para la Unión Europea y promover los valores esenciales de la UE.

2.1. Lograr la ciberresiliencia

Para impulsar la ciberresiliencia en la UE, tanto las administraciones públicas como el sector privado deben desarrollar capacidades y cooperar efectivamente. Sobre la base de los positivos resultados conseguidos en las actividades realizadas hasta la fecha[8], las nuevas actuaciones de la UE pueden facilitar, en particular, la lucha contra los riesgos y amenazas cibernéticos que tienen una dimensión transfronteriza y contribuir a una respuesta coordinada en situaciones de emergencia. Con ello se apoyará firmemente el buen funcionamiento del mercado interior y se incrementará la seguridad interna de la UE.

Europa seguirá siendo vulnerable si no se dedican considerables esfuerzos a impulsar las capacidades, recursos y procedimientos públicos y privados para prevenir, detectar y gestionar los incidentes de ciberseguridad. Por ello, la Comisión ha desarrollado una política de seguridad de las redes y de la información (SRI)[9]. En 2004 se creó **la Agencia Europea de Seguridad de las Redes y de la Información (ENISA)**[10] y en estos momentos el Consejo y el Parlamento están negociando un nuevo Reglamento para consolidarla y modernizar su mandato[11]. Además, la Directiva marco sobre las comunicaciones electrónicas[12] exige que los

---

7 Las medidas relativas al intercambio de información en que se manejen datos personales deben cumplir la normativa de protección de datos de la UE.

8 Véanse referencias en la presente Comunicación, así como en la evaluación de impacto que figura en el documento de trabajo de los servicios de la Comisión adjunto a la propuesta de Directiva de la Comisión relativa a la seguridad de las redes y la información, y en particular, las secciones 4.1.4 y 5.2, y los anexos 2, 6 y 8.

9 En 2001, la Comisión adoptó la Comunicación titulada *Seguridad de las redes y de la información: Propuesta para un enfoque político europeo* [COM(2001)298]; en 2006, adoptó una estrategia para una sociedad de la información segura [COM(2006)251]. Desde 2009, la Comisión también ha adoptado un plan de acción y una Comunicación sobre protección de infraestructuras críticas de información (PICI) [COM(2009)149, aprobado por la Resolución 2009/C 321/01 del Consejo, y COM(2011)163, aprobado por las conclusiones 10299/11 del Consejo].

10 Reglamento (CE) nº 460/2004.

11 COM(2010)521. Las medidas propuestas en la presente estrategia no entrañan la modificación del mandato actual o futuro de la ENISA.

12 Artículos 13 *bis* y 13 *ter* de la Directiva 2002/21/CE.

proveedores de comunicaciones electrónicas gestionen adecuadamente los riesgos a que se enfrentan sus redes y notifiquen las violaciones significativas de la seguridad. Asimismo, la normativa de la UE sobre protección de datos[13] establece que los responsables del tratamiento han de prever requisitos y salvaguardias que garanticen la protección de los datos, entre ellos medidas de seguridad, y, en el ámbito de los servicios de comunicaciones electrónicas disponibles para el público, los responsables del tratamiento están obligados a notificar incidentes que entrañen una violación de los datos personales a las autoridades nacionales competentes.

Pese a los avances logrados gracias a los compromisos voluntarios, aún se observan ciertas lagunas en la UE, especialmente en lo tocante a las capacidades nacionales, la coordinación ante incidentes que traspasan las fronteras, y la preparación y participación del sector privado. Adjunta a la presente estrategia figura una propuesta de **acto legislativo** cuyos principales objetivos son los siguientes:

- Establecer requisitos mínimos comunes de SRI a escala nacional que obligarían a los Estados miembros a designar autoridades nacionales competentes en materia de SRI, crear un CERT y velar por su correcto funcionamiento, y adoptar una estrategia nacional de SRI y un plan nacional de cooperación en materia de SRI. También corresponde a las instituciones de la UE velar por la capacitación y la coordinación: en 2012 se creó con carácter permanente un equipo de respuesta a emergencias informáticas, responsable de la seguridad de los sistemas de TI de las instituciones, agencias y organismos de la UE («CERT-UE»).
- Establecer mecanismos coordinados de prevención, detección, respuesta y atenuación que hagan posible el intercambio de información y la asistencia mutua entre las autoridades nacionales competentes en materia de SRI. Se instará a dichas autoridades a velar por una cooperación apropiada a escala de la UE sobre la base de un plan de cooperación de la Unión en materia de SRI, destinado a responder a los ciberincidentes de dimensión transfronteriza. Esta cooperación también sacará partido de los avances logrados en el Foro Europeo de Estados Miembros (EFMS)[14], que ha mantenido debates e intercambios muy fructuosos sobre la política de SRI y puede integrarse en el mecanismo de cooperación que se cree.
- Aumentar la preparación y el compromiso del sector privado. Dado que la titularidad y la explotación de la gran mayoría de las redes y los sistemas de información están en manos del sector privado, resulta crucial conseguir que dicho sector contribuya con mayor empeño a fomentar la ciberseguridad. Es conveniente que el sector privado desarrolle a nivel técnico sus propias capacidades de ciberresiliencia y comparta mejores prácticas con otros sectores. Los instrumentos creados por ese sector para responder a los incidentes, determinar sus causas y efectuar investigaciones forenses también deberían beneficiar al sector público.

No obstante, los agentes privados aún carecen de incentivos efectivos para proporcionar datos fidedignos sobre la existencia o las consecuencias de los incidentes de SRI, adoptar una cultura de gestión de riesgos o invertir en soluciones de seguridad. La normativa propuesta pretende, pues, asegurarse de que los agentes de una serie de sectores esenciales (energía, transportes, banca, bolsas y facilitadores de servicios clave de Internet, así como

[13] Artículo 17 de la Directiva 95/46/CE; artículo 4 de la Directiva 2002/58/CE.

[14] El Foro Europeo de Estados Miembros se creó mediante la Comunicación COM(2009) 149 como plataforma para fomentar el debate entre las administraciones públicas de los Estados miembros en relación con las buenas prácticas en materia de seguridad y resiliencia de las infraestructuras críticas de información.

administraciones públicas) evalúen los riesgos de ciberseguridad a que se enfrentan, garanticen que las redes y los sistemas de información son fiables y resilientes mediante la debida gestión de los riesgos, y compartan la información obtenida con las autoridades nacionales competentes en materia de SRI. La implantación de una cultura de ciberseguridad puede fomentar las oportunidades empresariales y la competitividad en el sector privado, lo cual podría hacer de la ciberseguridad un buen argumento de venta.

Esas entidades tendrían que notificar a las autoridades nacionales competentes en materia de SRI los incidentes que tuvieran efectos significativos en la continuidad de servicios básicos y el suministro de mercancías dependientes de las redes y los sistemas de información.

Las autoridades nacionales competentes en materia de SRI deben colaborar e intercambiar información con otros organismos reguladores y, en especial, con las autoridades responsables de la protección de datos personales. Las autoridades competentes en materia de SRI deberían, a su vez, notificar los incidentes de carácter supuestamente delictivo a las fuerzas de seguridad. Asimismo, las autoridades nacionales competentes deberían publicar periódicamente en un sitio web específico información no confidencial acerca de las alertas tempranas en curso sobre incidentes y riesgos y sobre respuestas coordinadas. Las obligaciones legales no reemplazan ni se oponen al desarrollo de lazos informales y voluntarios de cooperación, también entre los sectores público y privado, a fin de aumentar los niveles de seguridad e intercambiar información y mejores prácticas. Más concretamente, la Asociación público-privada europea de resiliencia (EP3R[15]) constituye una plataforma sólida y valiosa a escala de la UE y es conveniente potenciarla.

El Mecanismo «Conectar Europa» (MCE)[16] prestaría ayuda financiera para infraestructuras clave, aunando las capacidades de SRI de los Estados miembros y facilitando, por ende, la cooperación en toda la UE.

Por último, los ejercicios de simulación de ciberincidentes a escala de la UE son fundamentales para estimular la cooperación entre los Estados miembros y el sector privado. El primer ejercicio en que participaron los Estados miembros se desarrolló en 2010 (CiberEuropa 2010) y el segundo ejercicio, en el que también participó el sector privado, tuvo lugar en octubre de 2012 (CiberEuropa 2012). En noviembre de 2011 se organizó un ejercicio teórico de simulación UE-EE.UU. (CiberAtlántico 2011). En los próximos años están previstos nuevos ejercicios, en los que participarán socios internacionales.

La Comisión:

- proseguirá sus actividades, llevadas a cabo por el Centro Común de Investigación en estrecha colaboración con las autoridades de los Estados miembros y los titulares y operadores de infraestructuras críticas, con el fin de determinar los puntos vulnerables para la SRI de las infraestructuras críticas europeas e impulsar el desarrollo de sistemas resilientes;

[15] La Asociación público-privada europea de resiliencia se presentó en la Comunicación COM(2009) 149. Esta plataforma ha comenzado su labor fomentando la cooperación entre los sectores público y privado en torno a la determinación de los principales activos, recursos, funciones y requisitos básicos para garantizar la resiliencia, así como de las necesidades y mecanismos de cooperación precisos para responder a perturbaciones de gran alcance de las comunicaciones electrónicas.

[16] https://ec.europa.eu/digital-agenda/en/connecting-europe-facility. MCE Línea presupuestaria 09.03.02 – Redes de telecomunicaciones (promover la interconexión y la interoperabilidad de los servicios públicos nacionales en línea, así como el acceso a estas redes).

- pondrá en marcha a principios de 2013 un proyecto piloto financiado por la UE[17] sobre lucha contra **las redes infectadas y los programas maliciosos,** que ofrecerá un marco de coordinación y cooperación entre los Estados miembros de la UE, las organizaciones del sector privado tales como los proveedores de servicios de Internet y los socios internacionales.

La Comisión insta a la ENISA a:

- ayudar a los Estados miembros a crear **capacidades nacionales sólidas de ciberresiliencia** mediante la adquisición de conocimientos sobre la seguridad y la resiliencia de los sistemas de control industrial, los transportes y las infraestructuras de energía;
- examinar en 2013 la viabilidad del equipo de respuesta a incidentes de seguridad informática en sistemas de control industrial (ICS-CSIRT) de la UE;
- seguir apoyando a los Estados miembros y a las instituciones de la UE en la realización de **ejercicios** periódicos **paneuropeos de simulación de ciberincidentes**, que también constituirán la base operativa para la participación de la UE en ejercicios internacionales de este tipo.

La Comisión invita al Parlamento Europeo y al Consejo a:

- **adoptar** rápidamente la propuesta de Directiva referente a **un elevado nivel común de seguridad de las redes y de la información (SRI)** en toda la Unión, que aborda la capacitación y preparación a escala nacional, la cooperación a escala de la UE, la implantación de prácticas de gestión de riesgos y el intercambio de información sobre SRI.

La Comisión insta a la industria a:

- asumir el liderazgo e **invertir** en un elevado nivel de ciberseguridad, desarrollar mejores prácticas e intercambiar la información a escala sectorial y con las administraciones públicas para así garantizar una protección adecuada y efectiva de bienes y personas, en particular a través de asociaciones público-privadas como la EP3R y *Trust in Digital Life* (TDL)[18].

Concienciación

Velar por la ciberseguridad es una responsabilidad común. Los usuarios finales contribuyen de forma decisiva a garantizar la seguridad de las redes y los sistemas de información: es preciso que sean conscientes de los riesgos que corren en línea y sean capaces de adoptar medidas sencillas para protegerse de ellos.

En los últimos años se han tomado en este ámbito varias iniciativas, que deben continuar. En particular, la ENISA ha participado en labores de concienciación mediante la publicación de informes, la organización de talleres especializados y la creación de asociaciones público-privadas. Europol, Eurojust y las autoridades nacionales responsables de la protección de datos también intervienen en esas actividades de concienciación. En octubre de 2012, la ENISA y algunos Estados miembros patrocinaron el Mes Europeo de la Ciberseguridad. La

[17] CIP-ICT PSP-2012-6, 325188. El proyecto tiene un presupuesto global de 15 millones EUR, al que la UE contribuye con 7,7 millones EUR.

[18] http://www.trustindigitallife.eu/.

concienciación es una de las cuestiones abordadas por el Grupo de Trabajo UE-EE.UU. sobre Ciberseguridad y Ciberdelincuencia[19], y también es importante en el contexto del Programa «Una Internet más Segura»[20] (centrado en la seguridad de los niños en línea).

La Comisión pide a la ENISA que:

- proponga en 2013 orientaciones con respecto a un «permiso de conducción en el ámbito de la seguridad de las redes y la información», consistente en un programa de certificación voluntario que promueva la mejora de los conocimientos y competencias de los profesionales de las TI (por ejemplo, administradores de sitios web).

La Comisión:

- organizará en 2014, asistida por la ENISA, **un campeonato** de ciberseguridad entre los estudiantes universitarios, que competirán proponiendo soluciones de SRI.

La Comisión invita a los Estados miembros[21] a:

- organizar anualmente a partir de 2013 **un mes de la ciberseguridad** con el apoyo de la ENISA y la participación del sector privado, con el propósito de concienciar a los usuarios finales; a partir de 2014 se organizará un mes de la ciberseguridad sincronizado en los EE.UU. y la UE.
- **redoblar esfuerzos de educación y formación en materia de SRI,** integrando la formación en SRI en los centros escolares desde 2014; impartiendo formación en SRI, desarrollo de programas informáticos seguros y protección de datos personales entre los estudiantes de informática; y ofreciendo formación básica en SRI al personal de las administraciones públicas.

La Comisión invita a la industria a:

- **informar sobre la importancia** de la ciberseguridad **en todos los niveles**, tanto en las prácticas comerciales como en la interfaz con los consumidores; más concretamente, las empresas deberían estudiar la manera de hacer más responsables de la ciberseguridad a sus directores generales y consejos de administración.

2.2. Reducción drástica de la ciberdelincuencia

Cuanto más nos adentramos en el mundo digital, más oportunidades ofrecemos a los ciberdelincuentes. La ciberdelincuencia es una de las formas de delincuencia de crecimiento

[19] Este Grupo de Trabajo, creado en la Cumbre UE-EE.UU. de noviembre de 2010 (MEMO/10/597), se encarga de desarrollar planteamientos colaborativos con respecto a una amplia gama de cuestiones relacionadas con la ciberseguridad y la ciberdelincuencia.

[20] El programa «Una Internet más Segura» financia una red de ONG que promueven el bienestar de los niños en línea, una red de cuerpos de seguridad que intercambian información y mejores prácticas sobre la explotación delictiva de Internet mediante la difusión de material sobre abusos sexuales a menores y una red de investigadores que recopilan información sobre usos, riesgos y consecuencias de las tecnologías en línea en las vidas de los menores.

[21] Con la participación de las autoridades nacionales competentes, entre ellas las responsables de la SRI y de la protección de datos.

más rápido, con más de un millón de víctimas diarias en todo el mundo. Los ciberdelincuentes y las redes de ciberdelincuencia se perfeccionan cada vez más y tenemos que disponer de las herramientas y capacidades operativas idóneas para hacerles frente. Los ciberdelitos son actividades de bajo riesgo que generan grandes beneficios y los delincuentes se aprovechan a menudo del anonimato de los dominios de los sitios web. La ciberdelincuencia no conoce fronteras y, habida cuenta del alcance mundial de Internet, los cuerpos de seguridad deben adoptar un enfoque transfronterizo coordinado y colaborativo para responder a esta amenaza creciente.

Normativa estricta y eficaz

La UE y los Estados miembros necesitan una normativa rigurosa y eficaz para luchar contra la ciberdelincuencia. El Convenio sobre la Ciberdelincuencia del Consejo de Europa, también denominado Convenio de Budapest, es un tratado internacional vinculante que ofrece un marco efectivo para la adopción de normas nacionales.

La UE ya ha adoptado actos legislativos sobre la ciberdelincuencia, entre ellos una Directiva relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil[22]. Asimismo, la UE tiene previsto adoptar en breve una Directiva relativa a los ataques contra los sistemas de información, especialmente mediante el uso de redes infectadas.

La Comisión:

- velará por que se transpongan y apliquen rápidamente las directivas relacionadas con la ciberdelincuencia;
- emplazará a los Estados miembros que aún no hayan ratificado el **Convenio sobre la Ciberdelincuencia del Consejo de Europa** para que lo hagan y apliquen sus disposiciones lo antes posible.

Mayor capacidad operativa para luchar contra la ciberdelincuencia

Las técnicas de que se sirven los ciberdelincuentes evolucionan velozmente y los cuerpos de seguridad no pueden luchar contra este fenómeno con medios operativos obsoletos. Hoy en día, no todos los Estados miembros de la UE disponen de la capacidad operativa necesaria para combatir la ciberdelincuencia con eficacia. Es preciso que todos ellos cuenten con unidades nacionales especializadas en la lucha contra la ciberdelincuencia.

La Comisión:

- ayudará a los Estados miembros, a través de sus programas de financiación[23], a **detectar insuficiencias y a reforzar su capacidad** para investigar y combatir la ciberdelincuencia; además, prestará apoyo a los organismos que ponen en contacto a los mundos académico y de la investigación, a los profesionales de los cuerpos de seguridad y al sector privado, inspirándose en las actividades que llevan a cabo los centros de excelencia de ciberdelincuencia financiados por la

[22] Directiva 2011/93/UE, que sustituye la Decisión Marco 2004/68/JAI del Consejo.

[23] En 2013, en el marco del Programa «Prevención y lucha contra la delincuencia» (ISEC). A partir de 2013, en el marco del Fondo de Seguridad Interior (nuevo instrumento del MFP).

Comisión, ya creados en algunos Estados miembros;

- junto con los Estados miembros, coordinará los esfuerzos para determinar, con el apoyo del JRC, las mejores prácticas y técnicas disponibles para luchar contra la ciberdelincuencia (por ejemplo, en relación con el diseño y uso de herramientas forenses o con el análisis de amenazas);
- colaborará estrechamente con el **Centro Europeo de Ciberdelincuencia (EC3),** recién creado **en el marco de Europol, y con Eurojust** para adecuar estos enfoques a las mejores prácticas desde el punto de vista operativo.

Mayor coordinación en la UE

La UE puede completar el trabajo de los Estados miembros proponiendo un enfoque coordinado y colaborativo, y reuniendo a las autoridades policiales y judiciales, así como a las partes interesadas de los sectores público y privado de la UE y del exterior.

La Comisión:

- apoyará al recién creado **Centro Europeo de Ciberdelincuencia** (EC3) como centro de referencia en la lucha contra la ciberdelincuencia; el EC3 proporcionará análisis e información, respaldará las investigaciones, aportará conocimientos forenses de alto nivel, facilitará la cooperación, creará canales de intercambio de información entre las autoridades competentes de los Estados miembros, el sector privado y otras partes interesadas, y se convertirá progresivamente en portavoz de la comunidad de cuerpos de seguridad[24];
- respaldará los esfuerzos por incrementar la responsabilidad de los registradores de nombres de dominio y velará por la exactitud de la información sobre los titulares de sitios web, especialmente sobre la base de las recomendaciones de los cuerpos de seguridad a la Corporación de Internet para la Asignación de Nombres y Números (ICANN), de conformidad con la normativa de la Unión y, en particular, las normas sobre protección de datos;
- se basará en la normativa reciente para redoblar los esfuerzos de la UE contra el abuso sexual de menores en línea. La Comisión ha adoptado una estrategia europea en favor de una Internet más adecuada para los niños[25] y, junto con los Estados miembros y terceros países, ha creado una **Alianza Mundial contra el abuso sexual de menores en línea[26]**. Dicha Alianza impulsará nuevas medidas de los Estados miembros con el apoyo de la Comisión y el EC3.

La Comisión pide a Europol (EC3) que:

- centre inicialmente su apoyo analítico y operativo en las investigaciones sobre ciberdelincuencia de los Estados miembros con el fin de desmantelar y desbaratar

[24] El 28 de marzo de 2012, la Comisión Europea adoptó la Comunicación *La represión del delito en la era digital: creación de un centro europeo de ciberdelincuencia.*

[25] COM(2012) 196 final.

[26] Conclusiones del Consejo sobre una Alianza Mundial contra el abuso sexual de menores en línea (Declaración conjunta UE-EE.UU.) de 7 y 8 de junio de 2012, y Declaración sobre la creación de la Alianza Mundial contra el abuso sexual de menores en línea (http://europa.eu/rapid/press-release_MEMO-12-944_en.htm).

las redes de ciberdelincuencia, sobre todo en los ámbitos del abuso sexual de menores, los fraudes en los pagos, las redes infectadas y la intrusión;

- elabore periódicamente informes estratégicos y operativos sobre tendencias y amenazas incipientes a fin de determinar prioridades y centrar las actividades de investigación de los equipos de ciberdelincuencia de los Estados miembros.

La Comisión solicita a la Escuela Europea de Policía (CEPOL) que coopere con Europol a fin de:

- coordinar la preparación y planificación de cursos de formación que faciliten a los cuerpos de seguridad los conocimientos especializados necesarios para hacer frente a la ciberdelincuencia con eficacia.

La Comisión pide a Eurojust que:

- determine los principales obstáculos a la cooperación judicial en investigaciones de ciberdelincuencia y a la coordinación entre los Estados miembros y con terceros países, y apoye la investigación y represión de ciberdelitos a nivel operativo y estratégico, así como las actividades de formación en este ámbito.

La Comisión solicita a Eurojust y a Europol (EC3) que:

- cooperen estrechamente e intercambien información para ser más eficaces en la lucha contra la ciberdelincuencia, de acuerdo con sus respectivos mandatos y competencias.
-

2.3. Desarrollo de una política y de capacidades de ciberdefensa en el marco de la Política Común de Seguridad y Defensa (PCSD)

Los esfuerzos de ciberseguridad de la UE entrañan asimismo una dimensión de ciberdefensa. Para aumentar la resiliencia de los sistemas de comunicación e información que amparan los intereses de los Estados miembros en materia de defensa y seguridad nacional, el desarrollo de capacidades de ciberdefensa debería concentrarse en la detección, respuesta y recuperación frente a complejas ciberamenazas.

Ante tan polifacéticas amenazas, conviene potenciar las sinergias entre los enfoques civil y militar para la protección de ciberactivos críticos. Estos esfuerzos se han de apoyar con actividades de investigación y desarrollo y una mayor cooperación entre las administraciones públicas, el sector privado y la comunidad académica de la UE. Para evitar duplicaciones, la UE examinará de qué modo pueden ella y la OTAN aunar sus esfuerzos para aumentar la resiliencia de infraestructuras críticas públicas, de defensa y de información de las que dependen los miembros de ambas organizaciones.

La Alta Representante centrará su atención en las siguientes actividades clave e invitará a los Estados miembros y a la Agencia Europea de Defensa a colaborar en ellas:

- Evaluar los requisitos operativos de ciberdefensa de la UE y promover el desarrollo de sus capacidades y tecnologías de ciberdefensa en todos sus aspectos: doctrina, liderazgo, organización, personal, formación, tecnología, infraestructuras, logística e interoperabilidad.

- Elaborar un marco político de ciberdefensa de la UE para proteger las redes dentro de las misiones y operaciones de la PCSD, especialmente a través de la gestión dinámica de riesgos, la mejora del análisis de amenazas y el intercambio de información. Ofrecer mayores posibilidades al ejército para formarse y adiestrarse en el contexto europeo e internacional, incluyendo aspectos de ciberdefensa en los actuales manuales de ejercicios.

- Promover el diálogo y la coordinación entre las esferas civil y militar de la UE, haciendo especial hincapié en el intercambio de buenas prácticas, el intercambio de información y la alerta temprana, la respuesta a incidentes, la evaluación de riesgos, la concienciación y y la consideración de la ciberseguridad como objetivo prioritario.

- Garantizar el diálogo con los socios internacionales, entre ellos la OTAN, otras organizaciones internacionales y centros de excelencia plurinacionales con el fin de conseguir auténticas capacidades de defensa, determinar las áreas de cooperación y evitar la duplicación de esfuerzos.

2.4. Desarrollo de recursos industriales y tecnológicos de ciberseguridad

Europa dispone de excelentes capacidades de investigación y desarrollo, pero muchas de las empresas punteras mundiales proveedoras de productos y servicios de TIC innovadores están establecidas fuera de la UE. Europa corre el riesgo de depender excesivamente no solo de las TIC producidas en terceros países, sino también de las soluciones de seguridad desarrolladas fuera de sus fronteras. Es esencial velar por que los equipos y programas informáticos producidos en la UE y en terceros países que se utilizan en infraestructuras y servicios críticos —y cada vez más en dispositivos móviles— sean fiables y seguros y garanticen la protección de los datos personales.

Fomento de un mercado único de productos de ciberseguridad

Solo es posible garantizar un nivel elevado de seguridad si todos los que intervienen en la cadena de valor (fabricantes de equipos, desarrolladores de programas informáticos, proveedores de servicios de la sociedad de la información, etc.) hacen de la seguridad un objetivo prioritario. Parece ser[27], empero, que muchos de ellos siguen considerando que la seguridad es poco más que una carga suplementaria y prueba de ello es la limitada demanda de soluciones de seguridad. Es necesario establecer requisitos apropiados de eficacia en materia de ciberseguridad y aplicarlos en toda la cadena de valor de los productos de TIC utilizados en Europa. Hay que ofrecer al sector privado incentivos para garantizar un elevado nivel de ciberseguridad; así, por ejemplo, unas etiquetas que indiquen que los resultados en materia de ciberseguridad son adecuados permitirán a las empresas con buenos resultados e historial en este campo presentar argumentos de venta positivos respecto del producto y disfrutar de una ventaja competitiva. Asimismo, las obligaciones establecidas en la Directiva sobre SRI propuesta contribuirían significativamente a potenciar la competitividad de las empresas en los sectores regulados.

Por otra parte, conviene fomentar una demanda de mercado europea de productos de alta seguridad. En primer lugar, esta estrategia tiene por objetivo aumentar la cooperación y la transparencia en lo que respecta a la seguridad de los productos de las TIC. Aboga por la creación de una plataforma que reúna a las partes interesadas europeas, tanto del sector

[27] Véase la evaluación de impacto que figura en el documento de trabajo de los servicios de la Comisión adjunto a la propuesta de Directiva de la Comisión relativa a la seguridad de las redes y la información, sección 4.1.5.2.

público como del privado, con el fin de determinar buenas prácticas de ciberseguridad en toda la cadena de valor y crear condiciones de mercado favorables para el desarrollo y adopción de de soluciones de TIC seguras. Es importante ofrecer incentivos para realizar una gestión de riesgos adecuada y adoptar normas y soluciones de seguridad, así como, en su caso, establecer regímenes de certificación voluntarios en la UE, que se basarían en los regímenes existentes a escala europea e internacional. La Comisión fomentará la adopción de planteamientos coherentes entre los Estados miembros para evitar disparidades que les supongan desventajas de localización a las empresas.

En segundo lugar, la Comisión respaldará la elaboración de normas de seguridad y prestará asistencia en los regímenes de certificación voluntarios en el campo de la computación en nube, teniendo muy presente la necesidad de asegurar la protección de datos. El trabajo se debería centrar en la seguridad de la cadena de suministro, especialmente en los sectores económicos críticos (sistemas de control industrial, energía e infraestructuras de transportes). Dicho trabajo se debería inspirar en las actividades de normalización en curso de las organizaciones europeas de normalización (CEN, CENELEC y ETSI)[28], del Grupo de Coordinación de Ciberseguridad (CSCG), así como en los conocimientos y experiencia de la ENISA, la Comisión y otras partes interesadas.

La Comisión:

- creará en 2013 **una plataforma** público-privada **sobre soluciones de SRI** con el fin de impulsar la adopción de soluciones seguras de TIC y la adopción de requisitos de eficacia en materia de ciberseguridad que se apliquen a todos los productos de las TIC utilizados en Europa;
- propondrá en 2014 una serie de recomendaciones, basadas en los trabajos de dicha plataforma, para garantizar la ciberseguridad en la cadena de valor de las TIC;
- examinará cómo pueden los principales proveedores de equipos y programas informáticos de TIC informar a las autoridades nacionales competentes de los puntos vulnerables detectados que puedan tener efectos significativos en la seguridad.

La Comisión pide a la ENISA que:

- elabore, en cooperación con las autoridades nacionales competentes, las partes interesadas, los organismos europeos e internacionales de normalización y el Centro Común de Investigación de la Comisión Europea, **directrices y recomendaciones técnicas para la adopción de normas y buenas prácticas de SRI** en los sectores público y privado.

La Comisión invita a las partes interesadas de los sectores público y privado a:

- fomentar la elaboración y adopción, a iniciativa de la industria, de **normas de seguridad**, normas técnicas y principios de seguridad por diseño y privacidad por diseño por parte de los fabricantes de productos de TIC y proveedores de servicios, entre ellos los proveedores de servicios en nube; los equipos y programas informáticos de nueva generación deberán disponer de elementos de seguridad **más sólidos, integrados y de fácil utilización;**

[28] En particular, en relación con la norma M/490 sobre redes inteligentes para la primera serie de normas sobre redes inteligentes y arquitectura de referencia.

- elaborar, a iniciativa de la industria, normas sobre los resultados de las empresas en materia de ciberseguridad y proporcionar más información al público diseñando **etiquetas de seguridad** o marchamos de calidad que ayuden al consumidor a orientarse en el mercado.

Fomento de la inversión en I+D y de la innovación

La I+D puede respaldar una política industrial sólida, promover un sector europeo de las TIC fiable, impulsar el mercado interior y reducir la dependencia de Europa respecto de las tecnologías extranjeras. La I+D debe colmar las lagunas tecnológicas que comprometen la seguridad de las TIC, prever los problemas de seguridad que puedan plantearse en el futuro, tener en cuenta la constante evolución de las necesidades de los usuarios y sacar partido de las tecnologías de doble uso. También debería seguir apoyando el desarrollo de la criptografía. Todo ello ha de completarse con el esfuerzo por plasmar los resultados de I+D en soluciones comerciales, ofreciendo los incentivos necesarios y creando las condiciones adecuadas.

La UE debe sacar el máximo provecho del Programa Marco de Investigación e Innovación («Horizonte 2020»)[29], que comenzará su andadura en 2014. La propuesta de la Comisión establece unos objetivos específicos para garantizar la fiabilidad de las TIC y luchar contra la ciberdelincuencia que concuerdan con la presente estrategia. «Horizonte 2020» apoyará la investigación sobre seguridad en relación con las TIC emergentes; ofrecerá soluciones para sistemas, servicios y aplicaciones de TIC seguros de extremo a extremo; incentivará la aplicación y adopción de las soluciones existentes; y examinará la interoperabilidad de redes y sistemas de información. A escala de la UE, se pondrá especial empeño en optimizar y coordinar mejor los diversos programas de financiación («Horizonte 2020», Fondo de Seguridad Interior, investigación de la AED, incluido el Marco Europeo de Cooperación).

La Comisión:

- recurrirá a «Horizonte 2020» para abordar varios aspectos de protección de la intimidad y seguridad en las TIC, desde la I+D a la innovación y el despliegue; «Horizonte 2020» permitirá también desarrollar herramientas e instrumentos de lucha contra las actividades delictivas y terroristas que tienen el ciberespacio como objetivo;
- creará mecanismos con miras a una mayor coordinación de los programas de investigación de las instituciones de la Unión Europea y los Estados miembros, y alentará a estos a invertir más en I+D.

La Comisión invita a los Estados miembros a:

- elaborar para finales de 2013 buenas prácticas para el uso del **poder de compra de las administraciones públicas** (por ejemplo, a través de la contratación pública) a fin de fomentar el desarrollo y despliegue de elementos de seguridad en los productos y servicios de TIC;

[29] «Horizonte 2020» es el instrumento financiero de ejecución de la Unión por la Innovación, la iniciativa emblemática de la Estrategia Europa 2020 destinada a garantizar la competitividad de Europa a escala mundial. El nuevo Programa Marco de Investigación e Innovación de la UE para el período 2014-2020 se inscribe en un proceso que tiene por objeto generar crecimiento y crear nuevos puestos de trabajo en Europa.

- promover la rápida incorporación de la industria y del mundo académico a las actividades de elaboración y coordinación de soluciones; para ello se sacará el mayor partido posible de la base industrial europea y de las innovaciones tecnológicas de la I+D conexa, y se garantizará la coordinación entre los programas de investigación de los organismos civiles y militares.

La Comisión solicita a Europol y a la ENISA que:

- determinen las tendencias y necesidades emergentes en función de la evolución de las pautas de ciberdelincuencia y ciberseguridad para así desarrollar herramientas y tecnologías forenses digitales adecuadas.

La Comisión invita a las partes interesadas de los sectores público y privado a:

- elaborar, en cooperación con el sector de los seguros, **sistemas de medición armonizados para el cálculo de las primas de riesgo**, merced a los cuales las empresas que hayan invertido en seguridad puedan obtener primas de riesgo menos elevadas.

2.5. Creación de una política internacional coherente del ciberespacio para la Unión Europea y promoción de los valores esenciales de la UE

Mantener un ciberespacio abierto, libre y seguro es un reto mundial al que la UE ha de hacer frente junto con los socios y organizaciones internacionales pertinentes, el sector privado y la sociedad civil.

En su política internacional del ciberespacio, la UE promoverá la apertura y la libertad de Internet, alentará las actividades de elaboración de normas de conducta y aplicará el Derecho internacional existente en este campo. Asimismo, la UE tomará medidas para superar la brecha digital y participará activamente en los esfuerzos internacionales de creación de capacidades de ciberseguridad. El compromiso internacional de la Unión en este ámbito estará presidido por los valores esenciales de la UE; a saber: la dignidad humana, la libertad, la democracia, la igualdad, el Estado de derecho y el respeto de los derechos fundamentales.

Integración de las cuestiones vinculadas al ciberespacio en las relaciones exteriores y la Política Exterior y de Seguridad Común de la UE

La Comisión, la Alta Representante y los Estados miembros deben formular una política internacional de la UE coherente en relación con el ciberespacio, cuyo objetivo sea aumentar su compromiso y estrechar las relaciones con los principales socios y organizaciones internacionales, así como con la sociedad civil y el sector privado. Las consultas de la UE con sus socios internacionales sobre cuestiones referentes al ciberespacio deben prepararse, coordinarse y llevarse a la práctica de modo que supongan un valor añadido en los diálogos bilaterales existentes entre los Estados miembros de la UE y los terceros países. La UE podrá renovado empeño en el diálogo con los terceros países, favoreciendo los contactos con aquellos socios que persiguen los mismos objetivos y comparten sus valores. La UE promoverá un elevado nivel de protección de datos, especialmente en la transferencia a terceros países de datos personales. Para hacer frente a los problemas mundiales que plantea el ciberespacio, la UE procurará cooperar más estrechamente con organizaciones que trabajan en este campo, como el Consejo de Europa, la OCDE, las Naciones Unidas, la OSCE, la OTAN, la UA, la ASEAN y la OEA. A nivel bilateral, la cooperación con los Estados Unidos reviste especial importancia y se potenciará, en particular en el contexto del Grupo de Trabajo UE-EE.UU. sobre Ciberseguridad y Ciberdelincuencia.

Uno de los aspectos primordiales de la política internacional de ciberseguridad de la UE será la promoción del ciberespacio como ámbito de libertad y derechos fundamentales. Es de esperar que la ampliación del acceso a Internet impulse los procesos de reforma democrática y los promueva en todo el mundo. Esta mayor conectividad mundial no ha de ir acompañada de censura ni de actividades de vigilancia masiva. La UE debe promover la responsabilidad social de las empresas[30] y presentar iniciativas internacionales para mejorar la coordinación mundial en este campo.

Corresponde a todos los que intervienen en la sociedad de la información mundial, de los ciudadanos a los Estados, velar por un ciberespacio más seguro. La UE apoya los esfuerzos por establecer unas normas de conducta en el ciberespacio que sean respetadas por todas las partes interesadas. Así como los ciudadanos de la UE deben cumplir sus derechos cívicos, asumir sus responsabilidades sociales y respetar las leyes en línea, de igual modo deben los Estados observar las normas y leyes existentes. En cuestiones de seguridad internacional, la UE aboga por la adopción de medidas de fomento de la confianza en la ciberseguridad a fin de aumentar la transparencia y reducir el riesgo de que se malinterprete la manera de actuar de los Estados.

La UE no defiende la creación de nuevos instrumentos jurídicos internacionales para abordar las cuestiones relacionadas con el ciberespacio.

También deberán respetarse en línea las obligaciones jurídicas establecidas en el Pacto Internacional de Derechos Civiles y Políticos, el Convenio Europeo de Derechos Humanos y la Carta de los Derechos Fundamentales de la Unión Europea. La UE examinará de qué modo puede garantizarse que esas disposiciones se aplican también en el ciberespacio.

A fin de combatir la ciberdelincuencia, el Convenio de Budapest es un instrumento abierto a la adopción por los terceros países. Ofrece un modelo para redactar actos jurídicos nacionales en materia de ciberdelincuencia y una base para la cooperación internacional en este ámbito.

En caso de que los conflictos armados se extiendan al ciberespacio, se aplicarán el Derecho humanitario internacional y, en su caso, el Derecho internacional en materia de derechos humanos.

Capacitación en materia de ciberseguridad e infraestructuras de información resilientes en terceros países

Una mayor cooperación internacional facilitará el correcto funcionamiento de las infraestructuras subyacentes que prestan y facilitan servicios de comunicación. Esa cooperación consistirá en intercambiar mejores prácticas, compartir información, realizar ejercicios de alerta temprana y de gestión conjunta de incidentes, etc. La UE contribuirá al logro de este objetivo intensificando los esfuerzos internacionales en curso para reforzar las redes de cooperación entre las administraciones públicas y el sector privado con miras a la protección de las infraestructuras críticas de información (PICI).

No todas las zonas del mundo se benefician de los efectos positivos de Internet al no existir un acceso abierto, seguro, interoperable y fiable. Por consiguiente, la Unión Europea continuará respaldando los esfuerzos de los países por garantizar un mayor acceso y uso de

[30] *Estrategia renovada de la UE para 2011-2014 sobre la responsabilidad social de las empresas,* COM(2011) 681 final.

Internet a sus ciudadanos, asegurar su integridad y seguridad y luchar con eficacia contra la ciberdelincuencia.

En cooperación con los Estados miembros, la Comisión y la Alta Representante:

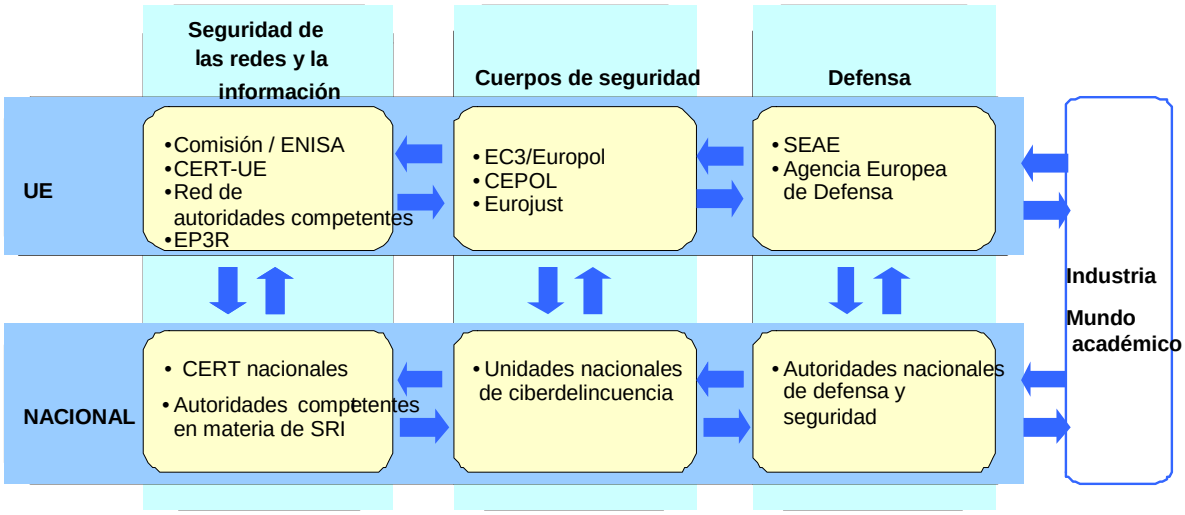
- trabajarán en pro de una política internacional coherente de la UE en el ámbito del ciberespacio para incrementar su colaboración con los socios y organizaciones internacionales clave, integrar las cuestiones vinculadas al ciberespacio en la PESC y mejorar la coordinación de las cuestiones de alcance mundial;
- apoyarán la elaboración de normas de conducta y medidas de fomento de la confianza en la ciberseguridad, facilitarán el diálogo sobre la manera de aplicar el Derecho internacional vigente en este ámbito y promoverán el Convenio de Budapest para hacer frente a la ciberdelincuencia;
- respaldarán la promoción y protección de los derechos fundamentales, en particular el acceso a la información y la libertad de expresión, centrándose en: a) la elaboración de nuevas directrices públicas sobre la libertad de expresión en línea y fuera de línea; b) el control de las exportaciones de productos o servicios que puedan utilizarse para fines de censura o vigilancia masiva en línea; c) la elaboración de medidas y herramientas para ampliar el acceso a Internet e incrementar su apertura y resiliencia para sustraerse a la censura o la vigilancia masiva mediante las tecnologías de la comunicación; d) el fomento entre las partes interesadas del uso de las tecnologías de la comunicación para promover los derechos fundamentales;
- apoyarán, junto con los socios y organizaciones internacionales clave, el sector privado y la sociedad civil, el desarrollo de capacidades globales en los terceros países para mejorar el acceso a la información y a una Internet abierta, prevenir y combatir las ciberamenazas, incluidos los incidentes accidentales, la ciberdelincuencia y el ciberterrorismo, e impulsar la coordinación entre los donantes para orientar los esfuerzos de desarrollo de capacidades;
- recurrirán a diversos instrumentos de ayuda de la UE para desarrollar capacidades en materia de ciberseguridad, subvencionando la formación del personal policial, judicial y técnico para hacer frente a las ciberamenazas, y apoyando asimismo la creación de las políticas, estrategias e instituciones pertinentes en los terceros países;
- intensificarán la coordinación de políticas y el intercambio de información a través de redes de protección de infraestructuras críticas de información, tales como la red *Meridian*, así como la cooperación entre las autoridades competentes en materia de SRI y otras autoridades.

3. FUNCIONES Y RESPONSABILIDADES

En una economía y una sociedad digitales interconectadas, los ciberincidentes no se detienen en las fronteras. Todas las partes interesadas, de las autoridades competentes en materia de SRI, los CERT y los cuerpos de seguridad a la industria, han de asumir sus responsabilidades a escala nacional y de la UE, y trabajar en común para aumentar la ciberseguridad. Como

pueden intervenir distintos marcos jurídicos y jurisdicciones, reviste suma importancia que la UE aclare las funciones y responsabilidades de las numerosas partes interesadas.

Dada la complejidad del problema y las muchas partes que intervienen, la solución no puede consistir en una supervisión europea centralizada. Las administraciones nacionales son las que se hallan en mejores condiciones para organizar las actividades de prevención y respuesta a incidentes y ataques cibernéticos, así como para establecer contactos y redes con el sector privado y los ciudadanos a través de los procedimientos y marcos jurídicos establecidos. Al mismo tiempo, habida cuenta del carácter transfronterizo potencial o real de los riesgos, una respuesta efectiva a escala nacional requeriría a menudo la intervención de la UE. Para abordar la ciberseguridad de forma global, las actividades deben articularse en torno a tres pilares esenciales—SRI, cuerpos de seguridad y defensa—, también regulados por diferentes marcos jurídicos:



3.1. Coordinación entre autoridades competentes en materia de SRI/CERT, cuerpos de seguridad y defensa

A escala nacional

Los Estados miembros deberían disponer, ya en la actualidad o como resultado de esta estrategia, de estructuras para abordar la ciberresiliencia, la ciberdelincuencia y la ciberdefensa; deben asimismo alcanzar el nivel de capacidades requerido para resolver los ciberincidentes. No obstante, dado que una serie de entidades pueden tener responsabilidades operativas en distintas dimensiones de la ciberseguridad y habida cuenta de la importancia que reviste la participación del sector privado, conviene lograr una coordinación óptima entre ministerios a escala nacional. Los Estados miembros deberán establecer en sus estrategias nacionales de ciberseguridad las funciones y responsabilidades de sus diversas entidades nacionales.

Debe fomentarse el intercambio de información entre entidades nacionales y con el sector privado para que este y los Estados miembros puedan tener una visión global de las diversas amenazas y comprender mejor las nuevas tendencias y las técnicas utilizadas tanto para cometer ciberataques como para reaccionar ante ellos con mayor rapidez. La elaboración de planes nacionales de cooperación en materia de SRI, que se han de activar en caso de que se produzcan ciberincidentes, facilitará a los Estados miembros la tarea de asignar claramente funciones y responsabilidades y optimizar las medidas de respuesta.

A escala de la UE

Como ocurre a escala nacional, en la UE hay distintas entidades responsables de ciberseguridad. Cabe citar, en particular, a la ENISA, Europol/EC3 y la AED, tres agencias que actúan desde la perspectiva de la SRI, los cuerpos de seguridad y la defensa, respectivamente. Estas agencias cuentan con consejos de administración en que están representados los Estados miembros y constituyen plataformas de coordinación a escala de la UE.

Se impulsarán la coordinación y la colaboración entre la ENISA, Europol/EC3 y la AED en una serie de ámbitos de interés para las tres agencias, en particular el análisis de tendencias, la evaluación de riesgos, la formación y el intercambio de mejores prácticas. Las tres han de colaborar, manteniendo al mismo tiempo sus especificidades. Estas agencias, junto con el CERT-UE, la Comisión y los Estados miembros, deberán apoyar la creación de una comunidad de especialistas técnicos y policiales de confianza en este campo.

Los canales informales de coordinación y colaboración se completarán con vínculos más estructurados. El personal militar de la UE y el equipo encargado del proyecto de ciberdefensa de la AED podrán servir de vector de coordinación en el ámbito de la defensa. El Consejo de Programación de Europol/EC3 reunirá, entre otros, a EUROJUST, CEPOL, los Estados miembros[31], la ENISA y la Comisión, y les ofrecerá la oportunidad de compartir sus respectivos conocimientos especializados y de comprobar que las actuaciones del EC3 se llevan a cabo en concertación, reconociéndose las aportaciones de cada parte y respetándose sus mandatos. El nuevo mandato de la ENISA permitirá que esta estreche sus relaciones con Europol y refuerce sus relaciones con la industria. Ante todo, la propuesta legislativa de la Comisión sobre la SRI establecerá un marco de cooperación a través de una red de autoridades nacionales competentes en materia de SRI y fomentará el intercambio de información entre dichas autoridades y los cuerpos de seguridad.

A escala internacional

La Comisión y la Alta Representante garantizan, junto con los Estados miembros, una actuación internacional coordinada en el ámbito de la ciberseguridad. En este marco, la Comisión y la Alta Representante defenderán los valores esenciales de la UE y promoverán una utilización pacífica, abierta y transparente de las cibertecnologías. La Comisión, la Alta Representante y los Estados miembros mantienen diálogos políticos con los socios internacionales y organizaciones internacionales tales como el Consejo de Europa, la OCDE, la OSCE, la OTAN y las Naciones Unidas.

3.2. Apoyo de la UE ante incidentes y ataques cibernéticos graves

Los incidentes o ataques cibernéticos graves pueden repercutir en las administraciones públicas, las empresas y los ciudadanos de la UE. Cabe esperar que, gracias a esta estrategia —y en particular la propuesta de Directiva sobre la SRI—, la prevención, la detección y la respuesta ante los ciberincidentes sean más eficaces, y los Estados miembros y la Comisión se mantengan mejor informados acerca de los incidentes o ataques cibernéticos graves. Con todo, los mecanismos de respuesta diferirán en función de la naturaleza, la magnitud y los efectos transfronterizos del incidente.

[31] Mediante la representación en el grupo de trabajo sobre ciberdelincuencia de la UE, integrado por los jefes de las unidades de ciberdelincuencia de los Estados miembros.

Si el incidente tiene efectos graves en la continuidad de las actividades, la Directiva sobre la SRI propone la activación de planes de cooperación nacionales o de la Unión en materia de SRI, según la naturaleza transfronteriza del incidente. En este contexto, se recurrirá a la red de autoridades competentes en materia de SRI para compartir información y prestar apoyo, lo cual permitirá mantener o restaurar las redes y los servicios afectados.

Si el incidente parece tener origen delictivo, se deberá informar a Europol/EC3 para que, junto con las autoridades policiales de los países afectados, pueda iniciar una investigación, conservar las pruebas, identificar a los autores y velar por que se castigue su delito.

Si el incidente parece estar relacionado con el ciberespionaje o con un ataque promovido por un Estado, o afecta a la seguridad nacional, las autoridades policiales y de defensa nacionales deberán alertar a sus homólogos de que sufren un ataque y se hallan en condiciones de defenderse. Entonces se activarán mecanismos de alerta temprana y, en caso necesario, procedimientos de gestión de crisis o de otros tipos. Un incidente o ataque cibernético de especial gravedad podría ser motivo suficiente para que un Estado miembro invocara la cláusula de solidaridad de la UE (artículo 222 del Tratado de Funcionamiento de la Unión Europea).

Si el incidente parece haber comprometido datos personales, intervendrán las autoridades nacionales responsables de la protección de datos o la autoridad reguladora nacional, de conformidad con la Directiva 2002/58/CE.

Por último, la gestión de ciberincidentes y ciberataques se verá facilitada por las redes de contacto y el apoyo de los socios internacionales, que podrá consistir en medidas técnicas de atenuación, investigaciones penales o la activación de mecanismos de gestión de crisis y respuesta.

4. CONCLUSIÓN Y PRÓXIMAS ETAPAS

La presente estrategia de ciberseguridad de la Unión Europea, presentada por la Comisión y la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad, expone la visión de la UE y describe las medidas necesarias, basadas en la defensa y la promoción tenaces de los derechos de los ciudadanos, con el fin de convertir el entorno en línea de la UE en el más seguro del mundo[32].

Esta visión solamente puede hacerse realidad mediante una auténtica cooperación entre las numerosas partes interesadas, que deberán comprometerse a asumir sus responsabilidades y a afrontar los retos que se planteen en el futuro.

La Comisión y la Alta Representante invitan, por tanto, al Consejo y al Parlamento Europeo a aprobar la estrategia y a contribuir a llevar a la práctica las medidas propuestas. También será

[32] La estrategia se financiará con los importes previstos para cada uno de los ámbitos de actuación (MCE, Horizonte 2020, Fondo de Seguridad Interior, PESC y Cooperación Exterior, en particular el Instrumento de Estabilidad), de conformidad con la propuesta de la Comisión referente al marco financiero plurianual para 2014-2020 (a reserva de la aprobación de la Autoridad Presupuestaria y de los importes finales del MFP adoptado para 2014-2020). En lo tocante a la necesidad de garantizar la compatibilidad global con el número de puestos disponibles para las agencias descentralizadas y el sublímite para las agencias descentralizadas de cada rúbrica de gastos del próximo MFP, las agencias (CEPOL, AED, ENISA, EUROJUST y EUROPOL/EC3) a las que la presente Comunicación confía nuevas tareas deberán asumirlas en la medida en que se hayan determinado tanto la capacidad real de la agencia para absorber nuevos recursos como todas las posibilidades de redistribución.

necesario contar con el firme apoyo y el compromiso del sector privado y la sociedad civil, cuya participación es crucial para aumentar nuestro nivel de seguridad y proteger los derechos de los ciudadanos.

Ha llegado el momento de actuar. La Comisión y la Alta Representante están dispuestas a colaborar con todas las partes interesadas para lograr la seguridad que Europa necesita. Para garantizar la pronta aplicación de la estrategia y su análisis en función de lo que acontezca, tienen la intención de reunir a todas las partes interesadas en una conferencia de alto nivel y evaluar los avances conseguidos en 12 meses.