COMISIÓN
EUROPEA

Bruselas, 7.2.2013
COM(2013) 48 final

2013/0027 (COD)

Propuesta de

DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO

relativa a medidas para garantizar un elevado nivel común de seguridad de las redes y de la información en la Unión

{SWD(2013) 31 final}
{SWD(2013) 32 final}

EXPOSICIÓN DE MOTIVOS

El objetivo de la Directiva propuesta es garantizar un elevado nivel común de seguridad de las redes y de la información (SRI). Para ello es preciso aumentar la seguridad de Internet y de las redes y los sistemas de información privados que sustentan el funcionamiento de nuestras sociedades y economías. A fin de alcanzar dicho objetivo, es necesario, por una parte, instar a los Estados miembros a estar más preparados e incrementar la cooperación entre ellos, y, por otra, exigir a los operadores de infraestructuras críticas tales como la energía o los transportes, a los proveedores clave de servicios de la sociedad de la información (plataformas de comercio electrónico, redes sociales, etc.) y a las administraciones públicas que adopten las medidas oportunas para gestionar los riesgos de seguridad y notificar los incidentes graves a las autoridades nacionales competentes.

Esta propuesta se presenta en relación con la Comunicación conjunta de la Comisión y la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad sobre una estrategia europea de ciberseguridad. La finalidad de dicha estrategia es garantizar un entorno digital seguro y fiable, sin olvidar la promoción y la protección de los derechos fundamentales y otros valores esenciales de la UE. La presente propuesta es el principal instrumento de la estrategia, que en este ámbito incluye asimismo otras medidas centradas en la concienciación, el desarrollo de un mercado interior de productos y servicios de ciberseguridad, y el fomento de las inversiones en I+D. Estas medidas se complementarán con otras destinadas a intensificar la lucha contra la ciberdelincuencia y elaborar una política internacional de ciberseguridad para la UE.

1.1. Motivación y objetivos de la propuesta

La SRI está adquiriendo una importancia creciente para nuestra economía y nuestra sociedad. También es un requisito previo imprescindible para crear un entorno fiable para el comercio mundial de servicios. Los sistemas de información, empero, pueden verse afectados por incidentes relacionados con la seguridad tales como errores humanos, fenómenos naturales, fallos técnicos o ataques malintencionados. La envergadura, frecuencia y complejidad de estos incidentes es cada vez mayor. Según la consulta pública en línea de la Comisión sobre la mejora de la seguridad de las redes y de la información en la UE[1], el 57 % de los participantes en ella habían sufrido a lo largo del año anterior incidentes de SRI que habían tenido graves consecuencias en sus actividades. La falta de SRI puede llegar a comprometer servicios vitales que dependen de la integridad de las redes y los sistemas de información, interrumpiendo las actividades de las empresas, generando cuantiosas pérdidas financieras para la economía de la UE e incidiendo negativamente en el bienestar de la sociedad.

Por otra parte, al tratarse de instrumentos de comunicación sin fronteras, los sistemas de información digitales —y en particular Internet— están interconectados entre los Estados miembros y contribuyen decisivamente a facilitar la circulación transfronteriza de bienes, servicios y personas. Un problema grave de estos sistemas en un Estado miembro puede afectar a otros Estados miembros y a la UE en su conjunto. Por consiguiente, la resiliencia y la estabilidad de las redes y los sistemas de información revisten suma importancia para la realización del mercado único digital y el buen funcionamiento del mercado interior. La mayor probabilidad o frecuencia de los incidentes y la incapacidad de ofrecer protección suficiente minan asimismo la confianza de los ciudadanos en los servicios de red e información. Así, por ejemplo, el Eurobarómetro de 2012 sobre ciberseguridad señalaba que al 38 % de los usuarios de Internet en la UE le preocupa la seguridad de los pagos en línea y ha modificado su comportamiento en consecuencia: probablemente un 18 % comprará menos en Internet y un 15 % no utilizará tanto los servicios bancarios en línea[2].

La situación actual en la UE es reflejo del planteamiento meramente voluntario seguido hasta el momento, que no ofrece protección suficiente frente a incidentes y riesgos relacionados con la SRI en la UE. Las capacidades y mecanismos de SRI actuales son sencillamente insuficientes para seguir el ritmo de unas amenazas en rápida mutación y garantizar un nivel elevado de protección igual en todos los Estados miembros.

Pese a las iniciativas emprendidas, los niveles de capacidad y preparación de los Estados miembros son muy distintos y dan lugar a enfoques fragmentados en la UE. Al estar redes y sistemas interconectados, la SRI global de la UE se ve perjudicada por esos Estados miembros cuyo nivel de protección es insuficiente. Esta situación dificulta asimismo la creación de lazos de confianza entre homólogos, requisito previo para la cooperación y el intercambio de información. Como consecuencia de ello, solamente mantienen relaciones de cooperación unos pocos Estados miembros con elevado nivel de capacidades.

Actualmente no existe, por tanto, un mecanismo efectivo a escala de la UE que haga posible una labor de cooperación y colaboración eficaz y un intercambio de información de confianza sobre incidentes y riesgos de SRI entre los Estados miembros. Estas carencias pueden dar lugar a intervenciones reglamentarias no coordinadas, estrategias incoherentes y normas divergentes, que a su vez llevan aparejada una protección insuficiente ante los problemas de SRI en toda la UE. Pueden incluso surgir obstáculos al mercado interior que generen gastos de observancia a las empresas que operan en más de un Estado miembro.

---

[1] La consulta pública en línea sobre la mejora de la seguridad de las redes y de la información en la UE se desarrolló del 23 de julio al 15 de octubre de 2012.

[2] Eurobarómetro 390/2012.

Por último, a los agentes que gestionan infraestructuras críticas o prestan servicios esenciales para el funcionamiento de nuestras sociedades no se les han impuesto las oportunas obligaciones de adoptar medidas de gestión de riesgos ni de intercambiar información con las autoridades competentes. Así pues, por una parte, no se ofrecen a las empresas incentivos reales para proceder a una gestión de riesgos como es debido, con una evaluación del riesgo y la adopción de medidas adecuadas para garantizar la SRI. Por otra parte, un elevado porcentaje de incidentes no llega a conocimiento de las autoridades competentes y pasa desapercibido. Y, sin embargo, la información sobre los incidentes es esencial para que las autoridades públicas reaccionen, adopten las medidas de atenuación apropiadas y fijen las prioridades estratégicas oportunas en materia de SRI.

El actual marco regulador solamente obliga a las empresas de telecomunicaciones a adoptar medidas de gestión de riesgos y a notificar los incidentes graves que ponen en peligro la SRI. No obstante, hay muchos otros sectores cuyo desarrollo depende de las TIC y que, por ende, deberían también prestar la debida atención a la SRI. Algunos proveedores de infraestructuras y servicios específicos son especialmente vulnerables al ser muy dependientes del correcto funcionamiento de las redes y los sistemas de información. Tales sectores desempeñan una función primordial, pues prestan servicios de apoyo cruciales para nuestra economía y nuestra sociedad, y la seguridad de sus sistemas reviste especial importancia para el funcionamiento del mercado interior. Entre estos sectores cabe citar la banca, la bolsa, la generación, el transporte y la distribución de energía, los transportes (aéreo, ferroviario y marítimo), la sanidad, los servicios de Internet y las administraciones públicas.

Así pues, en la UE hay que abordar la SRI de forma radicalmente distinta. Es necesario imponer obligaciones reglamentarias para establecer condiciones uniformes y colmar las actuales lagunas jurídicas. A fin de hacer frente a estos problemas e incrementar el nivel de SRI en toda la Unión Europea, la Directiva propuesta fija los objetivos que a continuación se exponen.

En primer lugar, la propuesta impone a todos los Estados miembros la obligación de velar por que exista un nivel mínimo de capacidades nacionales mediante la designación de autoridades competentes en materia de SRI, la creación de equipos de respuesta a emergencias informáticas (CERT) y la adopción de estrategias y planes de cooperación nacionales en el ámbito de la SRI.

En segundo lugar, las autoridades nacionales competentes deberán cooperar dentro de una red que garantice una coordinación segura y eficaz y, en particular, un intercambio coordinado de información y unas labores de detección y respuesta a escala de la UE. A través de esta red, los Estados miembros deberán intercambiar información y cooperar para hacer frente a las amenazas e incidentes que puedan poner en peligro la SRI sobre la base del plan de cooperación europeo en materia de SRI.

En tercer lugar, siguiendo el modelo de la Directiva Marco sobre las comunicaciones electrónicas, la propuesta pretende implantar una cultura de gestión de riesgos y garantizar el intercambio de información entre los sectores público y privado. Las empresas de los sectores críticos concretos antes citados y las administraciones públicas deberán evaluar los riesgos a que se enfrentan y adoptar medidas adecuadas y proporcionadas para garantizar la SRI. Estas empresas deberán notificar a las autoridades competentes todos los incidentes que supongan un peligro grave para el funcionamiento de sus redes y sistemas de información y comprometan de forma significativa la continuidad de los servicios críticos y el suministro de mercancías.

1.2. Contexto general

Ya en su Comunicación de 2001 titulada *Seguridad de las redes y de la información: Propuesta para un enfoque político europeo*, la Comisión destacaba la creciente importancia de la SRI[3]. Posteriormente, en 2006 se adoptó una estrategia para una sociedad de la información segura[4], que tenía como objetivo desarrollar una cultura de SRI en Europa. Sus principales aspectos fueron aprobados en una Resolución del Consejo[5].

El 30 de marzo de 2009, la Comisión adoptó una Comunicación sobre protección de infraestructuras críticas de información (PICI)[6], cuya finalidad era proteger a Europa de las ciberperturbaciones impulsando una mayor seguridad. En dicha Comunicación se presentaba un plan de acción para respaldar a los Estados miembros en sus esfuerzos de prevención y respuesta. El plan de acción se aprobó en las Conclusiones de la Presidencia de la Conferencia Ministerial sobre PICI celebrada en Tallin en 2009. El 18 de diciembre de 2009, el Consejo adoptó una Resolución relativa a un planteamiento de colaboración en materia de seguridad de las redes y de la información[7].

La Agenda Digital para Europa (ADE)[8], adoptada en mayo de 2010, y las conclusiones del Consejo correspondientes[9] ponían de relieve la convicción común de que la confianza y la seguridad son condiciones previas fundamentales para la adopción a gran escala de las TIC y, por ende, para el logro de los objetivos de una de las dimensiones de la Estrategia Europa 2020, la denominada «crecimiento inteligente»[10]. En su capítulo dedicado a la confianza y la seguridad, la ADE insistía en la necesidad de que todas las partes interesadas se unieran en un esfuerzo conjunto para garantizar la seguridad y la resiliencia de las infraestructuras de las TIC, centrándose en la prevención, la preparación y la sensibilización al objeto de desarrollar unos mecanismos de seguridad eficaces y coordinados. En particular, la acción clave 6 de la Agenda Digital para Europa instaba a adoptar medidas encaminadas a conseguir una política de SRI reforzada y de alto nivel.

En su Comunicación de marzo de 2011 sobre la protección de infraestructuras críticas de información titulada *Logros y próximas etapas: hacia la ciberseguridad global*[11], la Comisión hacía balance de los resultados logrados desde la adopción del plan de acción sobre la PICI en 2009 y concluía que la aplicación del plan demostraba que los enfoques puramente nacionales no bastaban para abordar cuestiones de seguridad y resiliencia y que Europa debía seguir esforzándose por construir una estrategia coherente y cooperativa para toda la UE. En la Comunicación sobre la PICI de 2011 se anunciaba una serie de medidas y la Comisión instaba a los Estados miembros a crear capacidades y mantener una cooperación transfronteriza en materia de SRI. La mayor parte de esas medidas tenía que haberse completado en 2012, pero aún no se ha llevado a la práctica.

En sus conclusiones de 27 de mayo de 2011 sobre la PICI, el Consejo de la Unión Europea subrayaba la acuciante necesidad de contar con unos sistemas y redes de TIC resilientes y seguros frente a todas las perturbaciones posibles, accidentales o intencionadas, lograr en toda la UE un nivel elevado de preparación, seguridad y resiliencia, mejorar las competencias técnicas a fin de que Europa pueda responder a los desafíos en materia de protección de las

---

3 COM(2001) 298.
4 COM(2006) 251 http://eur-lex.europa.eu/LexUriServ/site/es/com/2006/com2006_0251es01.pdf.
5 2007/068/01.
6 COM(2009) 149.
7 2009/C 321/01.
8 COM(2010) 245.
9 Conclusiones del Consejo de 31 de mayo de 2010 sobre la Agenda Digital para Europa (10130/10).
10 COM(2010) 2020 y Conclusiones del Consejo Europeo de 25 y 26 de marzo de 2010 (EUCO 7/10).
11 COM(2011) 163.

redes y las infraestructuras de información, e impulsar la cooperación entre los Estados miembros mediante el establecimiento de mecanismos de cooperación ante incidentes.

1.3. Disposiciones internacionales y de la Unión Europea existentes en este ámbito

En virtud del Reglamento (CE) nº 460/2004, la Comunidad Europea creó en 2004 la Agencia Europea de Seguridad de las Redes y de la Información (ENISA)[12] con el fin de contribuir a garantizar un elevado nivel de SRI y desarrollar una cultura en este ámbito en toda la UE. El 30 de septiembre de 2010 se adoptó una propuesta para modernizar el mandato de la ENISA[13], que se está debatiendo actualmente en el Consejo y el Parlamento Europeo. El marco regulador revisado de los servicios de comunicaciones electrónicas[14], en vigor desde noviembre de 2009, impone obligaciones en materia de seguridad a los proveedores de servicios de comunicaciones electrónicas[15]. Dichas obligaciones tenían que estar incorporadas a los ordenamientos jurídicos nacionales en mayo de 2011.

El marco regulador de protección de datos[16] obliga a todos los agentes que actúan como responsables del tratamiento de los datos (por ejemplo, bancos u hospitales) a implantar medidas de seguridad para proteger los datos personales. Asimismo, la propuesta de Reglamento general de protección de datos[17], presentada por la Comisión en 2012, establece que los responsables del tratamiento deben notificar los casos de violación de datos personales a las autoridades nacionales de control. Así pues, una violación de la SRI que afectara a la prestación de un servicio sin comprometer datos personales (por ejemplo, una avería de las TIC en una compañía eléctrica que ocasionara la interrupción del servicio) no debería notificarse.

Al amparo de la Directiva 2008/114/CE sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección, el Programa Europeo de Protección de Infraestructuras Críticas (PEPIC)[18] establece el marco global para la protección de las infraestructuras críticas en la UE. Los objetivos del PEPIC coinciden plenamente con los de la presente propuesta y la Directiva debería aplicarse sin perjuicio de la Directiva 2008/114/CE. El PEPIC no obliga a los operadores a notificar violaciones significativas de la seguridad ni establece mecanismos para que los Estados miembros cooperen y respondan ante los incidentes que se produzcan.

Los colegisladores están examinando actualmente la propuesta de Directiva de la Comisión relativa a los ataques contra los sistemas de información[19], que tiene como objetivo armonizar la tipificación como delitos de determinados tipos de conducta. Dicha propuesta abarca solamente la tipificación de determinados tipos de conducta y no aborda la prevención de riesgos e incidentes de SRI, la respuesta a los incidentes de SRI ni la atenuación de sus efectos. La presente Directiva debe aplicarse sin perjuicio de la Directiva relativa a los ataques contra los sistemas de información.

El 28 de marzo de 2012, la Comisión adoptó una Comunicación sobre la creación de un centro europeo de ciberdelincuencia (EC3)[20]. Este Centro, creado el 11 de enero de 2013, está

---

12 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:ES:HTML.

13 COM(2010) 521.

14 Véase http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf.

15 Artículos 13 *bis* y 13 *ter* de la Directiva Marco.

16 Directiva 2002/58/CE de 12 de julio de 2002.

17 COM(2012) 11.

18 COM(2006) 786, http://eur-lex.europa.eu/LexUriServ/site/es/com/2006/com2006_0786es01.pdf.

19 COM(2010) 517, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:ES:PDF.

20 COM(2012) 140 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:ES:PDF.

integrado en la Oficina Europea de Policía (Europol) y funcionará como punto central en la lucha contra la ciberdelincuencia en la UE. El EC3 está destinado a aunar los conocimientos sobre ciberdelincuencia europeos para contribuir a la capacitación de los Estados miembros, a prestar apoyo a los Estados miembros en investigaciones de ciberdelincuencia y, en estrecha cooperación con Eurojust, a ser la voz colectiva de los investigadores de ciberdelincuencia europeos ante los organismos de orden público y el estamento judicial.

Las instituciones, agencias y organismos europeos han creado su propio equipo de respuesta a emergencias informáticas, denominado CERT-UE.

A escala internacional, la UE desarrolla actividades bilaterales y multilaterales en el ámbito de la ciberseguridad. Con motivo de la Cumbre UE-EE.UU. de 2010[21], se creó el Grupo de Trabajo UE-EE.UU. sobre Ciberseguridad y Ciberdelincuencia. La UE también participa en otros foros multilaterales tales como la Organización de Cooperación y Desarrollo Económicos (OCDE), la Asamblea General de las Naciones Unidas (AGNU), la Unión Internacional de Telecomunicaciones (UIT), la Organización para la Seguridad y la Cooperación en Europa (OSCE), la Cumbre Mundial sobre la Sociedad de la Información (CMSI) y el Foro para la Gobernanza de Internet (IGF).

2. RESULTADOS DE LAS CONSULTAS CON LAS PARTES INTERESADAS Y DE LAS EVALUACIONES DE IMPACTO

2.1. Consulta con las partes interesadas y utilización de asesoramiento técnico

Del 23 de julio al 15 de octubre de 2012 estuvo abierta en línea una consulta pública sobre la mejora de la SRI en la UE. La Comisión recibió un total de 160 respuestas al cuestionario en línea.

La principal conclusión que puede extraerse de esas respuestas es el reconocimiento generalizado de la necesidad de aumentar la SRI en toda la UE. Más concretamente, el 82,8 % de los participantes en la consulta señala que los Gobiernos de la UE deberían adoptar más medidas para garantizar un elevado nivel de SRI; también el 82,8 % opina que los usuarios de sistemas de información no son conscientes de las amenazas e incidentes de SRI existentes; el 66,3 % estaría, en principio, a favor de la introducción de requisitos reglamentarios para gestionar los riesgos de SRI; y el 84,8 % afirma que tales requisitos se han de establecer a escala de la UE. Muchas respuestas indican que sería importante adoptar requisitos de SRI en los siguientes sectores específicos: banca y finanzas (91,1 %), energía (89,4 %), transportes (81,7 %), sanidad (89,4 %), servicios de Internet (89,1 %) y administraciones públicas (87,5 %). Los participantes en la consulta también consideran que, de introducirse la obligación de notificar violaciones de la SRI a la autoridad nacional competente, sería preciso hacerlo a escala de la UE (65,1 %) y estiman que las administraciones públicas también han de estar sujetas a esa obligación (93,5 %). Por último, afirman que la obligación de proceder a la gestión de riesgos de SRI de acuerdo con los conocimientos tecnológicos actuales no les supondría costes adicionales significativos (63,4 %), como tampoco se los supondría la obligación de notificar violaciones de la seguridad (72,3 %).

Se consultó a los Estados miembros en varias formaciones del Consejo, en el contexto del Foro Europeo de Estados Miembros (EFMS) en la Conferencia sobre Ciberseguridad organizada por la Comisión y el Servicio Europeo de Acción Exterior el 6 de julio de 2012, así como en reuniones bilaterales dedicadas a este tema que se convocaron a petición de algunos Estados miembros.

[21] http://europa.eu/rapid/press-release_MEMO-10-597_en.htm.

También se entablaron conversaciones con el sector privado en el marco de la Asociación público-privada europea de resiliencia[22] y a través de reuniones bilaterales. En cuanto al sector público, la Comisión mantuvo contactos con la ENISA y el CERT de las instituciones de la UE.

2.2. Evaluación de impacto

La Comisión ha efectuado una evaluación de impacto con respecto a tres opciones de actuación:

1ª opción: Mantenimiento del enfoque actual (hipótesis de referencia).

2ª opción: Enfoque reglamentario, con la presentación de una propuesta legislativa que establezca un marco jurídico común en materia de SRI para toda la UE y abarque las capacidades de los Estados miembros, los mecanismos de cooperación a escala de la UE y los requisitos que han de cumplir los principales agentes del sector privado y las administraciones públicas.

3ª opción: Enfoque mixto que combine las iniciativas de carácter voluntario en lo que respecta a las capacidades de los Estados miembros en el ámbito de la SRI y los mecanismos de cooperación a escala de la UE con requisitos reglamentarios aplicables a los principales agentes del sector privado y las administraciones públicas.

En opinión de la Comisión, la 2ª opción es la que puede tener mayores efectos positivos, pues incrementaría considerablemente la protección de consumidores, empresas y administraciones de la UE frente a los incidentes de SRI. Más concretamente, las obligaciones impuestas a los Estados miembros garantizarían la debida preparación a escala nacional y contribuirían a lograr un clima de confianza mutua, que es condición previa para una cooperación eficaz en la UE. La creación de mecanismos de cooperación a escala de la UE a través de una red facilitaría la adopción de medidas de prevención y respuesta coherentes y coordinadas ante incidentes y riesgos de SRI de carácter transfronterizo. Imponer a las administraciones públicas y a los principales agentes del sector privado la obligación de aplicar medidas de gestión de riesgos en el ámbito de la SRI supondría un poderoso incentivo para hacer frente con eficacia a los riesgos de seguridad. La obligación de notificar los incidentes de SRI con efectos significativos mejoraría la capacidad de respuesta a incidentes y fomentaría la transparencia. Por lo demás, al poner sus propios asuntos en orden, la UE podría ampliar su influencia internacional y convertirse en un socio todavía más fiable en las labores de cooperación bilateral y multilateral. Así pues, la UE se encontraría mejor situada para promover los derechos fundamentales y los valores esenciales de la Unión en el exterior.

La evaluación cuantitativa muestra que la 2ª opción no impondría una carga desproporcionada a los Estados miembros. Los costes que generaría para el sector privado también serían limitados por cuanto muchas de las entidades en cuestión ya están obligadas a cumplir los requisitos de seguridad existentes (los responsables del tratamiento de datos deben adoptar medidas técnicas y de organización, entre ellas medidas de SRI, para proteger los datos personales). También se han tomado en consideración los gastos de seguridad actuales en el sector privado.

La presente propuesta observa los principios reconocidos por la Carta de los Derechos Fundamentales de la Unión Europea y, en particular, el derecho al respeto de la vida privada y las comunicaciones, el derecho a la protección de los datos de carácter personal, el derecho a la libertad de empresa, el derecho a la propiedad, el derecho a una tutela judicial efectiva y el

[22] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r.

derecho a ser oído. La presente Directiva se deberá aplicar de acuerdo con estos derechos y principios.

3. ASPECTOS JURÍDICOS DE LA PROPUESTA

3.1. Base jurídica

La Unión Europea posee competencias para adoptar medidas destinadas a establecer el mercado interior o garantizar su funcionamiento, de conformidad con las disposiciones pertinentes de los Tratados (artículo 26 del Tratado de Funcionamiento de la Unión Europea — TFUE). En virtud del artículo 114 del TFUE, la UE puede adoptar «medidas relativas a *la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros* que tengan por objeto el establecimiento o el funcionamiento del mercado interior».

Como ya se ha indicado, las redes y los sistemas de información contribuyen de forma decisiva a facilitar la circulación transfronteriza de bienes, servicios y personas. A menudo están interconectados y huelga decir que la Internet tiene carácter global. Dada su dimensión transnacional intrínseca, una perturbación en un Estado miembro puede afectar también a otros Estados miembros y a la UE en su conjunto. Por consiguiente, la resiliencia y la estabilidad de las redes y los sistemas de información son esenciales para el buen funcionamiento del mercado interior.

El legislador de la UE ya ha reconocido la necesidad de armonizar las normas de SRI para asegurar el desarrollo del mercado interior. Cabe destacar a este respecto el Reglamento (CE) nº 460/2004 por el que se crea la ENISA[23], basado en el artículo 114 del TFUE.

Las grandes diferencias entre Estados miembros en lo que a capacidades, políticas y niveles de protección en materia de SRI se refiere han dado lugar a disparidades que representan un obstáculo para el mercado interior y justifican la actuación de la UE.

3.2. Subsidiariedad

La intervención europea en el campo de la SRI está justificada por el principio de subsidiariedad.

En primer lugar, dado el carácter transfronterizo de la SRI, de no intervenir la UE, cada Estado miembro actuaría por su cuenta, haciendo caso omiso de las interdependencias entre las redes y los sistemas de información de la UE. Un grado suficiente de coordinación entre los Estados miembros garantizaría una gestión correcta de los riesgos de SRI en el contexto transfronterizo en que surgen. Las divergencias entre las normativas sobre SRI representan una barrera para las empresas que quieren desarrollar sus actividades en varios países y para la consecución de economías de escala a nivel mundial.

En segundo lugar, es preciso imponer obligaciones reglamentarias a escala de la UE para lograr condiciones uniformes y colmar las lagunas jurídicas. Se ha demostrado que los planteamientos de carácter meramente voluntario dan lugar a una cooperación limitada a una minoría de Estados miembros con elevado nivel de capacidades. Para conseguir la participación de todos los Estados miembros, es necesario cerciorarse de que todos ellos poseen el nivel mínimo de capacidades requerido. Las medidas adoptadas por los Gobiernos para garantizar la SRI han de guardar coherencia unas con otras y estar coordinadas de modo que sea posible contener y reducir al mínimo las consecuencias de incidentes que pongan en peligro la SRI. En el marco de la red, a través del intercambio de las mejores prácticas y de la

[23] Reglamento (CE) n° 460/2004 del Parlamento Europeo y del Consejo, de 10 de marzo de 2004, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información (DO L 77 de 13.3.2004, p. 1).

colaboración permanente de la ENISA, las autoridades competentes y la Comisión cooperarán para facilitar una aplicación convergente de la Directiva en toda la UE. Además, las intervenciones concertadas en defensa de la SRI pueden contribuir de forma muy positiva a la protección efectiva de los derechos fundamentales, y en especial del derecho a la protección de los datos de carácter personal y a la intimidad. Una actuación a escala de la UE aumentaría por tanto la eficacia de las políticas nacionales vigentes y facilitaría su desarrollo.

Las medidas propuestas también quedan justificadas por el principio de proporcionalidad. Las obligaciones que han de cumplir los Estados miembros se fijan en el nivel mínimo necesario para lograr una preparación adecuada y posibilitar una cooperación basada en la confianza. Ello permite a los Estados miembros tomar debidamente en consideración las particularidades nacionales y garantiza la aplicación de los principios comunes de la UE de forma proporcionada. Gracias al amplio alcance de la Directiva, los Estados miembros podrán aplicarla en función de los riesgos reales que existan a escala nacional, expuestos en la estrategia nacional de SRI. La gestión de riesgos obligatoria solamente es aplicable a las entidades críticas e impone medidas proporcionales a los riesgos. En la consulta pública se destacaba la importancia de garantizar la seguridad de esas entidades críticas. Las obligaciones en materia de notificación únicamente se impondrían con respecto a los incidentes con efectos significativos. Como ya se ha señalado anteriormente, las medidas no ocasionarían gastos desproporcionados, ya que muchas de esas entidades que actúan como responsables del tratamiento ya están obligadas a asegurar la protección de los datos personales por la normativa de protección de datos vigente.

Para no imponer una carga desproporcionada a los pequeños operadores, y en especial a las pymes, los requisitos son proporcionales a los riesgos que presentan la red o el sistema de información de que se trate y no son aplicables a las microempresas. Las entidades sujetas a esas obligaciones deberán, en primer lugar, determinar los riesgos existentes y, a continuación, decidir las medidas que deban adoptarse para atenuarlos.

Los objetivos señalados pueden alcanzarse mejor a escala de la UE que de los Estados miembros, habida cuenta de los aspectos transfronterizos de los riesgos e incidentes de SRI. Por tanto, la UE puede adoptar medidas con arreglo al principio de subsidiariedad establecido en el artículo 5 del Tratado de la Unión Europea. De conformidad con el principio de proporcionalidad, la Directiva propuesta no excede de lo necesario para alcanzar esos objetivos.

Para alcanzar los objetivos, la Comisión debe ser autorizada a adoptar actos delegados, de conformidad con el artículo 290 del Tratado de Funcionamiento de la Unión Europea, al objeto de completar o modificar determinados elementos no esenciales del acto de base. Con la propuesta de la Comisión también se pretende respaldar un proceso de proporcionalidad en la aplicación de las obligaciones impuestas a los operadores públicos y privados.

A fin de garantizar condiciones uniformes de aplicación del acto de base, deben conferirse a la Comisión competencias para adoptar actos de ejecución con arreglo al artículo 291 del Tratado de Funcionamiento de la Unión Europea.

Teniendo presentes, en particular, el amplio alcance de la Directiva propuesta, el hecho de que afecta a ámbitos fuertemente regulados y las obligaciones jurídicas que se derivan de su capítulo IV, se considera necesario que se adjunten documentos explicativos a la notificación de las medidas de transposición. De conformidad con la Declaración política conjunta de los Estados miembros y de la Comisión sobre los documentos explicativos de 28 de septiembre de 2011, los Estados miembros se han comprometido a adjuntar a la notificación de sus medidas de transposición, cuando esté justificado, uno o varios documentos que expliquen la relación entre los elementos de una directiva y las partes correspondientes de los instrumentos

nacionales de transposición. Por lo que respecta a la presente Directiva, el legislador considera que la transmisión de tales documentos está justificada.

4. REPERCUSIONES PRESUPUESTARIAS

La cooperación y el intercambio de información entre los Estados miembros precisan infraestructuras seguras. La propuesta solamente tendrá repercusiones en el presupuesto de la UE si los Estados miembros optan por adaptar las infraestructuras existentes (por ejemplo, s-TESTA) y encomiendan las labores de ejecución a la Comisión dentro del MFP para el período 2014-2020. Se calcula que el coste único ascenderá a 1 250 000 EUR y se imputará al presupuesto de la UE, en la línea presupuestaria 09.03.02 (promover la interconexión y la interoperabilidad de los servicios públicos nacionales en línea, así como el acceso a estas redes — Capítulo 09.03, Mecanismo «Conectar Europa» — redes de telecomunicaciones), siempre que existan fondos disponibles en dicho Mecanismo. Los Estados miembros pueden compartir el coste único de adaptar las infraestructuras existentes o decidir crear nuevas infraestructuras y correr con los gastos de las mismas, que se estiman en unos 10 millones EUR anuales.

2013/0027 (COD)

Propuesta de

DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO

relativa a medidas para garantizar un elevado nivel común de seguridad de las redes y de la información en la Unión

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea y, en particular, su artículo 114,

Vista la propuesta de la Comisión Europea,

Previa transmisión del proyecto de acto legislativo a los parlamentos nacionales,

Visto el dictamen del Comité Económico y Social Europeo[1],

Previa consulta al Supervisor Europeo de Protección de Datos,

De conformidad con el procedimiento legislativo ordinario,

Considerando lo siguiente:

(1) Las redes y los sistemas y servicios de información desempeñan un papel crucial en la sociedad. Su fiabilidad y seguridad son esenciales para la actividad económica y el bienestar social y, en particular, para el funcionamiento del mercado interior.

(2) La magnitud y la frecuencia de los incidentes de seguridad, ya sean deliberados o accidentales, se están incrementando y representan una grave amenaza para el funcionamiento de las redes y los sistemas de información. Tales incidentes pueden interrumpir las actividades económicas, generar considerables pérdidas financieras, minar la confianza del usuario y causar grandes daños a la economía de la Unión.

(3) Al ser instrumentos de comunicación sin fronteras, los sistemas de información digitales —y sobre todo Internet— contribuyen decisivamente a facilitar la circulación transfronteriza de bienes, servicios y personas. Dado su carácter transnacional, una perturbación grave de esos sistemas en un Estado miembro puede afectar también a otros Estados miembros y a la Unión en su conjunto. Por consiguiente, la resiliencia y la estabilidad de las redes y los sistemas de información son fundamentales para el correcto funcionamiento del mercado interior.

(4) Es conveniente crear a escala de la Unión un mecanismo de cooperación que propicie el intercambio de información y una detección y respuesta coordinadas en relación con la seguridad de las redes y de la información (en lo sucesivo, «SRI»). Para que dicho mecanismo sea eficaz e integrador, es esencial que todos los Estados miembros posean unas capacidades mínimas y una estrategia que aseguren un elevado nivel de SRI en su territorio. Asimismo, procede imponer a las administraciones públicas y a los operadores de infraestructuras críticas de información requisitos mínimos en materia de seguridad para fomentar una cultura de gestión de riesgos y garantizar la notificación de los incidentes más graves.

[1] DO C […] de […], p. […].

(5) Para abarcar todos los incidentes y riesgos pertinentes, la presente Directiva debe aplicarse a todas las redes y a todos los sistemas de información. No obstante, las obligaciones impuestas a las administraciones públicas y a los operadores del mercado no deberían ser aplicables a las empresas que suministran redes públicas de comunicaciones o prestan servicios de comunicaciones electrónicas disponibles para el público con arreglo a la Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Directiva Marco)[2], que están sujetas a los requisitos específicos de seguridad e integridad establecidos en el artículo 13 *bis* de dicha Directiva, ni tampoco a los proveedores de servicios de confianza.

(6) Las capacidades existentes no bastan para garantizar un elevado nivel de SRI en la Unión. Los niveles de preparación de los Estados miembros son muy distintos, lo que da lugar a enfoques fragmentarios en la Unión. Esta situación engendra desiguales niveles de protección de los consumidores y las empresas, comprometiendo el nivel general de SRI de la Unión. A su vez, la inexistencia de requisitos mínimos comunes para las administraciones públicas y los operadores del mercado imposibilita la creación de un mecanismo global y efectivo de cooperación en la Unión.

(7) Para responder con eficacia a los problemas de seguridad de las redes y los sistemas de información es, pues, necesario un planteamiento global a escala de la Unión que integre requisitos mínimos comunes en materia de desarrollo de capacidades y planificación, actividades de intercambio de información y coordinación de medidas, así como requisitos mínimos comunes de seguridad para todos los operadores del mercado interesados y las administraciones públicas.

(8) Las disposiciones de la presente Directiva no han de obstar para que los Estados miembros adopten las medidas necesarias para asegurar la protección de sus intereses esenciales en materia de seguridad, salvaguardar el orden público y la seguridad pública, y permitir la investigación, detección y represión de delitos. De conformidad con el artículo 346 del TFUE, ningún Estado miembro debe estar obligado a facilitar información cuya divulgación considere contraria a los intereses esenciales de su seguridad.

(9) A fin de alcanzar y mantener un elevado nivel común de seguridad de las redes y los sistemas de información, los Estados miembros deben disponer de sendas estrategias nacionales de SRI que fijen los objetivos estratégicos y las medidas concretas que haya que aplicar. Deben elaborarse a escala nacional planes de cooperación en el ámbito de la SRI que cumplan los requisitos esenciales para así lograr niveles de capacidad de respuesta que hagan posible una cooperación efectiva y eficaz a escala nacional y de la Unión ante los incidentes que se produzcan.

(10) Con miras a una aplicación efectiva de las disposiciones adoptadas de conformidad con la presente Directiva, procede crear o designar en cada uno de los Estados miembros un organismo que coordine las cuestiones relacionadas con la SRI y actúe como centro de referencia nacional a efectos de cooperación transfronteriza a escala de la Unión. Estos organismos deben disponer de recursos técnicos, financieros y humanos suficientes para poder desempeñar efectiva y eficazmente las tareas que se les encomienden y alcanzar de este modo los objetivos de la presente Directiva.

(11) Todos los Estados miembros deben disponer de capacidades técnicas y de organización suficientes para poder adoptar las medidas de prevención, detección,

[2] DO L 108 de 24.4.2002, p. 33.

respuesta y atenuación oportunas ante los incidentes y riesgos que puedan afectar a las redes y los sistemas de información. Por consiguiente, procede crear en todos los Estados miembros equipos de respuesta a emergencias informáticas que funcionen correctamente y cumplan los requisitos esenciales para así disponer de capacidades efectivas y compatibles que permitan hacer frente a incidentes y riesgos y garantizar una cooperación eficaz a escala de la Unión.

(12) Sobre la base de los significativos avances logrados en el marco del Foro Europeo de Estados Miembros («EFMS») merced a los debates e intercambios sobre mejores prácticas, incluida la elaboración de principios de cooperación europea ante crisis cibernéticas, los Estados miembros y la Comisión deberían crear una red que los mantuviera en comunicación permanente y respaldara su cooperación. Se espera que este mecanismo seguro y efectivo de comunicación permita estructurar y coordinar a escala de la Unión las labores de intercambio de información, detección y respuesta.

(13) Es conveniente que la Agencia Europea de Seguridad de las Redes y de la Información («ENISA») preste asistencia a los Estados miembros y a la Comisión ofreciéndoles su experiencia, conocimientos y asesoramiento y facilitando el intercambio de mejores prácticas. En particular, la Comisión debe consultar a la ENISA a la hora de aplicar la presente Directiva. A fin de facilitar información eficaz y oportuna a los Estados miembros y la Comisión, deben lanzarse alertas tempranas sobre incidentes y riesgos en el marco de la red de cooperación. Al objeto de desarrollar capacidades y conocimientos entre los Estados miembros, la red de cooperación debe servir también de instrumento para el intercambio de mejores prácticas, ayudando a sus miembros a desarrollar capacidades y dirigiendo la organización de revisiones por homólogos y ejercicios de SRI.

(14) Es oportuno crear infraestructuras seguras para el intercambio de información delicada y confidencial en el marco de la red de cooperación. Sin perjuicio de la obligación de notificar a la red de cooperación los incidentes y riesgos que afecten a toda la Unión, el acceso a la información confidencial de otros Estados miembros solo debe permitirse a los Estados miembros que demuestren que sus recursos técnicos, financieros y humanos y sus procedimientos, así como sus infraestructuras de comunicación, garantizan su participación efectiva, eficiente y segura en la red.

(15) La cooperación entre los sectores público y privado reviste importancia esencial por cuanto la mayor parte de las redes y sistemas de información es de titularidad privada. Conviene alentar a los operadores del mercado a crear sus propios mecanismos de cooperación informal para garantizar la SRI. Asimismo, los operadores deben cooperar con el sector público e intercambiar información y mejores prácticas a cambio de obtener apoyo operativo en caso de que se produzcan incidentes.

(16) Para garantizar la transparencia e informar debidamente a los ciudadanos y operadores del mercado de la UE, conviene que las autoridades competentes creen un sitio web común para publicar información no confidencial sobre incidentes y riesgos.

(17) Cuando la información se considere confidencial de conformidad con las normas nacionales y de la Unión en materia de secreto comercial, debe mantenerse ese carácter confidencial a la hora de desarrollar las actividades y cumplir los objetivos establecidos en la presente Directiva.

(18) Basándose ante todo en las experiencias nacionales en materia de gestión de crisis y en cooperación con la ENISA, la Comisión y los Estados miembros deben elaborar un plan de cooperación de la Unión en materia de SRI que establezca mecanismos de

cooperación para hacer frente a riesgos e incidentes. Dicho plan debe tomarse debidamente en consideración a la hora de lanzar alertas tempranas en el marco de la red de cooperación.

(19) Las alertas tempranas solamente deben notificarse en el marco de la red cuando la dimensión y gravedad del incidente o riesgo en cuestión sean o puedan llegar a ser de tal envergadura que requieran medidas de información o coordinación de la respuesta a escala de la Unión. Por tanto, las alertas tempranas se deberían limitar a los incidentes o riesgos reales o potenciales que se extiendan rápidamente, superen la capacidad nacional de respuesta o afecten a más de un Estado miembro. Para poder proceder a un análisis adecuado, debe comunicarse a la red de cooperación toda la información pertinente para la evaluación del riesgo o incidente.

(20) Tras haber recibido y evaluado una alerta temprana, las autoridades competentes deben acordar una respuesta coordinada en el marco del plan de cooperación de la Unión en materia de SRI. Tanto las autoridades competentes como la Comisión deben estar informadas de las medidas adoptadas a escala nacional como resultado de la respuesta coordinada.

(21) El alcance mundial de los problemas de SRI hace necesaria una mayor cooperación internacional con miras a mejorar las normas de seguridad y el intercambio de información, y promover un planteamiento mundial común con respecto a las cuestiones de SRI.

(22) La responsabilidad de velar por la SRI recae en gran medida en las administraciones públicas y los operadores del mercado. Debe fomentarse una cultura de gestión de riesgos que entrañe una evaluación del riesgo y la aplicación de medidas de seguridad proporcionales a los riesgos existentes y que habrá de desarrollarse a través de requisitos reglamentarios adecuados y prácticas voluntarias del sector. Asimismo, son necesarias condiciones uniformes para garantizar el funcionamiento efectivo de la red de cooperación y, por ende, una colaboración eficaz de todos los Estados miembros.

(23) La Directiva 2002/21/CE establece que las empresas que suministran redes públicas de comunicaciones o prestan servicios de comunicaciones electrónicas disponibles para el público deben adoptar medidas adecuadas para salvaguardar su integridad y seguridad e introduce requisitos de notificación de las violaciones de la seguridad y las pérdidas de integridad. La Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas)[3] exige que los proveedores de servicios de comunicaciones electrónicas accesibles para el público tomen las medidas técnicas y de organización necesarias para velar por la seguridad de sus servicios.

(24) Estas obligaciones no solo han de imponerse al sector de las comunicaciones electrónicas, sino también a los principales proveedores de servicios de la sociedad de la información, tal y como se definen en la Directiva 98/34/CE del Parlamento Europeo y del Consejo, de 22 de junio de 1998, por la que se establece un procedimiento de información en materia de las normas y reglamentaciones técnicas y de las reglas relativas a los servicios de la sociedad de la información[4], que sirven de apoyo a los servicios de la sociedad de la información derivados o a las actividades en línea, tales como las plataformas de comercio electrónico, las pasarelas de pago por

[3] DO L 201 de 31.7.2002, p. 37.
[4] DO L 204 de 21.7.1998, p. 37.

Internet, las redes sociales, los motores de búsqueda, los servicios de computación en nube o las tiendas de aplicaciones. La interrupción de estos servicios de apoyo a la sociedad de la información impide la prestación de otros servicios de la sociedad de la información que dependen de ellos. Los desarrolladores de programas informáticos y los fabricantes de equipos físicos no son proveedores de servicios de la sociedad de la información y quedan, por tanto, excluidos. Procede imponer asimismo esas obligaciones a las administraciones públicas y a los operadores de infraestructuras críticas, que son muy dependientes de las tecnologías de la información y la comunicación y desempeñan un papel esencial en el mantenimiento de funciones económicas o sociales vitales, tales como el gas y la electricidad, los transportes, las entidades de crédito, las bolsas y la sanidad. Los trastornos que puedan sufrir tales redes y sistemas de información afectan al mercado interior.

(25) Las medidas técnicas y de organización impuestas a las administraciones públicas y a los operadores del mercado no requerirán que se diseñe, se desarrolle o fabrique de una manera especial un determinado producto comercial de tecnología de la información y la comunicación.

(26) Las administraciones públicas y los operadores del mercado deben velar por la seguridad de las redes y sistemas que se hallan bajo su control. Se trata fundamentalmente de redes y sistemas privados gestionados por el personal de TI interno o cuya seguridad se ha encomendado a empresas externas. Las obligaciones en materia de seguridad y notificación han de aplicarse a los operadores del mercado y a las administraciones públicas pertinentes, independientemente de si se encargan ellos mismos del mantenimiento de sus redes y sistemas de información o lo subcontratan.

(27) Para no imponer una carga financiera y administrativa desproporcionada a los pequeños operadores y a los usuarios, los requisitos han de ser proporcionales a los riesgos que presenta la red o el sistema de información en cuestión, habida cuenta del estado de la técnica. Dichos requisitos no deben aplicarse a las microempresas.

(28) Las autoridades competentes deben procurar que se mantengan los canales de intercambio de información informales y de confianza entre los operadores del mercado y entre los sectores público y privado. Antes de dar publicidad a los incidentes notificados a las autoridades competentes, es preciso sopesar debidamente el interés de los ciudadanos en ser informados sobre las amenazas existentes y los perjuicios que en términos comerciales y de reputación puedan sufrir las administraciones públicas y los operadores del mercado que notifican los incidentes. A la hora de cumplir sus obligaciones de notificación, las autoridades competentes han de tener muy en cuenta la necesidad de mantener estrictamente confidencial la información sobre los puntos vulnerables del producto antes de dar a conocer las soluciones de seguridad adecuadas.

(29) Es preciso que las autoridades competentes dispongan de los medios necesarios para desempeñar su cometido y, en particular, de competencias para obtener información suficiente de los operadores del mercado y las administraciones públicas a fin de evaluar el nivel de seguridad de las redes y los sistemas de información, así como datos fidedignos y exhaustivos sobre incidentes reales que hayan repercutido en el funcionamiento de las redes y los sistemas de información.

(30) Los incidentes suelen estar causados por actividades delictivas. Cabe suponer el carácter delictivo de los incidentes aun cuando las pruebas para demostrarlo no sean lo suficientemente claras desde el principio. A este respecto, una cooperación adecuada entre las autoridades competentes y los cuerpos de seguridad debería formar parte de

una respuesta efectiva y global ante la amenaza de que se produzcan incidentes de seguridad. En particular, para promover un entorno protegido, seguro y más resiliente es preciso notificar sistemáticamente los incidentes de carácter supuestamente delictivo a los cuerpos de seguridad. La naturaleza delictiva grave de los incidentes debe evaluarse a la luz de la normativa de la UE sobre ciberdelincuencia.

(31) En numerosas ocasiones los datos de carácter personal se ven comprometidos a raíz de incidentes. En este contexto, las autoridades competentes y las autoridades responsables de la protección de datos han de cooperar e intercambiar la información pertinente ante las violaciones de datos personales derivadas de incidentes. Los Estados miembros deben imponer la obligación de notificar los incidentes de seguridad de modo que se reduzca al mínimo la carga administrativa en caso de que el incidente de seguridad constituya también una violación de datos personales con arreglo al Reglamento del Parlamento Europeo y del Consejo 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[5]. En colaboración con las autoridades competentes y las autoridades responsables de la protección de datos, la ENISA podría contribuir a elaborar mecanismos de intercambio de información y modelos que evitaran la necesidad de contar con dos modelos de notificación. Este modelo único de notificación facilitaría la comunicación de incidentes que comprometan los datos personales, aliviando de este modo la carga administrativa para empresas y administraciones públicas.

(32) La normalización de los requisitos en materia de seguridad es un proceso impulsado por el mercado. Al objeto de garantizar una aplicación convergente de las normas de seguridad, es oportuno que los Estados miembros fomenten el cumplimiento de normas específicas o la conformidad con ellas para así lograr un elevado nivel de seguridad en la Unión. A tal fin, puede ser necesario elaborar normas armonizadas, de acuerdo con las disposiciones del Reglamento (UE) nº 1025/2012 del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre la normalización europea, por el que se modifican las Directivas 89/686/CEE y 93/15/CEE del Consejo y las Directivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE y 2009/105/CE del Parlamento Europeo y del Consejo y por el que se deroga la Decisión 87/95/CEE del Consejo y la Decisión nº 1673/2006/CE del Parlamento Europeo y del Consejo[6].

(33) La Comisión debe revisar periódicamente las disposiciones contenidas en la presente Directiva, en particular con vistas a determinar si es preciso modificarlas a la luz de la cambiante situación de la tecnología o el mercado.

(34) En aras del correcto funcionamiento de la red de cooperación, procede delegar en la Comisión poderes para adoptar actos de conformidad con el artículo 290 del Tratado de Funcionamiento de Unión Europea en relación con la determinación de los criterios que debe reunir un Estado miembro para poder ser autorizado a participar en el sistema de intercambio seguro de información, con la especificación de los hechos que activan la alterta temprana y con la definición de las circunstancias en que los operadores del mercado y las administraciones públicas están obligados a notificar incidentes.

(35) Reviste primordial importancia que la Comisión lleve a cabo las consultas oportunas durante la fase preparatoria, en particular con expertos. Al preparar y elaborar actos

[5] SEC(2012) 72 final.
[6] DO L 316 de 14.11.2012, p. 12.

delegados, la Comisión debe garantizar que los documentos pertinentes se transmitan al Parlamento Europeo y al Consejo de manera simultánea, oportuna y adecuada.

(36) A fin de garantizar condiciones uniformes de ejecución de la presente Directiva, procede conferir competencias de ejecución a la Comisión en lo que respecta a la cooperación entre las autoridades competentes y la Comisión en el marco de la red de cooperación, el acceso a las infraestructuras seguras de intercambio de información, el plan de cooperación de la Unión en materia de SRI, los formatos y procedimientos aplicables a la hora de informar a los ciudadanos sobre incidentes y las normas o especificaciones técnicas en materia de SRI. Dichas competencias deben ejercerse de conformidad con el Reglamento (UE) nº 182/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión[7].

(37) Es conveniente que, a la hora de aplicar la presente Directiva, la Comisión colabore, cuando proceda, con los comités sectoriales y organismos pertinentes establecidos a escala de la UE, especialmente en los ámbitos de la energía, los transportes y la sanidad.

(38) La información que una autoridad competente considere confidencial de acuerdo con las normas nacionales y de la Unión sobre secreto comercial únicamente debe intercambiarse con la Comisión y otras autoridades competentes cuando tal intercambio sea estrictamente necesario a los efectos de la aplicación de la presente Directiva. El intercambio se debe limitar a la información que resulte pertinente y proporcional a la finalidad perseguida.

(39) El intercambio de información sobre riesgos e incidentes en el marco de la red de cooperación y el cumplimiento de la obligación de notificar los incidentes a las autoridades nacionales competentes pueden hacer necesario el tratamiento de datos personales. Dicho tratamiento es necesario para alcanzar los objetivos de interés público perseguidos por la presente Directiva y es por tanto legítimo en virtud del artículo 7 de la Directiva 95/46/CE. No constituye, en relación con esos objetivos legítimos, una intervención desmesurada e intolerable que afecte a la propia esencia del derecho a la protección de los datos personales garantizado por el artículo 8 de la Carta de los Derechos Fundamentales. Al llevar a la práctica la presente Directiva, se debe aplicar, cuando proceda, el Reglamento (CE) nº 1049/2001 del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión[8]. Cuando las instituciones y órganos de la Unión procedan al tratamiento de datos a los efectos de la aplicación de la presente Directiva, dicho tratamiento deberá efectuarse de conformidad con los dispuesto en el Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos.

(40) Dado que el objetivo de la presente Directiva, a saber, garantizar un elevado nivel de SRI en la Unión, no puede ser alcanzado de manera suficiente por los Estados miembros de manera individual y, por consiguiente, debido a los efectos de la acción, puede lograrse mejor a nivel de la Unión, esta puede adoptar medidas, de acuerdo con el principio de subsidiariedad establecido en el artículo 5 del Tratado de la Unión

[7] DO L 55 de 28.2.2011, p. 13.
[8] DO L 145 de 31.5.2001, p. 43.

Europea. De conformidad con el principio de proporcionalidad enunciado en dicho artículo, la presente Directiva no excede de lo necesario para alcanzar estos objetivos.

(41) La presente Directiva observa los derechos fundamentales y los principios reconocidos por la Carta de los Derechos Fundamentales de la Unión Europea y, en particular, el derecho al respeto de la vida privada y las comunicaciones, el derecho a la protección de los datos de carácter personal, el derecho a la libertad de empresa, el derecho a la propiedad, el derecho a una tutela judicial efectiva y el derecho a ser oído. La presente Directiva debe aplicarse de acuerdo con estos derechos y principios.

HAN ADOPTADO LA PRESENTE DIRECTIVA:

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1

Objeto y ámbito de aplicación

1. La presente Directiva establece medidas para garantizar un elevado nivel común de seguridad de las redes y de la información (denominada en lo sucesivo «SRI») en la Unión.

2. A tal fin, la presente Directiva:

a) establece las obligaciones que han de cumplir todos los Estados miembros en materia de prevención, gestión y respuesta a riesgos e incidentes que afecten a las redes y los sistemas de información;

b) establece un mecanismo de cooperación entre los Estados miembros con el fin de garantizar la aplicación uniforme de la presente Directiva en la Unión y, en su caso, una gestión y una respuesta eficaces y coordinadas ante los riesgos e incidentes que afecten a las redes y los sistemas de información;

c) establece requisitos en materia de seguridad para los operadores del mercado y las administraciones públicas.

3. Los requisitos de seguridad previstos en el artículo 14 no serán aplicables a las empresas que suministran redes públicas de comunicaciones o prestan servicios de comunicaciones electrónicas disponibles para el público con arreglo a la Directiva 2002/21/CE, que están sujetas a los requisitos específicos de seguridad e integridad establecidos en los artículos 13 *bis* y 13 *ter* de dicha Directiva, ni tampoco a los proveedores de servicios de confianza.

4. La presente Directiva se entenderá sin perjuicio de la normativa sobre ciberdelincuencia de la UE y de la Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección[9].

5. Asimismo, la presente Directiva se entenderá sin perjuicio de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[10], de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de

[9] DO L 345 de 23.12.2008, p. 75.
[10] DO L 281 de 23.11.1995, p. 31.

los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, y del Reglamento del Parlamento Europeo y del Consejo 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[11].

6. El intercambio de información en el marco de la red de cooperación a que se hace referencia en el capítulo III y las notificaciones de incidentes de SRI contempladas en el artículo 14 pueden requerir el tratamiento de datos personales. Dicho tratamiento, que es necesario para alcanzar los objetivos de interés público perseguidos por la presente Directiva, será autorizado por el Estado miembro interesado de acuerdo con el artículo 7 de la Directiva 95/46/CE y con la Directiva 2002/58/CE según su adopción en el Derecho interno.

Artículo 2

Armonización mínima

No se impedirá que los Estados miembros adopten o mantengan disposiciones que garanticen un nivel de seguridad más elevado, sin perjuicio de las obligaciones que les impone la normativa de la Unión.

Artículo 3

Definiciones

A los efectos de la presente Directiva, se entenderá por:

1) «redes y sistemas de información»:

   a) una red de comunicaciones electrónicas en la acepción de la Directiva 2002/21/CE,

   b) todo dispositivo o grupo de dispositivos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos,

   c) los datos informáticos almacenados, tratados, recuperados o transmitidos por los elementos contemplados en las letras a) y b) para su funcionamiento, utilización, protección y mantenimiento;

2) «seguridad»: la capacidad de las redes y sistemas de información de resistir, con un nivel determinado de confianza, a acciones accidentales o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos;

3) «riesgo»: toda circunstancia o hecho que pueda tener efectos adversos en la seguridad;

4) «incidente»: toda circunstancia o hecho que tenga efectos adversos en la seguridad;

5) «servicio de la sociedad de la información»: un servicio en la acepción del artículo 1, número 2, de la Directiva 98/34/CE;

6) «plan de cooperación en materia de SRI»: un plan que constituye el marco para las funciones, responsabilidades y procedimientos de organización a fin de mantener o

[11] SEC(2012) 72 final.

restablecer el funcionamiento de las redes y los sistemas de información en caso de que se vean afectados por un riesgo o incidente;

7) «gestión de incidentes»: todos los procedimientos seguidos para analizar, limitar y responder a un incidente;

8) «operador del mercado»:

   a) un proveedor de servicios de la sociedad de la información que posibilitan la prestación de otros servicios de la sociedad de la información, una lista no exhaustiva de los cuales figura en el anexo II;

   b) un operador de infraestructuras críticas esenciales para el mantenimiento de actividades económicas y sociales vitales en los sectores de la energía, los transportes, la banca, la bolsa y la sanidad, una lista no exhaustiva de los cuales figura en el anexo II.

9) «norma»: una norma en la acepción del Reglamento (UE) nº 1025/2012;

10) «especificación»: una especificación en la acepción del Reglamento (UE) nº 1025/2012;

11) «proveedor de servicios de confianza»: una persona física o jurídica que presta un servicio electrónico consistente en la creación, verificación, validación, gestión y conservación de firmas electrónicas, sellos electrónicos, marcas de tiempo electrónicas, documentos electrónicos, servicios de entrega electrónica, autenticación de sitios web y certificados electrónicos, incluidos los certificados de firma electrónica y de sello electrónico.

CAPÍTULO II

MARCOS NACIONALES DE SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN

Artículo 4

Principio

Los Estados miembros garantizarán un elevado nivel común de seguridad de las redes y los sistemas de información en sus territorios de conformidad con lo dispuesto en la presente Directiva.

Artículo 5

Estrategia nacional de SRI y plan de cooperación nacional en materia de SRI

1. Cada Estado miembro adoptará una estrategia nacional de SRI que establezca los objetivos estratégicos y las medidas estratégicas y reglamentarias concretas para alcanzar y mantener un elevado nivel de seguridad de las redes y de la información. La estrategia nacional de SRI abordará, en particular, las cuestiones siguientes:

a) Determinación de los objetivos y prioridades de la estrategia sobre la base de un análisis actualizado de riesgos e incidentes.

b) Marco de gobernanza para lograr los objetivos y las prioridades de la estrategia, con una definición clara de las funciones y responsabilidades de las instituciones públicas y los demás agentes pertinentes.

c) Determinación de las medidas generales sobre preparación, respuesta y recuperación, incluidos los mecanismos de cooperación entre los sectores público y privado.

d) Indicación de los programas de educación, concienciación y formación.

e) Planes de investigación y desarrollo y explicación de la manera en que reflejan las prioridades establecidas.

2. La estrategia nacional de SRI incluirá un plan de cooperación nacional en materia de SRI que contemple como mínimo los siguientes aspectos:

a) Plan de evaluación de riesgos que permita determinarlos y evaluar los efectos de incidentes potenciales.

b) Determinación de las funciones y responsabilidades de los diversos agentes que participan en la ejecución del plan.

c) Determinación de los procedimientos de cooperación y comunicación necesarios para garantizar la prevención, detección, respuesta, reparación y recuperación, adaptados en función del nivel de alerta.

d) Hoja de ruta sobre ejercicios y actividades de formación en el ámbito de la SRI para reforzar, validar y someter a ensayo el plan. La experiencia adquirida se deberá documentar e incorporar a las actualizaciones del plan.

3. La estrategia nacional de SRI y el plan de cooperación nacional en materia de SRI se deberán remitir a la Comisión en el plazo de un mes a partir de su adopción.

Artículo 6

Autoridad nacional competente en materia de seguridad de las redes y los sistemas de información

1. Cada Estado miembro designará una autoridad nacional competente en materia de seguridad de las redes y los sistemas de información («la autoridad competente»).

2. Las autoridades competentes supervisarán la aplicación de la presente Directiva a escala nacional y contribuirán a una aplicación coherente de la misma en toda la Unión.

3. Los Estados miembros velarán por que las autoridades competentes dispongan de suficientes recursos técnicos, financieros y humanos para llevar a cabo las tareas a ellas asignadas de forma eficiente y eficaz y cumplir así los objetivos de la presente Directiva. Los Estados miembros garantizarán una cooperación eficiente, eficaz y segura entre las autoridades competentes a través de la red a que se hace referencia en el artículo 8.

4. Los Estados miembros velarán por que las autoridades competentes reciban las notificaciones de incidentes de las administraciones públicas y los operadores del mercado con arreglo al artículo 14, apartado 2, y se les confieran las competencias de aplicación a que se refiere el artículo 15.

5. Las autoridades competentes llevarán a cabo consultas y cooperarán, cuando proceda, con las fuerzas de seguridad nacionales y las autoridades responsables de la protección de datos.

6. Los Estados miembros notificarán sin demora a la Comisión la autoridad competente que hayan designado, su cometido y cualquier cambio posterior que se introduzca en él. Los Estados miembros harán pública la designación de la autoridad competente.

Artículo 7

Equipo de respuesta a emergencias informáticas

1. Cada Estado miembro creará un equipo de respuesta a emergencias informáticas (en lo sucesivo, «CERT») responsable de la gestión de incidentes y riesgos de acuerdo con un procedimiento claramente definido, que se ajustará a los requisitos establecidos en el anexo I, punto 1. Podrá crearse un CERT en el marco de la autoridad competente.

2. Los Estados miembros velarán por que los CERT cuenten con suficientes recursos técnicos, financieros y humanos para llevar a cabo efectivamente las tareas que les correspondan, establecidas en el anexo I, punto 2.

3. Los Estados miembros velarán por que los CERT dispongan a escala nacional de infraestructuras de comunicación e información seguras y resilientes, que serán compatibles e interoperables con el sistema seguro de intercambio de información a que se hace referencia en el artículo 9.

4. Los Estados miembros informarán a la Comisión de los recursos, el mandato y el procedimiento de gestión de incidentes de los CERT.

5. Los CERT actuarán bajo la supervisión de la autoridad competente, que comprobará periódicamente la adecuación de sus recursos, su mandato y la eficacia de su procedimiento de gestión de incidentes.

CAPÍTULO III

COOPERACIÓN ENTRE LAS AUTORIDADES COMPETENTES

Artículo 8

Red de cooperación

1. Las autoridades competentes y la Comisión crearán una red («red de cooperación») para colaborar contra los riesgos e incidentes que afecten a las redes y los sistemas de información.

2. La Comisión y las autoridades competentes mantendrán una comunicación constante en el marco de la red de cooperación. Cuando así se le solicite, la Agencia Europea de Seguridad de las Redes y de la Información («ENISA») asistirá a la red de cooperación ofreciéndole su experiencia, conocimientos y asesoramiento.

3. En el marco de la red de cooperación, las autoridades competentes:

   a) difundirán alertas tempranas sobre riesgos e incidentes de conformidad con el artículo 10;

   b) ofrecerán una respuesta coordinada de conformidad con el artículo 11;

   c) publicarán periódicamente en un sitio web común información no confidencial sobre las alertas tempranas y las respuestas coordinadas en curso;

   d) examinarán y evaluarán conjuntamente, a petición de un Estado miembro o de la Comisión, uno o varios planes de cooperación nacionales en materia de SRI y estrategias nacionales de SRI, contemplados en el artículo 5, en el marco de la presente Directiva;

e) examinarán y evaluarán conjuntamente, a petición de un Estado miembro o de la Comisión, la eficacia de los CERT, especialmente cuando los ejercicios de SRI se realicen a escala de la Unión;

f) cooperarán e intercambiarán información sobre todas las cuestiones pertinentes con el Centro Europeo de Ciberdelincuencia de Europol y con otros organismos europeos pertinentes, en particular en los sectores de la protección de datos, la energía, los transportes, la banca, la bolsa y la sanidad;

g) intercambiarán información y mejores prácticas entre sí y con la Comisión, y se ayudarán mutuamente con el fin de crear capacidades en materia de SRI;

h) organizarán revisiones por homólogos periódicas sobre capacidades y preparación;

i) organizarán ejercicios de SRI a escala de la Unión y participarán, en su caso, en ejercicios de SRI internacionales.

4. La Comisión establecerá mediante actos de ejecución las disposiciones necesarias para facilitar la cooperación entre las autoridades competentes y la Comisión a que se hace referencia en los apartados 2 y 3. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de consulta contemplado en el artículo 19, apartado 2.

Artículo 9

Sistema seguro de intercambio de información

1. El intercambio de información delicada y confidencial dentro de la red de cooperación se efectuará a través de una infraestructura segura.

2. La Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 18 a fin de fijar los criterios que ha de reunir un Estado miembro para ser autorizado a participar en el sistema seguro de intercambio de información, en relación con:

a) la disponibilidad a escala nacional de infraestructuras de comunicación e información seguras y resilientes que sean compatibles e interoperables con la infraestructura segura de la red de cooperación de conformidad con el artículo 7, apartado 3, y

b) la existencia de recursos y procedimientos técnicos, financieros y humanos adecuados para su autoridad competente y el CERT, de modo que sea posible una participación eficiente, eficaz y segura en el sistema seguro de intercambio de información contemplado en el artículo 6, apartado 3, el artículo 7, apartado 2, y el artículo 7, apartado 3.

3. La Comisión adoptará mediante actos de ejecución decisiones sobre el acceso de los Estados miembros a esta infraestructura segura, con arreglo a los criterios mencionados en los apartados 2 y 3. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 19, apartado 3.

Artículo 10

Alertas tempranas

1. Las autoridades competentes o la Comisión difundirán alertas tempranas en el marco de la red de cooperación en relación con los riesgos e incidentes que cumplan como mínimo una de las condiciones siguientes:

   a) riesgos e incidentes cuya magnitud aumente o pueda aumentar rápidamente;

   b) riesgos e incidentes que sobrepasen o puedan sobrepasar la capacidad nacional de respuesta;

   c) riesgos e incidentes que afecten o puedan afectar a más de un Estado miembro.

2. Las autoridades competentes y la Comisión incluirán en sus alertas tempranas toda la información pertinente que obre en su poder y pueda ser de utilidad para evaluar el riesgo o incidente.

3. A petición de un Estado miembro o por iniciativa propia, la Comisión podrá solicitar a un Estado miembro que proporcione la información pertinente sobre un riesgo o incidente concreto.

4. Cuando se sospeche que el riesgo o incidente objeto de una alerta temprana es de carácter delictivo, las autoridades competentes o la Comisión informarán de ello al Centro Europeo de Ciberdelincuencia de Europol.

5. La Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 18 con el fin de especificar los riesgos e incidentes que pueden activar la alerta temprana mencionada en el apartado 1.

Artículo 11

Respuesta cordinada

1. Cuando reciban la alerta temprana a que se refiere el artículo 10, las autoridades competentes evaluarán la información pertinente y acordarán una respuesta coordinada de conformidad con el plan de cooperación de la Unión en materia de SRI contemplado en el artículo 12.

2. Las diversas medidas adoptadas a escala nacional a raíz de la respuesta coordinada se notificarán a la red de cooperación.

Artículo 12

Plan de cooperación de la Unión en materia de SRI

1. La Comisión estará facultada para adoptar mediante actos de ejecución un plan de cooperación de la Unión en materia de SRI. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 19, apartado 3.

2. El plan de cooperación de la Unión en materia de SRI establecerá:

   a) a los efectos del artículo 10:

      – el formato y los procedimientos de recopilación e intercambio de información compatible y comparable sobre riesgos e incidentes por parte de las autoridades competentes,

– los procedimientos y criterios de evaluación de riesgos e incidentes por parte de la red de cooperación;

b) los procedimientos que se han de seguir para ofrecer las respuestas coordinadas previstas en el artículo 11, entre ellos el reparto de funciones y responsabilidades y los procedimientos de cooperación;

c) una hoja de ruta sobre ejercicios y actividades de formación en el ámbito de la SRI para reforzar, validar y someter a ensayo el plan;

d) un programa de transferencia de conocimientos entre los Estados miembros en materia de desarrollo de capacidades y aprendizaje entre homólogos;

e) un programa de concienciación y formación entre los Estados miembros.

3. El plan de cooperación de la Unión en materia de SRI deberá adoptarse dentro del año siguiente a la entrada en vigor de la presente Directiva y se revisará periódicamente.

Artículo 13

Cooperación internacional

Sin perjuicio de la posibilidad de que la red de cooperación mantenga relaciones informales de colaboración a escala internacional, la Unión podrá concluir acuerdos internacionales con terceros países u organizaciones internacionales que hagan posible y organicen su participación en algunas actividades de la red de cooperación. En tales acuerdos se tendrá en cuenta la necesidad de deparar una protección adecuada a los datos personales que circulen en la red de cooperación.

CAPÍTULO IV

SEGURIDAD DE LAS REDES Y SISTEMAS DE INFORMACIÓN DE LAS ADMINISTRACIONES PÚBLICAS Y LOS OPERADORES DEL MERCADO

Artículo 14

Requisitos en materia de seguridad y notificación de incidentes

1. Los Estados miembros velarán por que las administraciones públicas y los operadores del mercado tomen las medidas técnicas y de organización apropiadas para gestionar los riesgos existentes para la seguridad de las redes y los sistemas de información que controlan y utilizan en sus operaciones. Habida cuenta del estado de la técnica, dichas medidas garantizarán un nivel de seguridad adecuado en relación con el riesgo existente. En particular, adoptarán medidas para prevenir y reducir al mínimo los efectos de los incidentes que afecten a sus redes y sistemas de información en los servicios básicos que prestan, garantizando de este modo la continuidad de los servicios que dependen de tales redes y sistemas de información.

2. Los Estados miembros velarán por que las administraciones públicas y los operadores del mercado notifiquen a la autoridad competente los incidentes que tengan efectos significativos en la seguridad de los servicios básicos que prestan.

3. Los requisitos establecidos en los apartados 1 y 2 serán aplicables a todos los operadores del mercado que prestan servicios en la Unión Europea.

4. Cuando estime que la divulgación de un incidente redunda en el interés público, la autoridad competente podrá informar de él a los ciudadanos o pedir a las

administraciones públicas y los operadores del mercado que lo hagan. Una vez al año, la autoridad competente presentará a la red de cooperación un informe resumido sobre las notificaciones recibidas y las medidas adoptadas de acuerdo con el presente apartado.

5. La Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 18 con el fin de determinar las circunstancias en que las administraciones públicas y los operadores del mercado estarán obligados a notificar incidentes.

6. A reserva de cualesquiera actos delegados adoptados en virtud del apartado 5, las autoridades competentes podrán adoptar directrices y, en caso necesario, impartir instrucciones sobre las circunstancias en que las administraciones públicas y los operadores del mercado estarán obligados a notificar incidentes.

7. La Comisión estará facultada para determinar mediante actos de ejecución los formatos y procedimientos aplicables a los efectos del apartado 2. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 19, apartado 3.

8. Los apartados 1 y 2 no serán aplicables a las microempresas, según la definición que recoge la Recomendación 2003/361/CE de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas[12].

Artículo 15

Aplicación y observancia

1. Los Estados miembros velarán por que las autoridades competentes dispongan de todas las competencias necesarias para investigar los casos de incumplimiento por parte de las administraciones públicas o los operadores del mercado de las obligaciones que les impone el artículo 14 y los efectos que tengan en la seguridad de las redes y los sistemas de información.

2. Los Estados miembros velarán por que las autoridades competentes estén facultadas para exigir a los operadores del mercado y a las administraciones públicas:

   a) que proporcionen la información necesaria para evaluar la seguridad de sus redes y sistemas de información, incluida la documentación sobre las políticas de seguridad;

   b) que se sometan a una auditoría de seguridad practicada por un organismo independiente o una autoridad nacional cualificados y pongan los resultados en conocimiento de la autoridad competente.

3. Los Estados miembros velarán por que las autoridades competentes estén facultadas para impartir instrucciones vinculantes a los operadores del mercado y a las administraciones públicas.

4. Las autoridades competentes notificarán los incidentes de carácter grave y supuestamente delictivo a los cuerpos de seguridad.

5. Las autoridades competentes cooperarán estrechamente con las autoridades responsables de la protección de datos personales a la hora de hacer frente a incidentes que den lugar a violaciones de datos personales.

[12] DO L 124 de 20.5.2003, p. 36.

6. Los Estados miembros garantizarán que cualesquiera obligaciones impuestas a las administraciones públicas y a los operadores del mercado en virtud del presente capítulo puedan estar sujetas a control judicial.

Artículo 16

Normalización

1. A fin de garantizar una aplicación convergente de lo dispuesto en el artículo 14, apartado 1, los Estados miembros fomentarán la utilización de las normas y especificaciones pertinentes en materia de seguridad de las redes y la información.

2. La Comisión elaborará mediante actos de ejecución una lista de las normas mencionadas en el apartado 1. Dicha lista se publicará en el *Diario Oficial de la Unión Europea*.

CAPÍTULO V

DISPOSICIONES FINALES

Artículo 17

Sanciones

1. Los Estados miembros establecerán normas sobre las sanciones aplicables a las infracciones de las disposiciones nacionales adoptadas en virtud de la presente Directiva y tomarán todas las medidas necesarias para garantizar su aplicación. Las sanciones adoptadas deberán ser eficaces, proporcionadas y disuasorias. Los Estados miembros notificarán esas disposiciones a la Comisión a más tardar en la fecha de transposición de la presente Directiva, y le notificarán además sin demora cualquier modificación posterior que les afecte.

2. Los Estados miembros garantizarán que, en caso de que un incidente de seguridad afecte a datos personales, las sanciones previstas guarden coherencia con las sanciones establecidas en el Reglamento del Parlamento Europeo y del Consejo 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[13].

Artículo 18

Ejercicio de la delegación

1. Se otorgan a la Comisión poderes para adoptar actos delegados de acuerdo con las condiciones establecidas en el presente artículo.

2. Se otorgan a la Comisión los poderes para adoptar los actos delegados a que se refieren el artículo 9, apartado 2, el artículo 10, apartado 5, y el artículo 14, apartado 5. La Comisión elaborará un informe sobre los poderes delegados a más tardar nueve meses antes de que finalice el período de cinco años. La delegación de poderes se prorrogará automáticamente por períodos de idéntica duración, excepto si el Parlamento Europeo o el Consejo se oponen a dicha prórroga a más tardar tres meses antes del final de cada período.

3. La delegación de poderes a que se refieren el artículo 9, apartado 2, el artículo 10, apartado 5, y el artículo 14, apartado 5, podrá ser revocada en cualquier momento por

[13] SEC(2012) 72 final.

el Parlamento Europeo o por el Consejo. La decisión de revocación pondrá término a la delegación de los poderes que en ella se especifiquen. Surtirá efecto al día siguiente de la publicación de la decisión en el *Diario Oficial de la Unión Europea* o en una fecha posterior que se precisará en dicha decisión. No afectará a la validez de los actos delegados que ya estén en vigor.

4. En cuanto la Comisión adopte un acto delegado, lo notificará simultáneamente al Parlamento Europeo y al Consejo.

5. Los actos delegados adoptados en virtud del artículo 9, apartado 2, del artículo 10, apartado 5, y del artículo 14, apartado 5, entrarán en vigor únicamente si, en un plazo de dos meses desde su notificación al Parlamento Europeo y al Consejo, ni el Parlamento Europeo ni el Consejo formulan objeciones o si, antes del vencimiento de dicho plazo, tanto el uno como el otro informan a la Comisión de que no las formularán. Este plazo se prorrogará dos meses a iniciativa del Parlamento Europeo o del Consejo.

Artículo 19

Procedimiento de comité

1. La Comisión estará asistida por un comité (el Comité de Seguridad de las Redes y de la Información). Dicho comité será un comité en la acepción del Reglamento (UE) nº 182/2011.

2. En los casos en que se haga referencia al presente apartado, será de aplicación el artículo 4 del Reglamento (UE) nº 182/2011.

3. En los casos en que se haga referencia al presente apartado, será de aplicación el artículo 5 del Reglamento (UE) nº 182/2011.

Artículo 20

Revisión

La Comisión revisará periódicamente el funcionamiento de la presente Directiva e informará al Parlamento Europeo y al Consejo. El primer informe se presentará a más tardar tres años después de la fecha de transposición mencionada en el artículo 21. A tal fin, la Comisión podrá solicitar a los Estados miembros que faciliten información sin demoras injustificadas.

Artículo 21

Transposición

1. Los Estados miembros adoptarán y publicarán, a más tardar [un año y medio después de la fecha de adopción], las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la presente Directiva. Comunicarán inmediatamente a la Comisión el texto de dichas disposiciones.

   Aplicarán esas medidas a partir del [un año y medio después de la fecha de adopción].

   Cuando los Estados miembros adopten dichas disposiciones, estas harán referencia a la presente Directiva o irán acompañadas de dicha referencia en su publicación oficial. Los Estados miembros establecerán las modalidades de la mencionada referencia.

2. Los Estados miembros comunicarán a la Comisión el texto de las disposiciones básicas de Derecho interno que adopten en el ámbito regulado por la presente Directiva.

Artículo 22

Entrada en vigor

La presente Directiva entrará en vigor el [vigésimo] día siguiente al de su publicación en el *Diario Oficial de la Unión Europea.*

Artículo 23

Destinatarios

Los destinatarios de la presente Directiva serán los Estados miembros.

Hecho en Bruselas, el

Por el Parlamento Europeo	*Por el Consejo*
El Presidente	*El Presidente*

ANEXO I

Obligaciones y tareas del equipo de respuesta a emergencias informáticas (CERT)

Las obligaciones y tareas del CERT estarán adecuada y claramente definidas y se basarán en la política o la reglamentación nacional. Incluirán los siguientes elementos:

1) Obligaciones del CERT

a) El CERT garantizará una gran disponibilidad de sus servicios de comunicaciones evitando los fallos puntuales simples y contará con varios medios para ser contactado y contactar con otros. Además, los canales de comunicación estarán claramente especificados y serán bien conocidos por los grupos de usuarios y los socios colaboradores.

b) El CERT aplicará y gestionará medidas de seguridad para garantizar la confidencialidad, integridad, disponibilidad y autenticidad de la información que reciba y trate.

c) Las dependencias del CERT y los sistemas de información de apoyo estarán situados en lugares seguros.

d) Se creará un sistema de calidad de la gestión del servicio a fin de supervisar el funcionamiento del CERT y garantizar un proceso continuo de mejora. Se basará en sistemas de medición claramente definidos, entre los que figurarán niveles de servicio formales e indicadores de resultados clave.

e) Continuidad de las actividades:

- El CERT dispondrá de un sistema adecuado para gestionar y encaminar las solicitudes con el fin de facilitar los traspasos.
- El CERT contará con personal suficiente para garantizar su disponibilidad en todo momento.
- El CERT dependerá de infraestructuras cuya continuidad esté asegurada. A tal fin, se crearán sistemas redundantes y espacios de trabajo de reserva para el CERT al objeto de garantizar un acceso permanente a los medios de comunicación.

2) Tareas del CERT

a) Entre las tareas del CERT figurarán como mínimo las siguientes:

- Supervisar incidentes a escala nacional.
- Difundir alertas tempranas, alertas, avisos e información sobre riesgos e incidentes entre las partes interesadas.
- Responder a incidentes.
- Efectuar un análisis dinámico de riesgos e incidentes y de conocimiento de la situación.
- Lograr una amplia concienciación del público sobre los riesgos vinculados a las actividades en línea.
- Organizar campañas sobre la SRI.

b) El CERT entablará relaciones de cooperación con el sector privado.

c) A fin de facilitar la cooperación, el CERT fomentará la adopción y utilización de prácticas comunes o normalizadas:

- Procedimientos de gestión de incidentes y riesgos.
- Sistemas de clasificación de incidentes, riesgos e información.
- Taxonomías de sistemas de medición.
- Formatos de intercambio de información sobre riesgos e incidentes y convenciones sobre la denominación de sistemas.

ANEXO II

Lista de operadores del mercado

Contemplados en el artículo 3, apartado 8, letra a):

1. Plataformas de comercio electrónico.

2. Pasarelas de pago por Internet.

3. Redes sociales.

4. Motores de búsqueda.

5. Servicios de computación en nube.

6. Tiendas de aplicaciones.

Contemplados en el artículo 3, apartado 8, letra b):

1. Energía:

- Proveedores de gas y electricidad.
- Gestores de redes de distribución de gas o electricidad y minoristas para consumidores finales.
- Gestores de redes de transporte de gas natural, gestores de almacenamiento y gestores de GNL.
- Gestores de redes de transporte de electricidad.
- Oleoductos de transporte de crudo y almacenamiento de crudo.
- Operadores de los mercados del gas y la electricidad.
- Operadores de producción de crudo y gas natural, instalaciones de refinado y tratamiento.

2. Transportes:

- Compañías aéreas (transporte aéreo de mercancías y pasajeros).
- Compañías de transporte marítimo (empresas de transporte marítimo y de cabotaje de pasajeros y empresas de transporte marítimo y de cabotaje de mercancías).
- Compañías ferroviarias (gestores de infraestructuras, compañías integradas y operadores de transporte ferroviario).
- Aeropuertos.
- Puertos.
- Operadores de control de la gestión del tráfico.
- Servicios logísticos auxiliares [a) depósito y almacenamiento, b) manipulación de la carga y c) otras actividades auxiliares del transporte].

3. Banca: entidades de crédito con arreglo a la definición del artículo 4, número 1, de la Directiva 2006/48/CE.

4. Infraestructuras de los mercados financieros: bolsas y entidades de contrapartida central.

5. Sector sanitario: entornos de asistencia sanitaria (entre ellos hospitales y clínicas privadas) y otras entidades que prestan asistencia sanitaria.

FICHA FINANCIERA LEGISLATIVA

1. MARCO DE LA PROPUESTA/INICIATIVA

1.1. Denominación de la propuesta/iniciativa

1.2. Ámbito(s) político(s) afectado(s) en la estructura GPA/PPA

1.3. Naturaleza de la propuesta/iniciativa

1.4. Objetivos

1.5. Justificación de la propuesta/iniciativa

1.6. Duración e incidencia financiera

1.7. Modo(s) de gestión previsto(s)

2. MEDIDAS DE GESTIÓN

2.1. Disposiciones en materia de seguimiento e informes

2.2. Sistema de gestión y de control

2.3. Medidas de prevención del fraude y de las irregularidades

3. INCIDENCIA FINANCIERA ESTIMADA DE LA PROPUESTA/INICIATIVA

3.1. Rúbrica(s) del marco financiero plurianual y línea(s) presupuestaria(s) de gastos afectada(s)

3.2. Incidencia estimada en los gastos

3.2.1. Resumen de la incidencia estimada en los gastos

3.2.2. Incidencia estimada en los créditos de operaciones

3.2.3. Incidencia estimada en los créditos de carácter administrativo

3.2.4. Compatibilidad con el marco financiero plurianual vigente

3.2.5. Contribución de terceros

3.3. Incidencia estimada en los ingresos

FICHA FINANCIERA LEGISLATIVA

1. MARCO DE LA PROPUESTA/INICIATIVA

1.1. Denominación de la propuesta/iniciativa

Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a medidas para garantizar un elevado nivel común de seguridad de las redes y de la información en la Unión.

1.2. Ámbito(s) político(s) afectado(s) en la estructura GPA/PPA[37]

- 09 – Redes de Comunicación, Contenido y Tecnologías

1.3. Naturaleza de la propuesta/iniciativa

☒ La propuesta/iniciativa se refiere a **una acción nueva**

☐ La propuesta/iniciativa se refiere a **una acción nueva a raíz de un proyecto piloto / una acción preparatoria**[38]

☐ La propuesta/iniciativa se refiere a **la prolongación de una acción existente**

☐ La propuesta/iniciativa se refiere a **una acción reorientada hacia una nueva acción**

1.4. Objetivos

1.4.1. Objetivo(s) estratégico(s) plurianual(es) de la Comisión contemplado(s) en la propuesta/iniciativa

La Directiva propuesta tiene como objetivo garantizar un elevado nivel común de seguridad de las redes y de la información (SRI) en la Unión.

1.4.2. Objetivo(s) específico(s) y actividad(es) GPA/PPA afectada(s)

La propuesta establece medidas para garantizar un elevado nivel común de seguridad de las redes y de la información en la Unión.

Los objetivos específicos son los siguientes:

1. Instaurar un nivel mínimo de SRI en los Estados miembros e incrementar de este modo el nivel global de preparación y respuesta.

2. Aumentar la cooperación en materia de SRI a escala de la UE con el fin de hacer frente con eficacia a incidentes y amenazas transfronterizos. Se creará una infraestructura segura para compartir información delicada y confidencial entre las autoridades competentes.

3. Crear una cultura de gestión de riesgos y mejorar el intercambio de información entre los sectores público y privado.

Actividad(es) GPA/PPA afectada(s)

La Directiva se aplica a entidades (empresas y organizaciones, incluidas algunas pymes) de una serie de sectores (energía, transportes, entidades de crédito y bolsas, sanidad y facilitadores de servicios clave de Internet), así como a las administraciones públicas. Establece vínculos con los cuerpos de seguridad y la protección de datos, así como con aspectos de la SRI en el ámbito de las relaciones exteriores.

- 09 – Redes de Comunicación, Contenido y Tecnologías

[37] GPA: gestión por actividades. PPA: presupuestación por actividades.

[38] Tal como se contempla en el artículo 49, apartado 6, letra a) o b), del Reglamento Financiero.

- 02 - Empresa

- 32 - Energía

- 06 – Movilidad y Transporte

- 17 - Sanidad y Protección de los Consumidores

- 18 – Asuntos Internos

- 19 – Relaciones Exteriores

- 33 - Justicia

- 12- Mercado Interior

1.4.3. Resultado(s) e incidencia esperados

Especifíquense los efectos que la propuesta/iniciativa debería tener sobre los beneficiarios / la población destinataria.

La protección de los consumidores, las empresas y las administraciones de la UE frente a incidentes, amenazas y riesgos de SRI aumentaría considerablemente.

Para más información, consúltese la sección 8.2 (Efectos de la 2ª opción – Enfoque reglamentario) de la evaluación de impacto que figura en el documento de trabajo de los servicios de la Comisión adjunto a la presente propuesta legislativa.

1.4.4. Indicadores de resultados e incidencia

Especifíquense los indicadores que permiten realizar el seguimiento de la ejecución de la propuesta/iniciativa.

Los indicadores de control y evaluación pueden consultarse en la sección 10 de la evaluación de impacto.

1.5. Justificación de la propuesta/iniciativa

1.5.1. Necesidad(es) que debe(n) satisfacerse a corto o largo plazo

Cada Estado miembro deberá contar con:

- una estrategia nacional de SRI;

- un plan de cooperación nacional en materia de SRI;

- una autoridad nacional competente en materia de SRI; y

- un equipo de respuesta a emergencias informáticas (CERT).

A escala de la UE, los Estados miembros deberán cooperar a través de una red.

Las administraciones públicas y los agentes clave del sector privado deberán proceder a una gestión de riesgos de SRI y notificar a las autoridades competentes los incidentes de SRI con efectos significativos.

1.5.2. Valor añadido de la intervención de la Unión Europea

Dado el carácter transfronterizo de la SRI, las divergencias entre las legislaciones y estrategias pertinentes representan un obstáculo para que las empresas ejerzan sus actividades en varios países y logren economías de escala globales. Si la UE no interviniese, cada Estado miembro actuaría por separado sin tener en cuenta las interdependencias entre las redes y los sistemas de información.

Por consiguiente, los objetivos previstos pueden lograrse mejor mediante una actuación de la UE que mediante la intervención de cada Estado miembro por su cuenta.

1.5.3. Principales conclusiones extraídas de experiencias similares anteriores

La propuesta se deriva de la conclusión de que son precisas obligaciones reglamentarias para introducir condiciones de igualdad y colmar ciertas lagunas legislativas. En este ámbito, los planteamientos meramente voluntarios han dado lugar a una cooperación limitada a una minoría de Estados miembros con un elevado nivel de capacidades.

1.5.4. Coherencia y posibles sinergias con otros instrumentos pertinentes

La propuesta guarda total coherencia con la Agenda Digital para Europa y, por tanto, con la Estrategia Europa 2020. Es también coherente con el marco regulador de los servicios de comunicaciones electrónicas de la UE, la Directiva de la UE sobre infraestructuras críticas europeas y la Directiva de la UE sobre protección de datos.

La propuesta acompaña a la Comunicación de la Comisión y la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad sobre una estrategia europea de ciberseguridad, y forma parte esencial de la misma.

1.6. Duración e incidencia financiera

– ☐ Propuesta/iniciativa de duración limitada

– ☐ Propuesta/iniciativa en vigor desde [el] [DD/MM]AAAA hasta [el] [DD/MM]AAAA

– ☐ Incidencia financiera desde AAAA hasta AAAA

– ☒ Propuesta/iniciativa de duración ilimitada

– El período de transposición se iniciará inmediatamente después de la adopción (prevista para 2015) y durará 18 meses. La aplicación de la Directiva, sin embargo, comenzará tras su adopción y entrañará la implantación de infraestructuras seguras que respalden la cooperación entre los Estados miembros.

– y pleno funcionamiento a partir de la última fecha.

1.7. Modo(s) de gestión previsto(s)[39]

– ☒ Gestión centralizada directa a cargo de la Comisión

– ☒ Gestión centralizada indirecta mediante delegación de las tareas de ejecución en:

– ☐ agencias ejecutivas

– ☒ organismos creados por las Comunidades[40]

– ☐ organismos nacionales del sector público / organismos con misión de servicio público

– ☐ personas a quienes se haya encomendado la ejecución de acciones específicas de conformidad con el título V del Tratado de la Unión Europea y que estén identificadas en el acto de base pertinente a efectos de lo dispuesto en el artículo 49 del Reglamento Financiero

– ☐ Gestión compartida con los Estados miembros

– ☐ Gestión descentralizada con terceros países

– ☐ Gestión conjunta con organizaciones internacionales (Agencia Espacial Europea)

Si se indica más de un modo de gestión, facilítense los detalles en el recuadro de observaciones.

Observaciones:
La ENISA, agencia descentralizada creada por las Comunidades, puede asistir a los Estados miembros y la Comisión en la aplicación de la Directiva sobre la base de su mandato y mediante la reasignación de recursos prevista en el MFP 2014-2020 para esta agencia.

[39] Las explicaciones sobre los modos de gestión y las referencias al Reglamento Financiero pueden consultarse en el sitio BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.htmlhttp://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

[40] Tal como se contemplan en el artículo 185 del Reglamento Financiero.

2. MEDIDAS DE GESTIÓN

2.1. Disposiciones en materia de seguimiento e informes

Especifíquense la frecuencia y las condiciones.

La Comisión revisará periódicamente el funcionamiento de la Directiva e informará de ello al Parlamento Europeo y al Consejo.

La Comisión también evaluará la correcta transposición de la Directiva por parte de los Estados miembros.

La propuesta de Mecanismo «Conectar Europa» (MCE) también prevé la posibilidad de proceder a una evaluación de las modalidades de realización de los proyectos, así como del impacto de su ejecución, a fin de determinar si se han conseguido los objetivos, incluidos los correspondientes a la protección del medio ambiente.

2.2. Sistema de gestión y de control

2.2.1. Riesgos definidos

- Retrasos en la ejecución del proyecto debidos a la construcción de infraestructuras seguras.

2.2.2. Método(s) de control previsto(s)

En los acuerdos y decisiones suscritos para llevar a cabo las medidas integradas en el MCE deben preverse la supervisión y el control financiero por la Comisión o cualquier representante autorizado de esta, así como las auditorías del Tribunal de Cuentas y las verificaciones *in situ* a cargo de la Oficina Europea de Lucha contra el Fraude (OLAF).

2.2.3. Costes y beneficios de los controles y porcentaje probable de incumplimiento

Gracias a los controles *ex ante* y *ex post* basados en el riesgo, así como a la posibilidad de efectuar auditorías *in situ*, los costes de los controles serán razonables.

2.3. Medidas de prevención del fraude y de las irregularidades

Especifíquense las medidas de prevención y protección existentes o previstas.

La Comisión adoptará las medidas adecuadas para garantizar que, cuando se realicen las acciones financiadas en el marco de la presente Directiva, los intereses financieros de la Unión queden protegidos mediante la aplicación de medidas preventivas contra el fraude, la corrupción y cualquier otra actividad ilegal, mediante la realización de controles efectivos y, si se detectan irregularidades, mediante la recuperación de las cantidades abonadas indebidamente y, cuando proceda, la imposición de sanciones efectivas, proporcionadas y disuasorias.

La Comisión o sus representantes y el Tribunal de Cuentas estarán facultados para auditar, sobre la base de documentos e *in situ*, a todos los beneficiarios de subvenciones, contratistas y subcontratistas que hayan recibido fondos de la Unión en el marco del programa.

La Oficina Europea de Lucha contra el Fraude (OLAF) podrá realizar controles y verificaciones *in situ* de los operadores económicos afectados directa o indirectamente por dicha financiación de conformidad con los procedimientos previstos en el Reglamento (Euratom, CE) nº 2185/96, con vistas a establecer cualquier posible fraude, corrupción u otra actividad ilegal que ataña a los intereses

financieros de la Unión en relación con un convenio o decisión de subvención o con un contrato relativo a la financiación de la Unión.

Sin perjuicio de lo dispuesto en los párrafos anteriores, los acuerdos de cooperación con terceros países y con organizaciones internacionales, así como los convenios y decisiones de subvención y los contratos derivados de la aplicación de la presente Directiva, facultarán expresamente a la Comisión, al Tribunal de Cuentas y a la OLAF para llevar a cabo las auditorías y los controles y verificaciones *in situ* mencionados.

En el marco del MCE, los contratos de subvención y los contratos públicos se basarán en modelos normalizados en los que constarán las medidas antifraude generalmente aplicables.

3. INCIDENCIA FINANCIERA ESTIMADA DE LA PROPUESTA/INICIATIVA

3.1. Rúbrica(s) del marco financiero plurianual y línea(s) presupuestaria(s) de gastos afectada(s)

- Líneas presupuestarias existentes

En el orden de las rúbricas del marco financiero plurianual y las líneas presupuestarias.

Rúbrica del marco financiero plurianual	Línea presupuestaria	Tipo de gasto	Contribución			
	Número [Descripción……...…….]	CD / CND (41)	de países de la AELC[42]	de países candidatos [43]	de terceros países	a efectos de lo dispuesto en el artículo 18.1.a *bis*) del Reglamento Financiero
	09 03 02 Promover la interconexión e interoperabilidad de los servicios públicos nacionales en línea, así como el acceso a dichas redes.	CD	NO	NO	NO	NO

- Nuevas líneas presupuestarias solicitadas (no aplicable)

En el orden de las rúbricas del marco financiero plurianual y las líneas presupuestarias.

Rúbrica del marco financiero plurianual	Línea presupuestaria	Tipo de gasto	Contribución			
	Número [Rúbrica……...…….]	CD / CND	de países de la AELC	de países candidatos	de terceros países	a efectos de lo dispuesto en el artículo 18.1.a *bis*) del Reglamento Financiero
	[XX.YY.YY.YY]		SÍ/NO	SÍ/NO	SÍ/NO	SÍ/NO

41 CD = créditos disociados / CND = créditos no disociados.

42 AELC: Asociación Europea de Libre Comercio.

43 Países candidatos y, en su caso, países candidatos potenciales de los Balcanes Occidentales.

3.2. Incidencia estimada en los gastos

3.2.1. Resumen de la incidencia estimada en los gastos

En millones EUR (al tercer decimal)

Rúbrica del marco financiero plurianual:	1	Crecimiento inteligente e integrador

DG: <…….>			2015* [44]	Año **2016**	Año **2017**	Año **2018**	Años siguientes (2019-2021) y posteriormente			**TOTAL**
• Créditos de operaciones										
09 03 02	Compromisos	(1)	1,250**	0,000						**1,250**
	Pagos	(2)	0,750	0,250	0,250					**1,250**
Créditos de carácter administrativo financiados mediante la dotación de programas específicos[45]			**0,000**							**0,000**
Número de línea presupuestaria		(3)	**0,000**							**0,000**
TOTAL de los créditos para la DG <…….>	Compromisos	=1+1a +3	1,250	0,000						**1,250**
	Pagos	=2+2a +3	0,750	0,250	0,250					**1,250**

• TOTAL de los créditos de operaciones	Compromisos	(4)	1,250	0,000						**1,250**
	Pagos	(5)	0,750	0,250	0,250					**1,250**
• TOTAL de los créditos de carácter administrativo		(6)	**0,000**							

[44] El año N es el año de comienzo de la ejecución de la propuesta/iniciativa.

[45] Asistencia técnica y/o administrativa y gastos de apoyo a la ejecución de programas y/o acciones de la UE (antiguas líneas «BA»), investigación indirecta, investigación directa.

financiados mediante la dotación de programas específicos										
TOTAL de los créditos para la RÚBRICA 1 del marco financiero plurianual	Compromisos	=4+ 6	1,250	0,000						**1,250**
	Pagos	=5+ 6	0,750	0,250	0,250					**1,250**

* El calendario exacto dependerá de la fecha de adopción de la propuesta por la autoridad legislativa (por ejemplo, si la Directiva se aprueba en el transcurso de 2014, la adaptación de las infraestructuras existentes comenzará en 2015 y, si no, un año después).

** Si los Estados miembros optan por utilizar infraestructuras existentes y recurrir al coste único de adaptación con cargo al presupuesto de la UE, tal como se explica en los puntos 1.4.3 y 1.7, se calcula que el coste de la adecuación de una red para respaldar la cooperación entre los Estados miembros, de conformidad con el capítulo III de la Directiva (alerta temprana, respuesta coordinada, etc.) ascenderá a 1 250 000 EUR. Este importe es ligeramente superior al mencionado en la evaluación de impacto («aproximadamente 1 millón EUR») por cuanto se basa en una estimación más precisa de los bloques componentes necesarios para dichas infraestructuras. Los bloques componentes necesarios y sus costes se basan en una estimación efectuada por el JRC en función de su experiencia en el desarrollo de sistemas similares para otros sectores, como el sanitario, y constarían de lo siguiente: sistema de alerta rápida y notificación para SRI (275 000 EUR), plataforma de intercambio de información (400 000 EUR), sistema de alerta temprana y respuesta (275 000 EUR) y sala de control (300 000 EUR), todo ello por un valor total de 1 250 000 EUR. Se presentará un plan de ejecución más pormenorizado en el estudio de viabilidad previsto en el contrato específico SMART 2012/0010 (*Feasibility study and preparatory activities for the implementation of a European early warning and response system against cyber-attacks and disruptions*).

Si la propuesta/iniciativa afecta a más de una rúbrica:

• TOTAL de los créditos de operaciones	Compromisos	(4)	0,000	0,000						
	Pagos	(5)	0,000	0,000						
• TOTAL de los créditos de carácter administrativo financiados mediante la dotación de programas específicos		(6)	**0,000**	**0,000**						
TOTAL de los créditos para las RÚBRICAS 1 a 4 del marco financiero plurianual (Importe de referencia)	Compromisos	=4+ 6	1,250	0,000						1,250
	Pagos	=5+ 6	0,750	0,250	0,250					1,250

Rúbrica del marco financiero plurianual	**5**	«Gastos administrativos»

En millones EUR (al tercer decimal)

		Año **2015**	Año **2016**	Año **2017**	Año **2018**	Años siguientes (2019-2021) y posteriormente			**TOTAL**
DG:CNECT									
• Recursos humanos		0,572	0,572	0,572	0,572	0,572	0,572	**0,572**	**4,004**
• Otros gastos administrativos		0,318	0,118	0,318	0,118	0,318	0,118	**0,118**	**1,426**
TOTAL para la DG CNECT	Créditos	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

TOTAL de los créditos para la RÚBRICA 5 del marco financiero plurianual	(Total de los compromisos = total de los pagos)	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

En millones EUR (al tercer decimal)

		Año **2015**[46]	Año **2016**	Año **2017**	Año **2018**	Años siguientes (2019-2021) y posteriormente			**TOTAL**
TOTAL de los créditos para las RÚBRICAS 1 a 5 del marco financiero plurianual	Compromisos	2,140	0,690	0,890	0,690	0,890	0,690	0,690	**6,680**
	Pagos	1,640	0,940	1,140	0,690	0,890	0,690	0,690	**6,680**

[46] El año N es el año de comienzo de la ejecución de la propuesta/iniciativa.

3.2.2. Incidencia estimada en los créditos de operaciones

– ☐ La propuesta/iniciativa no exige la utilización de créditos de operaciones

– ☑ La propuesta/iniciativa exige la utilización de créditos de operaciones, tal como se explica a continuación:

– Créditos de compromiso en millones EUR (al tercer decimal)

Indíquense los objetivos y los resultados ⇩			Año **2015***		Año **2016**		Año **2017**		Año **2018**		Años siguientes (2019-2021) y posteriormente						**TOTAL**	
	RESULTADOS																	
	Tipo de resultado[47]	Coste medio del resultado	Número	Coste	Número	Coste	Número	Coste	Número	Coste	Número	Coste	Número	Coste	Número	Coste	Número total	Coste total
OBJETIVO ESPECÍFICO n° 2[48] Infraestructuras de intercambio de información seguras																		
- Resultado	Adaptar infraestructur																	
Subtotal del objetivo específico nº 2			1	1,250**													1	1,250
COSTE TOTAL				1,250														1,250

47 Los resultados son los productos y servicios que van a suministrarse (por ejemplo, número de intercambios de estudiantes financiados, número de kilómetros de carreteras construidos, etc.).

48 Tal como se describe en el punto 1.4.2, «Objetivo(s) específico(s)».

* El calendario exacto dependerá de la fecha de adopción de la propuesta por la autoridad legislativa (por ejemplo, si la Directiva se aprueba en el transcurso de 2014, la adaptación de las infraestructuras existentes comenzará en 2015 y, si no, un año después).

** Véase el punto 3.2.1.

3.2.3. Incidencia estimada en los créditos de carácter administrativo

3.2.3.1. Resumen

– ☐ La propuesta/iniciativa no exige la utilización de créditos administrativos

– ☑ La propuesta/iniciativa exige la utilización de créditos administrativos, tal como se explica a continuación:

En millones EUR (al tercer decimal)

	Año **2015**[49]	Año **2016**	Año **2017**	Año **2018**	Años siguientes (2019-2021) y posteriormente			**TOTAL**
RÚBRICA 5 del marco financiero plurianual								
Recursos humanos	0,572	0,572	0,572	0,572	0,572	0,572	0,572	**4,004**
Otros gastos administrativos	0,318	0,118	0,318	0,118	0,318	0,118	0,118	**1,426**
Subtotal para la RÚBRICA 5 del marco financiero plurianual	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**
Al margen de la RÚBRICA 5[50] **del marco financiero plurianual**								
Recursos humanos	0,000	0,000						**0,000**
Otros gastos de carácter administrativo								
Subtotal al margen de la RÚBRICA 5 del marco financiero plurianual	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**
TOTAL	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

Las necesidades en materia de créditos administrativos las cubrirán los créditos de la DG CNECT ya destinados a la gestión de la acción y/o reasignados en la DG, que se complementarán en caso necesario con cualquier dotación adicional que pudiera asignarse a la DG gestora en el marco del procedimiento de asignación anual y a la luz de los imperativos presupuestarios existentes.

49 El año N es el año de comienzo de la ejecución de la propuesta/iniciativa.

50 Asistencia técnica y/o administrativa y gastos de apoyo a la ejecución de programas y/o acciones de la UE (antiguas líneas «BA»), investigación indirecta, investigación directa.

La Agencia Europea de Seguridad de las Redes y de la Información (ENISA) puede asistir a los Estados miembros y la Comisión en la aplicación de la Directiva sobre la base de su mandato y mediante la reasignación de recursos prevista en el MFP 2014-2020 para esta agencia, es decir, sin ninguna asignación adicional de recursos presupuestarios o humanos.

3.2.3.2. Necesidades estimadas de recursos humanos

– ☐ La propuesta/iniciativa no exige la utilización de recursos humanos

– ☑ La propuesta/iniciativa exige la utilización de recursos humanos de la Comisión, tal como se explica a continuación:

En principio, no se necesitará personal suplementario. Los recursos humanos necesarios serán muy limitados y los cubrirá el personal de la DG ya adscrito a la gestión de la acción.

Estimación que debe expresarse en valores enteros (o, a lo sumo, con un decimal)

		Año **2015**	Año **2016**	Año **2017**	Año **2018**	Años siguientes (2019-2021) y posteriormente		
• Empleos de plantilla (funcionarios y agentes temporales)								
09 01 01 01 (Sede y Oficinas de Representación de la Comisión)		4	4	4	4	4	4	4
XX 01 01 02 (Delegaciones)								
XX 01 05 01 (investigación indirecta)								
10 01 05 01 ((investigación directa)								
• Personal externo (en unidades de equivalente a jornada completa)[51]								
09 01 02 01 (AC, INT, ENCS de la dotación global)		1	1	1	1	1	1	1
XX 01 02 02 (AC, INT, JED, AL y ENCS en las delegaciones)								
XX 01 04 ***aa*** [52]	- en la sede[53]							
	- en las delegaciones							
XX 01 05 02 (AC, INT, ENCS; investigación indirecta)								
10 01 05 02 (AC, INT, ENCS; investigación directa)								
Otras líneas presupuestarias (especifíquense)								
TOTAL		**5**	**5**	**5**	**5**	**5**	**5**	**5**

XX es el ámbito político o título presupuestario en cuestión.

Las necesidades en materia de recursos humanos las cubrirá el personal de la DG CNECT ya destinado a la gestión de la acción y/o reasignados en la DG, que se complementarán en caso necesario con cualquier dotación adicional que pudiera asignarse a la DG gestora en el marco del procedimiento de asignación anual y a la luz de los imperativos presupuestarios existentes.

51 AC = agente contractual; INT = personal de empresas de trabajo temporal («intérimaires»); JED = joven experto en delegación; AL = agente local; ENCS = experto nacional en comisión de servicios.

52 Por debajo del límite de personal externo con cargo a créditos de operaciones (antiguas líneas «BA»).

53 Básicamente para los Fondos Estructurales, el Fondo Europeo Agrícola de Desarrollo Rural (Feader) y el Fondo Europeo de Pesca (FEP).

La Agencia Europea de Seguridad de las Redes y de la Información (ENISA) puede asistir a los Estados miembros y la Comisión en la aplicación de la Directiva sobre la base de su mandato y mediante la reasignación de recursos prevista en el MFP 2014-2020 para esta agencia, es decir, sin ninguna asignación adicional de recursos presupuestarios o humanos.

Descripción de las tareas que deben llevarse a cabo:

Funcionarios y agentes temporales	- Elaborar actos delegados de conformidad con el artículo 14, apartado 3. - Elaborar actos de ejecución de conformidad con el artículo 8, el artículo 9, apartado 2, el artículo 12, el artículo 14, apartado 5 y el artículo 16. - Contribuir a la cooperación a través de la red a nivel estratégico y operativo. - Entablar conversaciones internacionales y, probablemente, celebrar acuerdos internacionales
Personal externo	Prestar apoyo en la realización de las anteriores tareas cuando proceda.

3.2.4. Compatibilidad con el marco financiero plurianual vigente

– ☑ La propuesta/iniciativa es compatible con el marco financiero plurianual vigente.

– ☐ La propuesta/iniciativa implicará la reprogramación de la rúbrica correspondiente del marco financiero plurianual.

La incidencia financiera estimada en los gastos operativos de la propuesta corresponde al caso en que los Estados miembros opten por adaptar infraestructuras existentes y encomendar a la Comisión dicha adaptación con arreglo al MFP 2014-2020. El coste único correspondiente estará a cargo del MCE, siempre que estén disponibles fondos suficientes. De otro modo, los Estados miembros pueden compartir los gastos de adaptación de las infraestructuras o los costes de creación de nuevas infraestructuras.

– ☐ La propuesta/iniciativa requiere la aplicación del Instrumento de Flexibilidad o la revisión del marco financiero plurianual[54].

No procede.

3.2.5. Contribución de terceros

– La propuesta/iniciativa no prevé la cofinanciación por terceros.

3.3. Incidencia estimada en los ingresos

– ☑ La propuesta/iniciativa no tiene incidencia financiera en los ingresos.

[54] Véanse los puntos 19 y 24 del Acuerdo Interinstitucional.