



Bruselas, 7.2.2013
SWD(2013) 31 final

DOCUMENTO DE TRABAJO DE LOS SERVICIOS DE LA COMISIÓN

RESUMEN DE LA EVALUACIÓN DE IMPACTO

que acompaña al documento

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

{COM(2013) 48 final}

{SWD(2013) 32 final}

DOCUMENTO DE TRABAJO DE LOS SERVICIOS DE LA COMISIÓN

RESUMEN DE LA EVALUACIÓN DE IMPACTO

que acompaña al documento

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. ÁMBITO DE APLICACIÓN

En esta evaluación de impacto se presentan opciones de actuación para aumentar la seguridad de Internet y de otras redes y sistemas de información que sirven de apoyo a servicios que hacen posible el funcionamiento de nuestra sociedad (por ejemplo, administraciones públicas, finanzas y banca, energía, transportes, sanidad y algunos servicios de Internet que posibilitan grandes transformaciones económicas y sociales, tales como las plataformas de comercio electrónico o las redes sociales). Es lo que se ha dado en llamar «seguridad de las redes y de la información» (SRI).

2. CONTEXTO

Ya en 2001, la Comisión reconoció la creciente importancia de la SRI para nuestras economías y sociedades. A fin de lograr un nivel elevado y efectivo de SRI en la UE, la Comunidad Europea decidió en 2004 crear la Agencia Europea de Seguridad de las Redes y de la Información (ENISA). Hasta el momento, la intervención de la Unión Europea en el ámbito de la SRI ha consistido fundamentalmente en adoptar una serie de planes de acción y estrategias en los que instaba a los Estados miembros a aumentar sus capacidades de SRI y a cooperar para hacer frente a los problemas de SRI de dimensión transfronteriza.

Se ha consultado a las partes interesadas sobre los diversos aspectos de la iniciativa (definición del problema y opciones para subsanar las actuales deficiencias) mediante:

- **una consulta pública en línea** acerca de la manera de mejorar la SRI en la UE, que se desarrolló del 23 de julio al 15 de octubre de 2012. Se recibieron en total 169 respuestas a través de la herramienta en línea, y otras 10 respuestas más en cartas a la Comisión;
- los debates con **los Estados miembros** en el contexto del Foro Europeo de Estados Miembros (EFMS), en reuniones bilaterales y en la Conferencia sobre Ciberseguridad en la UE organizada por la Comisión y el Servicio Europeo de Acción Exterior el 6 de julio de 2012;
- los debates con las empresas y asociaciones **del sector privado** en el marco de la Asociación público-privada europea de resiliencia (EP3R) y en reuniones bilaterales;
- los debates con **la ENISA y el CERT-UE**;
- los debates en el contexto de la **Asamblea de la Agenda Digital de 2012**.

3. DESCRIPCIÓN DEL PROBLEMA

3.1. Definición del problema

El problema consiste en *un nivel general insuficiente de protección contra incidentes, riesgos y amenazas para la seguridad de las redes y la información en la UE que compromete el correcto funcionamiento del mercado interior.*

Habida cuenta de la interconexión de las redes y los sistemas de información y del carácter global de Internet, muchos incidentes de SRI traspasan las fronteras nacionales y entorpecen el funcionamiento del mercado interior.

Los servicios transfronterizos pueden quedar indisponibles, suspendidos o interrumpidos debido a violaciones de la seguridad, como ocurre con los ataques que afectan a eBay y PayPal. Los ataques contra la empresa de certificación neerlandesa Diginotar pusieron claramente de manifiesto que, para resolver los problemas, es preciso actuar con rapidez e intercambiar información sobre los incidentes significativos. A raíz de los incidentes pasados, los Estados miembros están comenzando a establecer sus propias reglamentaciones. Las intervenciones reguladoras no coordinadas pueden causar fragmentación y crear barreras para el mercado interior, generando gastos de cumplimiento para las empresas que desarrollan sus actividades en más de un Estado miembro.

Este problema afecta a todos los segmentos de la sociedad y de la economía (administraciones, empresas y consumidores). Merece mención especial una serie de sectores que desempeñan una función primordial, como es la de prestar servicios de apoyo fundamentales para nuestra economía y sociedad, por lo que la seguridad de sus sistemas reviste especial interés para el funcionamiento del mercado interior. Entre esos sectores figuran la banca, la bolsa, la generación, el transporte y la distribución de energía, los transportes (aéreo, ferroviario y marítimo), la sanidad, los canalizadores de servicios clave de Internet y las administraciones públicas. La consulta pública mostró que las partes interesadas reconocían mayoritariamente la necesidad de resolver los problemas de SRI en dichos sectores y de adoptar las consiguientes medidas a escala de la UE.

Si no se toman nuevas medidas para hacer frente al creciente número de incidentes, la confianza del consumidor en los servicios en línea podría decaer, lo cual, a su vez, comprometería el logro de los objetivos de la Agenda Digital.

3.2. Causas del problema

El problema definido se deriva de una serie de factores.

En primer lugar, deben destacarse **las divergencias en el nivel de capacidades a escala nacional en la UE**, lo cual dificulta el establecimiento de relaciones de confianza entre homólogos, requisito previo para la cooperación y el intercambio de información.

En segundo lugar, **el intercambio de información sobre incidentes, riesgos y amenazas es insuficiente**. La mayor parte de los incidentes de SRI no se notifican y pasan desapercibidos, debido ante todo a lo reacias que se muestran las empresas a compartir esta información por miedo a que su reputación se resienta o a que se les exija responsabilidad por los daños. El intercambio de información entre las asociaciones/plataformas público-privadas existentes, como el EFMS y la EP3R, se limita a las mejores prácticas.

4. EFICACIA DE LAS MEDIDAS EXISTENTES

4.1. Lagunas en el marco regulador vigente

La normativa actual no obliga a las entidades que no sean empresas de telecomunicaciones a adoptar medidas de gestión de riesgos de SRI ni a notificar los incidentes de SRI. Y, sin embargo, todos los agentes que dependen de redes y sistemas de información corren riesgos de seguridad. Esta situación entraña condiciones desiguales por cuanto un mismo incidente que afecte, por ejemplo, a un proveedor de servicios de telecomunicaciones y a una empresa que preste servicios de voz sobre IP, deberá ser notificado a la autoridad nacional competente por el primero, pero no por la segunda.

El marco regulador de la protección de datos obliga a todos los agentes que son responsables del tratamiento (por ejemplo, bancos u hospitales) a implantar medidas de seguridad proporcionales a los riesgos existentes. Los responsables del tratamiento, empero, solamente tienen que notificar las violaciones de seguridad que comprometan datos personales.

La Directiva 2008/114/CE del Consejo, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección, abarca exclusivamente los sectores de la energía y los transportes y, hasta la fecha, los Estados miembros han identificado pocas infraestructuras críticas europeas como tales. La Directiva no obliga a los operadores a notificar las violaciones de seguridad significativas y tampoco establece mecanismos para que los Estados miembros cooperen y respondan a los incidentes.

Los colegisladores examinan en estos momentos la propuesta de Directiva de la Comisión relativa a los ataques contra los sistemas de información¹. Esta propuesta solo se refiere a la penalización de determinados comportamientos, pero no aborda la prevención de riesgos e incidentes de SRI, la respuesta a incidentes de SRI ni la atenuación de sus efectos.

4.2. Límites del planteamiento voluntario

El planteamiento voluntario seguido hasta ahora ha dado lugar a un nivel desigual de preparación y una cooperación limitada.

El EFMS tiene competencias limitadas por cuanto los Estados miembros no comparten información sobre incidentes, riesgos o amenazas ni cooperan para hacer frente a las amenazas transfronterizas. El EFMS no está facultado para exigir a sus miembros que dispongan de unas capacidades mínimas.

La ENISA carece de competencias operativas y, por ejemplo, no puede intervenir en la resolución de problemas de SRI.

La EP3R no tiene estatuto oficial y no puede exigir al sector privado que notifique incidentes a las autoridades nacionales. No existe en la EP3R un marco para el intercambio de información de confianza ni para la notificación de información sobre amenazas, riesgos e incidentes de SRI.

5. NECESIDAD DE UNA INTERVENCIÓN DE LA UE, SUBSIDIARIEDAD Y PROPORCIONALIDAD

Garantizar la SRI reviste suma importancia para el buen funcionamiento del mercado interior y el bienestar de nuestra sociedad. El artículo 114 del TFUE constituye una base jurídica

¹ COM(2010) 517,
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:ES:PDF>

adecuada para armonizar los requisitos en materia de SRI y establecer un nivel mínimo de seguridad común en la UE.

La intervención de la Unión en el ámbito de la SRI está justificada por motivos de **subsidiariedad** debido al carácter transfronterizo del problema y a la mayor eficacia (y, por ende, valor añadido) de las políticas nacionales existentes que se derivaría de la actuación a escala de la UE.

A fin de que todos los Estados miembros participen en las actividades de cooperación, es preciso cerciorarse de que todos ellos cuentan con el nivel de capacidad mínimo requerido. Por lo demás, no cabe duda alguna de que las actuaciones estratégicas concertadas y en colaboración en el ámbito de la SRI pueden tener notables efectos positivos en la protección efectiva de los derechos fundamentales y, en particular, del derecho a la protección de los datos personales y a la intimidad.

Las medidas recogidas en la opción preferida están justificadas por motivos de **proporcionalidad**, ya que los requisitos que se imponen a los Estados miembros se han fijado en el nivel mínimo necesario para conseguir una preparación adecuada y hacer posible una cooperación basada en la confianza, mientras que las obligaciones aplicables a las empresas y las administraciones públicas de proceder a la gestión de riesgos y notificar incidentes solo se dirigen a entidades críticas, imponen medidas proporcionales a los riesgos y se limitan a incidentes de efectos significativos. Además, las medidas contempladas en la opción preferida no entrañan costes desproporcionados.

6. OBJETIVOS

El objetivo general es aumentar el nivel de protección contra incidentes, riesgos y amenazas que afectan a la seguridad de las redes y la información en la UE. Los objetivos específicos son los siguientes:

- **1^{er} objetivo** – Alcanzar un nivel mínimo común de SRI en los Estados miembros, incrementando de este modo el nivel general de preparación y respuesta.
- **2^o objetivo** – Incrementar la cooperación en materia de SRI a escala de la UE para poder hacer frente con eficacia a incidentes y amenazas de naturaleza transfronteriza.
- **3^{er} objetivo** – Crear una cultura de gestión de riesgos y mejorar el intercambio de información entre los sectores público y privado.

7. OPCIONES DE ACTUACIÓN

Las opciones de actuación que se examinan en la presente evaluación de impacto son el mantenimiento de la situación actual, el enfoque reglamentario y el enfoque mixto. Se ha desestimado la posible opción de interrumpir todas las actividades de la UE en el ámbito de la SRI.

7.1. 1^a opción – Mantenimiento de la situación actual (hipótesis de referencia)

La Comisión, con la asistencia de la ENISA, seguiría el planteamiento voluntario actual, instando a los Estados miembros a crear capacidades de SRI a escala nacional (por ejemplo, CERT, planes nacionales de contingencia para ciberincidentes o estrategias nacionales de ciberseguridad) y a cooperar a escala de la UE (por ejemplo, a través de una red de CERT en toda Europa y un plan europeo de cooperación/contingencia para ciberincidentes).

7.2. 2ª opción – Enfoque reglamentario

La Comisión exigiría a todos los Estados miembros que lograran al menos un nivel mínimo de capacidades nacionales (CERT, autoridades competentes, planes nacionales de contingencia para ciberincidentes o estrategias nacionales de ciberseguridad).

De acuerdo con esta opción reglamentaria, las autoridades nacionales competentes y los CERT formarían parte de **una red** de cooperación a escala europea. Dentro de esa red, las autoridades y los CERT intercambiarían información y cooperarían en la lucha contra amenazas e incidentes de SRI, ateniéndose al **plan europeo de cooperación/contingencia para ciberincidentes**, sobre el que tendrían que ponerse de acuerdo los Estados miembros.

Las empresas (excluidas las microempresas) de determinados sectores críticos —como, por ejemplo la banca, la energía (gas natural y electricidad), los transportes, la sanidad, los facilitadores de servicios básicos de Internet y las administraciones públicas—, estarían obligadas a evaluar los riesgos que corren y a adoptar medidas adecuadas y proporcionales a los riesgos reales. Además, estas entidades deberían notificar a las autoridades competentes los incidentes que pusieran gravemente en peligro el funcionamiento de sus redes y sistemas de información y que, por tanto, tuvieran efectos significativos en la continuidad de los servicios y el suministro de mercancías dependientes de las redes y los sistemas de información. Este sistema sigue el modelo de los artículos 13 *bis* y 13 *ter* de la Directiva Marco sobre las comunicaciones electrónicas.

7.3. 3ª opción - Enfoque mixto

La Comisión combinaría las iniciativas de carácter voluntario de los Estados miembros, encaminadas a crear o reforzar sus capacidades en materia de SRI y a establecer mecanismos de cooperación a escala de la UE, y requisitos reglamentarios dirigidos a los agentes clave del sector privado y a las administraciones públicas.

Las iniciativas de carácter voluntario serían esencialmente similares a las emprendidas con arreglo a la 1ª opción, mientras que los requisitos reglamentarios serían idénticos a los impuestos en el marco de la 2ª opción, tanto en lo que respecta a las entidades contempladas como al contenido de las obligaciones.

La ENISA prestaría apoyo con su experiencia y sus conocimientos a la Comisión, a los Estados miembros y al sector privado, por ejemplo publicando directrices técnicas y recomendaciones.

8. ANÁLISIS DE IMPACTO

La evaluación abarca, amén del nivel de seguridad, el impacto económico y social de las tres opciones. También contempla los costes que ocasionarían las opciones 2ª y 3ª.

Ninguna de las opciones expuestas tiene efectos en el medio ambiente que puedan preverse con exactitud.

8.1. 1ª opción – Mantenimiento de la situación actual (hipótesis de referencia)

Nivel de seguridad: Es poco probable que todos los Estados miembros alcanzaran los niveles nacionales de capacidad y preparación comparables necesarios para incrementar la seguridad y hacer posible la cooperación y el intercambio de información de confianza a escala de la UE. No se lograrían condiciones uniformes en relación con la gestión de riesgos y una mayor transparencia sobre los incidentes y, por tanto, seguiría habiendo lagunas reglamentarias.

Impacto económico: Dependería de la medida en que los Estados miembros siguieran las recomendaciones de la Comisión. El insuficiente nivel de seguridad de los Estados miembros

menos desarrollados comprometería su competitividad y crecimiento y los expondría a riesgos e incidentes. Dadas las tendencias actuales, los incidentes de SRI serían cada vez más visibles para empresas y consumidores y obstaculizarían la realización del mercado interior.

Impacto social: Los incidentes, riesgos y amenazas no solo seguirían existiendo, sino que serían cada vez más graves, lo cual minaría la confianza de los ciudadanos en las actividades en línea.

8.2. 2ª opción – Enfoque reglamentario

Nivel de seguridad: Las obligaciones impuestas a los Estados miembros garantizarían que todos ellos dispusieran de los equipamientos necesarios y contribuirían a la creación de un clima de confianza mutua, condición previa para una cooperación efectiva a escala de la UE.

Imponer la gestión de riesgos de SRI a las administraciones públicas y a los agentes privados clave supondría un poderoso incentivo para gestionar y dimensionar eficazmente los riesgos de seguridad. Los costes adicionales totales con los que deberían correr los diversos sectores de la UE para cumplir estos requisitos oscilarían entre **1 000 y 2 000 millones EUR. A cada pequeña o mediana empresa le costaría de 2 500 a 5 000 EUR cumplir esas obligaciones.**

Impacto económico: Al incrementarse el nivel de seguridad, se reducirían las pérdidas financieras ocasionadas por riesgos e incidentes de SRI. Se renovaría la confianza de empresas y consumidores en el mundo digital, lo cual beneficiaría al mercado interior. El fomento de una mayor cultura de gestión de riesgos también estimularía la demanda de productos y soluciones de TIC seguros.

Impacto social: Un mayor nivel de seguridad aumentaría la confianza en las actividades en línea de los ciudadanos, quienes podrían sacar pleno partido del mundo digital (por ejemplo, medios sociales de comunicación, aprendizaje virtual, sanidad electrónica).

8.3. 3ª opción – Enfoque mixto

Nivel de seguridad: Como en el caso de la 1ª opción, no puede garantizarse que el nivel de seguridad basado en las capacidades nacionales en materia de SRI y la cooperación a escala de la UE mejoraran como resultado de las iniciativas de carácter voluntario. Por otra parte, la imposición de requisitos de seguridad a las administraciones públicas y a los agentes privados clave supondría un poderoso incentivo para gestionar y dimensionar eficazmente los riesgos de seguridad. Con todo, estos mecanismos no resultarían eficaces en los Estados miembros que no siguieran las recomendaciones de la Comisión sobre la creación de capacidades de SRI.

Impacto económico: El ritmo de desarrollo variaría significativamente de un Estado miembro a otro. El insuficiente nivel de seguridad en los Estados miembros menos desarrollados comprometería su competitividad y crecimiento y los expondría a los efectos negativos de los riesgos e incidentes.

Impacto social: Los incidentes, riesgos y amenazas no solo seguirían existiendo, sino que serían cada vez más graves, lo cual minaría la confianza de los ciudadanos en las actividades en línea, sobre todo en aquellos Estados miembros que no consideran prioritaria la SRI.

9. COMPARACIÓN DE LAS OPCIONES

Las opciones 1ª y 3ª no se consideran viables para alcanzar los objetivos estratégicos y por tanto no se recomiendan, ya que su eficacia dependería de la consecución de un nivel mínimo de SRI mediante el enfoque voluntario y, en lo tocante a la 3ª opción, dependería del empeño

que pusieran los Estados miembros en crear capacidades y cooperar en asuntos transfronterizos.

La 2ª opción es la preferida, pues con ella aumentaría considerablemente la protección de los consumidores, las empresas y las administraciones de la UE frente a los incidentes, amenazas y riesgos de SRI. Por lo demás, al poner sus propios asuntos en orden, la UE podría ampliar su influencia internacional y convertirse en un socio aún 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 UE en el exterior.

10. SUPERVISIÓN Y EVALUACIÓN

El capítulo 10 del informe de evaluación de impacto presenta una serie de indicadores básicos de progreso hacia el logro de los objetivos. Entre dichos indicadores figuran, por ejemplo:

- Objetivo nº 1: Número de Estados miembros que han nombrado una autoridad competente en materia de SRI y un CERT o han adoptado una estrategia nacional de ciberseguridad y un plan nacional de contingencia/cooperación para ciberincidentes.
- Objetivo nº 2: Número de autoridades competentes y CERT de los Estados miembros que participan en la red y volumen de información intercambiado en la red sobre riesgos e incidentes de SRI. En lo que al objetivo nº 3 se refiere, nivel de las inversiones en SRI por parte de los agentes privados clave y las administraciones públicas y número de notificaciones de incidentes de SRI con efectos significativos.