PARLAMENTO EUROPEO 2009 - 2014

Documento de sesión

A7-0103/2014

12.2.2014

***I
INFORME

sobre la 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)0048 – C7-0035/2013 – 2013/0027(COD))

Comisión de Mercado Interior y Protección del Consumidor

Ponente: Andreas Schwab

Ponentes de opinión (*):
Pilar del Castillo Vera, Comisión de Industria, Investigación y Energía,
Carl Schlyter, Comisión de Libertades Civiles, Justicia y Asuntos de Interior

(*) Procedimiento de comisiones asociadas – artículo 50 del Reglamento

PR_COD_1amCom

Explicación de los signos utilizados

*	Procedimiento de consulta
***	Procedimiento de aprobación
***I	Procedimiento legislativo ordinario (primera lectura)
***II	Procedimiento legislativo ordinario (segunda lectura)
***III	Procedimiento legislativo ordinario (tercera lectura)

(El procedimiento indicado se basa en el fundamento jurídico propuesto en el proyecto de acto.)

Enmiendas a un proyecto de acto

En las enmiendas del Parlamento las modificaciones introducidas en el proyecto de acto se señalan en ***cursiva negrita***. La utilización de la *cursiva fina* constituye una indicación para los servicios técnicos referente a elementos del proyecto de acto para los que se propone una corrección con miras a la elaboración del texto final (por ejemplo, elementos claramente erróneos u omitidos en alguna versión lingüística). Estas propuestas de corrección están supeditadas al acuerdo de los servicios técnicos interesados.

En las cabeceras de las enmiendas relativas a un acto existente que se quiere modificar con el proyecto de acto, figuran una tercera y cuarta líneas en las que se indican, respectivamente, el acto existente y la disposición en cuestión. Las partes retomadas de una disposición de un acto existente que el Parlamento desee modificar pero que no se hayan modificado en el proyecto de acto se señalarán en **negrita**. Las supresiones que se refieran a dichos pasajes se indicarán de la siguiente manera: **[...]**.

ÍNDICE

Página

(*) Procedimiento de comisiones asociadas – artículo 50 del Reglamento

PROYECTO DE RESOLUCIÓN LEGISLATIVA DEL PARLAMENTO EUROPEO

sobre la 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)0048 – C7-0035/2013 – 2013/0027(COD))

(Procedimiento legislativo ordinario: primera lectura)

El Parlamento Europeo,

– Vista la propuesta de la Comisión al Parlamento Europeo y al Consejo (COM(2013)0048),

– Vistos el artículo 294, apartado 2, y el artículo 114 del Tratado de Funcionamiento de la Unión Europea, conforme a los cuales la Comisión le ha presentado su propuesta (C7-0035/2013),

– Visto el artículo 294, apartado 3, del Tratado de Funcionamiento de la Unión Europea,

– Visto el artículo 55 de su Reglamento,

– Visto el dictamen del Comité Económico y Social Europeo, de 22 de mayo de 2013[1],

– Vista la Resolución del Parlamento Europeo, de 12 de septiembre de 2013, sobre una Estrategia de ciberseguridad de la Unión Europea: «Un ciberespacio abierto, protegido y seguro»[2];

– Vistos el informe de la Comisión de Mercado Interior y Protección del Consumidor y las opiniones de la Comisión de Industria, Investigación y Energía, de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior y de la Comisión de Asuntos Exteriores (A7-0103/2014),

1. Aprueba la Posición en primera lectura que figura a continuación;

2. Pide a la Comisión que le consulte de nuevo si se propone modificar sustancialmente su propuesta o sustituirla por otro texto;

3. Encarga a su Presidente que transmita la Posición del Parlamento al Consejo y a la Comisión, así como a los Parlamentos nacionales.

Enmienda 1

Propuesta de Directiva

[1] DO C 0, 0.0.0000, p.0./Pendiente de publicación en el Diario Oficial.
[2] Textos Aprobados, P7_TA(2013)0376.

Considerando 1

Texto de la Comisión	*Enmienda*
(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.	(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 libertad y la seguridad general de los ciudadanos de la UE, así como*** para la actividad económica y el bienestar social y, en particular, para el funcionamiento del mercado interior.

Enmienda 2

Propuesta de Directiva
Considerando 2

Texto de la Comisión	*Enmienda*
(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.	(2) La magnitud***,*** la frecuencia ***y los efectos*** de los incidentes de seguridad se están incrementando y representan una grave amenaza para el funcionamiento de las redes y los sistemas de información. ***Estos sistemas podrían convertirse también en un objetivo fácil para acciones dañinas deliberadas con el propósito de perjudicar o interrumpir su funcionamiento.*** Tales incidentes pueden interrumpir las actividades económicas, generar considerables pérdidas financieras, minar la confianza del usuario ***y del inversor*** y causar grandes daños a la economía de la Unión ***y, en última instancia, poner en peligro el bienestar de los ciudadanos de la UE y la capacidad de los Estados miembros de la UE de protegerse y garantizar la seguridad de infraestructuras críticas***.

Enmienda 3

Propuesta de Directiva
Considerando 3 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(3 bis) Considerando que las causas más comunes de los fallos sistémicos siguen siendo accidentales, como causas naturales o errores humanos, las infraestructuras deben ser resilientes tanto ante perturbaciones intencionadas como accidentales, y los operadores de infraestructuras críticas deben diseñar sistemas basados en la resiliencia.

Enmienda 4

Propuesta de Directiva
Considerando 4

Texto de la Comisión	*Enmienda*
(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.	(4) Es conveniente crear a escala de la Unión un mecanismo de cooperación que propicie el intercambio de información y una ***prevención,*** 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 ***al menos*** a ***algunos*** operadores de infraestructuras de información ***del mercado*** requisitos mínimos en materia de seguridad para fomentar una cultura de gestión de riesgos y garantizar la notificación de los incidentes más graves. ***Debe animarse a las sociedades cotizadas a que publiquen los incidentes en sus informes financieros de forma voluntaria. El marco jurídico deberá basarse en la necesidad de salvaguardar la privacidad y***

la integridad de los ciudadanos. La Red de información sobre alertas en infraestructuras críticas debe ampliarse a los operadores del mercado cubiertos por la presente Directiva.

Enmienda 5

Propuesta de Directiva
Considerando 4 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(4 bis) Si bien las administraciones públicas, dada su misión de servicio público, deben ejercer la debida diligencia en la gestión y la protección de sus propias redes y sistemas de información, la presente Directiva deberá centrarse en las infraestructuras críticas esenciales para el mantenimiento de actividades económicas y sociales vitales en los sectores de la energía, los transportes, la banca, las infraestructuras de los mercados financieros o la sanidad. Los desarrolladores de programas informáticos y los fabricantes de equipos físicos deben quedar excluidos del ámbito de la presente Directiva.

Enmienda 6

Propuesta de Directiva
Considerando 4 ter (nuevo)

Texto de la Comisión	*Enmienda*
	(4 ter) Ha de garantizarse la cooperación y la coordinación entre las autoridades pertinentes de la Unión y la Alta Representante / Vicepresidenta, responsable de la Política Exterior y de Seguridad Común y la Política Común de Seguridad y Defensa, así como el

Coordinador de la lucha contra el terrorismo de la UE en todos los casos en los que se perciba que incidentes con efectos significativos son de naturaleza exterior y terrorista.

Enmienda 7

Propuesta de Directiva
Considerando 6

Texto de la Comisión	*Enmienda*
(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.	(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 los operadores del mercado imposibilita la creación de un mecanismo global y efectivo de cooperación en la Unión. ***Las universidades y los centros de investigación tienen un papel determinante a la hora de impulsar la investigación, el desarrollo y la innovación en estos ámbitos y deben recibir la financiación adecuada.***

Enmienda 8

Propuesta de Directiva
Considerando 7

Texto de la Comisión	*Enmienda*
(7) Para responder con eficacia a los problemas de seguridad de las redes y los sistemas de información es, pues, necesario	(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***.	un planteamiento global a escala de la Unión que integre requisitos mínimos comunes en materia de desarrollo de capacidades y planificación, ***que desarrolle suficientes capacidades de ciberseguridad,*** actividades de intercambio de información y coordinación de medidas, así como requisitos mínimos comunes de seguridad. ***Deben aplicarse unas normas comunes mínimas con arreglo a las recomendaciones pertinentes formuladas por los grupos de coordinación en materia de ciberseguridad.***

Enmienda 9

Propuesta de Directiva
Considerando 8

Texto de la Comisión	*Enmienda*
(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.	(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. ***Ningún Estado miembro está obligado a publicar información clasificada de la UE de acuerdo con la Decisión del Consejo, de 31 de marzo de 2011, sobre las normas de seguridad para la protección de la información clasificada de la UE (2011/292/UE), ni información sujeta a acuerdos sobre confidencialidad o acuerdos informales de no divulgación, tales como el Protocolo para el intercambio de información.***

Justificación

La presente enmienda tiene como objetivo aclarar el tratamiento de la información confidencial dentro del ámbito de aplicación de la presente Directiva.

Enmienda 10

Propuesta de Directiva
Considerando 9

Texto de la Comisión	*Enmienda*
(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.	(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***, sobre la base de los requisitos mínimos establecidos en la presente Directiva,*** 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***, respetando y protegiendo la vida privada y los datos personales***. ***Procede, por tanto, que cada Estado miembro esté obligado a cumplir las normas comunes relativas al formato de los datos y la posibilidad de intercambio de los datos que se deban compartir y evaluar. Los Estados miembros podrán solicitar la asistencia de la Agencia de Seguridad de las Redes y de la Información de la Unión Europea («ENISA») para desarrollar sus estrategias nacionales de SRI, partiendo de un proyecto mínimo común de estrategia de SRI.***

Enmienda 11

Propuesta de Directiva
Considerando 10 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(10 bis) A la vista de las diferencias en las estructuras nacionales de gobernanza y con el fin de salvaguardar los acuerdos sectoriales o los organismos de regulación y supervisión de la Unión y evitar duplicidades, los Estados miembros deben tener competencia para designar a más de una autoridad nacional competente que se encargue de realizar las tareas vinculadas a la seguridad de las redes y de los sistemas de información de los operadores del mercado en virtud de la presente Directiva. No obstante, con el fin de garantizar una cooperación y una comunicación transfronterizas adecuadas, es necesario que cada Estado miembro designe, sin perjuicio de los acuerdos normativos sectoriales, solo una ventanilla única nacional que se encargue de la cooperación transfronteriza a escala de la Unión. Si fuera necesario en virtud de su estructura constitucional o de otros acuerdos, el Estado miembro deberá poder designar solo una única autoridad que se encargue de realizar las tareas de la autoridad competente y de la ventanilla única. Las autoridades competentes y a las ventanillas únicas deben ser organismos civiles sujetos a un pleno control democrático y no deben desempeñar funciones en los ámbitos de inteligencia, garantía del cumplimiento de la ley o defensa ni mantener ningún tipo de relaciones de organización con organismos activos en estos ámbitos.

Enmienda 12

Propuesta de Directiva
Considerando 11

Texto de la Comisión	*Enmienda*
(11) Todos los Estados miembros deben disponer de capacidades técnicas y de organización suficientes para poder adoptar las medidas de prevención, detección, 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.	(11) Todos los Estados miembros ***y los operadores del mercado*** deben disponer de capacidades técnicas y de organización suficientes para poder adoptar las medidas de prevención, detección, respuesta y atenuación oportunas ante los incidentes y riesgos que puedan afectar a las redes y los sistemas de información ***en cualquier momento***. ***Los sistemas de seguridad de las administraciones públicas deberán ser seguros y estar sujetos a control y examen democráticos. Los equipos y las capacidades generalmente necesarios deben cumplir las normas técnicas establecidas de común acuerdo y atenerse a los procedimientos normativos de funcionamiento.*** Por consiguiente, procede crear en todos los Estados miembros equipos de respuesta a emergencias informáticas ***(CERT)*** 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. ***Estos CERT deben poder interactuar basándose en normas técnicas comunes y procedimientos normativos de funcionamiento. A la vista de las diferentes características de los CERT existentes, que responden a necesidades temáticas y actores distintos, los Estados miembros deben garantizar que cada uno de los sectores que figuren en la lista de operadores del mercado recogida en la presente Directiva recibe servicios al menos de un CERT. En cuanto a la cooperación transfronteriza entre CERT, los Estados miembros deben garantizar que los CERT dispongan de los medios suficientes para participar en las redes de***

cooperación internacionales y europeas ya establecidas.

Justificación

Se ha de garantizar la interoperabilidad.

Enmienda 13

Propuesta de Directiva
Considerando 12

Texto de la Comisión	*Enmienda*
(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.	(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***, con el que se garantiza, en su caso, la participación de los operadores del mercado,*** permita estructurar y coordinar a escala de la Unión las labores de intercambio de información, detección y respuesta.

Enmienda 14

Propuesta de Directiva
Considerando 13

Texto de la Comisión	*Enmienda*
(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	(13) Es conveniente que la 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 ***y los***

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.

Estados miembros deben 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.

Enmienda 15

Propuesta de Directiva
Considerando 13 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(13 bis) Cuando proceda, los Estados miembros podrán utilizar o adaptar las estructuras o estrategias organizativas existentes al aplicar las disposiciones de la presente Directiva.

Enmienda 16

Propuesta de Directiva
Considerando 14

Texto de la Comisión	*Enmienda*
(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	(14) Es oportuno crear infraestructuras seguras para el intercambio de información delicada y confidencial en el marco de la red de cooperación. ***Las estructuras existentes en la UE deben utilizarse plenamente para este fin.*** Sin perjuicio de la obligación de notificar a la red de cooperación los incidentes y riesgos que

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.	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***, utilizando métodos transparentes***.

Enmienda 17

Propuesta de Directiva
Considerando 15

Texto de la Comisión	*Enmienda*
(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.	(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 mutuamente información y mejores prácticas***, incluido el intercambio recíproco de información pertinente y*** apoyo operativo ***e información analizada desde un punto de vista estratégico,*** en caso de que se produzcan incidentes. ***Para fomentar eficazmente el intercambio de información y de mejores prácticas, es esencial garantizar que los operadores del mercado que participan en dichos intercambios no queden en desventaja a causa de su cooperación. Se necesitan suficientes salvaguardias para garantizar que este tipo de cooperación no exponga a estos operadores a un mayor riesgo de cumplimiento o a nuevas responsabilidades en ámbitos como la competencia, la propiedad intelectual, la***

protección de datos o la legislación sobre ciberdelincuencia, entre otros, ni los exponga a mayores riesgos operativos o de seguridad.

Enmienda 18

Propuesta de Directiva
Considerando 16

Texto de la Comisión	*Enmienda*
(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.	(16) Para garantizar la transparencia e informar debidamente a los ciudadanos y operadores del mercado de la UE, conviene que las ***ventanillas únicas*** creen un sitio web común ***a escala de la Unión*** para publicar información no confidencial sobre incidentes y riesgos ***y medios para la mitigación de riesgos, así como, cuando sea necesario, sobre medidas de mantenimiento adecuadas***. ***La información ofrecida en el sitio web debe ser accesible con independencia del dispositivo que se utilice. Los datos personales publicados en este sitio web deben limitarse únicamente a lo necesario y mantenerse anónimos en la medida de lo posible.***

Enmienda 19

Propuesta de Directiva
Considerando 18

Texto de la Comisión	*Enmienda*
(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.	(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***, mejores prácticas y pautas de***

Dicho plan debe tomarse debidamente en consideración a la hora de lanzar alertas tempranas en el marco de la red de cooperación.

funcionamiento para prevenir, detectar y hacer frente a riesgos e incidentes ***e informar sobre ellos***. Dicho plan debe tomarse debidamente en consideración a la hora de lanzar alertas tempranas en el marco de la red de cooperación.

Enmienda 20

Propuesta de Directiva
Considerando 19

Texto de la Comisión	*Enmienda*
(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.	(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 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.

Enmienda 21

Propuesta de Directiva
Considerando 20

Texto de la Comisión	*Enmienda*
(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	(20) Tras haber recibido y evaluado una alerta temprana, las ***ventanillas únicas*** deben acordar una respuesta coordinada en el marco del plan de cooperación de la Unión en materia de SRI. Tanto las ***ventanillas únicas como la*** ENISA ***o*** la Comisión deben estar informadas de las medidas adoptadas a escala nacional como

como resultado de la respuesta coordinada.

resultado de la respuesta coordinada.

Enmienda 22

Propuesta de Directiva
Considerando 21

Texto de la Comisión	*Enmienda*
(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.	(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. ***Todo marco para dicha cooperación internacional debe someterse a las disposiciones de la Directiva 95/46/CE y del Reglamento (CE) nº 45/2001.***

Enmienda 23

Propuesta de Directiva
Considerando 22

Texto de la Comisión	*Enmienda*
(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	(22) La responsabilidad de velar por la SRI recae en gran medida en los operadores del mercado. Debe fomentarse una cultura de gestión de riesgos***, de estrecha cooperación y de confianza*** que entrañe una evaluación del riesgo y la aplicación de medidas de seguridad proporcionales a los riesgos ***e incidentes, ya sean deliberados o accidentales,*** y que habrá de desarrollarse a través de requisitos reglamentarios adecuados y prácticas voluntarias del sector. Asimismo, son necesarias condiciones uniformes ***y fiables*** para garantizar el funcionamiento efectivo de la red de cooperación y, por ende, una colaboración eficaz de todos los Estados

miembros.

miembros.

Enmienda 24

Propuesta de Directiva
Considerando 24

Texto de la Comisión	*Enmienda*
(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[27], 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 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***	(24) Estas obligaciones no solo han de imponerse al sector de las comunicaciones electrónicas, sino también a los ***operadores de infraestructuras, 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 la electricidad y el gas, los transportes, las entidades de crédito, las infraestructuras de los mercados financieros y la sanidad. Los trastornos que puedan sufrir tales redes y sistemas de información afectan al mercado interior. Si bien las obligaciones establecidas por la presente Directiva no deben extenderse 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[27], 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 Internet, las redes sociales, los motores de búsqueda, los servicios de computación en nube ***en general*** o las tiendas de aplicaciones***, podrían informar voluntariamente a las autoridades competentes o las ventanillas únicas de aquellos incidentes de seguridad de la red que consideren oportunos***. ***La autoridad***

bolsas y la sanidad. Los trastornos que puedan sufrir tales redes y sistemas de información afectan al mercado interior.

competente o la ventanilla única presentarán, si es posible, a las administraciones públicas o a los operadores del mercado que hayan informado del incidente información estratégica analizada que ayude a superar la amenaza de seguridad.

Enmienda 25

Propuesta de Directiva
Considerando 24 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(24 bis) Aunque los proveedores de equipos y programas informáticos no son operadores del mercado comparables a los cubiertos por la presente Directiva, sus productos facilitan la seguridad de las redes y los sistemas de información. Por consiguiente, tienen una función importante para capacitar a los operadores del mercado para garantizar la seguridad de sus redes e infraestructuras de información. Habida cuenta de que los equipos y los programas informáticos ya están sujetos a las normas vigentes sobre responsabilidad por los productos, los Estados miembros deben velar por el cumplimiento de estas normas.

Enmienda 26

Propuesta de Directiva
Considerando 25

Texto de la Comisión	*Enmienda*
(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	(25) Las medidas técnicas y de organización impuestas 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

comercial de tecnología de la información y la comunicación.

y la comunicación.

Enmienda 27

Propuesta de Directiva
Considerando 26

Texto de la Comisión	*Enmienda*
(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.	(26) 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 pertinentes, independientemente de si se encargan ellos mismos del mantenimiento de sus redes y sistemas de información o lo subcontratan.

Enmienda 28

Propuesta de Directiva
Considerando 28

Texto de la Comisión	*Enmienda*
(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	(28) Las autoridades competentes ***y las ventanillas únicas*** 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. ***Las autoridades competentes y las ventanillas únicas deben informar a los fabricantes y proveedores de los productos y servicios de TIC afectados de los incidentes con efectos significativos que les sean notificados.*** Antes de dar publicidad a los incidentes notificados a las autoridades

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.

competentes y a las ventanillas únicas, 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 los operadores del mercado que notifican los incidentes. A la hora de cumplir sus obligaciones de notificación, las autoridades competentes ***y las ventanillas únicas*** han de tener muy en cuenta la necesidad de mantener estrictamente confidencial la información sobre los puntos vulnerables del producto antes de ***desplegar*** las soluciones de seguridad adecuadas. ***Como norma general, las ventanillas únicas no divulgarán los datos personales de las personas implicadas en los incidentes. Las ventanillas únicas solo divulgarán datos de carácter personal si la divulgación de dichos datos es necesaria y guarda proporción con los objetivos perseguidos.***

Enmienda 29

Propuesta de Directiva
Considerando 29

Texto de la Comisión	*Enmienda*
(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.	(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 ***y medir la cantidad, la magnitud y el alcance de los incidentes***, así como datos fidedignos y exhaustivos sobre incidentes reales que hayan repercutido en el funcionamiento de las redes y los sistemas de información.

Enmienda 30

Propuesta de Directiva
Considerando 30

Texto de la Comisión	*Enmienda*
(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.	(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***, las ventanillas únicas*** y los cuerpos de seguridad***, así como la cooperación con el EC3 (Centro Europeo de Ciberdelincuencia de Europol) y la ENISA*** deberían 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.

Enmienda 31

Propuesta de Directiva
Considerando 31

Texto de la Comisión	*Enmienda*
(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	(31) En numerosas ocasiones los datos de carácter personal se ven comprometidos a raíz de incidentes. ***Los Estados miembros y los operadores del mercado deben proteger los datos personales almacenados, tratados o transmitidos de la destrucción accidental o ilícita, la pérdida o alteración accidental y el almacenamiento, el acceso, la divulgación o la difusión no autorizados o ilícitos, y***

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. 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.

garantizarán la aplicación de una política de seguridad con respecto al tratamiento de los datos personales. En este contexto, las autoridades competentes***, las ventanillas únicas*** y las autoridades responsables de la protección de datos han de cooperar e intercambiar información***, también con los operadores del mercado, cuando proceda, para hacer frente a*** las violaciones de datos personales derivadas de incidentes ***de acuerdo con las normas aplicables de protección de datos***. La obligación de notificar los incidentes de seguridad ***se cumplirá*** 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 ***que deba notificarse de conformidad con la legislación de la Unión en materia de protección de datos***. La ENISA deberá contribuir a elaborar mecanismos de intercambio de información y un modelo único de notificación que facilitaría la comunicación de incidentes que comprometan los datos personales, aliviando de este modo la carga administrativa para empresas y administraciones públicas.

Enmienda 32

Propuesta de Directiva
Considerando 32

Texto de la Comisión	*Enmienda*
(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	(32) La normalización de los requisitos en materia de seguridad es un proceso impulsado por el mercado ***y de carácter voluntario que debe permitir a los operadores del mercado utilizar medios alternativos para conseguir al menos resultados similares***. Al objeto de garantizar una aplicación convergente de las normas de seguridad, es oportuno que los Estados miembros fomenten el

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[29].

[29] DO L 316 de 14.11.2012, p. 12.

cumplimiento de normas específicas ***interoperables*** o la conformidad con ellas para así lograr un elevado nivel de seguridad en la Unión. A tal fin, ***se ha de considerar la aplicación de normas internacionales abiertas a la seguridad de las redes y de la información o el diseño de este tipo de instrumentos. Otro paso adelante necesario*** puede ser 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[29]. ***En particular, se debe encomendar al Instituto Europeo de Normas de Telecomunicación (ETSI), al Centro Europeo de Normalización (CEN) y al Comité Europeo de Normalización Electrotécnica (CENELEC) la tarea de proponer normas de seguridad abiertas a escala de la Unión que resulten eficaces y eficientes, donde se eviten todo lo posible preferencias tecnológicas, y que sean de fácil gestión para los operadores pequeños y medianos del mercado. Conviene examinar detenidamente las normas internacionales relativas a la ciberseguridad a fin de garantizar que no se hayan visto comprometidas y que ofrezcan unos niveles adecuados de seguridad, cerciorándose así de que el cumplimiento obligatorio de las normas de ciberseguridad mejora el nivel global de ciberseguridad de la Unión y no al contrario.***

[29] DO L 316 de 14.11.2012, p. 12.

Enmienda 33

Propuesta de Directiva
Considerando 33

Texto de la Comisión	*Enmienda*
(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.	(33) La Comisión debe revisar periódicamente las disposiciones contenidas en la presente Directiva***, en consulta con todas las partes interesadas,*** en particular con vistas a determinar si es preciso modificarlas a la luz de la cambiante situación ***societal, política,*** de la tecnología o el mercado.

Enmienda 34

Propuesta de Directiva
Considerando 34

Texto de la Comisión	*Enmienda*
(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***.	(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 ***el conjunto común de normas de interconexión y de seguridad para las infraestructuras para el*** intercambio seguro de información ***y*** con la especificación de los hechos que activan la alerta temprana.

Enmienda 35

Propuesta de Directiva

Considerando 36

Texto de la Comisión	*Enmienda*
(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.	(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 ***ventanillas únicas*** y la Comisión en el marco de la red de cooperación, ***sin perjuicio de los mecanismos de cooperación existentes a escala nacional,*** el plan de cooperación de la Unión en materia de SRI ***y*** los formatos y procedimientos aplicables a la ***notificación de*** incidentes ***con efectos significativos***. 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.

Justificación

Esta enmienda sustituye a la enmienda 20. Esta enmienda sustituye a la enmienda 20 y tiene como fin corregir un error en la propuesta de la Comisión respecto del contenido del acto de ejecución previsto y reflejar la nueva enmienda propuesta para el artículo 9, apartado 3.

Enmienda 36

Propuesta de Directiva
Considerando 37

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

Enmienda 37

Propuesta de Directiva
Considerando 38

Texto de la Comisión	*Enmienda*
(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.	(38) La información que una autoridad competente ***o una ventanilla única consideren*** confidencial de acuerdo con las normas nacionales y de la Unión sobre secreto comercial únicamente debe intercambiarse con la Comisión, ***sus agencias competentes, ventanillas únicas*** y***/u*** otras autoridades ***nacionales*** 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***,*** ***necesario*** y proporcional a la finalidad perseguida***, y debe respetar los criterios preestablecidos de confidencialidad y seguridad, de conformidad con la Decisión del Consejo, de 31 de marzo de 2011, sobre las normas de seguridad para la protección de la información clasificada de la UE (2011/292/UE), ni información sujeta a acuerdos sobre confidencialidad o acuerdos informales de no divulgación, tales como el Protocolo para el intercambio de información.***

Enmienda 38

Propuesta de Directiva
Considerando 39

Texto de la Comisión	*Enmienda*
(39) El intercambio de información sobre	(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. 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.

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 ***o a las ventanillas únicas*** 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. 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.

Enmienda 39

Propuesta de Directiva
Considerando 41 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(41 bis) 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.

Enmienda 40

Propuesta de Directiva
Artículo 1 – apartado 2 – letra b

Texto de la Comisión	*Enmienda*
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;	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 ***eficientes y*** eficaces y coordinadas ante los riesgos e incidentes que afecten a las redes y los sistemas de información ***con la participación de las partes interesadas pertinentes***;

Enmienda 41

Propuesta de Directiva
Artículo 1 – apartado 2 – letra c

Texto de la Comisión	*Enmienda*
c) establece requisitos en materia de seguridad para los operadores del mercado ***y las administraciones públicas***.	c) establece requisitos en materia de seguridad para los operadores del mercado.

Enmienda 42

Propuesta de Directiva
Artículo 1 – apartado 5

Texto de la Comisión	*Enmienda*
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, de 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, 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.	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, de 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, y del 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 órganos de la Comunidad*** y a la libre circulación de estos datos. ***Todo uso de datos personales debe limitarse a lo estrictamente necesario para los fines de la presente Directiva, y estos datos deben permanecer anónimos en la medida de lo posible, incluso anónimos por completo.***

Enmienda 43

Propuesta de Directiva
Artículo 1 bis (nuevo)

Texto de la Comisión	*Enmienda*
	Artículo 1 bis

	Tratamiento y protección de los datos personales
	1. El tratamiento de los datos personales en los Estados miembros con arreglo a la presente Directiva se llevará a cabo de conformidad con las Directivas 95/46/CE y 2002/58/CE.
	2. El tratamiento de los datos personales por la Comisión y la ENISA con arreglo al presente Reglamento se llevará a cabo de conformidad con el Reglamento (CE) nº 45/2001.
	3. El tratamiento de los datos personales por el Centro Europeo de Ciberdelincuencia de Europol a efectos de la presente Directiva se llevará a cabo de conformidad con la Decisión 2009/371/JAI.
	4. El tratamiento de los datos personales será justo y lícito y se limitará estrictamente a los datos mínimos necesarios para los efectos para los que se procesan. Los datos personales se conservarán en una forma que permita la identificación de los interesados durante un periodo no superior al necesario para los fines para los que se traten dichos datos personales.
	5. Las notificaciones de incidentes mencionadas en el artículo 14 se tramitarán sin perjuicio de las disposiciones y obligaciones en materia de notificación de violaciones de datos personales contempladas en el artículo 4 de la Directiva 2002/58/CE y en el Reglamento (UE) nº 611/2013.

Enmienda 44

Propuesta de Directiva
Artículo 3 – punto 1 – letra b

Texto de la Comisión	*Enmienda*
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***,	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 ***digitales***,

Enmienda 45

Propuesta de Directiva
Artículo 3 – punto 1 – letra c

Texto de la Comisión	*Enmienda*
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;	c) los datos ***digitales*** almacenados, tratados, recuperados o transmitidos por los elementos contemplados en las letras a) y b) para su funcionamiento, utilización, protección y mantenimiento;

Enmienda 46

Propuesta de Directiva
Artículo 3 – punto 2

Texto de la Comisión	*Enmienda*
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;	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; ***«seguridad» incluye los dispositivos técnicos, las soluciones y los procedimientos de funcionamiento pertinentes para el cumplimiento de los requisitos de seguridad establecidos en la presente***

Directiva;

Enmienda 47

Propuesta de Directiva
Artículo 3 – punto 3

Texto de la Comisión	*Enmienda*
3) «riesgo»: toda circunstancia o hecho que pueda tener efectos adversos en la seguridad;	3) «riesgo»: toda circunstancia o hecho ***razonablemente identificable*** que pueda tener efectos adversos en la seguridad;

Enmienda 48

Propuesta de Directiva
Artículo 3 – punto 4

Texto de la Comisión	*Enmienda*
4) «incidente»: ***toda circunstancia o*** hecho que tenga efectos adversos en la seguridad;	4) «incidente»: ***todo*** hecho que tenga efectos adversos en la seguridad;

Enmienda 49

Propuesta de Directiva
Artículo 3 – punto 5

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

Enmienda 50

Propuesta de Directiva
Artículo 3 – punto 7

Texto de la Comisión	*Enmienda*
7) «gestión de incidentes»: todos los procedimientos seguidos para analizar, limitar y responder a un incidente;	7) «gestión de incidentes»: todos los procedimientos seguidos para ***detectar, prevenir,*** analizar, limitar y responder a un incidente;

Enmienda 51

Propuesta de Directiva
Artículo 3 – punto 8 – letra a

Texto de la Comisión	*Enmienda*
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;	***suprimida***

Enmienda 52

Propuesta de Directiva
Artículo 3 – punto 8 – letra b

Texto de la Comisión	*Enmienda*
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.	b) un operador de infraestructuras esenciales para el mantenimiento de actividades económicas y sociales vitales en los sectores de la energía, los transportes, la banca, ***las infraestructuras de los mercados financieros, puntos de intercambio de Internet, la cadena de suministro alimentario*** y la sanidad, ***cuya interrupción o destrucción tendría efectos significativos en un Estado miembro como resultado de la incapacidad de mantener dichas funciones***, una lista no exhaustiva de los cuales figura en el anexo II***, en la medida en que las redes y los sistemas de información afectados están directamente relacionados con sus***

servicios básicos.

Enmienda 53

Propuesta de Directiva
Artículo 3 – punto 8 bis (nuevo)

Texto de la Comisión	*Enmienda*
	8 bis) «incidente que tenga efectos significativos»: incidente que afecta a la seguridad y la continuidad de una red o sistema de información y da lugar a la perturbación grave de funciones económicas o sociales esenciales;

Enmienda 54

Propuesta de Directiva
Artículo 3 – punto 11 bis (nuevo)

Texto de la Comisión	*Enmienda*
	11 bis) «mercado regulado»: mercado regulado con arreglo a la definición del artículo 4, punto 14, de la Directiva 2004/39/CE del Parlamento Europeo y del Consejo[1 bis];
	[1 bis] Directiva 2004/39/CE del Parlamento Europeo y del Consejo, de 21 de abril de 2004, relativa a los mercados de instrumentos financieros (DO L 45 de 16.2.2005, p. 18).

Justificación

Adaptación de la definición a la propuesta de Reglamento del Parlamento Europeo y del Consejo, relativa a los mercados de instrumentos financieros y por la que se modifica el Reglamento [EMIR] relativo a los derivados OTC, las entidades de contrapartida central y los registros de operaciones.

Enmienda 55

Propuesta de Directiva
Artículo 3 – punto 11 ter (nuevo)

Texto de la Comisión	*Enmienda*
	11 ter) «sistema multilateral de negociación (SMN)»: el definido en el artículo 4, punto 15, de la Directiva 2004/39/CE;

Justificación

Adaptación de la definición a la propuesta de Reglamento del Parlamento Europeo y del Consejo, relativa a los mercados de instrumentos financieros y por la que se modifica el Reglamento [EMIR] relativo a los derivados OTC, las entidades de contrapartida central y los registros de operaciones.

Enmienda 56

Propuesta de Directiva
Artículo 3 – punto 11 quater (nuevo)

Texto de la Comisión	*Enmienda*
	11 quater) «sistema organizado de negociación»: un sistema multilateral, distinto de un mercado regulado, un sistema multilateral de negociación o una entidad de contrapartida central, explotado por una empresa de inversión o por un operador del mercado, en el que interactúan los diversos intereses de compra y de venta sobre bonos y obligaciones, productos de financiación estructurados, derechos de emisión o derivados de múltiples terceros para dar lugar a contratos de conformidad con lo dispuesto en el título II de la Directiva 2004/39/CE;

Justificación

Introducción de la definición adaptada y sujeta al resultado de la propuesta de Reglamento del Parlamento Europeo y del Consejo, relativa a los mercados de instrumentos financieros y por la que se modifica el Reglamento [EMIR] relativo a los derivados OTC, las entidades de

contrapartida central y los registros de operaciones.

Enmienda 57

Propuesta de Directiva
Artículo 5 – apartado 1 – letra e bis (nueva)

Texto de la Comisión	*Enmienda*
	e bis) Los Estados miembros podrán solicitar la asistencia de la ENISA para el desarrollo de sus estrategias nacionales de SRI y sus planes nacionales de cooperación en el ámbito de la SRI sobre la base de una estrategia común de SRI.

Enmienda 58

Propuesta de Directiva
Artículo 5 – apartado 2 – letra a

Texto de la Comisión	*Enmienda*
a) ***Plan de*** evaluación de ***riesgos que permita determinarlos y evaluar*** los efectos de incidentes potenciales***.***	a) ***Marco de gestión de riesgos para establecer una metodología para la identificación, la priorización, la*** evaluación ***y el tratamiento*** de ***riesgos, la evaluación de*** los efectos de incidentes potenciales***, la prevención y las opciones de control y para definir criterios de selección de posibles contramedidas;***

Justificación

Esta enmienda sustituye a la enmienda 29. La propuesta de la Comisión habría ido demasiado lejos en lo que respecta a cuestiones de seguridad nacional de los Estados miembros y habría hecho que el plan de cooperación fuera impracticable y demasiado complejo para que fuese eficaz.

Enmienda 59

Propuesta de Directiva
Artículo 5 – apartado 2 – letra b

Texto de la Comisión	*Enmienda*
b) Determinación de las funciones y responsabilidades de ***los diversos*** agentes que participan en la ejecución del plan.	b) Determinación de las funciones y responsabilidades de ***las diversas autoridades y demás*** agentes que participan en la ejecución del marco.

Enmienda 60

Propuesta de Directiva
Artículo 5 – apartado 3

Texto de la Comisión	*Enmienda*
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.	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 ***tres meses*** a partir de su adopción.

Enmienda 61

Propuesta de Directiva
Artículo 6 – título

Texto de la Comisión	*Enmienda*
Autoridad nacional competente en materia de seguridad de las redes y los sistemas de información	***Autoridades nacionales competentes y ventanillas únicas*** en materia de seguridad de las redes y los sistemas de información

Enmienda 62

Propuesta de Directiva
Artículo 6 – apartado 1

Texto de la Comisión	*Enmienda*
1. Cada Estado miembro designará una ***autoridad nacional competente*** en materia de seguridad de las redes y los sistemas de información («la autoridad competente»).	1. Cada Estado miembro designará una ***o más autoridades nacionales civiles competentes*** en materia de seguridad de las redes y los sistemas de información (***en lo sucesivo,*** «la***(s)*** autoridad***(es)***

competente***(s)***»).

Justificación

Esta enmienda sustituye a la enmienda 32 y tiene como fin especificar qué tipo de institución debe desempeñar la función de autoridad nacional competente.

Enmienda 63

Propuesta de Directiva
Artículo 6 – apartado 2 bis (nuevo)

Texto de la Comisión	*Enmienda*
	2 bis. En caso de que un Estado miembro designe más de una autoridad competente, designará una autoridad civil nacional —por ejemplo, una autoridad competente— como ventanilla única nacional en materia de seguridad de las redes y los sistemas de información (en lo sucesivo denominada «ventanilla única»). Si un Estado miembro designa únicamente una autoridad competente, dicha autoridad también será la ventanilla única.

Justificación

Esta enmienda sustituye a la enmienda 33 y está en consonancia con la nueva enmienda al artículo 6, apartado 1, del ponente. Tiene como fin especificar qué tipo de institución debe desempeñar la función de ventanilla única.

Enmienda 64

Propuesta de Directiva
Artículo 6 – apartado 2 ter (nuevo)

Texto de la Comisión	*Enmienda*
	2 ter. Las autoridades competentes y la ventanilla única de un mismo Estado miembro cooperarán estrechamente en lo relativo a las obligaciones establecidas en la presente Directiva.

Enmienda 65

Propuesta de Directiva
Artículo 6 – apartado 2 quater (nuevo)

Texto de la Comisión	*Enmienda*
	2 quater. La ventanilla única garantizará la cooperación transfronteriza con otras ventanillas únicas.

Enmienda 66

Propuesta de Directiva
Artículo 6 – apartado 3

Texto de la Comisión	*Enmienda*
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.	3. Los Estados miembros velarán por que las autoridades competentes ***y las ventanillas únicas*** 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 ***ventanillas únicas*** a través de la red a que se hace referencia en el artículo 8.

Enmienda 67

Propuesta de Directiva
Artículo 6 – apartado 4

Texto de la Comisión	*Enmienda*
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	4. Los Estados miembros velarán por que las autoridades competentes ***y las ventanillas únicas, cuando proceda de conformidad con el apartado 2 bis del presente artículo,*** reciban las

artículo 14, apartado 2, y se les confieran las competencias de aplicación a que se refiere el artículo 15.	notificaciones de incidentes de 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.

Justificación

Esta enmienda sustituye a la enmienda 37 y tiene como fin aclarar la función de las distintas autoridades para evitar duplicidades de notificaciones tanto a las autoridades competentes como a las ventanillas únicas. Habida cuenta de que en algunos sectores las notificaciones de incidentes ya se comunican directamente a los organismos de la Unión, se deben evitar las duplicidades.

Enmienda 68

Propuesta de Directiva
Artículo 6 – apartado 4 bis (nuevo)

Texto de la Comisión	*Enmienda*
	4 bis. Cuando la legislación de la Unión prevea un organismo europeo de regulación o supervisión específico para un sector, por ejemplo sobre seguridad de las redes y los sistemas de información, este organismo recibirá de los operadores del mercado afectados de ese sector las notificaciones de incidentes con arreglo al artículo 14, apartado 2, y le serán concedidas las competencias de ejecución a que se refiere el artículo 15. Este organismo de la Unión cooperará estrechamente con las autoridades competentes y las ventanillas únicas del Estado miembro de acogida en lo que respecta a estas obligaciones. La ventanilla única del Estado miembro de acogida representará al organismo de la Unión en lo que respecta a las obligaciones del capítulo III.

Enmienda 69

Propuesta de Directiva
Artículo 6 – apartado 5

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

Enmienda 70

Propuesta de Directiva
Artículo 6 – apartado 6

Texto de la Comisión	*Enmienda*
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***.	6. Los Estados miembros notificarán sin demora a la Comisión ***las autoridades competentes y la ventanilla única*** que hayan designado, su cometido y cualquier cambio posterior que se introduzca en él. Los Estados miembros harán pública la designación de ***las autoridades competentes***.

Enmienda 71

Propuesta de Directiva
Artículo 7 – apartado 1

Texto de la Comisión	*Enmienda*
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	1. Cada Estado miembro creará ***al menos*** un equipo de respuesta a emergencias informáticas (en lo sucesivo, «CERT») ***para cada uno de los sectores establecidos en el anexo II,*** responsable de la gestión de incidentes y riesgos de acuerdo con un procedimiento claramente definido, que se ajustará a los requisitos establecidos en el

autoridad competente.	anexo I, punto 1 Podrá crearse un CERT en el marco de la autoridad competente.

Enmienda 72

Propuesta de Directiva
Artículo 7 – apartado 5

Texto de la Comisión	*Enmienda*
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.	5. Los CERT actuarán bajo la supervisión de la autoridad competente ***o de la ventanilla única***, que comprobará periódicamente la adecuación de sus recursos, su mandato y la eficacia de su procedimiento de gestión de incidentes.

Enmienda 73

Propuesta de Directiva
Artículo 7 – apartado 5 bis (nuevo)

Texto de la Comisión	*Enmienda*
	5 bis. Los Estados miembros garantizarán que los CERT dispongan de los recursos humanos y financieros adecuados para participar en redes de cooperación internacionales y, en particular, de la Unión.

Enmienda 74

Propuesta de Directiva
Artículo 7 – apartado 5 ter (nuevo)

Texto de la Comisión	*Enmienda*
	5 ter. Se permitirá y fomentará que los CERT inicien ejercicios conjuntos y participen en ellos con otros CERT, con CERT de todos los Estados miembros y

	con las entidades oportunas de Estados no pertenecientes a la UE, así como con CERT de instituciones multinacionales e internacionales, como la OTAN y las Naciones Unidas.

Enmienda 75

Propuesta de Directiva
Artículo 7 – apartado 5 quater (nuevo)

Texto de la Comisión	*Enmienda*
	5 quater. Los Estados miembros podrán solicitar la asistencia de la ENISA o de otros Estados miembros cuando desarrollen sus CERT nacionales.

Enmienda 76

Propuesta de Directiva
Artículo 8 – apartado 1

Texto de la Comisión	*Enmienda*
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.	1. Las ***ventanillas únicas,*** la Comisión ***y la ENISA*** crearán una red (***en lo sucesivo,*** «red de cooperación») para colaborar contra los riesgos e incidentes que afecten a las redes y los sistemas de información.

Enmienda 77

Propuesta de Directiva
Artículo 8 – apartado 2

Texto de la Comisión	*Enmienda*
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***	2. La Comisión y las ***ventanillas únicas*** mantendrán una comunicación constante en el marco de la red de cooperación. Cuando así se le solicite, la ENISA asistirá a la red de cooperación ofreciéndole su experiencia, conocimientos y

(«ENISA***»)*** asistirá a la red de cooperación ofreciéndole su experiencia, conocimientos y asesoramiento.

asesoramiento. ***Cuando proceda, podrá invitarse también a operadores del mercado y proveedores de soluciones de ciberseguridad a participar en las actividades de la red de cooperación a que se refiere el apartado 3, letras g) e i).***

Cuando proceda, la red de cooperación cooperará con las autoridades de protección de datos.

La Comisión informará regularmente a la red de cooperación de la investigación sobre seguridad y otros programas pertinentes de Horizonte 2020.

Enmienda 78

Propuesta de Directiva
Artículo 8 – apartado 3

Texto de la Comisión	*Enmienda*
3. En el marco de la red de cooperación, las ***autoridades competentes***:	3. En el marco de la red de cooperación, las ***ventanillas únicas***:
a) difundirán alertas tempranas sobre riesgos e incidentes de conformidad con el artículo 10;	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;	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;	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;	d) examinarán y evaluarán conjuntamente 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	e) examinarán y evaluarán conjuntamente la eficacia de los CERT, especialmente cuando los ejercicios de SRI se realicen a escala de la Unión;

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;

f) cooperarán e intercambiarán ***conocimientos especializados*** sobre cuestiones pertinentes ***en materia de redes y seguridad de la información***, en particular en los sectores de la protección de datos, la energía, los transportes, la banca, ***los mercados financieros*** y la sanidad***, con el Centro Europeo de Ciberdelincuencia en Europol y con otros organismos europeos pertinentes***;

f bis) cuando proceda, informarán al Coordinador de la lucha contra el terrorismo de la UE mediante un informe y podrán solicitar asistencia para análisis, trabajos preparatorios y acciones de la red de cooperación;

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;

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.

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

i bis) fomentarán la participación de los operadores del mercado, les consultarán e intercambiarán información con ellos, cuando proceda, sobre riesgos e incidentes que afecten a su red y sus sistemas de información;

i ter) desarrollarán, con la cooperación de la ENISA, orientaciones sobre los criterios específicos del sector para la notificación de incidentes significativos, además de los parámetros establecidos en el artículo 14, apartado 2, para la interpretación común, la aplicación coherente y la ejecución armoniosa en la Unión.

Enmienda 79

Propuesta de Directiva
Artículo 8 – apartado 3 bis (nuevo)

Texto de la Comisión	*Enmienda*
	3 bis. La red de cooperación publicará un informe anual basado en las actividades de la red y en el informe resumido presentado con arreglo al artículo 14, apartado 4, de la presente Directiva, referido a los doce meses precedentes.

Enmienda 80

Propuesta de Directiva
Artículo 8 – apartado 4

Texto de la Comisión	*Enmienda*
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***.	4. La Comisión establecerá mediante actos de ejecución las disposiciones necesarias para facilitar la cooperación entre las ***ventanillas únicas,*** la Comisión ***y la ENISA*** a que se hace referencia en los apartados 2 y 3. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de ***examen*** contemplado en el artículo 19, apartado ***3***.

Enmienda 81

Propuesta de Directiva
Artículo 9 – apartado 1 bis (nuevo)

Texto de la Comisión	*Enmienda*
	1 bis. Los participantes en la infraestructura segura cumplirán, entre otras cosas, las medidas adecuadas de seguridad y de confidencialidad con arreglo a la Directiva 95/46/CE y al Reglamento (CE) nº 45/2001 en todas las fases del procedimiento.

Enmienda 82

Propuesta de Directiva
Artículo 9 – apartado 2

Texto de la Comisión	*Enmienda*
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:	***suprimido***
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.	

Enmienda 83

Propuesta de Directiva
Artículo 9 – apartado 3

Texto de la Comisión	*Enmienda*
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,***	3. La Comisión adoptará mediante actos ***delegados un conjunto común de normas de interconexión y de seguridad que las ventanillas únicas deberán cumplir antes de intercambiar información sensible y confidencial en la red de cooperación***.

apartado 3.

Enmienda 84

Propuesta de Directiva
Artículo 10 – apartado 1

Texto de la Comisión	*Enmienda*
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:	1. Las ***ventanillas únicas*** 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;	b) riesgos e incidentes que ***las ventanillas únicas consideren que posiblemente exceden*** la capacidad nacional de respuesta;
c) riesgos e incidentes que ***afecten o puedan afectar*** a más de un Estado miembro.	c) riesgos e incidentes que ***las ventanillas únicas o la Comisión consideren que afectan*** a más de un Estado miembro.

Enmienda 85

Propuesta de Directiva
Artículo 10 – apartado 2

Texto de la Comisión	*Enmienda*
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.	2. Las ***ventanillas únicas*** y la Comisión incluirán en sus alertas tempranas***, sin demoras injustificadas,*** toda la información no clasificada pertinente que obre en su poder y pueda ser de utilidad para evaluar el riesgo o incidente.

Enmienda 86

Propuesta de Directiva
Artículo 10 – apartado 3

Texto de la Comisión	*Enmienda*
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.	***suprimido***

Enmienda 87

Propuesta de Directiva
Artículo 10 – apartado 4

Texto de la Comisión	*Enmienda*
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.	4. Cuando se sospeche que el riesgo o incidente objeto de una alerta temprana es de carácter delictivo ***y cuando el operador del mercado en cuestión haya notificado incidentes de carácter grave y supuestamente delictivo con arreglo al artículo 15, apartado 4, los Estados miembros se asegurarán de que el*** Centro Europeo de Ciberdelincuencia de Europol ***esté informado, si procede***.

Enmienda 88

Propuesta de Directiva
Artículo 10 – apartado 4 bis (nuevo)

Texto de la Comisión	*Enmienda*
	4 bis. Los miembros de la red de cooperación no harán pública ninguna información que reciban sobre los riesgos e incidentes a los que se refiere el apartado 1 sin haber recibido la aprobación previa de la ventanilla única responsable de la notificación.
	Además, antes de intercambiar información en la red de cooperación, la ventanilla única responsable de la notificación informará de su intención al

	operador del mercado al que hace referencia la información y, cuando lo considere apropiado, mantendrá anónima la información de que se trate.

Enmienda 89

Propuesta de Directiva
Artículo 10 – apartado 4 ter (nuevo)

Texto de la Comisión	*Enmienda*
	4 ter. Cuando se sospeche que el riesgo o incidente objeto de una alerta temprana es de carácter técnico, transfronterizo y grave, las ventanilla únicas o la Comisión informarán de ello a la ENISA.

Enmienda 90

Propuesta de Directiva
Artículo 11 – apartado 1

Texto de la Comisión	*Enmienda*
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.	1. Cuando reciban la alerta temprana a que se refiere el artículo 10, las ***ventanillas únicas*** evaluarán la información pertinente y acordarán***, sin demoras injustificadas,*** una respuesta coordinada de conformidad con el plan de cooperación de la Unión en materia de SRI contemplado en el artículo 12.

Enmienda 91

Propuesta de Directiva
Artículo 12 – apartado 2 – letra a – guión 1

Texto de la Comisión	*Enmienda*
– el formato y los procedimientos de recopilación e intercambio de información compatible y comparable sobre riesgos e incidentes por parte de las ***autoridades***	– el formato y los procedimientos de recopilación e intercambio de información compatible y comparable sobre riesgos e incidentes por parte de las ***ventanillas***

competentes,	***únicas***,

Enmienda 92

Propuesta de Directiva
Artículo 12 – apartado 3

Texto de la Comisión	*Enmienda*
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.	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. ***Los resultados de cada revisión se notificarán al Parlamento Europeo.***

Enmienda 93

Propuesta de Directiva
Artículo 12 – apartado 3 bis (nuevo)

Texto de la Comisión	*Enmienda*
	3 bis. Se velará por la coherencia entre el plan de cooperación en materia de SRI de la Unión y las estrategias nacionales de SRI con arreglo a lo establecido en el artículo 5 de la presente Directiva.

Enmienda 94

Propuesta de Directiva
Artículo 13 – apartado 1

Texto de la Comisión	*Enmienda*
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	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.	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 ***y se especificará el procedimiento de control que deberá realizarse para garantizar la protección de los datos personales que circulen en la red de cooperación. Se informará al Parlamento Europeo de la negociación de los acuerdos. Toda transferencia de datos de carácter personal a destinatarios de países de fuera de la Unión se llevará a cabo con arreglo a los artículos 25 y 26 de la Directiva 95/46/CE, y al artículo 9 del Reglamento (CE) nº 45/2001.***

Enmienda 95

Propuesta de Directiva
Artículo 13 bis (nuevo)

Texto de la Comisión	*Enmienda*
	Artículo 13 bis
	Nivel de criticidad de los operadores del mercado
	Los Estados miembros podrán determinar el nivel de criticidad de los operadores del mercado, teniendo en cuenta las particularidades de los sectores, parámetros como la importancia de un operador del mercado en particular para mantener un nivel suficiente del servicio sectorial, el número de partes proporcionadas por el operador del mercado, y que el plazo hasta la discontinuidad de los servicios básicos del operador tenga un efecto negativo en el mantenimiento de actividades sociales y económicas vitales.

Justificación

Esta enmienda es parte del capítulo IV y debe preceder al artículo 14 más abajo. Este artículo tiene como fin permitir una clasificación más diferenciada del anexo II y, como consecuencia de ello, las obligaciones establecidas en el capítulo IV. Si bien la notificación de incidentes corresponderá a todos los operadores del mercado, independientemente de su nivel de criticidad, podrá adaptarse la forma de las auditorías de seguridad al nivel de criticidad del operador del mercado.

Enmienda 96

Propuesta de Directiva
Artículo 14 – apartado 1

Texto de la Comisión	*Enmienda*
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.	1. Los Estados miembros velarán por que los operadores del mercado tomen medidas técnicas y de organización apropiadas ***y proporcionadas*** para ***detectar y*** gestionar ***eficazmente*** los riesgos existentes para la seguridad de las redes y los sistemas de información que controlan y utilizan en sus operaciones. Considerando el estado de la técnica, dichas medidas garantizarán un nivel de seguridad adecuado al riesgo presente. En particular, adoptarán medidas para prevenir y reducir al mínimo los incidentes que afecten a ***la seguridad de*** 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.

Enmienda 97

Propuesta de Directiva
Artículo 14 – apartado 2

Texto de la Comisión	*Enmienda*
2. Los Estados miembros velarán por que ***las administraciones públicas y*** los operadores del mercado notifiquen a la	2. Los Estados miembros velarán por que los operadores del mercado notifiquen ***sin demoras injustificadas*** a la autoridad

autoridad competente los incidentes que tengan efectos significativos en la ***seguridad*** de los servicios básicos que prestan.	competente ***o a la ventanilla única*** los incidentes que tengan efectos significativos en la ***continuidad*** de los servicios básicos que prestan. ***La notificación no expondrá a la parte que notifica a una mayor responsabilidad.*** ***A fin de determinar la importancia del impacto de un incidente, se tendrán en cuenta, entre otros, los siguientes parámetros:***

Enmienda 98

Propuesta de Directiva
Artículo 14 – apartado 2 – letra a (nueva)

Texto de la Comisión	*Enmienda*
	a) el número de usuarios cuyo servicio básico se ve afectado;

Enmienda 99

Propuesta de Directiva
Artículo 14 – apartado 2 – letra b (nueva)

Texto de la Comisión	*Enmienda*
	b) la duración del incidente;

Enmienda 100

Propuesta de Directiva
Artículo 14 – apartado 2 – letra c (nueva)

Texto de la Comisión	*Enmienda*
	c) la extensión geográfica con respecto a la zona afectada por el incidente.

Enmienda 101

Propuesta de Directiva
Artículo 14 – apartado 2 – párrafo 1 bis (nuevo)

Texto de la Comisión	*Enmienda*
	Dichos parámetros se especificarán en más detalle de conformidad con lo dispuesto en la letra i ter) del artículo 8, apartado 3.

Enmienda 102

Propuesta de Directiva
Artículo 14 – apartado 2 bis (nuevo)

Texto de la Comisión	*Enmienda*
	2 bis. Los operadores del mercado notificarán los incidentes contemplados en los apartados 1 y 2 a la autoridad competente o a la ventanilla única del Estado miembro donde se haya visto afectado el servicio básico. Si se han visto afectados servicios básicos en más de un Estado miembro, la ventanilla única que reciba la notificación alertará, basándose en la información proporcionada por el operador del mercado, a las demás ventanillas únicas afectadas. El operador del mercado será informado lo antes posible de qué otras ventanillas únicas han sido informadas del incidente, así como de las medidas adoptadas, los resultados o cualquier información relacionada con el incidente.

Enmienda 103

Propuesta de Directiva
Artículo 14 – apartado 2 ter (nuevo)

Texto de la Comisión	*Enmienda*
	2 ter. Si la notificación contiene datos

personales, se divulgará solamente a los destinatarios de la autoridad competente notificada o de la ventanilla única que tengan que procesarlos para desempeñar sus cometidos de conformidad con las normas de protección de datos. Los datos divulgados se limitarán a lo necesario para el ejercicio de sus funciones.

Enmienda 104

Propuesta de Directiva
Artículo 14 – apartado 2 quater (nuevo)

Texto de la Comisión	*Enmienda*
	2 quater. Los operadores del mercado no contempladas en el anexo II podrán notificar incidentes con arreglo al artículo 14, apartado 2, de forma voluntaria.

Enmienda 105

Propuesta de Directiva
Artículo 14 – apartado 4

Texto de la Comisión	*Enmienda*
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.	4. ***Tras consultar con*** la autoridad competente ***notificada y con el operador del mercado de que se trate, la ventanilla única*** podrá informar a los ciudadanos ***acerca de incidentes individuales, donde la concienciación pública sea necesaria para evitar un incidente o tratar con un incidente en curso, o donde el operador*** del mercado***, sujeto a un incidente, haya rechazado solucionar sin retrasos indebidos una vulnerabilidad estructural grave relacionada con dicho incidente.*** ***Antes de divulgar la información al público, la autoridad competente notificada garantizará que el operador del mercado en cuestión tiene la posibilidad***

	de ser oído y que la decisión de divulgación pública guarda el debido equilibrio con el interés público.
	Cuando se publique información sobre incidentes concretos, la autoridad competente notificada o la ventanilla única garantizarán que sea lo más anónima posible.
	La autoridad competente o la ventanilla única proporcionarán, si es razonablemente posible, al operador del mercado afectado información de apoyo para una gestión eficaz del incidente notificado.
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.	Una vez al año, la ***ventanilla única*** presentará a la red de cooperación un informe resumido sobre las notificaciones recibidas***, con el número de notificaciones y en relación con los parámetros para incidentes enumerados en el apartado 2 del presente artículo,*** y las medidas adoptadas de acuerdo con el presente apartado.

Enmienda 106

Propuesta de Directiva
Artículo 14 – apartado 4 bis (nuevo)

Texto de la Comisión	*Enmienda*
	4 bis. Los Estados miembros recomendarán a los operadores del mercado que anuncien los incidentes que afecten a su empresa en sus informes financieros de forma voluntaria.

Enmienda 107

Propuesta de Directiva
Artículo 14 – apartado 5

Texto de la Comisión	*Enmienda*
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.	***suprimido***

Enmienda 108

Propuesta de Directiva
Artículo 14 – apartado 6

Texto de la Comisión	*Enmienda*
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.	6. Las autoridades competentes ***o las ventanillas únicas*** podrán adoptar directrices sobre las circunstancias en que los operadores del mercado estarán obligados a notificar incidentes.

Enmienda 109

Propuesta de Directiva
Artículo 14 – apartado 8

Texto de la Comisión	*Enmienda*
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[35].	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[35]***, a menos que la microempresa funcione como subsidiario de un operador con arreglo a la definición del artículo 3, apartado 8, letra b)***.
[35] DO L 124 de 20.5.2003, p. 36.	[35] DO L 124 de 20.5.2003, p. 36.

Enmienda 110

Propuesta de Directiva
Artículo 14 – apartado 8 bis (nuevo)

Texto de la Comisión	*Enmienda*
	8 bis. Los Estados miembros podrán decidir aplicar el presente artículo y el artículo 15 a las administraciones públicas mutatis mutandis.

Enmienda 111

Propuesta de Directiva
Artículo 15 – apartado 1

Texto de la Comisión	*Enmienda*
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.	1. Los Estados miembros velarán por que las autoridades competentes ***y las ventanillas únicas*** dispongan de las competencias necesarias para ***garantizar el cumplimiento*** por parte de los operadores del mercado de las obligaciones que impone el artículo 14 y los efectos que tengan en la seguridad de las redes y los sistemas de información.

Enmienda 112

Propuesta de Directiva
Artículo 15 – apartado 2 – parte introductoria

Texto de la Comisión	*Enmienda*
2. Los Estados miembros velarán por que las autoridades competentes estén facultadas para exigir a los operadores del mercado ***y a las administraciones públicas***:	2. Los Estados miembros velarán por que las autoridades competentes ***y las ventanillas únicas*** estén facultadas para exigir a los operadores del mercado:

Enmienda 113

Propuesta de Directiva
Artículo 15 – apartado 2 – letra b

Texto de la Comisión	*Enmienda*
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.	b) que ***ofrezcan pruebas de la aplicación eficaz de las políticas de seguridad, como los resultados de*** una auditoría de seguridad practicada por un organismo independiente o una autoridad nacional cualificados y pongan ***las pruebas*** en conocimiento de la autoridad competente ***o de la ventanilla única***.

Enmienda 114

Propuesta de Directiva
Artículo 15 – apartado 2 – párrafo 1 bis (nuevo)

Texto de la Comisión	*Enmienda*
	Cuando formulen dicha exigencia, las autoridades competentes y las ventanillas únicas expondrán el objetivo de la misma y especificarán en el grado suficiente la información exigida.

Enmienda 115

Propuesta de Directiva
Artículo 15 – apartado 3

Texto de la Comisión	*Enmienda*
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***.	3. Los Estados miembros velarán por que las autoridades competentes ***y las ventanillas únicas*** estén facultadas para impartir instrucciones vinculantes a los operadores del mercado.

Enmienda 116

Propuesta de Directiva
Artículo 15 – apartados 3 bis y 3 ter (nuevos)

Texto de la Comisión	*Enmienda*
	3 bis. Con carácter de excepción a lo dispuesto en la letra b) del apartado 2 del presente artículo, los Estados miembros podrán decidir que las autoridades competentes o las ventanillas únicas, según sea aplicable, apliquen un procedimiento diferente a determinados operadores del mercado, sobre la base de su nivel de criticidad establecido de conformidad con el artículo 13 bis. En caso que así lo decidan los Estados miembros:
	a) las autoridades competentes o las ventanillas únicas, según sea aplicable, tendrán la facultad de presentar una petición suficientemente específica a los operadores del mercado solicitándoles que aporten pruebas de la aplicación efectiva de políticas de seguridad, tales como los resultados de una auditoría de seguridad realizada por un auditor interno cualificado, y que pongan las pruebas a disposición de la autoridad competente o la ventanilla única;
	b) cuando proceda, tras la presentación de la petición del operador del mercado mencionada en la letra a), la autoridad competente o la ventanilla única podrán solicitar pruebas o una auditoría adicionales que deberá realizar o bien un organismo independiente cualificado o una autoridad nacional.
	3 ter. Los Estados miembros podrán reducir el número y la intensidad de las auditorías para un operador del mercado determinado si su auditoría de seguridad indica el cumplimiento de forma consecuente de lo dispuesto en el capítulo IV.

Enmienda 117

Propuesta de Directiva
Artículo 15 – apartado 4

Texto de la Comisión	*Enmienda*
4. Las autoridades competentes ***notificarán*** los incidentes de carácter grave y supuestamente delictivo a los cuerpos de seguridad.	4. Las autoridades competentes ***y las ventanillas únicas informarán a los operadores del mercado en cuestión sobre la posibilidad de notificar*** incidentes de carácter grave y supuestamente delictivo a los cuerpos de seguridad.

Enmienda 118

Propuesta de Directiva
Artículo 15 – apartado 5

Texto de la Comisión	*Enmienda*
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.	5. ***Sin perjuicio de las normas aplicables sobre protección de datos,*** las autoridades competentes ***y las ventanillas únicas*** 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. ***Las ventanillas únicas y las autoridades de protección de datos desarrollarán, con la cooperación de ENISA, mecanismos de intercambio de información y un modelo único que ambas utilizarán para las notificaciones en virtud del artículo 14, apartado 2, de la presente Directiva y de la restante legislación de la Unión en materia de protección de datos.***

Enmienda 119

Propuesta de Directiva
Artículo 15 – apartado 6

Texto de la Comisión	*Enmienda*
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.	6. Los Estados miembros garantizarán que cualesquiera obligaciones impuestas a los operadores del mercado en virtud del presente capítulo puedan estar sujetas a control judicial.

Enmienda 120

Propuesta de Directiva
Artículo 15 – apartado 6 bis (nuevo)

Texto de la Comisión	*Enmienda*
	6 bis. Los Estados miembros podrán decidir aplicar el artículo 14 y el presente artículo a las administraciones públicas mutatis mutandis.

Enmienda 121

Propuesta de Directiva
Artículo 16 – apartado 1

Texto de la Comisión	*Enmienda*
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.	1. A fin de garantizar una aplicación convergente de lo dispuesto en el artículo 14, apartado 1, los Estados miembros***, sin prescribir el empleo de ninguna tecnología en particular,*** fomentarán la utilización de las normas y***/o*** especificaciones ***internacionales interoperables*** pertinentes en materia de seguridad de las redes y la información.

Enmienda 122

Propuesta de Directiva
Artículo 16 – apartado 2

Texto de la Comisión	*Enmienda*
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.	2. La Comisión ***conferirá a un organismo europeo de normalización pertinente el mandato de elaborar, en consulta con las partes interesadas pertinentes,*** una lista de las normas y***/o especificaciones*** mencionadas en el apartado 1. Dicha lista se publicará en el Diario Oficial de la Unión Europea.

Enmienda 123

Propuesta de Directiva
Artículo 17 – apartado 1 bis (nuevo)

Texto de la Comisión	*Enmienda*
	1 bis. Los Estados miembros garantizarán que la sanciones contempladas en el apartado 1 del presente artículo solo se apliquen cuando el operador del mercado no haya cumplido las obligaciones con arreglo al capítulo IV de forma deliberada o por negligencia grave.

Enmienda 124

Propuesta de Directiva
Artículo 18 – apartado 3

Texto de la Comisión	*Enmienda*
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 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	3. La delegación de poderes a que se ***refiere*** el artículo 9, apartado 2, podrá ser revocada en cualquier momento por 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

decisión. No afectará a la validez de los actos delegados que ya estén en vigor.	los actos delegados que ya estén en vigor.

Enmienda 125

Propuesta de Directiva
Artículo 18 – apartado 5

Texto de la Comisión	*Enmienda*
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.	5. Los actos delegados adoptados en virtud del artículo 9, apartado 2, 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.

Enmienda 126

Propuesta de Directiva
Artículo 20 – apartado 1

Texto de la Comisión	*Enmienda*
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.	La Comisión revisará periódicamente el funcionamiento de la presente Directiva***, en particular la lista contenida en el anexo II,*** 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.

Enmienda 127

Propuesta de Directiva
Anexo 1 – título 1

Texto de la Comisión	*Enmienda*
Obligaciones y tareas ***del equipo*** de respuesta a emergencias informáticas (CERT)	Obligaciones y tareas de ***los equipos*** de respuesta a emergencias informáticas (CERT)

Enmienda 128

Propuesta de Directiva
Anexo 1 – apartado 1 – punto 1 – letra a

Texto de la Comisión	*Enmienda*
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.	a) Los CERT ***garantizarán*** una gran disponibilidad de sus servicios de comunicaciones evitando los fallos puntuales simples y contarán con varios medios para ser contactados y contactar con otros ***en todo momento***. Además, los canales de comunicación estarán claramente especificados y serán bien conocidos por los grupos de usuarios y los socios colaboradores.

Enmienda 129

Propuesta de Directiva
Anexo 1 – apartado 1 – punto 1 – letra c

Texto de la Comisión	*Enmienda*
c) Las dependencias ***del*** CERT y los sistemas de información de apoyo estarán situados en lugares seguros.	c) Las dependencias ***de los*** CERT y los sistemas de información de apoyo estarán situados en lugares seguros ***con redes y sistemas de información protegidos***.

Enmienda 130

Propuesta de Directiva
Anexo 1 – apartado 1 – punto 2 – letra a – guión 1

Texto de la Comisión	*Enmienda*
– Supervisar incidentes a escala nacional.	– ***Detectar y*** supervisar incidentes a escala nacional.

Enmienda 131

Propuesta de Directiva
Anexo 1 – apartado 1 – punto 2 – letra a – guión 5 bis (nuevo)

Texto de la Comisión	*Enmienda*
	- Participar activamente en las redes internacionales y de la Unión de cooperación entre CERT.

Enmienda 132

Propuesta de Directiva
Anexo II – parte introductoria

Texto de la Comisión	*Enmienda*
Lista de operadores del mercado	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):	

Enmienda 133

Propuesta de Directiva
Anexo II – punto 1

Texto de la Comisión	*Enmienda*
Lista de operadores del mercado	Lista de operadores del mercado
1. Energía:	1. Energía:
	a) Electricidad
- Proveedores ***de gas y electricidad.***	- Proveedores
- Gestores de redes de distribución ***de gas o electricidad*** y minoristas para consumidores finales.	- Gestores de redes de distribución 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.	- Gestores de redes de transporte de electricidad.
	b) Petróleo
- Oleoductos de transporte de crudo y almacenamiento de crudo.	- Oleoductos de transporte de crudo y almacenamiento de crudo.
	- Operadores de producción de crudo, instalaciones de refinado y tratamiento, almacenamiento y transporte
	c) Gas
- Operadores de los mercados del gas y la electricidad.	***- Proveedores***
	- Gestores de redes de distribución y minoristas para consumidores finales
	- Gestores de redes de transporte de gas natural, gestores de redes de almacenamiento y gestores de GNL.
- Operadores de producción de ***crudo y*** gas natural, instalaciones de refinado y tratamiento***.***	- Operadores de producción de gas natural, instalaciones de refinado y tratamiento***, almacenamiento y transporte***
	- Operadores de los mercados del gas

Enmienda 134

Propuesta de Directiva
Anexo II – punto 2

Texto de la Comisión	*Enmienda*
2. Transportes:	2. Transportes:
- Compañías aéreas (transporte aéreo de mercancías y pasajeros).	***a) Transporte por carretera***
- Compañías de transporte marítimo (empresas de transporte marítimo y de cabotaje de pasajeros y empresas de transporte marítimo y de cabotaje de mercancías).	***i) Operadores de control de la gestión del tráfico.***
- Compañías ferroviarias (gestores de infraestructuras, compañías integradas y operadores de transporte ferroviario).	***ii) Servicios logísticos auxiliares:***
- Aeropuertos.	***- depósito y almacenamiento,***
- Puertos.	***- manipulación de la carga, y***
- Operadores de control de la gestión del tráfico.	***- otras actividades auxiliares del transporte.***
- Servicios logísticos auxiliares [a) depósito y almacenamiento, b) manipulación de la carga y c) otras actividades auxiliares del transporte].	***b) Transporte por ferrocarril***
	i) Compañías ferroviarias (administradores de infraestructuras, compañías integradas y operadores de transporte ferroviario).
	ii) Operadores de control de la gestión del tráfico.
	iii) Servicios logísticos auxiliares:
	- depósito y almacenamiento,
	- manipulación de la carga, y
	- otras actividades auxiliares del transporte.
	c) Transporte aéreo
	i) Compañías aéreas (transporte aéreo de mercancías y pasajeros).
	ii) Aeropuertos.

	iii) Operadores de control de la gestión del tráfico.
	iv) Servicios logísticos auxiliares:
	- explotación de almacenes de depósito,
	- manipulación de la carga, y
	- otras actividades auxiliares del transporte.
	d) Transporte marítimo
	i) Compañías de transporte marítimo (empresas de transporte marítimo, fluvial y de cabotaje de pasajeros y empresas de transporte marítimo, fluvial y de cabotaje de mercancías).

Enmienda 135

Propuesta de Directiva
Anexo II – punto 4

Texto de la Comisión	*Enmienda*
4. Infraestructuras de los mercados financieros: ***bolsas*** y entidades de contrapartida central.	4. Infraestructuras de los mercados financieros: ***mercados regulados, sistemas multilaterales de negociación, sistemas organizados de negociación*** y entidades de contrapartida central.

Enmienda 136

Propuesta de Directiva
Anexo II – punto 5 bis (nuevo)

Texto de la Comisión	*Enmienda*
	5 bis. Producción y el abastecimiento de aguas.

Enmienda 137

Propuesta de Directiva
Anexo II – punto 5 ter (nuevo)

Texto de la Comisión	*Enmienda*
	5 ter. Cadena alimentaria.

Enmienda 138

Propuesta de Directiva
Anexo II – punto 5 quater (nuevo)

Texto de la Comisión	*Enmienda*
	5 quater. Puntos de intercambio de Internet.

EXPOSICIÓN DE MOTIVOS

1. Antecedentes

Ya en 2010, la Agenda Digital para Europa pidió la introducción de instrumentos legislativos destinados a una política de elevado nivel de seguridad de las redes y la información. Debido a la interconexión de las redes y los sistemas de información, las interrupciones significativas de dichos sistemas en un Estado miembro pueden afectar a los demás Estados miembros y a la Unión en su conjunto. La resistencia y estabilidad de las redes y los sistemas de información, así como la continuidad de los servicios básicos, son fundamentales para el correcto funcionamiento del mercado interior, en particular para el continuo desarrollo del mercado único digital.

A la vista de los distintos niveles de capacidad y de los enfoques fragmentados en toda la Unión, la Comisión Europea, con la presente propuesta de Directiva relativa a las medidas para garantizar un elevado nivel común de seguridad de las redes y de la información en la Unión, pretende mejorar la seguridad de Internet y de las redes privadas y de los sistemas de información que apoyan el funcionamiento de nuestras sociedades y economías.

A este fin, la Comisión exige a los Estados miembros que mejoren su preparación y la cooperación entre Estados. Para ello, los operadores de infraestructuras críticas, tales como la energía, el transporte y los principales proveedores de servicios de la sociedad de la información, así como las administraciones públicas, deberán tomar medidas adecuadas para gestionar los riesgos de seguridad y comunicar los incidentes graves a las autoridades nacionales competentes.

2. Proyecto de informe

El ponente apoya el objetivo general de la propuesta de Directiva, que es el de garantizar un elevado nivel común de seguridad de las redes y de la información. Con el fin de reforzar la eficacia de las medidas propuestas, el ponente considera que la presente Directiva, como punto de partida, debería limitarse a determinados operadores, a salvaguardar las inversiones en seguridad de las redes y de la información que ya se hayan hecho y a evitar duplicidades de estructuras institucionales y de las obligaciones impuestas a los operadores del mercado. Asimismo, el ponente opina que la presente Directiva debe apoyar el desarrollo de relaciones e intercambios de confianza entre actores públicos y privados, y que deben evitarse las reacciones negativas en forma de una mera «cultura de cumplimiento» en lugar de la deseable «cultura de gestión de los riesgos». A la vista de estas consideraciones, el ponente propone reforzar el impacto de la presente Directiva con las siguientes modificaciones principales.

A. Campo de aplicación

La propuesta de Directiva pretende imponer obligaciones a las administraciones públicas y a

los operadores del mercado, incluidas las infraestructuras críticas y los servicios de la sociedad de la información. Con el fin de que la Directiva logre proporcionalidad y resultados rápidos, el ponente considera que las medidas obligatorias establecidas en el capítulo IV deberían limitarse a las infraestructuras críticas en el más estricto sentido del término. El ponente considera que los servicios de la sociedad de la información, por tanto, deberían quedar excluidos del anexo II de la presente Directiva. En su lugar, la presente Directiva debería centrarse en los operadores del mercado que prestan servicios, entre otros, en los sectores de la energía y los transportes, así como los servicios relacionados con la sanidad y las infraestructuras de los mercados financieros.

En vista de su misión pública, las administraciones públicas deben ejercer la diligencia debida en la gestión de sus redes y sistemas de información. Por tanto, el ponente no considera que sea proporcionado imponerles las mismas obligaciones que a los operadores del mercado. Además de las modificaciones en el campo de aplicación, el ponente apoya la naturaleza no exhaustiva del anexo II y está conforme con una revisión periódica de la presente Directiva, también a la vista de los nuevos avances tecnológicos.

B. Autoridades nacionales competentes

La propuesta de Directiva prevé la designación de una autoridad nacional competente por cada Estado miembro, encargada de supervisar la aplicación de la Directiva. El ponente considera que esto no toma debidamente en cuenta las estructuras ya existentes.
En determinados sectores incluidos en el campo de aplicación de la presente Directiva, los operadores del mercado ya notifican a la autoridad reguladora específica de su sector, ya sea de manera formal o informal, determinados incidentes en la seguridad de las redes y la información. Habida cuenta de la vinculación directa y las estrechas relaciones con sus respectivos sectores, estas autoridades poseen información detallada sobre amenazas y vulnerabilidades, particulares de su sector y, por tanto, se encuentran en una posición única para valorar el impacto de los incidentes actuales o potenciales en dichos sectores.

Además de las inversiones existentes en cada sector, es posible que algunos Estados miembros requieran la designación de más de una autoridad nacional competente debido a su estructura constitucional o por otras consideraciones. Por tanto, el ponente propone modificar la Directiva a fin de que permita la designación de más de una autoridad nacional competente por cada Estado miembro. No obstante, con el fin de garantizar una aplicación coherente en los Estados miembros y para permitir una cooperación eficaz y sin fisuras a escala de la Unión, cada Estado miembro deberá designar una ventanilla única encargada, entre otros aspectos, de la participación en la red de cooperación contemplada en el artículo 8 y de difundir alertas tempranas con arreglo al artículo 10.

C. Red de cooperación

Con el fin de reforzar las actividades de la red de cooperación, el ponente opina que dicha red debe plantearse, cuando proceda, invitar a participar a los operadores del mercado. Asimismo, un informe anual de las actividades de la red proporcionaría valiosa información sobre los avances en el intercambio de mejores prácticas entre los Estados miembros y sobre la elaboración de notificaciones de incidentes en toda la Unión.

D. Requisitos en materia de seguridad y notificación de incidentes

Como principal novedad, la propuesta de Directiva introduce para los operadores del mercado la obligación de notificar los incidentes que tengan un impacto significativo sobre la seguridad de los servicios básicos. Con el fin de aclarar el alcance de las obligaciones y consagrarlas en el acto de base, el ponente propone sustituir los actos delegados del artículo 14, apartado 5, con criterios claros para determinar la importancia de los incidentes que deben notificarse. A la vista de la armonización prevista con la Directiva 2009/140/CE, los indicadores similares a los contemplados en las directrices técnicas de la ENISA sobre la notificación de incidentes para la Directiva 2009/140/CE, aclararían el campo de aplicación y los criterios de notificación. Igualmente, el ponente recomienda reforzar las salvaguardas en relación con la publicación de información relativa a los incidentes, y aclara la aplicabilidad de la ley, en caso de que un incidente afecte a los servicios básicos en varios Estados miembros, a fin de no imponer obligaciones de notificación múltiples o poco claras.

E. Aplicación y observancia

El ponente considera fundamental fomentar una cultura de gestión de los riesgos y crecer a partir de los esfuerzos realizados por los operadores del mercado. Para ello, opina que, más que la forma en que se proporciona la información sobre las actividades concretas de gestión de los riesgos, es fundamental la cooperación global y las medidas concretas adoptadas por los operadores del mercado.

Por consiguiente, en el contexto del artículo 15, es necesario permitir la flexibilidad en relación con la prueba de cumplimiento de los requisitos de seguridad impuestos a los operadores del mercado. Debería admitirse la prueba de cumplimiento que se facilita en un formato distinto al de las auditorías de seguridad.

F. Sanciones

Si bien el ponente cree necesario prever sanciones para los operadores del mercado que no cumplan para reforzar la eficacia de la presente Directiva, opina que las sanciones potenciales no deben restar incentivos a la notificación de incidentes ni generar efectos adversos. Debe evitarse que la rápida notificación de incidentes se vea socavada por el riesgo de sanciones, entre otras cosas, por el mero incumplimiento de los requisitos de procedimiento. Por tanto, el ponente propone aclarar que, si el operador del mercado no ha cumplido con sus obligaciones con arreglo al capítulo IV, pero no ha actuado de forma deliberada o por negligencia grave, no se le debería imponer sanción alguna.

19.12.2013

OPINIÓN DE LA COMISIÓN DE INDUSTRIA, INVESTIGACIÓN Y ENERGÍA

para la Comisión de Mercado Interior y Protección del Consumidor

sobre la 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)0048 – C7-0035/2013 – 2013/0027(COD))

Ponente de opinión (*): Pilar del Castillo Vera

(*) Procedimiento de comisiones asociadas – artículo 50 del Reglamento

BREVE JUSTIFICACIÓN

En febrero de 2013, la Comisión Europea, tal como había solicitado el Parlamento Europeo en su informe de propia iniciativa sobre una Agenda Digital para Europa, presentó una propuesta de Directiva relativa a medidas para garantizar un elevado nivel común de seguridad de las redes y de la información en la Unión, junto con la primera estrategia de la UE en materia de seguridad cibernética. La ponente acoge la propuesta con satisfacción, teniendo en cuenta que, analizando los datos disponibles, puede estimarse que los incidentes relativos a las TIC de carácter doloso pueden comportar costes directos de más de 560 millones EUR al año solo para las PYME, y que todos los tipos de incidentes (incluidos problemas en fases anteriores, de entorno o físicos, tales como catástrofes naturales) podrían provocar costes directos de más de 2 300 millones EUR.

En cuanto a la estructura, la ponente está de acuerdo con varias de las medidas propuestas, tales como la ampliación de las disposiciones en materia de información sobre incidentes en materia de seguridad, que se limita actualmente a los proveedores de telecomunicaciones en virtud del artículo 13 bis de la Directiva marco de 2009, también a otros sectores de infraestructuras críticas. En consecuencia, propuestas tales como exigir que todos los Estados miembros dispongan de equipos de respuesta a emergencias informáticas que funcionen correctamente y designen a una autoridad competente como parte de una red paneuropea segura de intercambio de datos electrónicos para permitir la puesta en común y el intercambio seguros de información relativa a la seguridad cibernética son bienvenidas y presentan potencial para contribuir en gran medida al objetivo de la propuesta de Directiva, es decir, garantizar un elevado nivel común de seguridad de las redes y de la información en la Unión.

Sin embargo, la ponente considera que es posible mejorar la propuesta aplicando el prisma de dos principios importantes: eficacia y confianza.

Primer principio – Eficacia

Habida cuenta de las obligaciones de los Estados miembros de designar a una autoridad competente responsable de supervisar la aplicación de la Directiva a todos los sectores enumerados en el anexo II de la propuesta, la ponente opina que cada Estado miembro no solo debe elegir libremente el modelo de gobernanza de la seguridad cibernética que considere más adecuado, sino que también se impone evitar la duplicación de estructuras institucionales que potencialmente podrían comportar conflictos de competencia y la interrupción de las comunicaciones. Por lo tanto, la ponente considera que no deben interrumpirse las estructuras nacionales existentes que ya funcionan de manera eficaz y responden a las necesidades de los Estados miembros y a sus requisitos constitucionales. No obstante, estima que, a fin de garantizar el intercambio de información en el ámbito de la Unión, la notificación de alertas tempranas ante amenazas y la participación eficaz en la red de cooperación, cada Estado miembro debe disponer de una **ventanilla única**.

Con el mismo espíritu de optimizar la eficacia de la propuesta de Directiva, la ponente considera que las medidas propuestas en relación con la creación de un **equipo de respuesta a emergencias informáticas («CERT»)** nacional puede que no resulte el requisito más adecuado, puesto que no tienen en cuenta la diversidad de naturaleza y de composición de los CERT existentes. No solo la mayor parte de los Estados miembros disponen de más de un CERT, sino que también se ocupan de tipos distintos de incidentes. La cantidad y la calidad de las actividades también varía dependiendo de qué instituciones las acogen y las gestionan, que pueden ser académicas o de investigación, administraciones o el sector privado. Por otra parte, la propuesta actual pondría fin a las redes de cooperación internacionales y europeas existentes, a las que ya pertenecen los CERT existentes, que han demostrado su eficacia a la hora de coordinar las respuestas internacionales y europeas a los incidentes. En consecuencia, la ponente considera que, en lugar de hacer referencia a un único CERT nacional, la Directiva debería orientarse a aquellos CERT que prestan sus servicios en los sectores del anexo II, con lo que se permitiría, por ejemplo, que un CERT preste servicio a todos los sectores del anexo II o que varios CERT presten servicios en el mismo sector. Sin embargo, la ponente opina que los Estados miembros deben garantizar la plena operabilidad en todo momento de sus CERT y garantizar que disponen de suficientes recursos técnicos, económicos y humanos para funcionar correctamente y participar en redes de cooperación internacionales y de la Unión.

Asimismo, el principio de eficacia impone cambios en la propuesta de Directiva en lo que se refiere al **ámbito de aplicación**. Si bien la ponente admite que es necesario ampliar las obligaciones del sistema de informes a los sectores de la energía, el transporte, la salud y las finanzas, la propuesta de ampliar las medidas obligatorias establecidas en el capítulo IV a todos los operadores del mercado en la «economía de Internet» es desproporcionada e imposible de administrar. Desproporcionada porque la imposición indiscriminada de nuevas obligaciones a una categoría abierta y no definida tal como todo «proveedor de servicios de la sociedad de la información que posibilitan la prestación de otros servicios de la sociedad de la información» no solo es incomprensible sino que tampoco está debidamente justificada en relación con el posible daño provocado por un incidente de seguridad, y conlleva el potencial de añadir un estrato más de burocracia para nuestro sector industrial, especialmente para las PYME. Imposible de administrar porque se plantean serias dudas acerca de si las autoridades competentes podrán gestionar todas las potenciales notificaciones de una manera proactiva

que fomente un diálogo bidireccional con los operadores del mercado con miras a resolver la amenaza para la seguridad.

En cuanto a las **administraciones públicas**, la Directiva debe equilibrar la necesidad de un mayor desarrollo de los servicios de administración electrónica con las obligaciones existentes de diligencia debida en las administraciones públicas en lo relativo a la gestión y a la protección de sus redes y sistemas de información. En consecuencia, la ponente estima que, si bien el intercambio de requisitos de información establecido en el artículo 14 debe aplicarse plenamente a las administraciones públicas, estas no deben estar sujetas a las obligaciones del artículo 15.

Segundo principio – Confianza

La posición de la ponente es que una gran parte del éxito de la Directiva recae en su capacidad para incentivar la participación de los operadores del mercado, lo que llevaría a la creación de un entorno SRI fiable en el que los que se encuentren en el terreno deseen participar de manera activa. Si no se consigue, fracasará. En este sentido, la ponente propone garantizar que la participación y la notificación de los operadores del mercado no queden afectadas negativamente por la publicación innecesaria de incidentes de seguridad que estos han notificado, o que las autoridades responsables o las ventanillas únicas puedan considerarlos responsables de pérdida de información. Además, debe abrirse un diálogo bidireccional entre los operadores y las autoridades competentes, y debe fomentarse la participación de los operadores del mercado en todos los foros, incluida la red de cooperación.

La ponente considera asimismo que la confianza debe ser el pilar de la participación de las autoridades competentes y de las ventanillas únicas, especialmente en cuanto al intercambio de información. Con el fin de garantizarlo, deben reflejarse en la Directiva disposiciones relativas a los requisitos de confidencialidad y seguridad de la red.

ENMIENDAS

La Comisión de Industria, Investigación y Energía pide a la Comisión de Mercado Interior y Protección del Consumidor, competente para el fondo, que incorpore en su informe las siguientes enmiendas:

Enmienda 1

Propuesta de Directiva
Considerando 1

Texto de la Comisión	*Enmienda*
(1) Las redes y los sistemas y servicios de información desempeñan un papel crucial en la sociedad. Su fiabilidad y seguridad	(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.	son esenciales ***para la libertad y la seguridad general de los ciudadanos de la UE, así como*** para la actividad económica y el bienestar social y, en particular, para el funcionamiento del mercado interior.

Enmienda 2

Propuesta de Directiva
Considerando 2

Texto de la Comisión	*Enmienda*
(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.	(2) La magnitud***,*** la frecuencia ***y los efectos*** de los incidentes de seguridad se están incrementando y representan una grave amenaza para el funcionamiento de las redes y los sistemas de información. ***Es posible que estos sistemas también se conviertan en un objetivo fácil de acciones dañinas deliberadas con el propósito de perjudicar o interrumpir el funcionamiento de los sistemas.*** Tales incidentes pueden ***amenazar la salud y seguridad de la población,*** interrumpir las actividades económicas, generar considerables pérdidas financieras, minar la confianza del usuario ***y del inversor*** y causar grandes daños a la economía de la Unión.

Justificación

Los ataques informáticos a sociedades cotizadas se han generalizado e incluyen el robo de activos financieros, propiedad intelectual o la perturbación de las operaciones de sus clientes o sus socios y podrían repercutir en las relaciones con los accionistas y en la decisión de inversores potenciales.

Enmienda 3

Propuesta de Directiva
Considerando 3

Texto de la Comisión	*Enmienda*
(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.	(3) Al ser instrumentos de comunicación sin fronteras ***tradicionales***, los sistemas de información digitales —y sobre todo Internet— contribuyen decisivamente a facilitar la circulación transfronteriza de bienes, servicios***, ideas*** 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 ***y también para el funcionamiento de los mercados exteriores***.

Justificación

La resiliencia y la estabilidad de las redes y los sistemas de información del mercado interior también son esenciales para la interacción con mercados mundiales y regionales como América del Norte o Asia, entre otros.

Enmienda 4

Propuesta de Directiva
Considerando 4

Texto de la Comisión	*Enmienda*
(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	(4) Es conveniente crear a escala de la Unión un mecanismo de cooperación que propicie el intercambio de información y una prevención, 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 los operadores ***públicos y***

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.	***privados*** de infraestructuras de información ***y a las sociedades cotizadas*** requisitos mínimos en materia de seguridad para fomentar una cultura de gestión de riesgos y garantizar la notificación de los incidentes más graves. ***El marco jurídico deberá basarse en la necesidad de salvaguardar la privacidad y la integridad de los ciudadanos. La Red de información sobre alertas en infraestructuras críticas debe ampliarse a estos operadores concretos.***

Justificación

Las violaciones de la seguridad por parte de las sociedades cotizadas podrían afectar considerablemente a los productos y servicios de la sociedad, a las relaciones con sus clientes y proveedores y a las condiciones competitivas en general y, por tanto, podrían tener repercusiones importantes en el funcionamiento del mercado interior (y exterior). Por consiguiente, esta Directiva debería abarcar también a las sociedades cotizadas.

Enmienda 5

Propuesta de Directiva
Considerando 4 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(4 bis) La presente Directiva debe centrarse en las infraestructuras críticas esenciales para el mantenimiento de actividades económicas y sociales vitales en los sectores de la energía, los transportes, la banca, las infraestructuras de los mercados financieros y la sanidad.

Enmienda 6

Propuesta de Directiva
Considerando 4 ter (nuevo)

Texto de la Comisión	*Enmienda*
	(4 ter) Para garantizar que los gobiernos no hagan un uso excesivo o indebido de sus competencias, es de vital importancia que los sistemas de información y seguridad de las autoridades públicas sean transparentes y legítimos, estén bien definidos y se adopten de forma transparente mediante un proceso democrático.

Enmienda 7

Propuesta de Directiva
Considerando 6

Texto de la Comisión	*Enmienda*
(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.	(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 los operadores del mercado imposibilita la creación de un mecanismo global y efectivo de cooperación en la Unión***, lo que perjudica asimismo a la eficacia de la cooperación internacional y, en consecuencia, a la lucha contra retos mundiales en materia de seguridad y socava el liderazgo a escala internacional de la Unión en la salvaguardia y la promoción de una red de internet libre, eficiente y segura.***

Enmienda 8

Propuesta de Directiva
Considerando 7

Texto de la Comisión	*Enmienda*
(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***.	(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, ***que desarrolle suficientes capacidades de ciberseguridad,*** actividades de intercambio de información y coordinación de medidas, así como requisitos mínimos comunes de seguridad. ***Procede aplicar unas normas comunes mínimas con arreglo a las recomendaciones pertinentes formuladas por los grupos de coordinación en materia de ciberseguridad.***

Enmienda 9

Propuesta de Directiva
Considerando 9

Texto de la Comisión	*Enmienda*
(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.	(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***, teniendo en cuenta los requisitos mínimos establecidos en la presente Directiva,*** 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. ***Procede, por tanto, que cada Estado miembro esté obligado a cumplir las normas comunes relativas al formato de los datos y la posibilidad de intercambio de los datos que se deban compartir y evaluar. Los Estados miembros podrán solicitar la asistencia de la Agencia Europea de Seguridad de las Redes y de la Información («ENISA») para desarrollar sus estrategias nacionales de SRI, partiendo de un proyecto mínimo común de estrategia de SRI.***

Justificación

Las partes interesadas pertinentes ya han reconocido a la ENISA como centro de excelencia sumamente competente e instrumento digno de confianza para promover la ciberseguridad en la UE. Por lo tanto, la UE debería evitar la duplicación de esfuerzos y estructuras aprovechando los conocimientos de la ENISA y exigir que dicho organismo ofrezca servicios de asesoramiento a aquellos Estados miembros que carezcan de instituciones y conocimientos de SRI y soliciten este tipo de ayuda.

Enmienda 10

Propuesta de Directiva
Considerando 10

Texto de la Comisión	*Enmienda*
(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.	(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 ***único*** centro de referencia nacional a efectos ***de coordinación interna y*** de cooperación transfronteriza a escala de la Unión. ***Estas ventanillas únicas a escala nacional deben designarse sin perjuicio de que cada Estado miembro designe más de una autoridad nacional competente encargada de la seguridad de las redes y la información, conforme a sus obligaciones***

	constitucionales, jurisdiccionales o administrativas, pero no obstante se les debe asignar un mandato de coordinación a escala nacional y de la Unión. Estos organismos deben disponer de recursos técnicos, financieros y humanos suficientes para poder desempeñar ***continua,*** efectiva y eficazmente las tareas que se les encomienden y alcanzar de este modo los objetivos de la presente Directiva.

Enmienda 11

Propuesta de Directiva
Considerando 10 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(10 bis) A la vista de las diferencias en las estructuras nacionales de gobernanza y con el fin de salvaguardar los acuerdos sectoriales y evitar duplicidades, los Estados miembros deben tener competencia para designar a más de una autoridad nacional competente que se encargue de realizar las tareas vinculadas a la seguridad de las redes y de los sistemas de información de los operadores del mercado en virtud de la presente Directiva. No obstante, con el fin de garantizar la buena cooperación y comunicación transfronterizas, es necesario que cada Estado miembro designe solo una ventanilla única nacional que se encargue de la cooperación transfronteriza a escala de la Unión. Si fuera necesario en virtud de su estructura constitucional o de otros acuerdos, el Estado miembro debe poder designar solo una única autoridad que se encargue de realizar las tareas de la autoridad competente y de la ventanilla única.

Enmienda 12

Propuesta de Directiva
Considerando 11

Texto de la Comisión	*Enmienda*
(11) Todos los Estados miembros deben disponer de capacidades técnicas y de organización suficientes para poder adoptar las medidas de prevención, detección, 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.	(11) Todos los Estados miembros ***y los operadores del mercado*** deben disponer de capacidades técnicas y de organización suficientes para poder adoptar las medidas de prevención, detección, respuesta y atenuación oportunas ante los incidentes y riesgos que puedan afectar a las redes y los sistemas de información ***en cualquier momento***. ***Los sistemas de seguridad de las administraciones públicas deberán ser seguros y estar sujetos al control y examen democráticos. Los equipos y las capacidades que por lo general sean necesarios deben cumplir con las normas técnicas establecidas de común acuerdo y con los procedimientos normativos de funcionamiento.*** Por consiguiente, procede crear en todos los Estados miembros equipos de respuesta a emergencias informáticas ***(CERT)*** 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. ***Se debe permitir que estos CERT interactúen basándose en normas técnicas comunes y procedimientos normativos de funcionamiento. A la vista de las diferentes características de los CERT existentes, que responden a necesidades temáticas y actores distintos, los Estados miembros deben garantizar que cada uno de los sectores cubiertos por el anexo II recibe servicios al menos por parte de un CERT. En cuanto a la cooperación transfronteriza entre CERT, los Estados miembros deben garantizar que los CERT dispongan de los medios suficientes para participar en las redes de cooperación internacionales y europeas ya en***

funcionamiento.

Justificación

Se ha de garantizar la interoperabilidad.

Enmienda 13

Propuesta de Directiva
Considerando 12

Texto de la Comisión	*Enmienda*
(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.	(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***, con el que se garantiza la participación de los operadores del mercado,*** permita estructurar y coordinar a escala de la Unión las labores de intercambio de información, detección y respuesta.

Enmienda 14

Propuesta de Directiva
Considerando 13

Texto de la Comisión	*Enmienda*
(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	(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.

prácticas. En particular, la Comisión ***y los Estados miembros*** deben 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.

Enmienda 15

Propuesta de Directiva
Considerando 14

Texto de la Comisión	*Enmienda*
(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.	(14) Es oportuno crear infraestructuras seguras***, bajo la supervisión de la ENISA,*** 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. ***A fin de que la red de cooperación pueda cumplir eficazmente su misión, la Comisión debe crear una línea presupuestaria para esta red.***

Enmienda 16

Propuesta de Directiva
Considerando 14 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(14 bis) Cuando proceda, también podrá invitarse a los operadores del mercado a participar en las actividades de la red de cooperación.

Enmienda 17

Propuesta de Directiva
Considerando 15

Texto de la Comisión	*Enmienda*
(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.	(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 ***mutuamente*** información y mejores prácticas***, incluido el intercambio recíproco de información pertinente y*** apoyo operativo ***e información analizada desde un punto de vista estratégico,*** en caso de que se produzcan incidentes. ***Para fomentar eficazmente el intercambio de información y de mejores prácticas, es esencial garantizar que los operadores del mercado que participan en dichos intercambios no queden en desventaja a causa de su cooperación. Se necesitan suficientes salvaguardias para garantizar que este tipo de cooperación no exponga a estos operadores a un mayor riesgo de cumplimiento o a nuevas responsabilidades en ámbitos como la***

	competencia, la propiedad intelectual, la protección de datos o la legislación sobre ciberdelincuencia, entre otros, ni los exponga a mayores riesgos operativos o de seguridad.

Enmienda 18

Propuesta de Directiva
Considerando 16

Texto de la Comisión	*Enmienda*
(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.	(16) Para garantizar la transparencia e informar debidamente a los ciudadanos y operadores del mercado de la UE, conviene que las ***ventanillas únicas*** creen un sitio web común ***a escala de la Unión*** para publicar información no confidencial sobre incidentes***,*** riesgos ***y, finalmente, para asesorar sobre medidas de mantenimiento adecuadas***.

Enmienda 19

Propuesta de Directiva
Considerando 17

Texto de la Comisión	*Enmienda*
(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.	(17) ***La política de clasificación de información mencionada en el considerando 14 debe seguir el protocolo para el intercambio de información recomendado por la ENISA. Toda información intercambiada se deberá clasificar y gestionar conforme a su nivel de sensibilidad según lo determine la fuente de la información.*** 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.

Enmienda 20

Propuesta de Directiva
Considerando 18

Texto de la Comisión	*Enmienda*
(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.	(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***, mejores prácticas y pautas de funcionamiento*** para ***prevenir, detectar y*** hacer frente a riesgos e incidentes ***e informar sobre ellos***. Dicho plan debe tomarse debidamente en consideración a la hora de lanzar alertas tempranas en el marco de la red de cooperación.

Enmienda 21

Propuesta de Directiva
Considerando 19

Texto de la Comisión	*Enmienda*
(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	(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 que se extiendan rápidamente, superen la capacidad nacional de respuesta o afecten a más de un Estado miembro. Para poder

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.	proceder a un análisis adecuado, debe comunicarse a la red de cooperación toda la información pertinente para la evaluación del riesgo o incidente.

Enmienda 22

Propuesta de Directiva
Considerando 20

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

Enmienda 23

Propuesta de Directiva
Considerando 22

Texto de la Comisión	*Enmienda*
(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	(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***, de estrecha cooperación y de confianza*** 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 ***y fiables*** para garantizar el funcionamiento efectivo

colaboración eficaz de todos los Estados miembros.

de la red de cooperación y, por ende, una colaboración eficaz de todos los Estados miembros.

Enmienda 24

Propuesta de Directiva
Considerando 24

Texto de la Comisión	*Enmienda*
(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 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,***	(24) Estas obligaciones no solo han de imponerse al sector de las comunicaciones electrónicas, sino también a los ***operadores de infraestructuras, 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 societales vitales, tales como el gas y la electricidad, los transportes, las entidades de crédito, las infraestructuras de los mercados financieros y la sanidad. Los trastornos que puedan sufrir tales redes y sistemas de información afectan al mercado interior. Si bien las obligaciones definidas en la presente Directiva no se extienden*** 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 Internet, las redes sociales, los motores de búsqueda, los servicios de computación en nube ***en general*** o las tiendas de aplicaciones, ***estos pueden notificar voluntariamente a la autoridad competente o a la ventanilla única***

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.	***aquellos incidentes de seguridad que consideren oportunos, y la autoridad competente o la ventanilla única deben presentar, cuando sea razonablemente posible, a los operadores del mercado que hayan informado del incidente, cuando sea razonablemente posible, información analizada desde un punto vista estratégico que ayude a superar la amenaza para la seguridad.***
[4] DO L 204 de 21.7.1998, p. 37.	[4] DO L 204 de 21.7.1998, p. 37.

Enmienda 25

Propuesta de Directiva
Considerando 25

Texto de la Comisión	*Enmienda*
(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.	(25) Las medidas técnicas y de organización impuestas 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. ***Por otro lado, conviene que sea obligatorio el uso de normas internacionales relativas a la ciberseguridad.***

Enmienda 26

Propuesta de Directiva
Considerando 28

Texto de la Comisión	*Enmienda*
(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	(28) Las autoridades competentes ***y las ventanillas únicas*** deben procurar que se mantengan los canales de intercambio de información informales y de confianza entre los operadores del mercado y entre

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.

los sectores público y privado. ***Es conveniente que las vulnerabilidades o los incidentes que se desconocían previamente y que son notificados a las autoridades competentes también se notifiquen a los fabricantes y proveedores de los productos y servicios de TIC afectados.*** Antes de dar publicidad a los incidentes notificados a las autoridades competentes ***y a las ventanillas únicas***, 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 los operadores del mercado que notifican los incidentes. ***Con objeto de salvaguardar la confianza y la eficiencia, únicamente se hará público un incidente después de consultar con quien haya informado del mismo y solo cuando sea estrictamente necesario para alcanzar los objetivos de la presente Directiva.*** A la hora de cumplir sus obligaciones de notificación, las autoridades competentes ***y las ventanillas únicas*** han de tener muy en cuenta la necesidad de mantener estrictamente confidencial la información sobre los puntos vulnerables del producto antes de ***desplegar*** las soluciones de seguridad adecuadas ***aunque sin demorar ninguna notificación más de lo obligatoriamente necesario***. ***Como norma general, las ventanillas únicas no revelarán datos de carácter personal de las personas implicadas en los incidentes. Las ventanillas únicas solo revelarán datos de carácter personal si la revelación de dichos datos es necesaria y proporcional a la vista de los objetivos perseguidos.***

Justificación

En caso de que las autoridades tengan conocimiento de las vulnerabilidades de determinados productos o servicios de TIC, deben notificar a los fabricantes y los proveedores de servicios para que puedan adaptar sus productos o servicios de forma oportuna.

Enmienda 27

Propuesta de Directiva
Considerando 29

Texto de la Comisión	*Enmienda*
(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.	(29) Es preciso que las autoridades competentes ***y las ventanillas únicas*** 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 ***y medir la cantidad, la magnitud y el alcance de los incidentes***, así como datos fidedignos y exhaustivos sobre incidentes reales que hayan repercutido en el funcionamiento de las redes y los sistemas de información.

Enmienda 28

Propuesta de Directiva
Considerando 30

Texto de la Comisión	*Enmienda*
(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	(30) Los incidentes suelen estar causados por actividades delictivas ***o de guerra cibernética***. 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***, las ventanillas únicas*** y los cuerpos de seguridad***, así como la cooperación con el EC3 (Centro Europeo de Ciberdelincuencia de Europol) y la ENISA*** deberían 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

normativa de la UE sobre ciberdelincuencia.

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.

Enmienda 29

Propuesta de Directiva
Considerando 31

Texto de la Comisión	*Enmienda*
(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	(31) En numerosas ocasiones los datos de carácter personal se ven comprometidos a raíz de incidentes. ***Los Estados miembros y los operadores del mercado deben proteger los datos personales almacenados, procesados o transmitidos de la destrucción accidental o ilícita, la pérdida o alteración accidental y el almacenamiento, el acceso o la revelación, la difusión o el acceso no autorizados o ilícitos; y garantizarán la aplicación de una política de seguridad con respecto al tratamiento de los datos personales.*** En este contexto, las autoridades competentes***, las ventanillas únicas*** 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. La obligación de notificar los incidentes de seguridad ***debe aplicarse*** 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 ***que sea obligatorio notificar de conformidad con la legislación aplicable***. La ENISA ***debe*** contribuir a elaborar mecanismos de intercambio de información y ***un*** modelo único de notificación ***que facilite*** la comunicación de incidentes que comprometan los datos

administraciones públicas.	personales, aliviando de este modo la carga administrativa para empresas y administraciones públicas.

[5] ***SEC(2012)0072.***

Justificación

En consonancia con el proyecto de Directiva sobre protección de datos.

Enmienda 30

Propuesta de Directiva
Considerando 32

Texto de la Comisión	*Enmienda*
(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].	(32) La normalización de los requisitos en materia de seguridad es un proceso impulsado por el mercado ***y de carácter voluntario que debe permitir a los operadores del mercado utilizar medios alternativos para conseguir al menos resultados similares***. Al objeto de garantizar una aplicación convergente de las normas de seguridad, es oportuno que los Estados miembros fomenten el cumplimiento de normas específicas ***interoperables*** o la conformidad con ellas para así lograr un elevado nivel de seguridad en la Unión. A tal fin, ***se ha de considerar la aplicación de normas internacionales abiertas a la seguridad de las redes y de la información o el diseño de este tipo de instrumentos. Otro paso adelante necesario*** puede ser 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]. ***En particular, se debe encomendar al Instituto Europeo de Normas de Telecomunicación (ETSI), al Centro Europeo de Normalización (CEN) y al Comité Europeo de Normalización Electrotécnica (CENELEC) la tarea de proponer normas de seguridad abiertas a escala de la UE que resulten eficaces y eficientes, donde se eviten todo lo posible preferencias tecnológicas, y que sean de fácil gestión para los operadores pequeños y medianos del mercado. Conviene examinar detenidamente las normas internacionales relativas a la ciberseguridad a fin de garantizar que no se hayan visto comprometidas y que ofrezcan unos niveles adecuados de seguridad, garantizando así que el cumplimiento obligatorio de las normas de ciberseguridad mejore el nivel global de ciberseguridad de la Unión y no al contrario.***
[6] DO L 316 de 14.11.2012, p. 12.	[6] DO L 316 de 14.11.2012, p. 12.

Enmienda 31

Propuesta de Directiva
Considerando 33

Texto de la Comisión	*Enmienda*
(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.	(33) La Comisión debe revisar periódicamente las disposiciones contenidas en la presente Directiva, ***en consulta con todas las partes interesadas,*** en particular con vistas a determinar si es preciso modificarlas a la luz de la cambiante situación ***societal, política,*** de la

tecnología o el mercado.

Enmienda 32

Propuesta de Directiva
Considerando 34

Texto de la Comisión	*Enmienda*
(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 alerta temprana y con la definición de las circunstancias en que los operadores del mercado y las administraciones públicas están obligados a notificar incidentes.	***suprimido***

Enmienda 33

Propuesta de Directiva
Considerando 35

Texto de la Comisión	*Enmienda*
(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 delegados,*** la Comisión debe garantizar que los documentos pertinentes se transmitan al Parlamento Europeo y al Consejo de manera simultánea, oportuna y adecuada.	(35) Reviste primordial importancia que la Comisión lleve a cabo las consultas oportunas durante la fase preparatoria***, con todas las partes interesadas y***, en particular, con expertos. La Comisión debe garantizar una transmisión simultánea, oportuna y adecuada de los documentos pertinentes al Parlamento Europeo y al Consejo.

Enmienda 34

Propuesta de Directiva
Considerando 36

Texto de la Comisión	*Enmienda*
(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].	(36) A fin de garantizar condiciones uniformes de ejecución de la presente Directiva, deben conferirse a la Comisión competencias de ejecución en lo que respecta a la cooperación entre las ***ventanillas únicas*** y la Comisión en el marco de la red de cooperación, ***sin perjuicio de los mecanismos de cooperación existentes a escala nacional, el conjunto común de normas de interconexión y de seguridad para*** las infraestructuras seguras de intercambio de información, el plan de cooperación de la Unión en materia de SRI y los formatos y procedimientos aplicables a la hora de ***notificar*** incidentes ***importantes***. 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].
[30] DO L 55 de 28.2.2011, p.13.	[30] DO L 55 de 28.2.2011, p.13.

Enmienda 35

Propuesta de Directiva
Considerando 37

Texto de la Comisión	*Enmienda*
(37) Es conveniente que, a la hora de aplicar la presente Directiva, la Comisión	(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.

colabore, cuando proceda, con los comités sectoriales y organismos pertinentes establecidos a escala de la UE, especialmente en los ámbitos de ***la administración electrónica,*** la energía, los transportes y la sanidad.

Enmienda 36

Propuesta de Directiva
Considerando 38

Texto de la Comisión	*Enmienda*
(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.	(38) La información que una autoridad competente ***o ventanilla única*** considere confidencial de acuerdo con las normas nacionales y de la Unión sobre secreto comercial únicamente debe intercambiarse con la Comisión***, sus organismos pertinentes, ventanillas únicas*** y***/u*** 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***, necesaria*** y proporcional a la finalidad perseguida***, respetando los criterios predefinidos de confidencialidad y los protocolos de seguridad y clasificación, por los que se rige el procedimiento de intercambio de información***.

Enmienda 37

Propuesta de Directiva
Considerando 39

Texto de la Comisión	*Enmienda*
(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	(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 ***o a las***

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.

[8] DO L 145 de 31.5.2001, p. 43.

ventanillas únicas 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.

[8] DO L 145 de 31.5.2001, p. 43.

Enmienda 38

Propuesta de Directiva
Considerando 41 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(41 bis) De conformidad con la Declaración política común 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, en aquellos casos en que 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.

Enmienda 39

Propuesta de Directiva
Artículo 1 – apartado 2 – letra b

Texto de la Comisión	*Enmienda*
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;	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 ***con la participación de las partes interesadas pertinentes***;

Enmienda 40

Propuesta de Directiva
Artículo 1 – apartado 6

Texto de la Comisión	*Enmienda*
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	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 ***la comunicación con terceras partes de confianza y*** el tratamiento de

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.	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. ***Los Estados miembros deberán adoptar medidas legislativas de conformidad con el artículo 13 de la Directiva 95/46/CE para garantizar que las administraciones públicas, los operadores del mercado y las autoridades competentes queden exentos de toda responsabilidad por el tratamiento de datos personales, que es necesario para el intercambio de información dentro de la red de cooperación y la notificación de incidentes.***

Enmienda 41

Propuesta de Directiva
Artículo 2 – párrafo 1

Texto de la Comisión	*Enmienda*
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.	No se impedirá que los Estados miembros adopten o mantengan disposiciones que garanticen un nivel de seguridad más elevado ***de conformidad con la Carta de Derechos Fundamentales de la UE***, sin perjuicio de las obligaciones que les impone la normativa de la Unión.

Justificación

La discrecionalidad que se otorga a los Estados miembros en materia de seguridad debe estar supeditada al respeto de los derechos reconocidos en la Carta de Derechos Fundamentales de la UE, en concreto y entre otros, el derecho al respeto de la vida privada y las comunicaciones, el derecho a la protección de datos de carácter personal, el derecho a la libertad de empresa y el derecho a una tutela judicial efectiva.

Enmienda 42

Propuesta de Directiva
Artículo 3 – párrafo 1 – punto 1 – letra b

Texto de la Comisión	*Enmienda*
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***,	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 ***digitales***,

Enmienda 43

Propuesta de Directiva
Artículo 3 – párrafo 1 – punto 1 – letra c

Texto de la Comisión	*Enmienda*
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;	c) los datos ***digitales*** almacenados, tratados, recuperados o transmitidos por los elementos contemplados en las letras a) y b) para su funcionamiento, utilización, protección y mantenimiento;

Enmienda 44

Propuesta de Directiva
Artículo 3 – párrafo 1 – punto 2

Texto de la Comisión	*Enmienda*
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;	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; ***la «seguridad» según se define aquí incluye los***

	dispositivos técnicos, las soluciones y los procedimientos de funcionamiento pertinentes que garantizan los requisitos de seguridad establecidos en la presente Directiva;

Enmienda 45

Propuesta de Directiva
Artículo 3 – párrafo 1 – punto 4

Texto de la Comisión	*Enmienda*
4) «incidente»: toda circunstancia o hecho que tenga efectos adversos en la seguridad;	4) «incidente»: toda circunstancia o hecho ***razonablemente identificable*** que tenga efectos adversos en la seguridad;

Justificación

La redacción original era demasiado amplia y habría complicado la aplicación de la definición.

Enmienda 46

Propuesta de Directiva
Artículo 3 – párrafo 1 – punto 5

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

Enmienda 47

Propuesta de Directiva
Artículo 3 – párrafo 1 – punto 8 – letra a

Texto de la Comisión	*Enmienda*
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;	***suprimida***

Enmienda 48

Propuesta de Directiva
Artículo 3 – párrafo 1 – punto 7

Texto de la Comisión	*Enmienda*
7) «gestión de incidentes»: todos los procedimientos seguidos para analizar, limitar y responder a un incidente;	7) «gestión de incidentes»: todos los procedimientos seguidos para ***detectar, prevenir,*** analizar, limitar y responder a un incidente;

Enmienda 49

Propuesta de Directiva
Artículo 3 – párrafo 1 – punto 8 – letra a

Texto de la Comisión	*Enmienda*
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.	b) un operador ***público o privado*** de infraestructuras esenciales para el mantenimiento de actividades económicas y sociales vitales en los sectores de la energía, los transportes, la banca, ***los mercados financieros*** y la sanidad***, y cuya perturbación o destrucción tendría un importante impacto negativo en un Estado miembro como resultado de la incapacidad***

de mantener dichas funciones, una lista de los cuales figura en el anexo II.

Enmienda 50

Propuesta de Directiva
Artículo 3 – párrafo 1 – punto 8 bis (nuevo)

Texto de la Comisión	*Enmienda*
	8 bis) «incidente que provoca repercusiones importantes»: incidente que afecta a la seguridad y la continuidad de una red o sistema de información que da lugar a la perturbación importante de funciones económicas o societales esenciales;

Enmienda 51

Propuesta de Directiva
Artículo 3 – párrafo 1 – punto 8 ter (nuevo)

Texto de la Comisión	*Enmienda*
	8 ter) «servicio»: el servicio prestado por un operador del mercado, con exclusión de cualquier otro servicio de la misma entidad;

Enmienda 52

Propuesta de Directiva
Artículo 3 – párrafo 1 – punto 11 bis (nuevo)

Texto de la Comisión	*Enmienda*
	11 bis) «mercado regulado»: mercado regulado según se define en el artículo 4,

punto 14, de la Directiva 2004/39/CE del Parlamento Europeo y del Consejo[28bis];

[28bis] Directiva 2004/39/CE del Parlamento Europeo y del Consejo, de 21 de abril de 2004, relativa a los mercados de instrumentos financieros (DO L 45 de 16.2.2005, p. 18).

Enmienda 53

Propuesta de Directiva
Artículo 3 – párrafo 1 – punto 11 ter (nuevo)

Texto de la Comisión	*Enmienda*
	11 ter) «sistema multilateral de negociación (SMN)»: el sistema multilateral de negociación definido en el artículo 4, punto 15, de la Directiva 2004/39/CE;

Enmienda 54

Propuesta de Directiva
Artículo 3 – párrafo 1 – punto 11 quater (nuevo)

Texto de la Comisión	*Enmienda*
	11 quater) «sistema organizado de negociación»: un sistema multilateral, que no sea un mercado regulado, un sistema multilateral de negociación ni una entidad de contrapartida central, operado por una empresa de inversión o por un gestor del mercado, en el que interactúan los diversos intereses de compra y de venta sobre bonos y obligaciones, productos de financiación estructurados, derechos de emisión o derivados de múltiples terceros para dar lugar a contratos, de conformidad con lo dispuesto en el título II de la Directiva 2004/39/CE;

Enmienda 55

Propuesta de Directiva
Artículo 4 – párrafo 1

Texto de la Comisión	*Enmienda*
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.	Los Estados miembros garantizarán un nivel común de seguridad elevado***, sostenido y continuo*** de las redes y los sistemas de información en sus territorios de conformidad ***con la Carta de Derechos Fundamentales de la UE y*** con lo dispuesto en la presente Directiva.

Justificación

La discrecionalidad que se otorga a los Estados miembros en materia de seguridad debe estar supeditada al respeto de los derechos reconocidos en la Carta de Derechos Fundamentales de la UE, en concreto y entre otros, el derecho al respeto de la vida privada y las comunicaciones, el derecho a la protección de datos de carácter personal, el derecho a la libertad de empresa y el derecho a una tutela judicial efectiva.

Enmienda 56

Propuesta de Directiva
Artículo 5 – apartado 1 – letra e bis (nueva)

Texto de la Comisión	*Enmienda*
	e bis) Los Estados miembros podrán solicitar la asistencia de la Agencia Europea de Seguridad de las Redes y de la Información («ENISA») para desarrollar sus estrategias nacionales de SRI y sus planes nacionales de cooperación en materia de SRI, partiendo de un proyecto mínimo común de cooperación y estrategia de SRI.

Enmienda 57

Propuesta de Directiva
Artículo 5 – apartado 2 – letra a

Texto de la Comisión	*Enmienda*
a) ***Plan de evaluación*** de riesgos que ***permita determinarlos y evaluar*** los efectos de incidentes potenciales.	a) ***Marco de gestión*** de riesgos que ***incluya la identificación, la priorización, la evaluación y el tratamiento de los riesgos, la evaluación de*** los efectos de incidentes potenciales***, las opciones de prevención y control y los criterios para la elección de las posibles contramedidas***;

Enmienda 58

Propuesta de Directiva
Artículo 5 – apartado 2 – letra b

Texto de la Comisión	*Enmienda*
b) Determinación de las funciones y responsabilidades de ***los diversos*** agentes que participan en la ejecución del ***plan***.	b) Determinación de las funciones y responsabilidades de ***las diversas autoridades y demás*** agentes que participan en la ejecución del ***marco***.

Enmienda 59

Propuesta de Directiva
Artículo 6 – título

Texto de la Comisión	*Enmienda*
Autoridad nacional competente en materia de seguridad de las redes y los sistemas de información	***Autoridades nacionales competentes y ventanillas únicas*** en materia de seguridad de las redes y los sistemas de información

Enmienda 60

Propuesta de Directiva
Artículo 6 – apartado 1

Texto de la Comisión	*Enmienda*
1. Cada Estado miembro designará una ***autoridad nacional competente*** en materia de seguridad de las redes y los sistemas de información («la autoridad competente»).	1. Cada Estado miembro designará una ***o más autoridades nacionales competentes*** en materia de seguridad de las redes y los sistemas de información (***en lo sucesivo, denominada*** «la autoridad competente»).

Enmienda 61

Propuesta de Directiva
Artículo 6 – apartado 2 bis (nuevo)

Texto de la Comisión	*Enmienda*
	2 bis. En caso de que un Estado miembro designe más de una autoridad competente, designará una autoridad nacional —por ejemplo, una autoridad competente— como ventanilla única nacional en materia de seguridad de las redes y los sistemas de información (en lo sucesivo, denominada «ventanilla única»). Si un Estado miembro designa únicamente una autoridad competente, dicha autoridad también será la ventanilla única.

Enmienda 62

Propuesta de Directiva
Artículo 6 – apartado 2 ter (nuevo)

Texto de la Comisión	*Enmienda*
	2 ter. Las autoridades competentes y la ventanilla única de un mismo Estado miembro cooperarán estrechamente en lo relativo a las obligaciones establecidas en la presente Directiva.

Enmienda 63

Propuesta de Directiva
Artículo 6 – apartado 2 quater (nuevo)

Texto de la Comisión	*Enmienda*
	2 quater. La ventanilla única garantizará la cooperación transfronteriza con otras ventanillas únicas.

Enmienda 64

Propuesta de Directiva
Artículo 6 – apartado 3

Texto de la Comisión	*Enmienda*
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.	3. Los Estados miembros velarán por que las autoridades competentes ***y las ventanillas únicas*** 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 ***ventanillas únicas*** a través de la red a que se hace referencia en el artículo 8.

Enmienda 65

Propuesta de Directiva
Artículo 6 – apartado 4

Texto de la Comisión	*Enmienda*
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.	4. Los Estados miembros velarán por que las autoridades competentes ***y las ventanillas únicas*** reciban las notificaciones de incidentes de 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.

Enmienda 66

Propuesta de Directiva
Artículo 6 – apartado 5

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

Justificación

La existencia de una única autoridad competente para ejercer el poder controlador a nivel nacional sin la colaboración de otro organismo compensatorio, no resulta proporcionado en el equilibrio entre la salvaguardia de la seguridad y de la libertad.

Enmienda 67

Propuesta de Directiva
Artículo 6 – apartado 5

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

Enmienda 68

Propuesta de Directiva
Artículo 6 – apartado 6

Texto de la Comisión	*Enmienda*
6. Los Estados miembros notificarán sin demora a la Comisión ***la autoridad competente*** que hayan designado, su cometido y cualquier cambio posterior que	6. Los Estados miembros notificarán sin demora a la Comisión ***las autoridades competentes y la ventanilla única*** que hayan designado, su cometido y cualquier

se introduzca en él. Los Estados miembros harán pública la designación de ***la autoridad competente***.	cambio posterior que se introduzca en él. Los Estados miembros harán pública la designación de ***las autoridades competentes***.

Enmienda 69

Propuesta de Directiva
Artículo 7 – apartado 1

Texto de la Comisión	*Enmienda*
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.	1. Cada Estado miembro creará ***al menos*** un equipo de respuesta a emergencias informáticas (en lo sucesivo, «CERT») ***para cada uno de los sectores establecidos en el anexo II,*** 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.

Enmienda 70

Propuesta de Directiva
Artículo 7 – apartado 5

Texto de la Comisión	*Enmienda*
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.	5. Los CERT actuarán bajo la supervisión de la autoridad competente ***o la ventanilla única***, que comprobará periódicamente la adecuación de sus recursos, su mandato y la eficacia de su procedimiento de gestión de incidentes.

Enmienda 71

Propuesta de Directiva
Artículo 7 - apartado 5 bis (nuevo)

Texto de la Comisión	*Enmienda*
	5 bis. Los Estados miembros velarán por que los CERT estén dotados de los recursos humanos y financieros suficientes para participar activamente en las redes de cooperación internacionales y, en particular, en las de la Unión.

Enmienda 72

Propuesta de Directiva
Artículo 7 – apartado 5 – punto 1 (nuevo)

Texto de la Comisión	*Enmienda*
	1) Se permitirá y fomentará que los CERT inicien ejercicios conjuntos y participen en ellos con otros CERT, con todos los CERT de los Estados miembros y con las instituciones pertinentes de terceros Estados, así como con CERT de instituciones multinacionales e internacionales como la OTAN y las Naciones Unidas.

Enmienda 73

Propuesta de Directiva
Artículo 7 - apartado 5 bis (nuevo)

Texto de la Comisión	*Enmienda*
	5 bis. Los Estados miembros podrán solicitar la asistencia de la Agencia Europea de Seguridad de las Redes y de la Información («ENISA») para desarrollar sus CERT nacionales.

Enmienda 74

Propuesta de Directiva
Artículo 8

Texto de la Comisión	*Enmienda*
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.	1. Las ***ventanillas únicas, la Agencia Europea de Seguridad de las Redes y de la Información (ENISA)*** y la Comisión crearán una red («red de cooperación») ***en la que colaborarán*** 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.	2. La Comisión y las ***ventanillas únicas*** mantendrán una comunicación constante en el marco de la red de cooperación. 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. ***Cuando proceda, la red de cooperación cooperará con las autoridades de protección de datos.***
3. En el marco de la red de cooperación, las ***autoridades competentes***:	3. En el marco de la red de cooperación, las ***ventanillas únicas***:
a) difundirán alertas tempranas sobre riesgos e incidentes de conformidad con el artículo 10;	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;	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;	c) publicarán periódicamente en un sitio web común información no confidencial sobre las alertas tempranas y las respuestas coordinadas en curso;
	c bis) debatirán y acordarán conjuntamente una interpretación común y la aplicación consecuente de sus medidas en relación con los requisitos de seguridad y la notificación de incidentes contemplados en el artículo 14 y en relación con la aplicación y observancia mencionadas en el artículo 15, y coordinarán conjuntamente dichas medidas;

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;	d) examinarán y evaluarán conjuntamente 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;	e) examinarán y evaluarán conjuntamente, a petición de ***la ENISA,*** 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***, y aplicarán medidas para resolver deficiencias identificadas sin mayor dilación***;
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;	f) cooperarán e intercambiarán información sobre todas las cuestiones pertinentes ***de seguridad de las redes y de la información*** con otros organismos europeos pertinentes, en particular en los sectores de la protección de datos, la energía, los transportes, la banca, ***los mercados financieros*** y la sanidad;
	f bis) debatirán y acordarán conjuntamente la interpretación común, la aplicación coherente y la ejecución armoniosa dentro de la Unión de las disposiciones del capítulo IV;
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;	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;	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.	i) organizarán ejercicios de SRI a escala de la Unión y participarán, en su caso, en ejercicios de SRI internacionales.
	i bis) promoverán activamente la participación de los operadores del mercado y consultarán e intercambiarán información con ellos.
	La Comisión informará regularmente a la red de cooperación de la investigación

sobre seguridad y otros programas pertinentes de Horizonte 2020.

Cuando proceda, la administración pública pertinente y los operadores del mercado podrán ser invitados a participar en las actividades de la red de cooperación contempladas en el apartado 3, letras c), g), h) e i).

3 ter. Cuando la información, las alertas tempranas o las mejores prácticas procedentes de los operadores del mercado o las administraciones públicas se compartan dentro de la red de cooperación o sean divulgadas por esta, tal intercambio o divulgación estará en consonancia con la clasificación de la información determinada por la fuente original conforme al artículo 9, apartado 1.

3 quater. La Comisión publicará cada año respecto de los doce meses anteriores un informe basado en las actividades de la red y en el informe resumido presentado con arreglo al artículo 14, apartado 4, de la presente Directiva. Antes de dar publicidad a los incidentes notificados a las autoridades competentes y a las ventanillas únicas, es preciso realizar consultas previas y 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 los operadores del mercado que hayan notificado los incidentes.

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.

4. La Comisión establecerá mediante actos de ejecución las disposiciones necesarias para facilitar la cooperación entre las ***ventanillas únicas, la ENISA*** 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.

Enmienda 75

Propuesta de Directiva
Artículo 9 – apartado 1

Texto de la Comisión	*Enmienda*
1. El intercambio de información delicada y confidencial dentro de la red de cooperación se efectuará a través de una infraestructura segura.	El intercambio de información delicada y confidencial dentro de la red de cooperación se efectuará a través de una infraestructura segura ***explotada bajo la supervisión de la ENISA***. ***Los Estados miembros garantizarán que la información sensible o confidencial comunicada por otros Estados o por la Comisión no sea compartida con Estados terceros ni utilizada para fines no previstos, como para las actividades de los servicios secretos o la toma de decisiones económicas.***

Enmienda 76

Propuesta de Directiva
Artículo 9 – apartado 2 – parte introductoria

Texto de la Comisión	*Enmienda*
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:	2. Se otorgan a la Comisión los poderes para adoptar actos ***de ejecución*** con arreglo al artículo ***19*** en lo referente a la definición de los criterios que ha de reunir ***una ventanilla única*** para ser ***autorizada*** a participar en el sistema seguro de intercambio de información, en relación con:

Enmienda 77

Propuesta de Directiva
Artículo 9 – apartado 3

Texto de la Comisión	*Enmienda*
3. La Comisión adoptará mediante actos de	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.

ejecución ***un conjunto común de normas de seguridad e interconexiones que las ventanillas únicas deben respetar para intercambiar información***. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 19, apartado 3.

Enmienda 78

Propuesta de Directiva
Artículo 10

Texto de la Comisión	*Enmienda*
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:	1. Las ***ventanillas únicas*** 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;	b) ***que las ventanillas únicas estimen que el riesgo o incidente aumenta o puede aumentar rápidamente en magnitud y puede*** sobrepasar la capacidad nacional de respuesta;
c) ***riesgos e incidentes que afecten o puedan afectar*** a más de un Estado miembro.	c) ***que las ventanillas únicas o la Comisión estimen que el riesgo o incidente afecta*** 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.	2. Las ***ventanillas únicas*** y la Comisión incluirán en sus alertas tempranas***, sin demoras injustificadas,*** toda la información no clasificada pertinente que obre en su poder y pueda ser de utilidad para evaluar el riesgo o incidente. ***La información que el operador del mercado afectado considere clasificada o confidencial y su identidad solo se facilitarán en la medida que sea necesario para evaluar el riesgo o incidente.***
3. A petición de un Estado miembro o por	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.	iniciativa propia, la Comisión podrá solicitar a un Estado miembro que proporcione la información ***no clasificada*** 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.	4. Cuando se sospeche que el riesgo o incidente objeto de una alerta temprana es de carácter ***gravemente*** delictivo, las ***ventanillas únicas*** o la Comisión***, si procede, establecerán contacto sin demoras injustificadas con las autoridades nacionales en materia de ciberdelincuencia para hacer posible su cooperación y el intercambio de información con el*** Centro Europeo de Ciberdelincuencia de Europol.
	4 bis. Los miembros de la red de cooperación no harán pública ninguna información que reciban sobre los riesgos e incidentes de conformidad con el apartado 1 sin haber recibido la aprobación previa de la ventanilla única responsable de la notificación.
	4 ter. Cuando se sospeche que el riesgo o incidente objeto de una alerta temprana es de carácter técnico, transfronterizo y grave, las ventanilla únicas o la Comisión informarán de ello a la ENISA.
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.	5. La Comisión estará facultada para adoptar actos ***de ejecución*** de conformidad con el artículo ***19*** con el fin de especificar los riesgos e incidentes que pueden activar la alerta temprana mencionada en el apartado 1***, así como los procedimientos para compartir información sensible para los operadores del mercado***.

Enmienda 79

Propuesta de Directiva
Artículo 11 – apartado 1

Texto de la Comisión	*Enmienda*
1. Cuando reciban la alerta temprana a que	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.	se refiere el artículo 10, las ***ventanillas únicas*** evaluarán la información pertinente y acordarán, ***sin demoras injustificadas***, una respuesta coordinada de conformidad con el plan de cooperación de la Unión en materia de SRI contemplado en el artículo 12.

Enmienda 80

Propuesta de Directiva
Artículo 12 – apartado 2 – letra a – guión 1

Texto de la Comisión	*Enmienda*
– el formato y los procedimientos de recopilación e intercambio de información compatible y comparable sobre riesgos e incidentes por parte de las ***autoridades competentes***,	– el formato y los procedimientos de recopilación e intercambio de información compatible y comparable sobre riesgos e incidentes por parte de las ***ventanillas únicas***,

Enmienda 81

Propuesta de Directiva
Artículo 12 – apartado 3

Texto de la Comisión	*Enmienda*
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.	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. ***Los resultados de cada revisión deberán notificarse al Parlamento Europeo.***

Enmienda 82

Propuesta de Directiva
Artículo 12 - apartado 3 bis (nuevo)

Texto de la Comisión	*Enmienda*
	3 bis. La Comisión dotará al plan de cooperación de la Unión en materia de SRI de un presupuesto para su desarrollo.

Enmienda 83

Propuesta de Directiva
Artículo 13 – párrafo 1

Texto de la Comisión	*Enmienda*
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.	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 ***los*** acuerdos ***se especificará el procedimiento de control que deberá realizarse para garantizar*** la protección ***de*** los datos personales que circulen en la red de cooperación. ***El Parlamento Europeo será informado de la negociación del acuerdo y se garantizará la transparencia del contenido del mismo. Toda transferencia de datos de carácter personal a destinatarios de países de fuera de la Unión se llevará a cabo con arreglo a los artículos 25 y 26 de la Directiva 95/46/CE, y al artículo 9 del Reglamento (CE) nº 45/2001.***

Justificación

Los acuerdos internacionales celebrados con otros países o agencias de seguridad deben contemplar obligatoriamente un mecanismo de control del respeto de los derechos civiles. Debe además ejercerse un control democrático efectivo de los acuerdos por parte del Parlamento Europeo, que deberá ser informado en tiempo debido sobre el contenido de las negociaciones del acuerdo.

Enmienda 84

Propuesta de Directiva
Artículo 14

Texto de la Comisión	*Enmienda*
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.	1. Los Estados miembros velarán por que los operadores del mercado tomen las medidas técnicas y de organización apropiadas para ***detectar y*** gestionar ***eficazmente*** los riesgos existentes para la seguridad de las redes y los sistemas de información que controlan y utilizan en sus operaciones. Habida cuenta del ***desarrollo tecnológico***, dichas medidas ***adecuadas*** garantizarán un nivel de seguridad adecuado en relación con el riesgo existente. En particular, adoptarán medidas para prevenir y reducir al mínimo los incidentes que afecten a ***la seguridad de*** 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.	2. Los Estados miembros ***introducirán mecanismos para garantizar*** que los operadores del mercado notifiquen ***sin demoras injustificadas*** a la autoridad competente ***o a la ventanilla única*** los incidentes que tengan efectos significativos en la seguridad ***o la continuidad*** de los servicios básicos que prestan. ***La notificación no expondrá a la parte que notifica a una mayor responsabilidad. A fin de determinar la magnitud del impacto de un incidente, se tendrán en cuenta, entre otros, los siguientes parámetros:*** ***a) el número de usuarios cuyo servicio básico se ve afectado;*** ***b) la duración del incidente;*** ***c) la extensión geográfica con respecto a la zona afectada por el incidente.*** ***Estos criterios se detallarán conforme al***

artículo 8, apartado 3, letra c bis) (nueva).

2 bis. Las entidades no contempladas en el anexo II podrán notificar incidentes con arreglo al artículo 14, apartado 2, de forma voluntaria.

2 ter. El destinatario de una notificación de incidentes comunicará lo antes posible a la entidad que notificó el incidente las medidas tomadas o las decisiones o recomendaciones adoptadas, así como las de cualquier tercero al que se haya informado, y los protocolos de seguridad y confidencialidad que regulan el intercambio de información.

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.

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. ***Los operadores del mercado que no presten servicios en la Unión Europea podrán notificar incidentes de forma voluntaria.***

3 bis. Los Estados miembros velarán por que los operadores del mercado notifiquen los incidentes contemplados en los apartados 1 y 2 a la autoridad competente o a la ventanilla única del Estado miembro donde se haya visto afectado el servicio básico. Si se han visto afectados servicios básicos en más de un Estado miembro, la ventanilla única que reciba la notificación alertará, basándose en la información proporcionada por el operador del mercado, a las demás ventanillas únicas afectadas. El operador del mercado será informado lo antes posible de qué otras ventanillas únicas han sido informadas del incidente, así como de las medidas adoptadas, los resultados o cualquier información relacionada con el incidente.

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***.

4. ***Tras consultar con*** la autoridad competente ***y con el operador del mercado de que se trate, la ventanilla única informará*** a los ciudadanos ***acerca de incidentes individuales si establece que la concienciación pública es necesaria para***

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.

evitar un incidente o tratar con un incidente en curso, para que los ciudadanos puedan paliar los riesgos que ellos mismos corren a causa del incidente o si el operador del mercado, afectado por un incidente, ha rehusado solucionar sin demoras injustificadas una vulnerabilidad estructural grave relacionada con dicho incidente. La ventanilla única justificará debidamente esta decisión. La autoridad competente o la ventanilla única presentarán, si es razonablemente posible, a las administraciones públicas o a los operadores del mercado que hayan informado del incidente información estratégica analizada que ayude a superar la amenaza de seguridad. Dos veces al año, la ***ventanilla única*** presentará a la red de cooperación un informe resumido sobre las notificaciones recibidas y las medidas adoptadas de acuerdo con el presente apartado. ***En la publicidad de incidentes determinados notificados a las autoridades competentes y a las ventanillas únicas es preciso ponderar debidamente el interés de los ciudadanos en ser informados sobre amenazas con los perjuicios comerciales y para su reputación que pueden sufrir los operadores del mercado que han notificado los incidentes, y dicha publicidad solamente podrá tener lugar con consultas previas.***

En el caso de los incidentes notificados a la red de cooperación mencionada en el artículo 8, otras autoridades nacionales competentes no publicarán ninguna información recibida sobre riesgos o incidentes sin la aprobación de la autoridad competente que los haya notificado.

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.	6. Las autoridades competentes ***o las ventanillas únicas adoptarán*** directrices sobre las circunstancias en que 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.	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[35].	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[35].
[35] DO L 124 de 20.5.2003, p. 36.	[35] DO L 124 de 20.5.2003, p. 36.

Enmienda 85

Propuesta de Directiva
Artículo 14 – apartado 4 – párrafo 1 (nuevo)

Texto de la Comisión	*Enmienda*
	Además de notificar a la autoridad competente, se recomendará a los operadores del mercado que anuncien los incidentes que impliquen a su corporación en sus informes financieros de forma voluntaria.

Justificación

Los incidentes cibernéticos podrían conllevar pérdidas financieras y costes sustanciales. Las partes interesadas y los inversores deberían estar informados de las consecuencias de estos

incidentes. Alentando a las empresas a publicar los incidentes cibernéticos de forma voluntaria se podría impulsar el debate intersectorial sobre la probabilidad de futuros incidentes, la dimensión de esos riesgos y la pertinencia de que se adopten medidas preventivas para reducir las vulneraciones de la ciberseguridad.

Enmienda 86

Propuesta de Directiva
Artículo 15

Texto de la Comisión	*Enmienda*
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.	1. Los Estados miembros velarán por que las autoridades competentes ***y las ventanillas únicas*** dispongan de las competencias necesarias para ***garantizar el cumplimiento*** de las obligaciones que 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***:	2. Los Estados miembros velarán por que las autoridades competentes y las ventanillas únicas estén facultadas para exigir a los operadores del mercado:
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;	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.	b) que ***ofrezcan pruebas de la aplicación eficaz de las políticas de seguridad, como los resultados de*** una auditoría de seguridad practicada por auditores internos, un organismo independiente o una autoridad nacional cualificados y pongan ***dichas pruebas*** en conocimiento de la autoridad competente ***o de la ventanilla única***. ***Cuando sea necesario, la autoridad competente o la ventanilla única podrán exigir pruebas adicionales o, de forma excepcional y justificándolo debidamente, llevar a cabo una auditoría adicional.***
	Si se envía dicha petición, las autoridades

	competentes y las ventanillas únicas establecerán el objetivo de dicha petición y especificarán de modo suficiente la información necesaria.
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***.	3. Los Estados miembros velarán por que las autoridades competentes ***y las ventanillas únicas*** estén facultadas para impartir instrucciones vinculantes a ***todos*** los operadores del mercado ***que figuran en el anexo II***.
4. Las autoridades competentes ***notificarán los*** incidentes de carácter grave y supuestamente delictivo ***a los cuerpos de seguridad***.	4. Las autoridades competentes ***y la ventanilla única informarán a los operadores del mercado interesados de la posibilidad de iniciar acciones penales ante los cuerpos de seguridad en caso de*** incidentes de carácter grave y supuestamente delictivo.
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.	5. ***Sin perjuicio de la legislación aplicable sobre protección de datos,*** las autoridades competentes ***y las ventanillas únicas*** 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. ***Las ventanillas únicas y las autoridades responsables de la protección de datos elaborarán, en cooperación con la ENISA, mecanismos de intercambio de información y un modelo único que se utilizará para las notificaciones en virtud del artículo 14, apartado 2, de la presente Directiva, y de la Directiva 95/46/CE del Parlamento Europeo y del Consejo 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.***
	La Comisión podrá adoptar, mediante actos de ejecución y teniendo en cuenta en la mayor medida posible todos los mecanismos de intercambio de información y el modelo único de notificación desarrollados por las ventanillas únicas y las autoridades responsables de la protección de datos, en

	colaboración con la ENISA, procedimientos para los mecanismos de intercambio de información y el modelo único de notificación.
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.	6. Los Estados miembros garantizarán que cualesquiera obligaciones impuestas a los operadores del mercado en virtud del presente capítulo puedan estar sujetas a control judicial.

Enmienda 87

Propuesta de Directiva
Artículo 16

Texto de la Comisión	*Enmienda*
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.	1. A fin de garantizar una aplicación convergente de lo dispuesto en el artículo 14, apartado 1, los Estados miembros***, sin prescribir el empleo de ninguna tecnología en particular,*** fomentarán la utilización de las normas y especificaciones ***internacionales abiertas e interoperables que resulten pertinentes*** en materia de seguridad de las redes y la información***, de conformidad con la legislación de la UE***.
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.	2. La Comisión ***conferirá a un organismo europeo de normalización pertinente el mandato de elaborar, en consulta con las partes interesadas pertinentes,*** una lista de las normas ***y/o especificaciones*** mencionadas en el apartado 1. Dicha lista se publicará en el Diario Oficial de la Unión Europea.

Enmienda 88

Propuesta de Directiva
Artículo 17 – apartado 1

Texto de la Comisión	*Enmienda*
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.	1. Los Estados miembros establecerán normas sobre las sanciones aplicables a las infracciones ***negligentes e intencionadas*** 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.

Justificación

Conviene aclarar que las sanciones solo se pueden aplicar a infracciones en las que los operadores del mercado no adopten todas las medidas que cabría esperar de ellos. De lo contrario, se disuadiría a los operadores del mercado de notificar los incidentes.

Enmienda 89

Propuesta de Directiva
Artículo 17 - apartado 1 bis (nuevo)

Texto de la Comisión	*Enmienda*
	1 bis. Los Estados miembros garantizarán que las sanciones contempladas en el apartado 1 del presente artículo únicamente se aplicarán cuando el operador del mercado no haya cumplido sus obligaciones con arreglo al capítulo IV de forma deliberada o por negligencia grave.

Enmienda 90

Propuesta de Directiva
Artículo 18

Texto de la Comisión	*Enmienda*
Artículo 18	***suprimido***
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 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.

Enmienda 91

Propuesta de Directiva
Artículo 20 – párrafo 1

Texto de la Comisión	*Enmienda*
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.	La Comisión revisará ***cada tres años*** el funcionamiento de la presente Directiva e informará al Parlamento Europeo y al Consejo. El primer informe se presentará a más tardar ***dos*** 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.

Justificación

Para mantenerse al corriente de las cambiantes amenazas y condiciones en el ámbito de la ciberseguridad, el anexo II se revisará y editará de forma periódica.

Enmienda 92

Propuesta de Directiva
Anexo I – epígrafe 1

Texto de la Comisión	*Enmienda*
Obligaciones y tareas ***del equipo*** de respuesta a emergencias informáticas (CERT)	Obligaciones y tareas ***de los equipos*** de respuesta a emergencias informáticas (CERT)

Enmienda 93

Propuesta de Directiva
Anexo I – párrafo 1 – parte introductoria

Texto de la Comisión	*Enmienda*
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:	Las obligaciones y tareas ***de los*** CERT estarán adecuada y claramente definidas y se basarán en la política o la reglamentación nacional. Incluirán los siguientes elementos: *(Esta modificación se aplica a la totalidad del texto del anexo I.)*

Enmienda 94

Propuesta de Directiva
Anexo I – párrafo 1 – punto 1 – letra a

Texto de la Comisión	*Enmienda*
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.	a) ***Los*** CERT garantizarán una gran disponibilidad de sus servicios de comunicaciones evitando los fallos puntuales simples y contarán con varios medios para ser contactados y contactar con otros ***en todo momento***. Además, los canales de comunicación estarán claramente especificados y serán bien conocidos por los grupos de usuarios y los socios colaboradores.

Enmienda 95

Propuesta de Directiva
Anexo I – párrafo 1 – punto 1 – letra c

Texto de la Comisión	*Enmienda*
c) Las dependencias ***del*** CERT y los sistemas de información de apoyo estarán situados en lugares seguros.	c) Las dependencias ***de los*** CERT y los sistemas de información de apoyo estarán situados en lugares seguros ***con redes y sistemas de información protegidos***.

Enmienda 96

Propuesta de Directiva
Anexo I – párrafo 1 – punto 2 – letra a – guión 1

Texto de la Comisión	*Enmienda*
– Supervisar incidentes a escala nacional.	– ***Detectar y*** supervisar incidentes a escala nacional.

Enmienda 97

Propuesta de Directiva
Anexo I – párrafo 1 – punto 2 – letra a – guión 5 bis (nuevo)

Texto de la Comisión	*Enmienda*
	- Participar activamente en las redes de cooperación entre CERT internacionales y de la Unión.

Enmienda 98

Propuesta de Directiva
Anexo II

Texto de la Comisión	*Enmienda*
Lista de operadores del mercado	Lista de operadores del mercado
1. Energía:	1. Energía:
	a) Electricidad
	- Proveedores
	- Gestores de redes de distribución y minoristas para consumidores finales
	- Gestores de redes de transporte de electricidad
	- Operadores de los mercados de la electricidad
	b) Petróleo

	- Oleoductos de transporte de crudo y almacenamiento de crudo.
	- Operadores de producción de crudo, instalaciones de refinado y tratamiento, almacenamiento y transporte
	c) Gas
	- Proveedores
	- Gestores de redes de distribución y minoristas para consumidores finales
	- Gestores de redes de transporte de gas natural, gestores de redes de almacenamiento y gestores de redes GNL
	- Operadores de producción de gas natural, instalaciones de refinado y tratamiento, almacenamiento y transporte
	- Operadores de los mercados de gas
2. Transportes:	2. Transportes:
	a) Transporte por carretera
	i) Operadores de control de la gestión del tráfico.
	ii) Servicios logísticos auxiliares:
	- depósito y almacenamiento,
	- manipulación de la carga, y
	- otras actividades auxiliares del transporte.
	b) Transporte por ferrocarril
	i) Compañías ferroviarias (gestores de infraestructuras, compañías integradas y operadores de transporte ferroviario).
	ii) Operadores de control de la gestión del tráfico.
	iii) Servicios logísticos auxiliares:
	- depósito y almacenamiento,
	- manipulación de la carga, y
	- otras actividades auxiliares del transporte.
	c) Transporte aéreo

	i) Compañías aéreas (transporte aéreo de mercancías y pasajeros).
	ii) Aeropuertos.
	iii) Operadores de control de la gestión del tráfico
	iv) Servicios logísticos auxiliares:
	- depósito,
	- manipulación de la carga, y
	- otras actividades auxiliares del transporte.
	d) Transporte marítimo
	i) Compañías de transporte marítimo (empresas de transporte terrestre, marítimo y de cabotaje de pasajeros y empresas de transporte terrestre, marítimo y de cabotaje de mercancías)
	ii) Puertos.
	iii) Operadores de control de la gestión del tráfico
	iv) Servicios logísticos auxiliares:
	- depósito y almacenamiento,
	- manipulación de la carga, y
	- otras actividades auxiliares del transporte.
	2 bis. Servicios hídricos
3. Banca: entidades de crédito con arreglo a la definición del artículo 4, número 1, de la Directiva 2006/48/CE.	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.	4. Infraestructuras de los mercados financieros: ***mercados regulados, sistemas multilaterales de negociación, sistemas organizados de negociación, pasarelas de pago por Internet*** 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.	5. Sector sanitario: entornos de asistencia sanitaria (entre ellos hospitales y clínicas privadas) y otras entidades que prestan asistencia sanitaria.
	6. TIC: Servicios de computación en nube utilizados por los operadores para prestar

los servicios enumerados en los puntos 1 a 5.

La presente lista será revisada cada dos años.

PROCEDIMIENTO

Título	Medidas para garantizar un elevado nivel común de seguridad de las redes y de la información en la Unión
Referencias	COM(2013)0048 – C7-0035/2013 – 2013/0027(COD)
Comisión competente para el fondo Fecha del anuncio en el Pleno	IMCO 15.4.2013
Opinión emitida por Fecha del anuncio en el Pleno	ITRE 15.4.2013
Comisión(es) asociada(s) - fecha del anuncio en el pleno	12.9.2013
Ponente de opinión Fecha de designación	Pilar del Castillo Vera 23.5.2013
Examen en comisión	14.10.2013 4.11.2013
Fecha de aprobación	16.12.2013
Resultado de la votación final	+: 36 –: 5 0: 0
Miembros presentes en la votación final	Amelia Andersdotter, Josefa Andrés Barea, Bendt Bendtsen, Fabrizio Bertot, Reinhard Bütikofer, Maria Da Graça Carvalho, Giles Chichester, Pilar del Castillo Vera, Christian Ehler, Vicky Ford, Adam Gierek, Norbert Glante, Robert Goebbels, Fiona Hall, Romana Jordan, Philippe Lamberts, Marisa Matias, Judith A. Merkies, Angelika Niebler, Jaroslav Paška, Vittorio Prodi, Miloslav Ransdorf, Herbert Reul, Teresa Riera Madurell, Paul Rübig, Amalia Sartori, Salvador Sedó i Alabart, Evžen Tošenovský, Claude Turmes, Marita Ulvskog, Vladimir Urutchev
Suplente(s) presente(s) en la votación final	Daniel Caspary, António Fernando Correia de Campos, Françoise Grossetête, Roger Helmer, Jolanta Emilia Hibner, Seán Kelly, Eija-Riitta Korhola, Holger Krahmer, Zofija Mazej Kukovič, Silvia-Adriana Ţicău, Lambert van Nistelrooij
Suplente(s) (art. 187, apdo. 2) presente(s) en la votación final	María Auxiliadora Correa Zamora

15.1.2014

OPINIÓN DE LA COMISIÓN DE LIBERTADES CIVILES, JUSTICIA Y ASUNTOS DE INTERIOR

para la Comisión de Mercado Interior y Protección del Consumidor

sobre la 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)0048 – C7-0035/2013 – 2013/0027(COD))

Ponente de opinión (*): Carl Schlyter

(*) Procedimiento de comisiones asociadas – artículo 50 del Reglamento

BREVE JUSTIFICACIÓN

El objetivo de la propuesta es garantizar un elevado nivel común de seguridad de las redes y de la información. El ponente apoya los objetivos de la propuesta, recomendando enmiendas que mejorarán la seguridad jurídica y reforzarán las salvaguardias y protecciones de los ciudadanos y de su intimidad para garantizar que estos asuman el control de sus datos personales y confíen en el entorno digital, y para crear una cultura de gestión del riesgo y de mejora de la información compartida entre los sectores privado y público.

Las enmiendas propuestas se refieren al refuerzo de la referencia a la legislación sobre protección de datos, aclarando que «las infraestructuras críticas» no deben incluir las redes sociales ni las tiendas de aplicaciones (véase la lista del anexo II modificada) y asegurándose de que se respete la proporcionalidad subrayando el aspecto civil de la empresa: la mayor parte de los problemas y causas comunes de los fallos sistémicos no son ataques cibernéticos intencionales causados por terroristas, delincuentes o espías extranjeros, sino errores humanos y causas naturales no premeditados. Es de suma importancia que la UE distinga entre la aplicación de la legislación propuesta y cualquier militarización del asunto, excluyendo los objetivos de seguridad y vigilancia de la industria, teniendo en cuenta el contexto de un mercado digital globalizado.

Siguen constituyendo un importante motivo de preocupación la relación entre el sistema propuesto y el sistema de notificación propuesto con arreglo al Reglamento general sobre protección de datos, y su coexistencia efectiva, que es una de las razones que destacan el hecho de que toda legislación de la UE en materia de seguridad cibernética debe seguir a la aprobación del Reglamento general sobre protección de datos y no precederla. Además, deben tenerse en cuenta las verdaderas implicaciones financieras y administrativas, incluidos los costes sociales totales y no solo los costes de una notificación. Las empresas de programas informáticos que elaboran programas descuidados para ahorrar dinero, exponiendo así a sus clientes a riesgos, no pueden estar protegidas en todos los casos por la norma que figura en las

condiciones de uso y que excluye su responsabilidad en caso de funcionamiento defectuoso de sus programas. Hay que incentivarlas para asegurarse de que sus programas son razonablemente seguros. Por último deben aclararse conceptos fundamentales para no dejarlos a la libre interpretación de los Estados miembros (como el significado de «administraciones públicas» y de «efecto significativo» y una definición concreta de «ciberdelincuencia»).

ENMIENDAS

La Comisión de Libertades Civiles, Justicia y Asuntos de Interior pide a la Comisión de Mercado Interior y Protección del Consumidor, competente para el fondo, que incorpore en su informe las siguientes enmiendas:

Enmienda 1

Propuesta de Directiva
Considerando 1

Texto de la Comisión	*Enmienda*
(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***.	(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, el bienestar social y ***las comunicaciones y los intercambios entre personas***, ***organizaciones de la sociedad civil y empresas, así como para la protección y el respeto de la intimidad y los datos personales***.

Enmienda 2

Propuesta de Directiva
Considerando 2

Texto de la Comisión	*Enmienda*
(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	(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.

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. ***Se reconoce cada vez más que los sistemas de control son vulnerables a los ataques cibernéticos procedentes de numerosas fuentes, incluidos gobiernos hostiles, grupos terroristas y otros intrusos malintencionados. Los ataques inteligentes y los ataques coordinados podrían tener graves repercusiones para la estabilidad, el rendimiento y los aspectos económicos de la infraestructura.***

Enmienda 3

Propuesta de Directiva
Considerando 3

Texto de la Comisión	*Enmienda*
(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.	(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 ***y para las comunicaciones y los intercambios entre personas, organizaciones de la sociedad civil y empresas***.

Enmienda 4

Propuesta de Directiva
Considerando 3 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(3 bis) Puesto que las causas más comunes de los fallos sistémicos siguen siendo involuntarias, como las causas naturales o los errores humanos, las infraestructuras deben poder resistir tanto a perturbaciones intencionales como no intencionales, y los operadores de infraestructuras críticas deben diseñar sistemas basados en la resistencia que sean operativos incluso cuando fallen otros sistemas que estén fuera de su control.

Enmienda 5

Propuesta de Directiva
Considerando 6 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(6 bis) Es vital reconocer la incertidumbre inherente a los complejos sistemas que nos mantienen. Ello exige una mejor comprensión común de lo que es crítico, entre quienes protegen una organización y quienes fijan su dirección estratégica.

Enmienda 6

Propuesta de Directiva
Considerando 8

Texto de la Comisión	*Enmienda*
(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	(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.	seguridad, salvaguardar el orden público y la seguridad pública, y permitir la investigación, detección y represión de delitos***, a condición de que ello no les sirva de pretexto para no cumplir sus obligaciones más generales en materia de respeto de la protección de la intimidad y los datos personales***. 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.

Enmienda 7

Propuesta de Directiva
Considerando 9

Texto de la Comisión	*Enmienda*
(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.	(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***, respetando y protegiendo la intimidad y los datos personales***.

Enmienda 8

Propuesta de Directiva
Considerando 10

Texto de la Comisión	*Enmienda*
(10) Con miras a una aplicación efectiva de	(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.	las disposiciones adoptadas de conformidad con la presente Directiva, procede crear o designar en cada uno de los Estados miembros ***una autoridad nacional competente bajo control civil con pleno control democrático y transparencia en sus operaciones*** 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.

Enmienda 9

Propuesta de Directiva
Considerando 14 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(14 bis) Aumenta el número de sectores que adoptan servicios en la nube en su entorno informático, como los servicios informáticos que utilizan infraestructuras críticas. Hay que prever medidas de seguridad suficientes para garantizar la confidencialidad, la integridad y la disponibilidad de los datos en la nube. El alojamiento de servicios de infraestructuras y el almacenamiento de datos sensibles en la nube implican requisitos de seguridad y resistencia que los actuales servicios en la nube no pueden abordar. Por ello, es necesaria una garantía de que el entorno de computación en nube pueda ofrecer una protección completa de los datos sobre infraestructuras críticas sensibles.

Enmienda 10

Propuesta de Directiva
Considerando 15

Texto de la Comisión	*Enmienda*
(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.	(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 ***mutuamente*** información y mejores prácticas ***así como*** apoyo operativo ***recíproco cuando sea necesario*** en caso de que se produzcan incidentes.

Enmienda 11

Propuesta de Directiva
Considerando 15 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(15 bis) Los actuales mecanismos nacionales de cooperación entre operadores privados y públicos deben respetarse plenamente, en la medida de lo posible y de conformidad con la Directiva 95/46/CE, y las disposiciones estipuladas en la presente Directiva no deben socavar este tipo de acuerdos de cooperación establecidos.

Enmienda 12

Propuesta de Directiva
Considerando 16

Texto de la Comisión	*Enmienda*
(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.	(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 ***rápidamente*** información no confidencial ***integral*** sobre incidentes y riesgos.

Enmienda 13

Propuesta de Directiva
Considerando 21

Texto de la Comisión	*Enmienda*
(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.	(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***, a condición de que los Estados con los que se prevé esta cooperación estén dotados de instrumentos de control y de protección de datos que garanticen la misma seguridad que los de la UE***.

Enmienda 14

Propuesta de Directiva
Considerando 22

Texto de la Comisión	*Enmienda*
(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	(22) La responsabilidad de velar por la SRI recae en gran medida en las administraciones públicas y ***las empresas***. Debe fomentarse una cultura de gestión de riesgos que entrañe una evaluación del riesgo y la aplicación de medidas de seguridad ***dirigidas a prever los incidentes de seguridad, ya sean deliberados o***

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.

accidentales, y que habrá de desarrollarse a través de requisitos reglamentarios adecuados y prácticas voluntarias del sector. ***Si ya existe tal cultura de gestión de riesgos y, en particular, si se basa en prácticas voluntarias, debe apoyarse, reforzarse y compartirse.*** 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.

Enmienda 15

Propuesta de Directiva
Considerando 22 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(22 bis) Las administraciones públicas y las empresas privadas, incluidos los proveedores de servicios de redes y de información y programas, deben considerar la protección de sus sistemas de información y de los datos que contengan como parte de su obligación de diligencia. Es menester garantizar niveles adaptados de protección frente a amenazas y sectores vulnerables razonablemente identificables. Los costes y las cargas de esa protección deben reflejar el posible riesgo de ciberataque para los afectados.

Enmienda 16

Propuesta de Directiva
Considerando 26 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(26 bis) Los niños están expuestos a Internet y otras tecnologías modernas, así como a las amenazas que proceden de ellas, desde muy jóvenes. Una buena

	gestión de un espacio en línea favorable a los niños es crucial para mitigar los daños y garantizar que no se comprometan la protección de los niños y sus derechos.

Enmienda 17

Propuesta de Directiva
Considerando 28

Texto de la Comisión	*Enmienda*
(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***.	(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. ***En la publicidad de*** los incidentes notificados a las autoridades competentes ***debe darse prioridad, por encima de las consideraciones económicas a corto plazo, al*** interés de los ciudadanos en ser informados sobre las amenazas existentes.

Enmienda 18

Propuesta de Directiva
Considerando 29 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(29 bis) Un uso fraudulento de Internet permite a la delincuencia organizada ampliar sus actividades en línea para el blanqueo de dinero, la falsificación y

	otros productos y servicios que violan los derechos de propiedad intelectual, así como para experimentar con nuevas actividades criminales, lo que refleja una temible habilidad para adaptarse a las tecnologías modernas.

Enmienda 19

Propuesta de Directiva
Considerando 30 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(30 bis) La delincuencia informática causa daños económicos y sociales cada vez mayores, afecta a millones de consumidores y provoca pérdidas anuales estimadas en 290 000 millones de euros[1].
	[4a] Informe Norton sobre ciberdelincuencia 2012.

Enmienda 20

Propuesta de Directiva
Considerando 33

Texto de la Comisión	*Enmienda*
(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.	(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 ***y de las obligaciones relativas al máximo nivel de seguridad e integridad de las redes y de la información y protección de la intimidad y los datos personales***.

Enmienda 21

Propuesta de Directiva
Considerando 39

Texto de la Comisión	*Enmienda*
(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.	(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. ***Si*** dicho tratamiento es necesario para alcanzar los objetivos de interés público perseguidos por la presente Directiva***, puede ser*** legítimo en virtud del artículo 7 de la Directiva 95/46/CE. No ***exime, sin embargo, a las autoridades competentes de la obligación de*** una intervención ***proporcional que no atente contra el*** 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.
[31] DO L 145 de 31.5.2001, p. 43.	[31] DO L 145 de 31.5.2001, p. 43.

Enmienda 22

Propuesta de Directiva
Considerando 41 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(41 bis) En todas las medidas debe asegurarse una protección de los derechos humanos fundamentales, en especial, de los mencionados en el Convenio Europeo de Derechos Humanos (artículo 8, respeto de la vida privada), y debe respetarse el principio de proporcionalidad.

Enmienda 23

Propuesta de Directiva
Artículo 1 – apartado 5

Texto de la Comisión	*Enmienda*
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, ***de*** 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, 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.	5. La presente Directiva ***respetará totalmente*** 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, 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, y ***el*** Reglamento ***(CE) n° 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 ***órganos de la UE y*** a la libre circulación de estos datos.

Enmienda 24

Propuesta de Directiva
Artículo 2

Texto de la Comisión	*Enmienda*
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.	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***, pero dichas disposiciones deben cumplir las expectativas mínimas comunes aplicables en este caso, consagradas en la presente Directiva***.

Enmienda 25

Propuesta de Directiva
Artículo 3 – punto 2

Texto de la Comisión	*Enmienda*
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;	***(***2***)*** «seguridad»: la capacidad de las redes y sistemas de información de resistir 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;

Enmienda 26

Propuesta de Directiva
Artículo 3 – apartado 2 – letra a (nueva)

Texto de la Comisión	*Enmienda*
	«resistencia cibernética»: la capacidad de una red y de un sistema de información de resistir y recuperar toda su capacidad operativa después de un incidente, debido entre otras cosas a: averías técnicas, cortes de energía o incidentes de seguridad;

Enmienda 27

Propuesta de Directiva
Artículo 3 – apartado 4

Texto de la Comisión	*Enmienda*
«incidente»: toda circunstancia o hecho que tenga efectos adversos en la seguridad;	«incidente»: toda circunstancia o hecho que tenga efectos adversos en la seguridad ***y la prestación de servicios fundamentales***;

Enmienda 28

Propuesta de Directiva
Artículo 3 – punto 8 – letra b

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

Enmienda 29

Propuesta de Directiva
Artículo 5 – apartado 2 – letra a

Texto de la Comisión	*Enmienda*
a) ***Plan de*** evaluación de riesgos que permita determinarlos y evaluar los efectos de incidentes potenciales.	a) ***Marco de gestión de riesgos con, al menos, una*** evaluación ***regular*** de riesgos que permita determinarlos y evaluar los efectos de incidentes potenciales***, y medidas de salvaguardia de la seguridad y la integridad de la información, incluida una alerta rápida***.

Justificación

Un plan de evaluación no es suficiente y no incluye otras medidas necesarias para la gestión de riesgos en materia de seguridad de las redes y de la información. El SEPD recomienda que se establezca un marco de gestión de riesgos, lo que implica una evaluación de los riesgos.

Enmienda 30

Propuesta de Directiva
Artículo 5 – apartado 3

Texto de la Comisión	*Enmienda*
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.	3. La estrategia nacional de SRI y el plan de cooperación nacional en materia de SRI se deberán remitir a la Comisión***, el Parlamento Europeo, el Consejo y el Supervisor Europeo de Protección de Datos*** en el plazo de un mes a partir de su adopción ***y no más tarde de 12 meses después de la entrada en vigor de la presente Directiva***.

Enmienda 31

Propuesta de Directiva
Artículo 5 – apartado 3 bis (nuevo)

Texto de la Comisión	*Enmienda*
	3 bis. La Comisión elaborará un resumen con las estrategias de SRI de todos los Estados miembros y lo remitirá a los mismos de forma organizada.

Justificación

Es conveniente que los Estados miembros puedan consultar también los planes del resto de Estados. Esto les ayudará a determinar sus planteamientos e incluso podrían surgir oportunidades para un intercambio de mejores prácticas.

Enmienda 32

Propuesta de Directiva

Artículo 5 - apartado 3 ter (nuevo)

Texto de la Comisión	*Enmienda*
	3 ter. En un plazo de seis meses tras la aprobación de la presente Directiva, la Comisión confeccionará una guía relativa a la estructura de la estrategia de SRI. Tendrá por finalidad ayudar a los Estados miembros a elaborar y aprobar documentos que tengan aproximadamente la misma estructura.

Justificación

La labor de organización y resumen a escala comunitaria sería más efectiva si los veintiocho documentos en los que se basa cumpliesen una cierta estructura general. Aunque la guía de la Comisión no fuera vinculante, aun así induciría a los Estados miembros a cumplir con esta estructura o modelo recomendado a la hora de elaborar sus propias estrategias nacionales.

Enmienda 33

Propuesta de Directiva
Artículo 6 – apartado 1

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

Enmienda 34

Propuesta de Directiva
Artículo 6 – apartado 5

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

en cuenta el principio de proporcionalidad.

Enmienda 35

Propuesta de Directiva
Artículo 6 – apartado 5 (nuevo)

Texto de la Comisión	*Enmienda*
	5. Las autoridades competentes cumplirán, en relación con la información recogida, procesada e intercambiada, los requisitos relativos a la protección de los datos personales tal como se establecen en el artículo 17 de la Directiva 95/46/CE.

Enmienda 36

Propuesta de Directiva
Artículo 7 – apartado 1

Texto de la Comisión	*Enmienda*
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.	1. Cada Estado miembro creará ***equipos*** 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. ***Si procede, se creará*** un CERT en el marco de la autoridad competente.

Enmienda 37

Propuesta de Directiva
Artículo 8 – apartado 2

Texto de la Comisión	*Enmienda*
2. La Comisión y las autoridades competentes mantendrán una comunicación constante en el marco de la	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***.	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 ***orientación tecnológica neutra con medidas adecuadas tanto para el sector público como para el privado***.

Enmienda 38

Propuesta de Directiva
Artículo 9 – apartado 2 - letra b bis (nueva)

Texto de la Comisión	*Enmienda*
	b bis) los criterios de participación de los Estados miembros en el sistema para compartir información segura para garantizar en todos los participantes un elevado nivel de seguridad y resistencia en todas las fases del proceso, incluso mediante medidas apropiadas de confidencialidad y seguridad de conformidad con los artículos 16 y 17 de la Directiva 95/46/CE y los artículos 21 y 22 del Reglamento (CE) n° 45/2001.

Enmienda 39

Propuesta de Directiva
Artículo 9 – apartado 3

Texto de la Comisión	*Enmienda*
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.	***suprimido***

Enmienda 40

Propuesta de Directiva
Artículo 12 – apartado 2 – letra a – guión 2

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

Enmienda 41

Propuesta de Directiva
Artículo 13

Texto de la Comisión	*Enmienda*
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.	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. Tales acuerdos ***solo*** se ***concluirán si puede garantizarse un nivel de*** protección ***de*** los datos personales que circulen en la red de cooperación ***adecuado y comparable al de la Unión***.

Enmienda 42

Propuesta de Directiva
Artículo 14 –apartado 1

Texto de la Comisión	*Enmienda*
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	1. Los Estados miembros velarán por que las administraciones públicas y los operadores del mercado tomen las medidas técnicas y de organización apropiadas para ***detectar,*** gestionar ***eficazmente y limitar*** los riesgos existentes para la seguridad de las redes y los sistemas de información que

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.	controlan y utilizan en sus operaciones. Habida cuenta del estado de la técnica, dichas medidas garantizarán un nivel de seguridad adecuado ***y proporcional*** 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 ***y la seguridad de los datos*** que dependen de tales redes y sistemas de información.

Enmienda 43

Propuesta de Directiva
Artículo 14 – apartado 2 – letra a (nueva)

	Enmienda
	a) Los fabricantes de programas informáticos comerciales serán considerados responsables a pesar de las cláusulas de exención de responsabilidad del acuerdo con el usuario en caso de grave negligencia en relación con la seguridad.

Justificación

En el acuerdo de licencia, los fabricantes de programas informáticos comerciales se eximen de toda responsabilidad que pueda surgir debido a un sistema deficiente en materia de seguridad y una programación inferior. Para fomentar que los fabricantes de programas informáticos inviertan en medidas de seguridad es necesaria una cultura diferente. Solo puede lograrse si los fabricantes de programas informáticos son considerados responsables de cualquier déficit en materia de seguridad.

Enmienda 44

Propuesta de Directiva
Artículo 14 – apartado 3

Texto de la Comisión	*Enmienda*
3. Los requisitos establecidos en los	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.	apartados 1 y 2 serán aplicables a todos los operadores del mercado ***y productores de programas informáticos*** que prestan servicios en la Unión Europea.

Enmienda 45

Propuesta de Directiva
Artículo 14 - apartado 6

Texto de la Comisión	*Enmienda*
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.	***suprimido***

Enmienda 46

Propuesta de Directiva
Artículo 15 – apartado 1

Texto de la Comisión	*Enmienda*
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.	1. Los Estados miembros velarán por que las autoridades competentes dispongan de 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.

Enmienda 47

Propuesta de Directiva
Artículo 15 – apartado 5

Texto de la Comisión	*Enmienda*
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.	5. ***Sin perjuicio de la legislación aplicable en materia de protección de datos, y en plena consulta con los correspondientes responsables del tratamiento de datos,*** las autoridades competentes ***y las ventanillas únicas*** 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.

Enmienda 48

Propuesta de Directiva
Artículo 19 bis (nuevo)

Texto de la Comisión	*Enmienda*
	Artículo 19 bis
	Tratamiento y protección de los datos personales
	1. El tratamiento de los datos personales en los Estados miembros con arreglo a la presente Directiva se llevará a cabo de conformidad con las Directivas 95/46/CE y 2002/58/CE.
	2. El tratamiento de los datos personales por la Comisión y ENISA con arreglo al presente Reglamento se llevará a cabo de conformidad con el Reglamento (CE) n° 45/2001.
	3. El tratamiento de los datos personales por el Centro Europeo de Ciberdelincuencia de Europol a efectos de la presente Directiva se llevará a cabo de conformidad con la Decisión 2009/371/JAI.
	4. El tratamiento de los datos personales será justo y legítimo y se limitará estrictamente a los datos mínimos necesarios para los efectos para los que se procesan. Deberán conservarse en una

	forma que permita la identificación de los interesados durante un periodo no superior al necesario para los fines para los que dichos datos personales son procesados.
	5. Las notificaciones de incidentes mencionadas en el artículo 14 se tramitarán sin perjuicio de las disposiciones y obligaciones en materia de notificación de violaciones de datos personales contempladas en el artículo 4 de la Directiva 2002/58/CE y en el Reglamento (UE) n° 611/2013.
	6. Las referencias a la Directiva 95/46/CE se interpretarán como referencias 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 (Reglamento general sobre protección de dato), una vez que entre en vigor.

Enmienda 49

Propuesta de Directiva
Artículo 20 – apartado 1

Texto de la Comisión	*Enmienda*
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.	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 ***dos*** 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.

Enmienda 50

Propuesta de Directiva
Anexo – apartado 1 – punto 1 – letra b

Texto de la Comisión	*Enmienda*
b) El CERT aplicará y gestionará medidas de seguridad para garantizar la confidencialidad, integridad, disponibilidad y autenticidad de la información que reciba y trate.	b) El CERT aplicará y gestionará medidas de seguridad para garantizar la confidencialidad, integridad, disponibilidad y autenticidad de la información que reciba y trate***, y garantizará la protección de datos***.

Enmienda 51

Propuesta de Directiva
Anexo 2 – apartado 1

Texto de la Comisión	*Enmienda*
Lista de operadores del mercado	Lista de operadores del mercado
Contemplados en el artículo 3, apartado 8, letra a)***:***	Contemplados en el artículo 3, apartado 8, letra a)
1. Plataformas de comercio electrónico.	1. Plataformas de comercio electrónico.
2. Pasarelas de pago por Internet.	2. Pasarelas de pago por Internet.
3. Redes sociales.	
4. Motores de búsqueda.	***3***. Motores de búsqueda.
5. Servicios de computación en nube.	***4***. Servicios de computación en nube ***que almacenen datos sobre infraestructuras críticas de la Unión Europea***.
6. Tiendas de aplicaciones.	

Enmienda 52

Propuesta de Directiva
Anexo 2 – apartado 2 – punto 5 bis (nuevo)

Texto de la Comisión	*Enmienda*
	5 bis. Cadena alimentaria

PROCEDIMIENTO

Título	Medidas para garantizar un elevado nivel común de seguridad de las redes y de la información en la Unión			
Referencias	COM(2013)0048 – C7-0035/2013 – 2013/0027(COD)			
Comisión competente para el fondo Fecha del anuncio en el Pleno	IMCO 15.4.2013			
Opinión emitida por Fecha del anuncio en el Pleno	LIBE 15.4.2013			
Comisión(es) asociada(s) - fecha del anuncio en el pleno	12.9.2013			
Ponente de opinión Fecha de designación	Carl Schlyter 7.3.2013			
Examen en comisión	25.4.2013	18.9.2013	4.11.2013	13.1.2014
Fecha de aprobación	13.1.2014			
Resultado de la votación final	+: –: 0:	36 6 0		
Miembros presentes en la votación final	Jan Philipp Albrecht, Roberta Angelilli, Edit Bauer, Rita Borsellino, Arkadiusz Tomasz Bratkowski, Philip Claeys, Frank Engel, Cornelia Ernst, Tanja Fajon, Monika Flašíková Beňová, Kinga Gál, Kinga Göncz, Salvatore Iacolino, Sophia in ‘t Veld, Timothy Kirkhope, Juan Fernando López Aguilar, Baroness Sarah Ludford, Monica Luisa Macovei, Svetoslav Hristov Malinov, Véronique Mathieu Houillon, Anthea McIntyre, Nuno Melo, Roberta Metsola, Claude Moraes, Jacek Protasiewicz, Carmen Romero López, Birgit Sippel, Csaba Sógor, Renate Sommer, Axel Voss, Renate Weber, Josef Weidenholzer, Cecilia Wikström, Tatjana Ždanoka, Auke Zijlstra			
Suplente(s) presente(s) en la votación final	Monika Hohlmeier, Jean Lambert, Ulrike Lunacek, Jan Mulder, Carl Schlyter, Marco Scurria			
Suplente(s) (art. 187, apdo. 2) presente(s) en la votación final	Katarína Neveďalová			

6.12.2013

OPINIÓN DE LA COMISIÓN DE ASUNTOS EXTERIORES

para la Comisión de Mercado Interior y Protección del Consumidor

sobre la 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)0048 – C7-0035/2013 – 2013/0027(COD))

Ponente de opinión: Ana Gomes

ENMIENDAS

La Comisión de Asuntos Exteriores pide a la Comisión de Mercado Interior y Protección del Consumidor, competente para el fondo, que incorpore en su informe las siguientes enmiendas:

Enmienda 1

Propuesta de Directiva
Considerando 1

Texto de la Comisión	*Enmienda*
(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.	(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***, así como para la seguridad exterior de la UE***.

Enmienda 2

Propuesta de Directiva
Considerando 2

Texto de la Comisión	*Enmienda*
(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.	(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 ***y, en última instancia, poner en peligro el bienestar de los ciudadanos de la UE y la capacidad de los Estados miembros de la UE de protegerse y garantizar la seguridad de infraestructuras críticas***.

Enmienda 3

Propuesta de Directiva
Considerando 2 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(2 bis) La cláusula de solidaridad, introducida en virtud del artículo 222 del TFUE, constituye el marco apropiado para la asistencia y la acción concertada entre los Estados miembros de la UE, en caso de un ataque terrorista o de actividad delictiva que ponga en peligro la seguridad de las redes y de la información. De igual modo, la cláusula de defensa mutua que establece el artículo 47, apartado 7, del TUE deberá constituir el marco de acción de la UE en el caso de que un Estado miembro fuera víctima de una agresión armada que afecte a la seguridad de las redes y la información. En los casos pertinentes, el artículo 222

	del TFUE y el artículo 42, apartado 7, del TUE se aplicarán de forma complementaria.

Enmienda 4

Propuesta de Directiva
Considerando 2 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(2 bis) Un gran número de incidentes cibernéticos se producen debido a la falta de resistencia y solidez de la infraestructura de la red privada y pública, unas bases de datos mal protegidas o mal aseguradas y otros defectos en las infraestructuras críticas de información; solo algunos Estados miembros consideran la protección de sus redes y sistemas de información y datos asociados como parte de su correspondiente deber de diligencia, lo cual explica la falta de inversión en tecnología de seguridad de vanguardia, formación y desarrollo de directrices adecuadas.

Enmienda 5

Propuesta de Directiva
Considerando 3

Texto de la Comisión	*Enmienda*
(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	(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.	de las redes y los sistemas de información son fundamentales para el correcto funcionamiento del mercado interior***, así como para la seguridad interior y exterior de la UE. Por consiguiente, la Estrategia de Seguridad Interior de la Unión y la Estrategia Europea de Seguridad deben hacer debidamente hincapié en la necesidad de mejorar la seguridad de las redes y la información, en particular a la vista de la futura revisión de esos documentos.***

Enmienda 6

Propuesta de Directiva
Considerando 3 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(3 bis) La concienciación y la educación de los usuarios de tecnologías de la información y la comunicación sobre mejores prácticas en cuanto a la protección de datos personales y el mantenimiento sostenible de servicios de comunicación deben constituir la base de cualquier estrategia global de ciberseguridad.

Enmienda 7

Propuesta de Directiva
Considerando 4 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(4 bis) La cooperación y la coordinación entre las autoridades europeas pertinentes con la VP/AR, con responsabilidad para la Política Exterior y de Seguridad Común y la Política Común de Seguridad y Defensa, así como el Coordinador de la UE para la lucha contra el terrorismo deben garantizarse en todos los casos en los que se perciban riesgos de naturaleza

exterior y terrorista.

Enmienda 8

Propuesta de Directiva
Considerando 4 ter (nuevo)

Texto de la Comisión	*Enmienda*
	(4 ter) Los servicios de inteligencia y el intercambio de información sensible entre los Estados miembros y entre los Estados miembros y las autoridades de la UE competentes deben reforzarse y anclarse en los principios de confianza, solidaridad y cooperación. Todo plan de acción encaminado a mejorar la seguridad de las redes y el sistema debe hacer pleno uso de las estructuras ya existentes en la UE, como el SitCen y el IntCen, y asegurar la coordinación entre todas las estructuras pertinentes para la seguridad de la información sensible en relación con la seguridad interior y exterior de la UE.

Enmienda 9

Propuesta de Directiva
Considerando 4 quater (nuevo)

Texto de la Comisión	*Enmienda*
	(4 quater) La cooperación y el intercambio de información a escala mundial con los socios internacionales pertinentes son esenciales para una estrategia eficaz de ciberseguridad y para una acción convincente con vistas a mejorar la seguridad de las redes y la información en la UE, teniendo en cuenta la naturaleza transnacional de las amenazas.

Enmienda 10

Propuesta de Directiva
Considerando 8 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(8 bis) Las medidas de seguridad han de respetar los derechos fundamentales que incumben a la UE y a sus Estados miembros de conformidad con los artículos 2, 6 y 21 del TFUE, como la libertad de expresión, la protección de datos y la intimidad; el derecho a la intimidad y el derecho a la protección de datos están consignados en la Carta de la UE y en el artículo 16 del TFUE.

Enmienda 11

Propuesta de Directiva
Considerando 11 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(11 bis) Todos los Estados miembros deben centrar las estrategias nacionales de ciberseguridad en la protección de los sistemas de información y los datos asociados, y han de considerar la protección de estas infraestructuras críticas como parte de su correspondiente deber de diligencia. Todos los Estados miembros deben adoptar y aplicar estrategias, directrices e instrumentos que ofrezcan niveles razonables de protección contra niveles de amenazas razonablemente identificables, en que los costes y las cargas de la protección sean proporcionales al daño probable a las partes implicadas. Asimismo, todos los Estados miembros deben adoptar las medidas adecuadas para obligar a las personas jurídicas bajo su jurisdicción a proteger los datos personales a su cuidado.

Enmienda 12

Propuesta de Directiva
Considerando 16

Texto de la Comisión	*Enmienda*
(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.	(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. ***Cualquier dato personal publicado en este sitio web debe limitarse únicamente a lo necesario y ser lo más anónimo posible.***

Enmienda 13

Propuesta de Directiva
Considerando 30 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(30 bis) La presente Directiva se entiende sin perjuicio del acervo de la Unión en lo que respecta a la protección de datos. Todo dato personal utilizado de conformidad con lo dispuesto en la presente Directiva debe mantenerse en el conjunto mínimo de datos personales estrictamente necesarios y solo ha de ser transmitido a los actores estrictamente necesarios, y debe ser lo más anónimo posible, cuando no totalmente anónimo.

Enmienda 14

Propuesta de Directiva
Considerando 32 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(32 bis) La presente Directiva (Directiva sobre SRI) no afecta a la adopción necesaria de legislación sobre protección general de datos a escala de la UE.

Enmienda 15

Propuesta de Directiva
Considerando 34 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(34 bis) Es necesario regular a escala de la UE la venta, el suministro, la transferencia o la exportación a terceros países de equipos o programas destinados principalmente a controlar o interceptar las comunicaciones telefónicas o por Internet en redes fijas y móviles, y la prestación de asistencia para instalar, manejar o actualizar dichos equipos o programas. La Comisión debe elaborar lo antes posible una legislación que evite que las empresas europeas exporten dichos productos de doble uso a regímenes represivos, autoritarios y no democráticos.

Enmienda 16

Propuesta de Directiva
Artículo 1 – apartado 2 – letra b

Texto de la Comisión	*Enmienda*
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	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***, eficientes*** y coordinadas ante los riesgos e incidentes que afecten a las redes y los

información;	sistemas de información;

Enmienda 17

Propuesta de Directiva
Artículo 3 – punto 1 – letra b

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

Enmienda 18

Propuesta de Directiva
Artículo 3 – punto 2 bis (nuevo)

Texto de la Comisión	*Enmienda*
	2 bis) «resistencia cibernética»: la capacidad de una red y de un sistema de información de resistir y recuperar toda su capacidad operativa después de un incidente, debido entre otras cosas a: averías técnicas, cortes de energía o incidentes de seguridad;

Enmienda 19

Propuesta de Directiva
Artículo 3 – punto 8 – letra b

Texto de la Comisión	*Enmienda*
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	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***,*** la sanidad***, la seguridad y la defensa***, una lista no

en el anexo II.

exhaustiva de los cuales figura en el anexo II.

Enmienda 20

Propuesta de Directiva
Artículo 3 – punto 8 – letra b bis (nueva)

Texto de la Comisión	*Enmienda*
	b bis) proveedores de dispositivos, redes y sistemas de información como los que se mencionan en el punto 1), o sus componentes que son fundamentales para un elevado nivel común de seguridad de las redes y la información.

Enmienda 21

Propuesta de Directiva
Artículo 6 – apartado 1

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

Enmienda 22

Propuesta de Directiva
Artículo 7 – apartado 1

Texto de la Comisión	*Enmienda*
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	1. Cada Estado miembro creará ***al menos*** 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

crearse un CERT en el marco de la autoridad competente.	1. Podrá crearse un CERT en el marco de la autoridad competente.

Enmienda 23

Propuesta de Directiva
Artículo 8 – apartado 3 – letra f bis (nueva)

Texto de la Comisión	*Enmienda*
	f bis) cuando sea pertinente, dada la naturaleza del riesgo o de la amenaza, deberá informarse al Coordinador de la UE para la lucha contra el terrorismo mediante informes y se le podrá pedir que contribuya con un análisis a la acción y los trabajos preparatorios de la red de cooperación;

Enmienda 24

Propuesta de Directiva
Artículo 9 – apartado 1 bis (nuevo)

Texto de la Comisión	*Enmienda*
	1 bis. Los datos personales solo se divulgarán a los destinatarios que necesiten procesarlos para el ejercicio de sus funciones, de conformidad con un fundamento jurídico apropiado. Los datos divulgados se limitarán a lo necesario para el ejercicio de sus funciones. Se garantizará el cumplimiento del principio de limitación del objetivo. El plazo límite de retención de estos datos se especificará para los efectos previstos en la presente Directiva.

Enmienda 25

Propuesta de Directiva
Artículo 10 – apartado 3

Texto de la Comisión	*Enmienda*
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.	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***, de conformidad con las disposiciones del Reglamento general sobre protección de datos***.

Enmienda 26

Propuesta de Directiva
Artículo 13 – párrafo –1 bis (nuevo)

Texto de la Comisión	***Enmienda***
	(–1 bis) La VP/AR integrará en las acciones exteriores de la UE, en particular en relación con los países terceros, los aspectos relativos a la ciberseguridad. El objetivo será intensificar el intercambio de las lecciones aprendidas y la cooperación sobre cuestiones de ciberseguridad.

Enmienda 27

Propuesta de Directiva
Artículo 13 – párrafo –1 ter (nuevo)

Texto de la Comisión	*Enmienda*
	(–1 ter) El Consejo y la Comisión insistirán en las normas mínimas para la seguridad de los sistemas de información, en el marco de sus relaciones y acuerdos de cooperación con terceros países, en particular los que implican la cooperación en materia de tecnologías.

Enmienda 28

Propuesta de Directiva
Artículo 20 – título

Texto de la Comisión	*Enmienda*
Revisión	***Presentación de informes y*** revisión

Enmienda 29

Propuesta de Directiva
Artículo 20 – párrafo –1 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(–1 bis) La Comisión presentará al Parlamento Europeo y al Consejo un informe anual sobre los incidentes y las medidas que se le notifiquen en virtud de la presente Directiva.

Enmienda 30

Propuesta de Directiva
Anexo 1 – punto 1 – letra b

Texto de la Comisión	*Enmienda*
b) El CERT aplicará y gestionará medidas de seguridad para garantizar la confidencialidad, integridad, disponibilidad y autenticidad de la información que reciba y trate.	b) El CERT aplicará y gestionará medidas de seguridad para garantizar la confidencialidad, integridad, disponibilidad y autenticidad de la información que reciba y trate***, cumpliendo los requisitos de protección de datos***.

Enmienda 31

Propuesta de Directiva
Anexo II – segundo subtítulo (Contemplados en el artículo 3, apartado 8, letra b) – apartado 5 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(5 bis) Sector de la seguridad y la defensa:

operadores económicos para trabajos y servicios a los que hace referencia la Directiva 2009/81/CE, en particular su artículo 46.

PROCEDIMIENTO

Título	Medidas para garantizar un elevado nivel común de seguridad de las redes y de la información en la Unión
Referencias	COM(2013)0048 – C7-0035/2013 – 2013/0027(COD)
Comisión competente para el fondo Fecha del anuncio en el Pleno	IMCO 15.4.2013
Opinión emitida por Fecha del anuncio en el Pleno	AFET 15.4.2013
Ponente de opinión Fecha de designación	Ana Gomes 19.2.2013
Examen en comisión	18.9.2013
Fecha de aprobación	5.12.2013
Resultado de la votación final	+: 31 –: 3 0: 8
Miembros presentes en la votación final	Elmar Brok, Jerzy Buzek, Mark Demesmaeker, Marietta Giannakou, Ana Gomes, Andrzej Grzyb, Anna Ibrisagic, Jelko Kacin, Tunne Kelam, Nicole Kiil-Nielsen, Andrey Kovatchev, Eduard Kukan, Marusya Lyubcheva, Annemie Neyts-Uyttebroeck, Norica Nicolai, Raimon Obiols, Kristiina Ojuland, Ria Oomen-Ruijten, Ioan Mircea Paşcu, Alojz Peterle, Mirosław Piotrowski, Bernd Posselt, Hans-Gert Pöttering, Cristian Dan Preda, Libor Rouček, Tokia Saïfi, José Ignacio Salafranca Sánchez-Neyra, György Schöpflin, Werner Schulz, Marek Siwiec, Charles Tannock, Geoffrey Van Orden, Nikola Vuljanić, Boris Zala
Suplente(s) presente(s) en la votación final	Marije Cornelissen, Barbara Lochbihler, Doris Pack, Marietje Schaake, Indrek Tarand, Ivo Vajgl, Paweł Zalewski
Suplente(s) (art. 187, apdo. 2) presente(s) en la votación final	Hiltrud Breyer

PROCEDIMIENTO

Título	Medidas para garantizar un elevado nivel común de seguridad de las redes y de la información en la Unión			
Referencias	COM(2013)0048 – C7-0035/2013 – 2013/0027(COD)			
Fecha de la presentación al PE	5.2.2013			
Comisión competente para el fondo Fecha del anuncio en el Pleno	IMCO 15.4.2013			
Comisión(es) competente(s) para emitir opinión Fecha del anuncio en el Pleno	AFET 15.4.2013	INTA 15.4.2013	BUDG 15.4.2013	ECON 15.4.2013
	ENVI 15.4.2013	ITRE 15.4.2013	TRAN 15.4.2013	JURI 15.4.2013
	LIBE 15.4.2013			
Opinión(es) no emitida(s) Fecha de la decisión	INTA 20.3.2013	BUDG 21.2.2013	ECON 18.6.2013	ENVI 19.2.2013
	TRAN 18.3.2013	JURI 20.2.2013		
Comisión(es) asociada(s) Fecha del anuncio en el Pleno	ITRE 12.9.2013	LIBE 12.9.2013		
Ponente(s) Fecha de designación	Andreas Schwab 20.3.2013			
Examen en comisión	25.4.2013	18.6.2013	5.9.2013	4.11.2013
	9.1.2014			
Fecha de aprobación	23.1.2014			
Resultado de la votación final	+: –: 0:	33 1 1		
Miembros presentes en la votación final	Claudette Abela Baldacchino, Pablo Arias Echeverría, Adam Bielan, Preslav Borissov, Sergio Gaetano Cofferati, Lara Comi, Anna Maria Corazza Bildt, Christian Engström, Vicente Miguel Garcés Ramón, Evelyne Gebhardt, Małgorzata Handzlik, Eduard-Raul Hellvig, Sandra Kalniete, Edvard Kožušník, Toine Manders, Hans-Peter Mayer, Franz Obermayr, Sirpa Pietikäinen, Zuzana Roithová, Heide Rühle, Andreas Schwab, Róża Gräfin von Thun und Hohenstein, Bernadette Vergnaud, Barbara Weiler			
Suplente(s) presente(s) en la votación final	Regina Bastos, Ashley Fox, María Irigoyen Pérez, Morten Løkkegaard, Tadeusz Ross, Marc Tarabella, Patricia van der Kammen, Sabine Verheyen, Josef Weidenholzer			
Suplente(s) (art. 187, apdo. 2) presente(s) en la votación final	Vital Moreira, Oreste Rossi			

Fecha de presentación	12.2.2014