COMISIÓN
EUROPEA

Bruselas, 4.10.2017
COM(2017) 476 final

ANNEX 1

NOTE
This language version reflects the corrections done to the original EN version transmitted under COM(2017) 476 final of 13.9.2017 and retransmitted (with corrections) under COM(2017) 476 final/2 of 4.10.2017

ANEXO

de la

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO

Sacar el máximo partido a la SRI: hacia la aplicación efectiva de la Directiva (UE) 2016/1148, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión

ÍNDICE

ANEXO

1. Introducción

El objetivo del presente anexo es contribuir a la aplicación y ejecución efectivas de la Directiva (EU) 2016/1148, sobre la seguridad de las redes y sistemas de información en la Unión[1] (en lo sucesivo denominada «la Directiva SRI» o «la Directiva») y ayudar a los Estados miembros en su labor de velar por la aplicación efectiva de la legislación de la UE. Más en concreto, su objetivo es triple: a) ofrecer mayor claridad a las autoridades nacionales acerca de las obligaciones contenidas en la Directiva que les son aplicables, b) garantizar el control efectivo del cumplimiento de las obligaciones de la Directiva aplicables a las entidades sujetas a los requisitos de seguridad y notificación de incidentes, y c) contribuir en general a crear seguridad jurídica para todos los agentes pertinentes.

A tal fin, el presente anexo ofrece orientaciones sobre los aspectos que figuran a continuación, que resultan esenciales para la consecución del objetivo de la Directiva SRI, a saber, garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la UE que sustente el funcionamiento de nuestra sociedad y nuestra economía:

- la obligación de los Estados miembros de adoptar una estrategia nacional de seguridad de las redes y sistemas de información (sección 2),
- la designación de autoridades nacionales competentes, puntos de contacto únicos y equipos de respuesta a incidentes de seguridad informática (sección 3),
- los requisitos en materia de seguridad y notificación de incidentes aplicables a los operadores de servicios esenciales y a los proveedores de servicios digitales (sección 4), y
- las relaciones entre la Directiva SRI y otros actos legislativos (sección 5).

Para preparar esas orientaciones, la Comisión ha utilizado las aportaciones y análisis recabados durante la preparación de la Directiva, así como las contribuciones de la Agencia de Seguridad de las Redes y de la Información de la Unión Europea («ENISA») y del Grupo de cooperación. Asimismo, ha aprovechado la experiencia de Estados miembros específicos. En la medida de lo necesario, la Comisión ha tenido en cuenta los principios rectores de la interpretación de la legislación de la UE: la formulación, el contexto y los objetivos de la Directiva SRI. Teniendo en cuenta que la Directiva no ha sido objeto de transposición, ni el Tribunal de Justicia de la Unión Europea (TJUE) ni los tribunales nacionales han dictado aún sentencias al respecto. Así pues, no se ha podido recurrir a la jurisprudencia como fuente de orientación.

La recopilación de esta información en un único documento puede facilitar que los Estados miembros tengan una buena visión de conjunto de la Directiva y tomen en consideración esa información al elaborar su legislación nacional. Al mismo tiempo, la Comisión recalca que el

[1] Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. La Directiva entró en vigor el 8 de agosto de 2016.

presente anexo no es vinculante y que con él no pretenden crearse nuevas normas. La competencia para interpretar la legislación de la UE reside en última instancia en el TJUE.

2. Estrategia nacional de seguridad de las redes y sistemas de información

Con arreglo al artículo 7 de la Directiva SRI, los Estados miembros deben adoptar una estrategia nacional de seguridad de las redes y sistemas de información que puede considerarse equivalente al concepto de Estrategia de Ciberseguridad Nacional («ECSN»). La función de una estrategia nacional es definir los objetivos estratégicos y las medidas políticas y reguladoras adecuadas en el ámbito de la ciberseguridad. El concepto de ECSN se utiliza extensamente en la esfera internacional y en Europa, sobre todo en el contexto de los trabajos emprendidos por ENISA con los Estados miembros en relación con las estrategias nacionales que culminaron recientemente con la actualización de la guía de buenas prácticas en ECSN.[2]

En esta sección, la Comisión explica cómo la Directiva SRI refuerza la preparación de los Estados miembros al exigirles contar con estrategias nacionales sólidas en materia de seguridad de las redes y sistemas de información (artículo 7). Se abordan los siguientes aspectos: a) el alcance de la estrategia, y b) el contenido y el procedimiento de adopción.

Tal como se detalla a continuación, la correcta transposición del artículo 7 de la Directiva SRI es esencial para la consecución de los objetivos de la Directiva y exige la asignación a tal fin de recursos financieros y humanos adecuados.

2.1. El alcance de la estrategia nacional

Según la redacción del artículo 7, la obligación de adoptar una ECSN solo se aplica a los sectores que figuran en el anexo II (es decir, energía, transporte, banca, mercados financieros, sanidad, suministro y distribución de agua potable e infraestructura digital) y los servicios que figuran en el anexo III (mercados en línea, motores de búsqueda en línea y servicios de computación en la nube).

El artículo 3 de la Directiva establece expresamente el principio de armonización mínima, según el cual los Estados miembros pueden adoptar o mantener disposiciones con el objeto de alcanzar un mayor nivel de seguridad de las redes y sistemas de información. La aplicación de este principio a la obligación de adoptar una ECSN permite a los Estados miembros incluir más sectores y servicios que los comprendidos en los anexos II y III de la Directiva.

En opinión de la Comisión, y a la luz del objetivo de la Directiva SRI, a saber, alcanzar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión[3], sería conveniente elaborar una estrategia nacional que abarcara todas las dimensiones pertinentes de la sociedad y la economía, y no solo los sectores y los servicios digitales comprendidos en los anexos II y III, respectivamente, de la Directiva SRI. Este planteamiento se ajusta a las mejores prácticas internacionales (véanse las orientaciones de la UIT y los análisis de la OCDE mencionados más adelante) y a la Directiva SRI.

[2] ENISA, *National Cyber-Security Strategy Good Practice* 2016). Disponible en https://www.enisa.europa.eu/publications/ncss-good-practice-guide

[3] Véase el artículo 1, apartado 1.

Como se explica más adelante, este es especialmente el caso de las administraciones públicas responsables de sectores y servicios distintos de los que figuran en los anexos II y III de la Directiva. Las administraciones públicas pueden procesar información sensible, lo que justifica la necesidad de ser incluidas en las ECSN y en planes de gestión que impidan las fugas y garanticen la protección adecuada de esa información.

2.2. Contenido y procedimiento de adopción de las estrategias nacionales

Con arreglo al artículo 7 de la Directiva SRI, la estrategia nacional debe incluir, como mínimo, los aspectos siguientes:

i) los objetivos y prioridades de la estrategia nacional de seguridad de las redes y sistemas de información,
ii) un marco de gobernanza para lograr los objetivos y las prioridades de la estrategia nacional,
iii) la identificación de medidas sobre preparación, respuesta y recuperación, incluida la cooperación entre los sectores público y privado,
iv) una indicación de los programas de educación, concienciación y formación,
v) una indicación de los programas de investigación y desarrollo,
vi) un plan de evaluación de riesgos para identificar riesgos, y
vii) una lista de los agentes que participan en la ejecución de la estrategia.

Ni el artículo 7 ni el considerando 29 correspondiente especifican los requisitos para la adopción de una ECSN ni ofrecen un mayor grado de detalle sobre el contenido de las ECSN. En lo que respecta a los procesos y otros elementos relacionados con el contenido de las ECSN, la Comisión considera que el enfoque que se expone a continuación es la vía adecuada para adoptar una ECSN. Esta conclusión se basa en el análisis de la experiencia de Estados miembros y terceros países en la elaboración de sus propias estrategias. Otra fuente de información a este respecto es la herramienta de formación en ECSN de ENISA, que está disponible en su sitio web en formato de vídeo y de archivos descargables[4].

2.3. Proceso y aspectos que deben abordarse

El proceso de elaboración y de subsiguiente adopción de una estrategia nacional es complejo y comprende múltiples facetas, razón por la cual exige un compromiso sostenido con expertos en ciberseguridad, con la sociedad civil y con el proceso político nacional para que sea efectivo y aporte los resultados deseados. Una condición imprescindible es el apoyo de las altas esferas de la Administración, como mínimo a nivel de secretario de Estado o equivalente en el ministerio que sea el responsable principal, así como el respaldo político. Para adoptar con éxito una ECSN, cabe considerar un proceso consistente en cinco etapas (véase el gráfico 1):

Primera etapa: **Fijación de los principios rectores y los objetivos estratégicos de la estrategia**

En primer lugar, las autoridades nacionales competentes deben definir una serie de elementos clave de la ECSN, a saber, cuáles son resultados esperados —en el lenguaje de la Directiva

[4] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-training-tool

[artículo 7, apartado 1, letra a)], *los objetivos y prioridades*—, cómo complementan esos resultados las políticas sociales y económicas y si son compatibles con los privilegios y obligaciones derivados de la condición de Estado miembro de la Unión Europea. Los objetivos deben ser específicos, medibles, alcanzables, realistas y acotados en el tiempo (objetivos «SMART»). Sirva como ejemplo ilustrativo el siguiente enunciado: *We will ensure that this [time bound] strategy is founded upon a rigorous and comprehensive set of metrics against which we measure progress towards the outcomes we need to achieve* [Garantizaremos que esta estrategia (acotada en el tiempo) se basa en un conjunto riguroso y completo de indicadores con los que medimos el progreso hacia los resultados que debemos alcanzar][5].

El requisito expuesto comprende también una evaluación política que determine si puede obtenerse un presupuesto considerable para financiar la aplicación de la estrategia. Asimismo, implica una descripción del alcance previsto de la estrategia y las distintas categorías de partes interesadas de los sectores público y privado que deben participar en la formulación de los distintos objetivos y medidas.

Esta primera etapa puede completarse mediante la organización de talleres específicos con altos funcionarios ministeriales y representantes políticos moderados por ciberespecialistas con capacidades de comunicación profesional que puedan resaltar las implicaciones que supone la ausencia o insuficiencia de ciberseguridad para una economía y sociedad digital moderna.

Segunda etapa: **Elaboración del contenido de la estrategia**

La estrategia debe contener medidas facilitadoras, actuaciones acotadas en el tiempo e indicadores clave de resultado que permitan, tras un periodo de aplicación definido, evaluar, perfeccionar y mejorar la estrategia. Esas medidas deben respaldar el objetivo, las prioridades y los resultados fijados como principios rectores. La necesidad de incluir medidas facilitadoras se establece en el artículo 7, apartado 1, letra c), de la Directiva SRI.

Se recomienda que se constituya un grupo de dirección presidido por el ministerio principal y encargado de gestionar el proceso de redacción y facilitar las aportaciones. A tal fin, podrían crearse una serie de grupos de redacción formados por funcionarios y expertos pertinentes en torno a algunos temas genéricos clave: por ejemplo, evaluación de riesgos, planificación de contingencias, gestión de incidentes, desarrollo de capacidades, sensibilización, investigación y desarrollo industrial, etc. Además, se invitaría por separado a cada sector —por ejemplo, de energía, transporte, etc.— a evaluar las implicaciones de su inclusión, en particular la asignación de recursos, y a implicar a los operadores de servicios esenciales designados y proveedores de servicios digitales clave en la fijación de las prioridades y la presentación de propuestas al proceso de redacción. La implicación de las partes interesadas sectoriales también es esencial por la necesidad de garantizar la aplicación armonizada de la Directiva en los distintos sectores, dejando al mismo tiempo un margen para las especificidades sectoriales.

Tercera etapa: **Desarrollo de un marco de gobernanza**

[5] Extracto de la Estrategia de Ciberseguridad Nacional del Reino Unido, 2016 -2021, página 67.

En aras de la eficiencia y la eficacia, el marco de gobernanza debería basarse en las partes interesadas clave, en las prioridades definidas en el proceso de redacción y en las limitaciones y el contexto de las estructuras administrativas y políticas nacionales. Sería deseable que la información se comunicara directamente al nivel político y que el marco tuviera capacidad para la toma de decisiones y la asignación de recursos y contara con las aportaciones de expertos en ciberseguridad y partes interesadas industriales. El artículo 7, apartado 1, letra b), de la Directiva SRI alude al marco de gobernanza y exige de manera específica las *responsabilidades de las instituciones públicas y de los demás agentes pertinentes.*

Cuarta etapa: **Compilación y revisión del borrador de estrategia**

En esta etapa, debería compilarse y revisarse el borrador de estrategia utilizando el análisis de debilidades, amenazas, fortalezas y oportunidades (análisis DAFO), que permitiría determinar la necesidad de revisar el contenido. Tras la revisión interna tendría lugar la consulta de las partes interesadas. Sería esencial realizar también una consulta pública para subrayar la importancia de la estrategia propuesta ante el público, recibir aportaciones de todas las fuentes posibles y buscar apoyo para la asignación de los recursos necesarios para la subsiguiente aplicación de la estrategia.

Quinta etapa: **Adopción formal**

Esta última etapa incluye la adopción formal a nivel político y la dotación de un presupuesto adecuado que refleje la seriedad que el Estado miembro atribuye a la ciberseguridad. Para alcanzar los objetivos de la Directiva SRI, y al comunicar el documento estratégico nacional a la Comisión de conformidad con el artículo 7, apartado 3, la Comisión anima a los Estados miembros a que faciliten información sobre el presupuesto. Los compromisos respecto a los recursos presupuestarios y humanos necesarios revisten una importancia esencial para la aplicación efectiva de la estrategia y la Directiva. Habida cuenta de que la ciberseguridad es un área de actuación pública relativamente nueva y en rápida expansión, en la mayoría de los casos se requieren nuevas inversiones, aun cuando la situación general de las haciendas públicas requiere recortes y medidas de ahorro.

Varias fuentes públicas y académicas ofrecen asesoramiento sobre el proceso y el contenido de las estrategias nacionales, entre ellas ENISA[6], la UIT[7], la OCDE[8], el Foro mundial sobre conocimientos cibernéticos (Global Forum for Cyber Expertise) y la Universidad de Oxford[9].

---

[6] ENISA, *National Cyber-Security Strategy Good Practice* 2016). Disponible en https://www.enisa.europa.eu/publications/ncss-good-practice-guide

[7] UIT, *National Cybersecurity Strategy Guide (2011).* Disponible en http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf
Asimismo, la UIT va a publicar en 2017 un manual de estrategias nacionales de seguridad (véase la presentación en http://www.itu.int/en/ITU-D/Cybersecurity/Documents/National%20Strategy%20Toolkit%20introduction.pdf)

[8] OCDE, *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies (2012).* Disponible en: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

[9] Global Cyber Security Capacity Centre y Universidad de Oxford, *Global Cyber Cybersecurity Capacity Maturity Model for Nations (CMM) - Revised Edition (2016).* Disponible en:

2.4. Pasos concretos que deben dar los Estados miembros antes de que concluya el plazo de transposición

Antes de la adopción de la Directiva, casi todos los Estados miembros[10] habían publicado ya documentos calificados de ECSN. La sección 6 del presente anexo enumera las estrategias implantadas en cada Estado miembro[11]. Por lo general incluyen principios estratégicos, directrices, objetivos y, en algunos casos, medidas específicas para mitigar los riesgos asociados a la ciberseguridad.

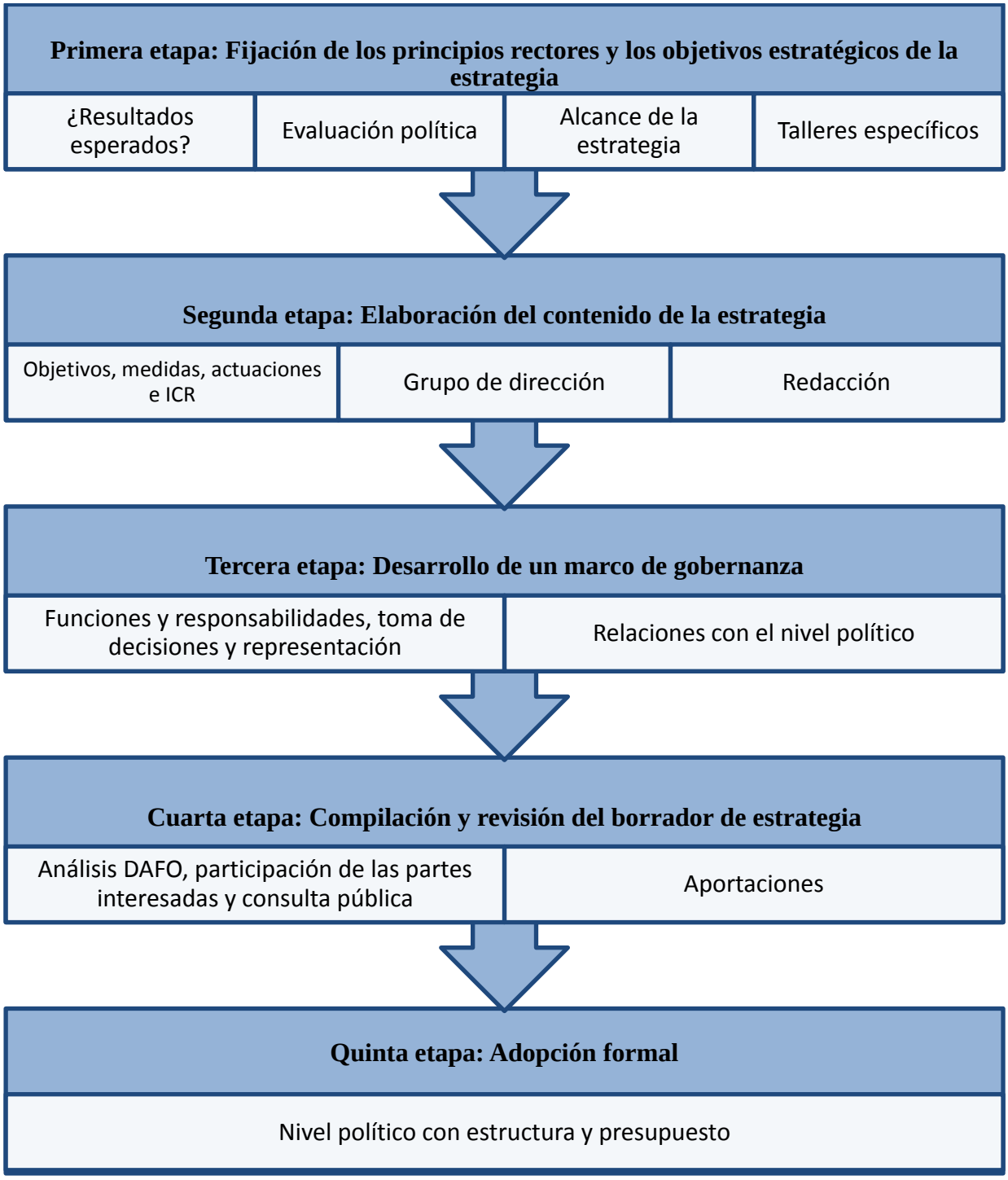
Dado que algunas de esas estrategias se adoptaron antes que la Directiva SRI, no necesariamente contienen todos los elementos enunciados en el artículo 7. Para garantizar la correcta transposición, los Estados miembros deberán realizar un análisis de deficiencias cotejando el contenido de su ECSN con cada uno de los siete requisitos enumerados en el artículo 7 respecto a cada sector enumerado en el anexo II de la Directiva y a cada servicio enumerado en su anexo III. A continuación, las deficiencias detectadas podrán abordarse revisando su ECSN existente u optando por una revisión completa desde cero de los principios de su estrategia nacional de SRI. Las orientaciones formuladas más arriba respecto al proceso de adopción de ECSN también resultan pertinentes para la revisión y actualización de las que ya existan.

https://www.thegfce.com/binaries/gfce/documents/publications/2017/02/13/cybersecurity-cmm-for-nations/CMM+revised+edition.pdf

[10] Aparte de Grecia, donde se está preparando una estrategia de ciberseguridad nacional desde 2014 (véase https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/national-cyber-security-strategy-greece/view)

[11] Esta información se basa en la presentación de las ECSN por parte de ENISA en https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map

Gráfico 1: Proceso de adopción de la ECSN en cinco etapas



3. Directiva SRI: Autoridades nacionales competentes, puntos de contacto únicos y equipos de respuesta a incidentes de seguridad informática (CSIRT, por las siglas en inglés de «Computer Security Incident Response Teams»)

Con arreglo al artículo 8, apartado 1, los Estados miembros deben designar a una o más autoridades nacionales competentes, que abarquen como mínimo los sectores que figuran en el anexo II de la Directiva y los servicios que figuran en su anexo III, a las que se atribuya la labor de supervisar la aplicación de la Directiva. Los Estados miembros podrán asignar esta función a una autoridad o autoridades existentes.

En esta sección se explica de qué manera la Directiva SRI refuerza la preparación de los Estados miembros al exigirles que cuenten con autoridades nacionales competentes y equipos de respuesta a incidentes de seguridad informática (CSIRT) efectivos. Más en concreto, se aborda la obligación de designar a autoridades nacionales competentes, incluida la función del punto de contacto único. Se analizan tres temas: a) las posibles estructuras nacionales de gobernanza (p. ej., modelos centralizados, descentralizados, etc.) y otros requisitos; b) la función del punto de contacto único, y c) los equipos de respuesta a incidentes de seguridad informática.

3.1. Tipo de autoridades

El artículo 8 de la Directiva SRI establece que los Estados miembros deben designar a autoridades nacionales competentes en materia de seguridad de las redes y sistemas de información, al tiempo que reconoce explícitamente la posibilidad de designar a *una o más autoridades nacionales competentes*. El considerando 30 de la Directiva explica esta opción de actuación: *Habida cuenta de las diferencias existentes entre las estructuras nacionales de gobernanza y con el fin de salvaguardar las disposiciones sectoriales vigentes o los organismos de supervisión y regulación de la Unión ya existentes, y para evitar duplicidades, los Estados miembros deben poder designar a más de una autoridad nacional competente responsable de ejercer las funciones vinculadas a la seguridad de las redes y sistemas de información de los operadores de servicios esenciales y los proveedores de servicios digitales en virtud de la presente Directiva.*

Por tanto, los Estados miembros pueden optar por designar a una autoridad central que abarque todos los sectores y servicios comprendidos en la Directiva o por designar a varias autoridades, dependiendo, por ejemplo, del tipo de sector.

Al optar por un planteamiento u otro, los Estados miembros pueden basarse en la experiencia de los planteamientos nacionales seguidos en el contexto de la legislación vigente en materia de protección de infraestructuras críticas de información (PICI). Tal como se describe en el cuadro 1, en el caso de la PICI, los Estados miembros optaron por un planteamiento centralizado o descentralizado al asignar competencias a nivel nacional. Los ejemplos nacionales se utilizan aquí exclusivamente a efectos ilustrativos y para que los Estados miembros conozcan los marcos organizativos existentes. Así, la Comisión no considera que el modelo empleado por los respectivos países para la PICI deba utilizarse necesariamente a efectos de transposición de la Directiva SRI.

Los Estados miembros pueden también optar por enfoques híbridos que contengan elementos de ambos planteamientos, el centralizado y el descentralizado. La elección puede hacerse en consonancia con mecanismos nacionales de gobernanza previos aplicados en los distintos sectores y servicios comprendidos en la Directiva o a partir de mecanismos nuevos determinados por las autoridades y por las partes interesadas pertinentes identificadas como operadores de servicios esenciales y proveedores de servicios digitales. Otros factores importantes que pueden incidir en la elección de los Estados miembros son la experiencia especializada en ciberseguridad, consideraciones ligadas a la asignación de recursos e intereses nacionales (por ejemplo, desarrollo económico, seguridad pública, etc.).

3.2. Publicidad y otros aspectos pertinentes

Con arreglo al artículo 8, apartado 7, los Estados miembros deben informar a la Comisión sobre la designación de las autoridades nacionales competentes y sus funciones. Deben hacerlo dentro del plazo de transposición.

Los artículos 15 y 17 de la Directiva SRI exigen a los Estados miembros que velen por que las autoridades competentes dispongan de competencias y medios específicos para desempeñar las tareas indicadas en dichos artículos.

Además, la designación de entidades concretas como autoridades nacionales competentes debe hacerse pública. La Directiva no especifica la manera en que debe hacerse tal publicidad. Dado que el objetivo de este requisito es alcanzar un elevado grado de sensibilización por parte de los agentes afectados por los SRI y el público en general, y sobre la base de la experiencia de otros sectores (telecomunicaciones, banca y medicina), la Comisión cree que esto podría hacerse, por ejemplo, a través de un portal debidamente publicitado.

El artículo 8, apartado 5, de la Directiva SRI exige que tales autoridades dispongan de *recursos adecuados* para ejercer las funciones que les asigna la Directiva.

Cuadro 1: Planteamientos nacionales en materia de protección de infraestructuras críticas (PICI)

En 2016 ENISA publicó un estudio[12] sobre los distintos planteamientos que siguen los Estados miembros para proteger sus infraestructuras críticas de información. Se describen dos perfiles respecto a la gobernanza de la PICI en los Estados miembros que pueden utilizarse en el contexto de la transposición de la Directiva SRI.

Perfil 1: Planteamiento descentralizado: hay múltiples autoridades sectoriales competentes respecto a sectores y servicios específicos de los anexos II y III de la Directiva

El planteamiento descentralizado se caracteriza por:

i) el principio de subsidiariedad,
ii) una sólida cooperación entre agencias públicas,
iii) legislación sectorial.

Principio de subsidiariedad

En lugar de establecer o designar a una sola agencia con responsabilidad global, el planteamiento descentralizado obedece al principio de subsidiariedad. Esto significa que la responsabilidad de la aplicación está en manos de una autoridad sectorial que es la que mejor conoce el sector local y tiene una relación previa sólida con las partes interesadas. Con arreglo a ese principio, las decisiones las toman las instancias más próximas a los destinatarios afectados.

Sólida cooperación entre agencias públicas

Debido a la variedad de agencias públicas implicadas en la PICI, muchos Estados miembros han elaborado regímenes de cooperación para coordinar los trabajos y esfuerzos de las distintas autoridades. Esos regímenes de cooperación pueden configurarse como redes informales o como foros o mecanismos más institucionalizados. Ahora bien, únicamente sirven para fines de intercambio de información y coordinación entre las distintas agencias públicas, pero no tienen autoridad sobre ellas.

Legislación sectorial

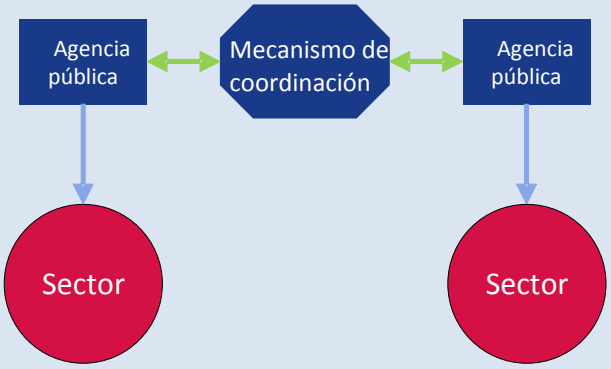
Los países que siguen el planteamiento descentralizado en sectores críticos a menudo se abstienen de legislar a efectos de la PICI, sino que la legislación y reglamentación sigue siendo sectorial, por lo que puede variar enormemente de un sector a otro. Este planteamiento tendría la ventaja de alinear las medidas relacionadas con los SRI con reglamentaciones sectoriales existentes a fin de mejorar tanto la aceptación por el sector como la efectividad del control del cumplimiento por la autoridad correspondiente.

Hay un riesgo considerable de que un planteamiento puramente descentralizado menoscabe la coherencia en la aplicación de la Directiva en los diversos sectores y servicios. En ese caso, la Directiva prevé el establecimiento de un punto de contacto nacional único que sirva de enlace

[12] *ENISA, Stocktaking, Analysis and Recommendations on the protection of CIIs (2016). Disponible* en: https://www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis

para los asuntos transfronterizos y al que el Estado miembro también podría asignar funciones de coordinación interna y de cooperación entre diversas autoridades nacionales competentes, de conformidad con el artículo 10 de la Directiva.

Gráfico 2: Planteamiento descentralizado



Ejemplos de planteamiento descentralizado

Suecia constituye un buen ejemplo de planteamiento descentralizado en materia de PICI. El país utiliza una «perspectiva sistémica», en virtud de la cual las principales tareas de la PICI, como la identificación de servicios vitales e infraestructuras críticas, la coordinación y el apoyo de operadores, las tareas de reglamentación y las medidas de preparación ante emergencias, son responsabilidad de distintas agencias y entes locales. Entre esas agencias figuran la Agencia de Contingencias Civiles de Suecia (MSB), la Agencia de Correos y Telecomunicaciones de Suecia (PTS) y varias agencias suecas de defensa, militares y policiales.

Para coordinar las actuaciones de las distintas agencias y entidades públicas, el Gobierno sueco ha desarrollado una red de cooperación compuesta por autoridades con «responsabilidades específicas en materia de seguridad de la sociedad de la información». Ese Grupo de cooperación en materia de Seguridad de la Información (SAMFI) está formado por representantes de las distintas autoridades y se reúne varias veces al año para debatir cuestiones ligadas a la seguridad de la información nacional. Las principales áreas de actuación del SAMFI son ámbitos político-estratégicos y tratan temas como las cuestiones técnicas y la normalización, el desarrollo nacional e internacional en el ámbito de la seguridad de la información, o la gestión y prevención de incidentes de las tecnologías de la información. [Agencia de Contingencias Civiles de Suecia (MSB) 2015].

Suecia no ha publicado una ley central sobre la PICI aplicable a los operadores de infraestructuras críticas de información en todos los sectores. La adopción de legislación con obligaciones para las empresas en sectores específicos es más bien responsabilidad de las respectivas autoridades públicas. Por ejemplo, la MSB tiene derecho a adoptar reglamentos aplicables a las autoridades gubernamentales en el ámbito de la seguridad de la información, mientras que la PTS puede exigir a los operadores que apliquen determinadas medidas de seguridad técnicas u organizativas sobre la base de legislación derivada.

Otro país que presenta rasgos propios de este perfil es Irlanda. Irlanda sigue una «doctrina de subsidiariedad» con arreglo a la cual cada ministerio es responsable de definir las infraestructuras críticas de información y la evaluación de riesgos en su propio sector. Además, no se han adoptado reglamentaciones específicas en materia de PICI a nivel nacional. La legislación sigue siendo sectorial y existe sobre todo en el sector de energía y telecomunicaciones (2015). Otros ejemplos son Austria, Chipre y Finlandia.

Perfil 2: Planteamiento centralizado: una autoridad central es competente respecto a todos los sectores y servicios de los anexos II y III de la Directiva

El planteamiento centralizado se caracteriza por:

i) una autoridad central para todos los sectores,
ii) una legislación general.

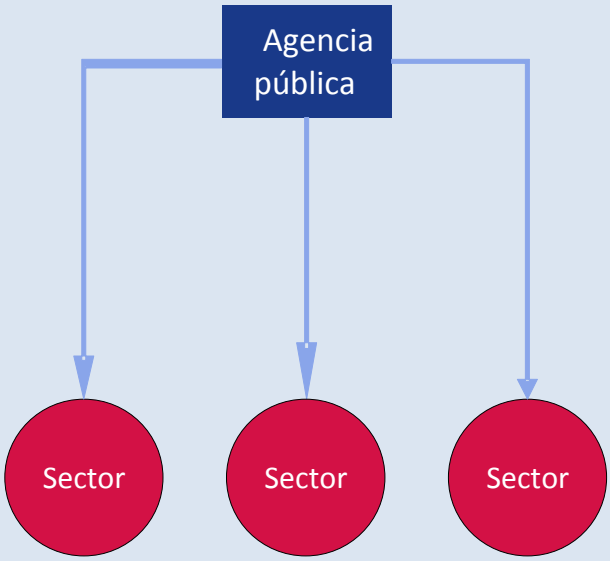
Una autoridad central para todos los sectores

Los Estados miembros con un planteamiento centralizado han designado a autoridades con responsabilidades y amplias competencias en varios o todos los sectores críticos, o han ampliado las responsabilidades de autoridades existentes. Esas autoridades PICI principales combinan varias tareas, tales como la planificación de contingencias, la gestión de emergencias, la reglamentación o el apoyo a los operadores privados. En muchos casos, el CSIRT es parte de la autoridad PICI principal. Dada la escasez general de capacidades en el terreno de la ciberseguridad, una autoridad central puede concentrar más los conocimientos especializados al respecto que una variedad de autoridades sectoriales.

Una legislación general

Una legislación general genera obligaciones y requisitos aplicables a todos los operadores de infraestructuras críticas de información de todos los sectores. Esto puede conseguirse adoptando leyes generales nuevas o completando reglamentaciones sectoriales específicas. Este planteamiento facilitaría la aplicación coherente de la Directiva SRI en todos los sectores y servicios comprendidos en ella. Evitaría el riesgo de que se produjeran deficiencias de aplicación derivadas de la existencia de múltiples autoridades con mandatos específicos.

Gráfico 3: Planteamiento centralizado



Ejemplos de planteamiento centralizado

Francia es un buen ejemplo de Estado miembro de la UE con un planteamiento centralizado. La Agencia nacional francesa de seguridad de los sistemas de información (*Agence Nationale de la Sécurité des Systèmes d'Information*, ANSSI) fue designada autoridad nacional principal para la defensa de los sistemas de información en 2011. La ANSSI desempeña una sólida función supervisora de los «operadores de vital importancia»: puede ordenar a esos operadores que se ajusten a medidas de seguridad determinadas y está autorizada para someterles a auditorías de seguridad. Además, es el principal punto de contacto único de dichos operadores, que están obligados a notificarle los incidentes de seguridad.

En caso de incidentes de seguridad, la ANSSI actúa como agencia de contingencia en materia de PICI y decide las medidas que deben adoptar los operadores para responder a la crisis. Las actuaciones gubernamentales se coordinan en el centro de operaciones de la ANSSI. La detección de amenazas y la respuesta a los incidentes a nivel operacional son responsabilidad de CERT-FR, que forma parte de la ANSSI.

Francia ha establecido un marco legal completo para la PICI. En 2006, el primer ministro ordenó fijar una lista de sectores de infraestructuras críticas. Sobre la base de esa lista, en la que se incluyeron doce sectores vitales, el gobierno ha determinado unos doscientos cincuenta operadores de vital importancia. En 2013 se promulgó la Ley de programación militar (LPM)[13]. Esta ley establece obligaciones diferenciadas para los operadores de vital importancia, tales como la notificación de incidentes o la aplicación de medidas de seguridad. Esos requisitos son obligatorios para todos los operadores de vital importancia de todos los sectores (Senado francés, 2013).

[13] *Loi de programmation militaire*.

3.3. Directiva SRI, artículo 9: equipos de respuesta a incidentes de seguridad informática (CSIRT)

Con arreglo al artículo 9, los Estados miembros deben designar a uno o varios CSIRT, a los que se confiere la tarea de gestionar riesgos e incidentes para los sectores comprendidos en el anexo II de la Directiva SRI y los servicios comprendidos en su anexo III. Teniendo en cuenta el requisito de armonización mínima establecido en el artículo 3 de la Directiva, los Estados miembros tienen libertad para utilizar también los CSIRT en otros sectores no comprendidos en la Directiva, como la Administración Pública.

Los Estados miembros pueden optar por establecer un CSIRT dentro de la autoridad nacional competente[14].

3.4. Funciones y requisitos

Las funciones de los CSIRT designados, expuestas en el anexo I de la Directiva SRI, incluyen las siguientes:

- supervisar incidentes a escala nacional,
- difundir alertas tempranas, alertas, avisos e información sobre riesgos e incidentes entre los interesados,
- responder a incidentes,
- efectuar un análisis dinámico de riesgos e incidentes y de conocimiento de la situación, y
- participar en la red de CSIRT nacionales (red de CSIRT) establecida con arreglo al artículo 12.

En el artículo 14, apartados 3, 5 y 6, y en el artículo 16, apartados 3, 6 y 7, se establecen funciones específicas adicionales en relación con la notificación de incidentes cuando un Estado miembro decide que el CSIRT, además de las autoridades nacionales competentes o sustituyéndolas, puede ejercer esas funciones.

En la transposición de la Directiva, los Estados miembros disponen de distintas opciones para configurar la función de los CSIRT en relación con los requisitos de notificación de incidentes. La notificación directa obligatoria a los CSIRT es posible, y ofrece ventajas de eficiencia administrativa; como alternativa, los Estados miembros pueden optar por la notificación directa a las autoridades nacionales competentes, teniendo los CSIRT derecho de acceso a la información notificada. En última instancia, los CSIRT se ocupan de la resolución de problemas en relación con la disuasión y detección de ciberincidentes, así como en la respuesta a los mismos y en la mitigación de su impacto (incluso cuando no se trate de incidentes críticos sujetos a notificación obligatoria) con sus partes interesadas, y la conformidad reglamentaria compete a las autoridades nacionales competentes.

[14] Véase el artículo 9, apartado 1, última frase.

Por otro lado, con arreglo al artículo 9, apartado 3, los Estados miembros deben velar por que los CSIRT tengan acceso a una infraestructura de comunicación e información apropiada.

El artículo 9, apartado 4, de la Directiva exige a los Estados miembros que informen a la Comisión del mandato y de los elementos principales del proceso de gestión de incidentes de los CSIRT designados.

Los requisitos de los CSIRT designados por los Estados miembros figuran en el anexo I de la Directiva SRI. Los CSIRT deben garantizar un elevado nivel de disponibilidad de sus servicios de comunicación. Sus dependencias y los sistemas de información de apoyo estarán situados en lugares seguros y tendrán la capacidad de garantizar la continuidad de las actividades. Además, los CSIRT deberían poder participar en redes de cooperación internacional.

3.5. Asistencia para el desarrollo de los CSIRT

El programa de infraestructuras de servicios digitales (ISD) del Mecanismo «Conectar Europa» (MCE) puede aportar fondos considerables de la UE para ayudar a los CSIRT de los Estados miembros en la mejora de sus capacidades y en la cooperación mutua a través de un mecanismo de cooperación en el intercambio de información. El mecanismo de cooperación que se está desarrollando en el proyecto SMART 2015/1089 tiene por objetivo favorecer una cooperación operativa fluida y efectiva, de carácter voluntario, entre los CSIRT de los Estados miembros, sobre todo en apoyo de las funciones encomendadas a la red de CSIRT de conformidad con el artículo 12 de la Directiva.

Para más información sobre las convocatorias de propuestas pertinentes para la creación de capacidades de los CSIRT de los Estados miembros, puede consultarse el sitio web de la Agencia Ejecutiva de Innovación y Redes (INEA) de la Comisión Europea[15].

El comité de gobernanza del programa ISD del MCE proporciona una estructura informal para el asesoramiento y la asistencia a los CSIRT de los Estados miembros, a nivel político, a efectos de creación de capacidades y de aplicación del mecanismo de cooperación voluntario.

Un CSIRT de nueva creación o uno designado para el desempeño de las funciones del anexo I de la Directiva SRI puede contar con el asesoramiento y los conocimientos especializados de ENISA para mejorar su rendimiento y obtener resultados eficaces[16]. A este respecto, cabe señalar que los CSIRT de los Estados miembros podrían tomar como referencia una parte del trabajo desarrollado recientemente por ENISA. En concreto, tal como se explica en la sección 7 del presente anexo, ENISA ha publicado una serie de documentos y estudios que describen buenas prácticas, recomendaciones técnicas, evaluaciones integrales del grado de madurez de los CSIRT, para varios de sus servicios y capacidades. Además, las redes de CSIRT han compartido orientaciones y buenas prácticas tanto a nivel global (FIRST[17]) como europeo (servicio *Trusted Introducer*, TI[18]).

[15] Disponible en: https://ec.europa.eu/inea/en/connecting-europe-facility
[16] Véase el artículo 9, apartado 5, de la Directiva SRI.
[17] Foro de Equipos de Respuesta a Incidentes de Seguridad (FIRST, por sus siglas en inglés) https://www.first.org/)
[18] https://www.trusted-introducer.org/

3.6. Función del punto de contacto único

Con arreglo al artículo 8, apartado 3, de la Directiva SRI, cada Estado miembro debe designar un punto de contacto nacional único que ejercerá una función de enlace para garantizar la cooperación transfronteriza entre las autoridades pertinentes de los Estados miembros y con el Grupo de cooperación y la red de CSIRT[19] creada por la propia Directiva. El considerando 31 y el artículo 8, apartado 4, explican la razón de ser de este requisito, a saber, facilitar la cooperación y comunicación transfronterizas. Esto resulta especialmente necesario teniendo en cuenta que los Estados miembros pueden optar por designar a más de una autoridad nacional. Así, un punto de contacto único facilitaría la identificación y cooperación de autoridades de diferentes Estados miembros.

La función de enlace del punto de contacto único puede implicar la interacción con los secretariados del Grupo de cooperación y de la red de CSIRT en los casos en los que el punto de contacto único nacional no sea un CSIRT ni un miembro del Grupo de cooperación. Además, los Estados miembros deben garantizar que el punto de contacto único sea informado de las notificaciones recibidas de operadores de servicios esenciales y proveedores de servicios digitales[20].

El artículo 8, apartado 3, de la Directiva especifica que, si un Estado miembro adopta un planteamiento centralizado, es decir, designa a una sola autoridad competente, esa autoridad ejercerá también la función de punto de contacto único. Si un Estado miembro opta por un planteamiento descentralizado, podrá elegir a una de las distintas autoridades competentes para que ejerza de punto de contacto único. Con independencia del modelo institucional elegido, siempre que una autoridad competente, el CSIRT y el punto de contacto único sean entidades distintas, los Estados miembros tendrán la obligación de garantizar la cooperación efectiva entre todos ellos para cumplir las obligaciones de la Directiva[21].

A más tardar el 9 de agosto de 2018 y, a partir de entonces, una vez al año, el punto de contacto único deberá presentar al Grupo de cooperación un informe resumido sobre las notificaciones recibidas, con mención del número de notificaciones y de la naturaleza de los incidentes notificados, así como de las medidas adoptadas por las autoridades, tales como informar a otros Estados miembros sobre el incidente o facilitar información pertinente a la empresa notificante para la gestión del incidente[22]. A petición de la autoridad competente o del CSIRT, el punto de contacto único deberá transmitir las notificaciones de operadores de servicios esenciales a los puntos de contacto únicos de los demás Estados miembros afectados por los incidentes[23].

Los Estados miembros deben informar a la Comisión sobre la designación del punto de contacto único y sus funciones dentro del plazo de transposición. La designación del punto de contacto único debe hacerse pública del mismo modo que la designación de las autoridades

[19] Una red de CSIRT nacionales para la cooperación operativa entre Estados miembros de conformidad con el artículo 12.
[20] Véase el artículo 10, apartado 3.
[21] Véase el artículo 10, apartado 1.
[22] *Ídem*.
[23] Véase el artículo 14, apartado 5.

nacionales competentes. La Comisión publicará la lista de los puntos de contacto únicos designados.

3.7. Sanciones

El artículo 21 ofrece margen a los Estados miembros para decidir el tipo y la naturaleza de las sanciones aplicables, a condición de que sean efectivas, proporcionadas y disuasorias. En otras palabras, en principio los Estados miembros tienen libertad para decidir el importe máximo de las sanciones que van a fijar en su legislación nacional, pero el importe o porcentaje fijado debería permitir que las sanciones impuestas en cada caso concreto por las autoridades nacionales fueran efectivas, proporcionadas y disuasorias, tomando en consideración distintos factores, tales como la gravedad o frecuencia de la infracción.

4. Entidades sujetas a obligaciones en materia de requisitos de seguridad y notificación de incidentes

Las entidades que desempeñan una función importante para la sociedad y la economía contempladas en el artículo 4, puntos 4 y 5, de la Directiva en calidad de operadores de servicios esenciales y proveedores de servicios digitales deben adoptar medidas de seguridad adecuadas y notificar los incidentes graves a las autoridades nacionales pertinentes. La razón de ser de ese requisito es que las repercusiones de los incidentes de seguridad en esos servicios pueden representar una grave amenaza para el funcionamiento de las actividades económicas y la sociedad en su conjunto, lo que puede menoscabar la confianza del usuario y causar graves daños a la economía de la Unión[24].

En esta sección se ofrece una visión de conjunto de las entidades incluidas en el ámbito de aplicación de los anexos II y III de la Directiva SRI y se enumeran sus obligaciones. Se analiza en profundidad el proceso de identificación de los operadores de servicios esenciales, dada su importancia para la aplicación armonizada de la Directiva SRI en toda la UE. Asimismo, se detallan las definiciones de los conceptos de infraestructuras digitales y proveedores de servicios digitales. Por otro lado, se examina la posibilidad de incluir otros sectores y se explica el planteamiento específico respecto a los proveedores de servicios digitales.

4.1. Operadores de servicios esenciales

La Directiva SRI no define explícitamente qué entidades concretas serán consideradas operadores de servicios esenciales comprendidos en su ámbito de aplicación. Más bien, presenta una serie de criterios que los Estados miembros tendrán que aplicar en un proceso de identificación que, en última instancia, determinará qué empresas concretas del tipo de entidades enumeradas en el anexo II se considerarán operadores de servicios esenciales y, por tanto, quedarán sujetos a las obligaciones de la Directiva.

[24] Véase el considerando 2.

4.1.1. Tipo de entidades enumeradas en el anexo II de la Directiva SRI

El artículo 4, punto 4, define a los operadores de servicios esenciales como entidades públicas o privadas de los tipos que figuran en el anexo II que reúnen los criterios establecidos en el artículo 5, apartado 2. En el anexo II se enumeran los sectores, subsectores y tipos de entidades respecto a los cuales los Estados miembros deben llevar a cabo el proceso de identificación previsto en el artículo 5, apartado 2[25]. Los sectores comprendidos son la energía, el transporte, la banca, las infraestructuras de los mercados financieros, el sector sanitario, el suministro y la distribución de agua potable y la infraestructura digital.

Respecto a la mayoría de entidades pertenecientes a los «sectores tradicionales», la legislación de la UE contiene definiciones bien arraigadas a las que remite el anexo II. Ahora bien, no este el caso del sector de la infraestructura digital (anexo II, punto 7), que incluye los puntos de intercambio de internet, los sistemas de nombres de dominio y los registros de nombres de dominio de primer nivel. A continuación, por tanto, se explican de manera pormenorizada esas definiciones con objeto de precisar su alcance.

1) Punto de intercambio de internet (IXP)

El término «punto de intercambio de internet» (IXP) se define en el artículo 4, punto 13, y se precisa en el considerando 18, pudiéndose describir como una instalación de la red que permite interconectar más de dos sistemas autónomos técnicamente independientes, principalmente para facilitar el intercambio de tráfico de internet. Un IXP puede describirse también como una ubicación física en la que una serie de redes pueden intercambiar entre sí tráfico de internet a través de un conmutador. El objetivo primordial de un IXP es permitir la interconexión directa de redes mediante el intercambio, en vez de a través de una o más redes de terceros. Por lo general, el proveedor de IXP no es responsable del enrutamiento del tráfico de internet. Del enrutamiento del tráfico se encargan los proveedores de redes. Las ventajas de la interconexión directa son numerosas, pero las principales aluden al coste, la latencia y el ancho de banda. Generalmente, el tráfico que pasa a través de un punto de intercambio no lo factura ninguna de las partes, mientras que el tráfico en el que interviene un proveedor de servicios de internet ascendente sí se factura. La interconexión directa, a menudo situada en la misma ciudad que ambas redes, evita la necesidad de que los datos tengan que recorrer largas distancias para desplazarse de una red a otra, de modo que se reduce la latencia.

Cabe señalar que la definición de IXP no comprende los puntos físicos en los que solamente se conectan dos redes físicas (es decir, proveedores de redes como BASE y Proximus). Por tanto, en la transposición de la Directiva, los Estados miembros deben diferenciar entre los operadores que facilitan el intercambio de tráfico agregado de internet entre múltiples operadores de redes y aquellos que son operadores de una sola red, que conectan físicamente sus redes sobre la base de un acuerdo de interconexión. En este último caso, los proveedores de redes no están comprendidos en la definición del artículo 4, punto 13. Esta cuestión se aclara en el considerando 18, donde se señala que el IXP no proporciona acceso a la red ni actúa como proveedor o transportista de servicios de tránsito. La última categoría de

[25] Para más detalles sobre el proceso de identificación, véase la sección 4.1.6.

proveedores la constituyen las empresas que suministran redes o servicios públicos de comunicaciones, que están sujetas a las obligaciones de seguridad y notificación establecidas en los artículos 13 *bis* y 13 *ter* de la Directiva 2002/21/CE y, por tanto, no entran en el ámbito de aplicación de la Directiva SRI[26].

2) Sistema de nombres de dominio (DNS)

El término «servidor de sistema de nombres de dominio» se define en el artículo 4, punto 14, como un *sistema de nombres de dominio distribuido jerárquicamente en una red que recibe consultas sobre nombres de dominio*. Más precisamente, el DNS puede describirse como un sistema de nombres de dominio distribuido jerárquicamente para ordenadores, servicios o cualquier otro recurso conectado a internet que permite la codificación de nombres de dominio en direcciones IP (Protocolo de Internet). La función principal del sistema consiste en traducir los nombres de dominio asignados en direcciones IP. A tal fin, el DNS opera una base de datos y utiliza servidores de nombres y resolutores para permitir este tipo de «traducción» de los nombres de dominio en direcciones IP operativas. Aunque la codificación de nombres de dominio no es la única responsabilidad del DNS, es una función esencial del sistema. La definición legal del artículo 4, punto 14, se centra en la función principal del sistema desde el punto de vista del usuario, sin entrar en más pormenores técnicos, como por ejemplo la gestión de espacio de nombres de dominio, servidores de nombres, resolutores, etc. Por último, el artículo 4, punto 15, aclara quién debe considerarse proveedor de servicios de DNS.

3) Registro de nombres de dominio de primer nivel (registro de nombres TLD)

El registro de nombres de dominio de primer nivel se define en el artículo 4, punto 16, como una entidad que administra y dirige el registro de nombres de dominio de internet en un dominio específico de primer nivel. La administración y gestión de los nombres de dominio incluye la codificación de nombres TLD en direcciones IP.

La Agencia de asignación de números de Internet (IANA, Internet Assigned Numbers Authority) es responsable de la coordinación global de la raíz del DNS, la asignación de direcciones IP y otros recursos IP. En concreto, tiene la responsabilidad de asignar dominios de primer nivel genéricos (gTLD) —p. ej., «com»— y dominios de primer nivel de código de país (ccTLD) —p. ej., «be»— a operadores (registros) y gestionar sus pormenores técnicos y administrativos. La IANA mantiene un registro global de los TLD asignados y desempeña una labor en la difusión de esa lista a usuarios de internet a nivel mundial, así como en la introducción de TLD nuevos.

Una labor importante de los registros consiste en asignar nombres de segundo nivel a los registrantes en su TLD respectivo. Por su parte, los registrantes también pueden, si lo desean, asignar nombres de dominio de tercer nivel. Los ccTLD son designados para representar a un país o territorio sobre la base de la norma ISO 3166-1. Por lo general, los TLD genéricos no tienen una designación geográfica o de país.

[26] Para más detalles sobre las relaciones entre la Directiva SRI y la Directiva 2002/21/CE, véase la sección 5.2.

Conviene señalar que la gestión de un registro de nombres TLD puede incluir la prestación de servicios de DNS. Por ejemplo, en virtud de las normas de delegación de la IANA, la entidad designada que se encarga de un ccTLD debe, entre otras cosas, supervisar los nombres de dominio y gestionar el DNS de ese país[27]. Los Estados miembros deben tener en cuenta esas circunstancias en el proceso de identificación de operadores de servicios esenciales en el marco del artículo 5, apartado 2.

4.1.2. Identificación de operadores de servicios esenciales

De conformidad con los requisitos del artículo 5 de la Directiva, cada Estado miembro debe llevar a cabo un proceso de identificación de todas las entidades de los tipos enumerados en el anexo II que tengan un establecimiento legal en su territorio. Como resultado de esa evaluación, todas las entidades que reúnan los criterios establecidos en el artículo 5, apartado 2, serán identificadas como operadores de servicios esenciales y quedarán sujetas a las obligaciones de seguridad y notificación del artículo 14.

Los Estados miembros tienen de plazo hasta el 9 de noviembre de 2018 para identificar a los operadores de servicios esenciales de cada sector y subsector. Con objeto de ayudar a los Estados miembros a lo largo de este proceso, el Grupo de cooperación está preparando un documento de orientación con información pertinente sobre los pasos necesarios y las mejores prácticas en relación con la identificación de operadores de servicios esenciales.

Además, de conformidad con el artículo 24, apartado 2, el Grupo de cooperación examinará el proceso, el contenido y el tipo de medidas nacionales que permitan la identificación de los operadores de servicios esenciales en sectores específicos. Antes del 9 de noviembre de 2018, los Estados miembros pueden pedir que el Grupo de Coordinación examine sus proyectos de medidas nacionales para la identificación de los operadores de servicios esenciales.

4.1.3. Incorporación de sectores adicionales

Teniendo en cuenta el requisito de armonización mínima recogido en el artículo 3, los Estados miembros pueden adoptar o mantener legislación que garantice un elevado nivel de seguridad de las redes y sistemas de información. En este contexto, por lo general los Estados miembros tienen libertad para hacer extensivas las obligaciones de seguridad y notificación previstas en el artículo 14 a entidades de sectores y subsectores distintos de los enumerados en el anexo II de la Directiva SRI. Varios Estados miembros han decidido o están considerando incluir algunos de los sectores adicionales que figuran a continuación:

i) Administraciones públicas

Las administraciones públicas pueden ofrecer servicios esenciales comprendidos en el anexo II de la Directiva que reúnan los requisitos del artículo 5, apartado 2. En tales casos, las administraciones públicas que ofrezcan esos servicios quedarán sujetas a los correspondientes requisitos de seguridad y obligaciones de notificación. A la inversa, si las administraciones públicas ofrecen servicios que no entran en el ámbito indicado, no quedarán sujetas a las obligaciones correspondientes.

Las administraciones públicas son responsables de la correcta prestación de servicios públicos por parte de organismos gubernamentales, autoridades regionales y locales, agencias

[27] Información disponible en: https://www.icann.org/resources/pages/delegation-2012-02-25-en

y empresas asociadas. Esos servicios a menudo implican la elaboración y gestión de datos personales y corporativos sobre personas y organizaciones, que pueden compartirse y ponerse a disposición de numerosas entidades públicas. En un sentido más amplio, un elevado nivel de seguridad de las redes y sistemas de información utilizados por las administraciones públicas reviste gran importancia para la sociedad y la economía en su conjunto. Por tanto, la Comisión considera que sería conveniente que los Estados miembros consideraran la inclusión de la administración pública en el ámbito de la legislación nacional de transposición de la Directiva, más allá de la prestación de servicios esenciales a que se refieren el anexo II y el artículo 5, apartado 2.

ii) Sector postal

El sector postal comprende la prestación de servicios postales, tales como la recogida, la clasificación, el transporte y la distribución de envíos postales.

iii) Sector alimentario

El sector alimentario comprende la producción de productos agrícolas y otros productos alimentarios y podría incluir servicios esenciales, tales como la seguridad alimentaria y la garantía de calidad y seguridad de los productos alimentarios.

iv) Industria química y nuclear

La industria química y nuclear incluye, en particular, el almacenamiento, la producción y el tratamiento de productos químicos y petroquímicos o materiales nucleares.

v) Sector medioambiental

Las actividades medioambientales abarcan el suministro de los bienes y servicios necesarios para proteger el medio ambiente y gestionar los recursos. Por tanto, esas actividades tienen por objeto prevenir, reducir y eliminar la contaminación y preservar los recursos naturales disponibles. En este sector podrían ser servicios esenciales el seguimiento y control de la contaminación (p. ej., del aire y el agua) y de fenómenos meteorológicos.

vi) Protección civil

El objetivo del sector de la protección civil es prevenir las catástrofes naturales y las provocadas por el hombre, así como prepararse ante tales catástrofes y responder a ellas. Los servicios prestados en este ámbito pueden ser la activación de números de emergencia y la aplicación de medidas de información, contención y respuesta en materia de emergencias.

4.1.4. Competencia

Con arreglo al artículo 5, apartado 1, cada Estado miembro debe identificar a los operadores de servicios esenciales establecidos en su territorio. Esa disposición no especifica el tipo de establecimiento legal, pero el considerando 21 aclara que tal establecimiento implica el ejercicio real y efectivo de una actividad mediante una organización estable, y que la forma jurídica de dicha organización no es un factor determinante. Esto significa que un Estado miembro puede ser competente respecto a un operador de servicios esenciales no solo cuando el operador tiene su domicilio social en su territorio, sino también cuando tiene, por ejemplo, una sucursal u otro tipo de establecimiento legal.

Como consecuencia de ello, varios Estados miembros podrían ser competentes en paralelo respecto a la misma entidad.

4.1.5. Información que debe presentarse a la Comisión

A efectos de la revisión que debe llevar a cabo la Comisión de conformidad con el artículo 23, apartado 1, de la Directiva SRI, los Estados miembros han de presentar a la Comisión, a más tardar el 9 de noviembre de 2018 y, a partir de entonces, cada dos años, la siguiente información:

- las medidas nacionales que permitan identificar a los operadores de servicios esenciales,
- la lista de servicios esenciales,
- el número de operadores de servicios esenciales identificados en cada uno de los sectores que figuran en el anexo II y una indicación de su importancia para dicho sector, y
- los umbrales, cuando existan, para determinar el nivel de suministro pertinente en función del número de usuarios que confían en ese servicio a que hace referencia el artículo 6, apartado 1, letra a), o la importancia de esa entidad a que hace referencia el artículo 6, apartado 1, letra f).

La revisión prevista en el artículo 23, apartado 1, que precede a la revisión completa de la Directiva, refleja la importancia que los colegisladores confieren a la correcta transposición de la Directiva en lo que respecta a la identificación de los operadores de servicios esenciales para evitar la fragmentación del mercado.

A fin de llevar a cabo ese proceso de la mejor manera posible, la Comisión anima a los Estados miembros a debatir este tema y a intercambiar experiencia pertinente en el Grupo de cooperación. Además, la Comisión anima a los Estados miembros a que compartan con la Comisión, en caso necesario sobre una base confidencial, las listas de los operadores de servicios esenciales identificados (que hayan sido seleccionados al término del proceso), además de toda la información que la Directiva les obliga a facilitar a la Comisión. La disponibilidad de esas listas facilitaría la evaluación de la coherencia del proceso de identificación por parte de la Comisión y mejoraría su calidad, y permitiría comparar los planteamientos de los distintos Estados miembros, lo que redundaría en una mejor consecución de los objetivos de la Directiva.

4.1.6. ¿Cómo debe llevarse a cabo el proceso de identificación?

Como muestra el gráfico 4, hay seis preguntas clave que debe analizar la autoridad nacional en el proceso de identificación de una entidad. En el párrafo siguiente, cada pregunta se corresponde con una de las etapas del proceso con arreglo al artículo 5, en combinación con el artículo 6, y teniendo en cuenta la aplicabilidad del artículo 1, apartado 7.

Primera etapa: **¿Pertenece la entidad a un sector/subsector y corresponde a un tipo de entidad de los enumerados en el anexo II de la Directiva?**

La autoridad nacional debe determinar si la entidad establecida en su territorio pertenece a uno de los sectores y subsectores enumerados en el anexo II de la Directiva. El anexo II incluye varios sectores económicos que se consideran importantes para garantizar el correcto

funcionamiento del mercado interior. En concreto, el anexo II se refiere a los siguientes sectores y subsectores:

- Energía: electricidad, crudo y gas.
- Transporte: aéreo, por ferrocarril, marítimo y fluvial y por carretera.
- Banca: entidades de crédito.
- Infraestructuras de los mercados financieros: gestores de centros de negociación y entidades de contrapartida central.
- Sector sanitario: entornos de asistencia sanitaria (entre ellos hospitales y clínicas privadas).
- Agua: suministro y distribución de agua potable.
- Infraestructura digital: puntos de intercambio de internet, proveedores de servicios de sistema de nombres de dominio y registros de nombres de dominio de primer nivel[28].

Segunda etapa: **¿Se aplica una *lex specialis*?**

En la siguiente etapa, la autoridad nacional debe valorar si se aplica la disposición sobre *lex specialis* establecida en el artículo 1, apartado 7. Esa disposición establece que, si un acto jurídico de la UE requiere que los operadores de servicios esenciales o los proveedores de servicios digitales cumplan requisitos de seguridad y/o notificación que tengan al menos un efecto equivalente al de los requisitos establecidos en la Directiva SRI, son de aplicación las obligaciones de la *lex specialis*. Además, el considerando 9 aclara que, si se cumplen los requisitos del artículo 1, apartado 7, los Estados miembros deben aplicar las disposiciones del acto jurídico sectorial de la UE, incluidas las relativas a cuestiones de competencia judicial. A la inversa, no se aplicarían las disposiciones pertinentes de la Directiva SRI. En este caso, la autoridad competente no debería proseguir el proceso de identificación con arreglo al artículo 5, apartado 2[29].

Tercera etapa: **¿Presta el operador un servicio esencial en la acepción de la Directiva?**

Con arreglo al artículo 5, apartado 2, letra a), la entidad sujeta al proceso de identificación debe prestar un servicio esencial para el mantenimiento de actividades sociales o económicas cruciales. En esta evaluación, el Estado miembro debe tener en cuenta que una entidad puede prestar servicios tanto esenciales como no esenciales. Esto significa que los requisitos de seguridad y notificación de la Directiva SRI se aplicarán a un operador determinado únicamente en la medida en que preste servicios esenciales.

De conformidad con el artículo 5, apartado 3, el Estado miembro debe establecer una lista de todos los servicios esenciales prestados por el operador de servicios esenciales en su territorio. Esta lista deberá presentarse a la Comisión a más tardar el 9 de noviembre de 2018 y, a partir de entonces, cada dos años[30].

Cuarta etapa: **¿Depende el servicio de una red y sistema de información?**

[28] Esas entidades se explican de forma más pormenorizada en la sección 4.1.1.

[29] Para más detalles sobre la aplicabilidad de *lex specialis,* véase la sección 5.1.

[30] Véase el artículo 5, apartado 7, letra b).

Además, debe determinarse si el servicio reúne el segundo criterio del artículo 5, apartado 2, letra b), en concreto si la prestación del servicio esencial depende de redes y sistemas de información conforme a la definición del artículo 4, punto 1.

Quinta etapa: **¿Tendría un incidente de seguridad un efecto perturbador significativo?**

El artículo 5, apartado 2, letra c), exige que la autoridad nacional determine si un incidente tendría un efecto perturbador significativo en la prestación del servicio. En este contexto, el artículo 6, apartado 1, establece varios factores intersectoriales que deben tenerse en cuenta al determinar la importancia de un efecto perturbador. Además, el artículo 6, apartado 2, establece que, cuando proceda, la determinación deberá tener también en cuenta factores específicos del sector.

Los **factores intersectoriales** enumerados en el artículo 6, apartado 1, son los siguientes:

- el número de usuarios que confían en los servicios prestados por la entidad de que se trate,
- la dependencia de otros sectores que figuran en el anexo II respecto al servicio prestado por esa entidad,
- la repercusión que podrían tener los incidentes, en términos de grado y duración, en las actividades económicas y sociales o en la seguridad pública,
- la cuota de mercado de la entidad,
- la extensión geográfica con respecto a la zona que podría verse afectada por un incidente,
- la importancia de la entidad para mantener un nivel suficiente del servicio, teniendo en cuenta la disponibilidad de alternativas para la prestación de ese servicio.

En cuanto a los **factores específicos del sector**, el considerando 28 ofrece algunos ejemplos (véase el cuadro 4) que pueden servir de orientación a las autoridades nacionales.

Cuadro 4: Ejemplos de factores específicos del sector que deben considerarse al determinar el efecto perturbador significativo en caso de incidente

Sector	Ejemplos de factores específicos del sector
Proveedores de energía	volumen o proporción de la energía nacional generada
Proveedores de petróleo	volumen diario suministrado
Transporte aéreo (incluidos aeropuertos y compañías aéreas) **Transporte ferroviario** **Puertos marítimos**	proporción del volumen de tráfico nacional, número de viajeros u operaciones de transporte de mercancías anuales
Banca o infraestructuras de los mercados financieros	su importancia sistémica, valorada según los activos totales o la razón entre estos y el PIB
Sector sanitario	número de pacientes atendidos cada año por el prestador de servicios sanitarios
Producción, tratamiento y abastecimiento de agua	volumen, número y tipos de usuarios abastecidos (incluidos, por ejemplo, hospitales, organismos que

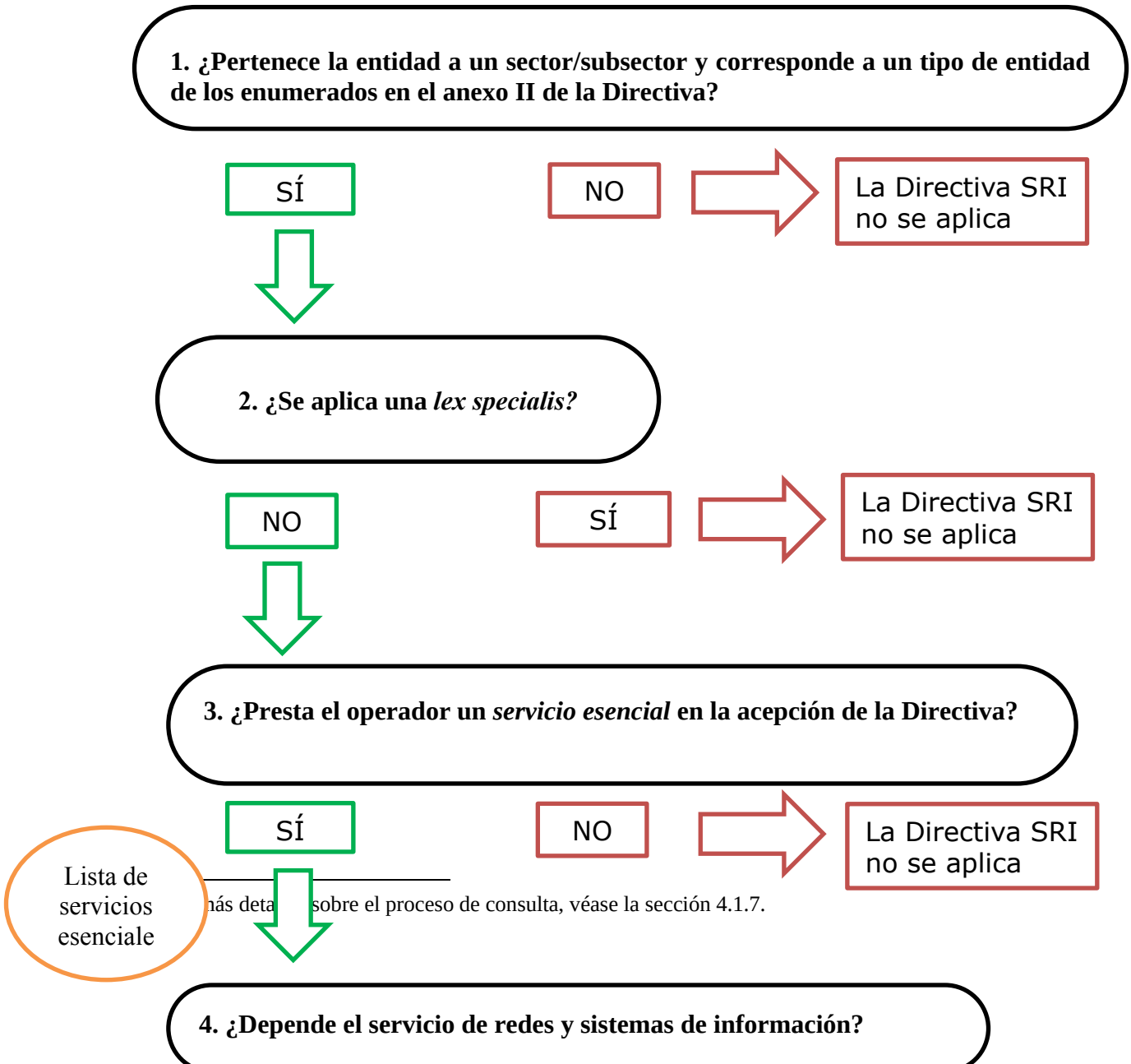
	presten servicios públicos o particulares), existencia de fuentes alternativas de suministro de agua para abastecer la misma zona geográfica

Debe subrayarse que, en la evaluación con arreglo al artículo 5, apartado 2, los Estados miembros no deben añadir criterios a los enumerados en esa disposición, porque ello podría reducir el número de operadores de servicios esenciales identificados y poner en peligro la armonización mínima respecto a esos operadores prevista en el artículo 3 de la Directiva.

Sexta etapa: **¿Presta el operador servicios esenciales en otros Estados miembros?**

Esta etapa se aplica en los casos en los que un operador presta sus servicios esenciales en dos o más Estados miembros. Antes de completar el proceso de identificación, el artículo 5, apartado 4, exige a los Estados miembros afectados que emprendan un proceso de consulta[31].

Gráfico 4: El proceso de identificación en seis etapas



[31] ...más deta... sobre el proceso de consulta, véase la sección 4.1.7.

5. ¿Tendría un incidente de seguridad un efecto perturbador significativo?

Factores intersectoriales (artículo 6, apartado 1)

- **Número de usuarios** que confían en los servicios
- **Dependencia** de otros sectores esenciales respecto al servicio
- Repercusión que podrían tener los incidentes en las **actividades económicas y sociales** o en la seguridad pública
- Posible **extensión geográfica**
- Importancia de la entidad para mantener un **nivel suficiente del servicio**

Factores específicos del sector (ejemplos mencionados en el considerando 28)

- **Energía**: volumen o proporción de la energía nacional generada
- **Transporte**: proporción del volumen de tráfico nacional y número de operaciones anuales
- **Sector sanitario**: número de pacientes atendidos cada año por el prestador de servicios sanitarios

SÍ

NO → La Directiva SRI no se aplica

6. ¿Presta el operador servicios esenciales en otros Estados miembros?

SÍ

NO → La Directiva SRI no se aplica

Consulta obligatoria con el Estado o Estados miembros afectados

Adopción de medidas nacionales (p. ej., lista de operadores de servicios esenciales, medidas políticas y legales)

4.1.7. Proceso de consulta transfronterizo

Cuando un operador presta servicios esenciales en dos o más Estados miembros, el artículo 5, apartado 4, exige a esos Estados miembros que emprendan consultas entre sí antes de completar el proceso de identificación. La finalidad de esas consultas es facilitar la evaluación sobre el carácter crítico del operador en términos de su impacto transfronterizo.

El resultado deseado de la consulta es que las autoridades nacionales afectadas intercambien argumentos y posiciones e, idealmente, lleguen al mismo resultado en la identificación del operador. Ahora bien, la Directiva SRI no impide que los Estados miembros lleguen a conclusiones divergentes acerca de si una entidad concreta se identifica o no como operador de servicios esenciales. El considerando 24 menciona la posibilidad de que los Estados miembros soliciten la asistencia del Grupo de Coordinación a este respecto.

En opinión de la Comisión, los Estados miembros deberían aspirar a alcanzar un consenso en la materia para evitar divergencias entre Estados miembros en lo que respecta al estatus legal de una misma empresa. Las divergencias deberían ser verdaderamente excepcionales y limitarse, por ejemplo, a los casos en los que una entidad identificada como operador de servicios esenciales en un Estado miembro ejerciera una actividad marginal y poco significativa en otro.

4.2. Requisitos de seguridad

Con arreglo al artículo 14, apartado 1, los Estados miembros deben velar por que, habida cuenta del estado de la técnica, los operadores de servicios esenciales tomen las medidas técnicas y de organización adecuadas y proporcionadas para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información que utilizan en la prestación de sus servicios. De conformidad con el artículo 14, apartado 2, se tomarán medidas adecuadas para prevenir y reducir al mínimo los efectos de los incidentes.

En una línea de trabajo específica del Grupo de Coordinación se están preparando actualmente unas orientaciones no vinculantes sobre las medidas de seguridad relativas a los operadores de servicios esenciales[32]. Está previsto que el Grupo tenga listo el documento de orientación en el cuarto trimestre de 2017. La Comisión anima a los Estados miembros a que sigan de cerca el documento de orientación del Grupo de Coordinación, de tal modo que las disposiciones nacionales sobre requisitos de seguridad estén lo más alineadas posible. La armonización de tales requisitos facilitaría en gran medida la conformidad de los operadores de servicios esenciales que a menudo prestan servicios esenciales en más de un Estado miembro y la labor de supervisión de las autoridades nacionales competentes y los CSIRT.

4.3. Requisitos de notificación

De conformidad con el artículo 14, apartado 3, los Estados miembros deben velar por que los operadores de servicios esenciales notifiquen *los incidentes que tengan efectos significativos en la continuidad de los servicios esenciales que prestan*. Por tanto, los operadores de

[32] En el marco de esta línea de trabajo, se distribuyeron listas de normas internacionales, buenas prácticas y metodologías de evaluación y gestión de riesgos en todos los sectores comprendidos en la Directiva SRI, que se utilizaron como aportaciones para la propuesta de medidas en el ámbito de la seguridad.

servicios esenciales no deben notificar los incidentes leves, sino solamente los incidentes graves que afecten a la continuidad del servicio esencial. En el artículo 4, punto 7, se define un incidente como *todo hecho que tenga efectos adversos reales en la seguridad de las redes y sistemas de información*. El término «seguridad de las redes y sistemas de información» se define en el artículo 4, punto 2, como *la capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos*. Así pues, todo hecho que tenga efectos adversos, no solo para la disponibilidad, sino también para la autenticidad, integridad o confidencialidad de los datos o los servicios correspondientes podría desencadenar la obligación de notificación. De hecho, la continuidad del servicio a que se refiere el artículo 14, apartado 3, puede verse en peligro no solo cuando el incidente afecta a la disponibilidad física, sino también cuando cualquier otro incidente de seguridad afecta a la prestación del servicio en sí misma[33].

En una línea de trabajo específica del Grupo de Coordinación se están preparando actualmente unas orientaciones no vinculantes sobre notificación que abordan las circunstancias en las que los operadores de servicios esenciales deben notificar incidentes con arreglo al artículo 14, apartado 7, así como el formato y el procedimiento de las notificaciones nacionales. Está previsto que las orientaciones estén listas en el cuarto trimestre de 2017.

La aplicación de requisitos nacionales de notificación diferentes puede entrañar inseguridad jurídica, procedimientos más complejos y farragosos, así como considerables gastos administrativos para los proveedores que desarrollan actividades transfronterizas. Por tanto, la Comisión acoge con satisfacción el trabajo del Grupo de cooperación. Al igual que en el caso de los requisitos de seguridad, la Comisión anima a los Estados miembros a que sigan de cerca el documento de orientación del Grupo de Coordinación, de tal modo que las disposiciones nacionales sobre la notificación de incidentes estén lo más alineadas posible.

4.4. Directiva SRI, anexo III: Proveedores de servicios digitales

Los proveedores de servicios digitales forman la segunda categoría de entidades incluidas en el ámbito de aplicación de la Directiva SRI. Esas entidades se consideran agentes económicos importantes por el hecho de que son utilizadas por muchas empresas para la prestación de sus propios servicios y de que una perturbación del servicio digital podría repercutir en las actividades sociales o económicas clave.

4.4.1. Categorías de proveedores de servicios digitales

El artículo 4, punto 5, que define los servicios digitales, remite a la definición del artículo 1, apartado 1, letra b), de la Directiva (UE) 2015/1535, reduciendo su alcance a los tipos de servicios que figuran en el anexo III. En concreto, el artículo 1, apartado 1, letra b), de la Directiva (UE) 2015/1535 define esos servicios como *todo servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios*, y el anexo III de la Directiva enumera tres tipos específicos de

[33] Lo mismo es aplicable a los proveedores de servicios digitales.

servicios: mercados en línea, motores de búsqueda en línea y servicios de computación en la nube. A diferencia de los operadores de servicios esenciales, la Directiva no exige a los Estados miembros que identifiquen a los proveedores de servicios digitales, que quedarían a continuación sujetos a las obligaciones pertinentes. Así pues, las obligaciones pertinentes de la Directiva, concretamente los requisitos de seguridad y notificación establecidos en el artículo 16, se aplicarán a todos los proveedores de servicios digitales comprendidos en su ámbito de aplicación.

En las secciones que figuran a continuación se facilitan explicaciones complementarias sobre los tres tipos de servicios digitales incluidos en el ámbito de aplicación de la Directiva.

1. Mercados en línea

Los mercados en línea permiten a un gran número y un amplio abanico de empresas ejercer sus actividades comerciales respecto a los consumidores y emprender relaciones con otras empresas. Proporcionan a las empresas la infraestructura básica para comerciar en línea y a través de las fronteras. Esos mercados desempeñan un papel significativo en la economía, sobre todo porque brindan a las pymes acceso al mercado único digital de la UE en su sentido más amplio. La prestación de servicios informáticos remotos que facilitan la actividad económica del cliente, que incluyen la tramitación de transacciones y la agregación de datos sobre compradores, proveedores y productos, también puede enmarcarse en las actividades de un mercado en línea, al igual que la facilitación de búsquedas de productos adecuados, el suministro de productos, los conocimientos especializados sobre transacciones y la coincidencia de compradores y vendedores.

El término «mercado en línea» se define en el artículo 4, punto 17, y se precisa en el considerando 15. Se describe como un servicio que permite a los consumidores y comerciantes celebrar contratos de compraventa o de servicios en línea con comerciantes, y que representa el destino final de la celebración de tales contratos. Por ejemplo, un proveedor como *E-bay* puede considerarse un mercado en línea, pues permite a otros establecer puntos de venta en su plataforma para que los consumidores y empresas puedan acceder en línea a sus productos y servicios. Igualmente, las tiendas de aplicaciones en línea que distribuyen aplicaciones y programas de *software* se consideran comprendidas en la definición de mercado en línea, porque permiten a los desarrolladores de aplicaciones vender o distribuir sus servicios a los consumidores o a otras empresas. En cambio, los intermediarios para acceder a servicios prestados por terceros, tales como *Skyscanner* y los servicios de comparación de precios, que redirigen al usuario al sitio web del comerciante donde se celebra el contrato real para el servicio o producto, no están comprendidos en la definición del artículo 4, punto 17.

2. Motores de búsqueda en línea

El término «motor de búsqueda en línea» se define en el artículo 4, punto 18, y se precisa en el considerando 16. Se describe como un servicio digital que permite a los usuarios hacer búsquedas en todos los sitios web, en principio, o en sitios web en una lengua en concreto mediante una consulta sobre cualquier tema. Las funciones de búsqueda que se limitan a buscar contenidos en un sitio web concreto y los sitios web de comparación de precios no están comprendidos en esa definición. Por ejemplo, el tipo de motor de búsqueda como el que

ofrece EUR LEX[34] no puede considerarse un motor de búsqueda en la acepción de la Directiva, pues su función de búsqueda se limita al contenido de ese sitio web específico.

3. Servicios de computación en la nube

El artículo 4, punto 19, describe el servicio de computación en la nube como *un servicio digital que hace posible el acceso a un conjunto modulable y elástico de recursos informáticos que se pueden compartir*, y el considerando 17 aclara los términos «servicios de computación», «modulable» y «elástico».

En resumen, la computación en la nube puede definirse como un tipo específico de servicio de computación que utiliza recursos compartidos para el tratamiento de datos a petición del usuario, mientras que los recursos compartidos son cualquier tipo de componentes de hardware o software (p. ej., redes, servidores u otras infraestructuras, sistemas de almacenamiento, aplicaciones y servicios) que se entregan previa petición a los usuarios para el tratamiento de datos. El término «que se pueden compartir» se refiere a los recursos informáticos que se proporcionan a múltiples usuarios que utilizan la misma infraestructura física para el tratamiento de datos. Se puede decir que los recursos informáticos se pueden compartir cuando el conjunto de recursos utilizados por el proveedor puede ampliarse o reducirse en cualquier momento, en función de los requisitos del usuario. Así, cabría la posibilidad de añadir o retirar centros de datos o componentes individuales dentro de un centro de datos en caso de que la cantidad total de capacidad de computación o almacenamiento necesitara una actualización. El término «conjunto elástico» se utiliza para describir los cambios en la carga de trabajo resultantes del abastecimiento y desabastecimiento de recursos de manera automática, de tal manera que en cada momento los recursos disponibles coincidan con la demanda en la mayor medida posible[35].

Actualmente, existen tres tipos principales de modelos de servicios de computación en la nube que puede ofrecer un proveedor:

- Infraestructura como servicio (*Infrastructure as a Service*, IaaS): Categoría de servicio en nube en la que el tipo de capacidades en nube que se proporcionan al cliente es una infraestructura. Incluye la entrega virtual de recursos informáticos en forma de hardware, servicios de redes y de almacenamiento. La IaaS presta servicio a servidores, sistemas de almacenamiento, redes y sistemas operativos. Proporciona infraestructura empresarial en la que una empresa puede almacenar sus datos y hacer funcionar las aplicaciones necesarias para sus actividades cotidianas.

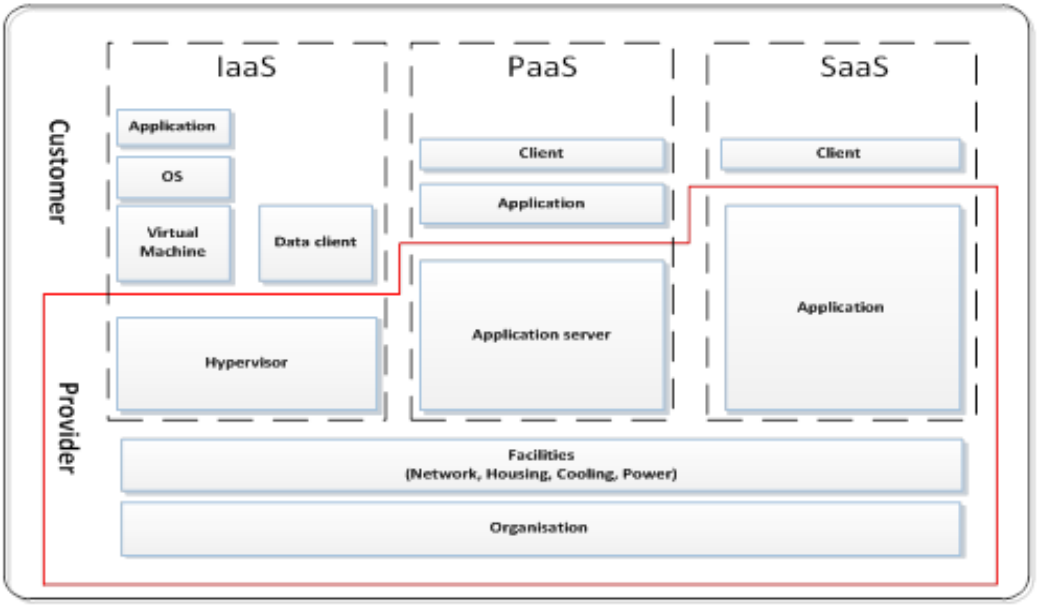
- Plataforma como servicio (*Platform as a Service*, PaaS): Categoría de servicio en nube en la que el tipo de capacidades en nube que se proporcionan al cliente es una plataforma. Incluye plataformas informáticas en línea que permiten a las empresas hacer funcionar aplicaciones existentes o desarrollar y probar aplicaciones nuevas.

[34] Disponible en: http://eur-lex.europa.eu/homepage.html.

[35] Nikolas Roman Herbst, Samuel Kounev, Ralf Reussner, Karlsruhe Institute of Technology, *Elasticity in Cloud Computing: What It Is, and What It Is Not*, disponible en: https://sdqweb.ipd.kit.edu/publications/pdfs/HeKoRe2013-ICAC-Elasticity.pdf. Véanse también las páginas 2-5 del documento COM(2012) 529.

- Software como servicio (*Software as a service*, SaaS): Categoría de servicio en nube en la que el tipo de capacidades en nube que se proporcionan al cliente es una aplicación o software desplegado en internet. Este tipo de servicios en nube eliminan la necesidad de que el usuario final compre, instale y gestione software, y presenta la ventaja de que se puede acceder al software desde cualquier lugar que disponga de una conexión a internet.

Gráfico 5: Modelos de servicio y activos de la computación en la nube



ENISA ha elaborado extensas directrices sobre temas específicos en el ámbito de la computación en la nube[36] y un documento de orientación sobre los fundamentos de la computación en la nube[37].

4.4.2. Requisitos de seguridad

Con arreglo al artículo 16, apartado 1, los Estados miembros deben velar por que los proveedores de servicios digitales tomen medidas técnicas y de organización adecuadas y proporcionadas para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información que las empresas utilizan en la prestación de sus servicios. Esas medidas deben tener en cuenta los avances técnicos y los cinco elementos siguientes: i) la seguridad de los sistemas e instalaciones; ii) la gestión de incidentes; iii) la gestión de la continuidad de las actividades; iv) la supervisión, auditorías y pruebas; v) el cumplimiento de las normas internacionales.

En este contexto, la Comisión está facultada, en virtud del artículo 16, apartado 8, para adoptar actos de ejecución que especifiquen de forma más pormenorizada esos elementos y garanticen un elevado nivel de armonización de esos proveedores de servicios. Está previsto

[36] Disponible en: https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security
[37] ENISA, *Cloud Security Guide for SMEs (2015).* Disponible en: https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes

que la Comisión adopte el acto de ejecución en el otoño de 2017. Además, se exige a los Estados miembros que velen por que los proveedores de servicios digitales tomen las medidas necesarias para prevenir y reducir al mínimo las repercusiones de los incidentes a fin de garantizar la continuidad de sus servicios.

4.4.3. Requisitos de notificación

Debe exigirse a los proveedores de servicios digitales que notifiquen los incidentes graves a las autoridades competentes o los CSIRT. De conformidad con el artículo 16, apartado 3, de la Directiva SRI, el requisito de notificación por parte de los proveedores de servicios digitales se activará cuando el incidente de seguridad tenga un impacto significativo en la prestación del servicio. Para determinar el impacto, el artículo 16, apartado 4, enumera cinco parámetros que deben considerar los proveedores de servicios digitales. A este respecto, la Comisión está facultada, en virtud del artículo 16, apartado 8, para adoptar actos de ejecución que proporcionen descripciones más detalladas de esos parámetros. La especificación de esos parámetros formará parte del acto de ejecución en el que se especifiquen los elementos de seguridad mencionados en el punto 4.4.2 que la Comisión pretende adoptar en otoño.

4.4.4. Enfoque normativo basado en los riesgos

El artículo 17 establece que los proveedores de servicios digitales están sujetos a supervisión *ex post* por parte de las autoridades nacionales competentes. Los Estados miembros deben velar por que las autoridades competentes tomen medidas cuando tengan pruebas de que un proveedor de servicios digitales no cumple los requisitos del artículo 16 de la Directiva.

Por otro lado, en virtud del artículo 16, apartados 8 y 9, la Comisión está facultada para adoptar actos de ejecución respecto a los requisitos de notificación y de seguridad que eleven el grado de armonización respecto a los proveedores de servicios digitales. Además, el artículo 16, apartado 10, prohíbe a los Estados miembros imponer a los proveedores de servicios digitales requisitos de seguridad y notificación adicionales a los previstos en la Directiva, excepto en los casos en los que esas medidas son necesarias para salvaguardar sus funciones estatales esenciales, en particular para salvaguardar la seguridad nacional, y para permitir la investigación, la detección y el enjuiciamiento de infracciones penales.

Por último, teniendo en cuenta la naturaleza transfronteriza de los servicios digitales, la Directiva no sigue el modelo de la competencia múltiple paralela, sino un enfoque basado en el criterio del establecimiento principal de la empresa en la UE[38]. De acuerdo con este enfoque, a los proveedores de servicios digitales se les aplicará un único conjunto de normas, y una sola autoridad competente será responsable de la supervisión, que resulta especialmente importante teniendo en cuenta que muchos proveedores de servicios digitales ofrecen sus servicios en muchos Estados miembros simultáneamente. La aplicación de este enfoque reduce al mínimo la carga de los proveedores de servicios digitales en materia de cumplimiento y garantiza el correcto funcionamiento del mercado único digital.

4.4.5. Competencia

Como se ha explicado anteriormente, el artículo 18, apartado 1, de la Directiva establece que el proveedor de servicios digitales estará sometido a la competencia del Estado miembro en el

[38] Véase, en particular, el artículo 17 de la Directiva.

que se encuentre su establecimiento principal. De acuerdo con el artículo 18, apartado 2, un proveedor de servicios digitales que presta servicios en la Unión pero no está establecido en su territorio debe designar a un representante en la Unión. En ese caso, la empresa estará sometida a la competencia del Estado miembro en el que se encuentre establecido su representante. En principio, un Estado miembro podrá emprender acciones contra un proveedor de servicios digitales que preste servicios en su territorio, pero no haya designado a un representante en la UE, por infringir las obligaciones que le impone la Directiva.

4.4.6. Exención de los proveedores de servicios digitales de escala reducida del ámbito de aplicación de los requisitos de seguridad y notificación

De conformidad con el artículo 16, apartado 11, los proveedores de servicios digitales que son microempresas o pequeñas empresas según la definición de la Recomendación 2003/361/CE de la Comisión[39] están excluidos del ámbito de aplicación de los requisitos de seguridad y notificación establecidos en el artículo 16. Es decir, las empresas que ocupan a menos de 50 personas y cuyo volumen de negocios anual o balance general anual no excede de 10 millones EUR no están sujetas a esos requisitos. Al determinar el tamaño de la entidad, es irrelevante si la empresa presta solamente servicios digitales en la acepción de la Directiva SRI o también otros servicios.

5. Las relaciones entre la Directiva SRI y otros actos legislativos

Esta sección centra su atención en las disposiciones sobre *lex specialis* establecidas en el artículo 1, apartado 7, de la Directiva SRI, e ilustra los tres ejemplos de *lex specialis* analizados por la Comisión hasta ahora, que aclaran la aplicación de los requisitos de seguridad y notificación a los proveedores de servicios de telecomunicaciones y de confianza.

5.1. Artículo 1, apartado 7, de la Directiva SRI: Disposición sobre *lex specialis*

De conformidad con el artículo 1, apartado 7, de la Directiva SRI, las disposiciones sobre los requisitos de seguridad y notificación aplicables a los proveedores de servicios digitales u operadores de servicios esenciales en el marco de la Directiva no se aplican si una legislación sectorial de la UE establece requisitos de seguridad y notificación que tengan al menos un efecto equivalente al de las obligaciones establecidas en la Directiva SRI. Los Estados miembros deben considerar el artículo 1, apartado 7, en la transposición completa de la Directiva y facilitar información a la Comisión sobre la aplicación de disposiciones de *lex specialis*.

Metodología

Al determinar la equivalencia de un acto legislativo sectorial de la UE con las disposiciones correspondientes de la Directiva SRI, debe atribuirse una especial importancia a la cuestión de si las obligaciones de seguridad establecidas en la legislación sectorial comprenden medidas que garanticen la seguridad de las redes y sistemas de información tal como se define en el artículo 4, punto 2, de la Directiva.

[39] DO L 24 de 20.5.2003, p. 36.

En cuanto a los requisitos de notificación, el artículo 14, apartado 3, y el artículo 16, apartado 3, de la Directiva SRI establecen que los operadores de servicios esenciales y los proveedores de servicios digitales deben notificar sin dilación indebida a las autoridades competentes o al CSIRT cualquier incidente que tenga un impacto significativo/sustancial en la prestación del servicio. En este contexto, debe prestarse especial atención a la obligación del operador o proveedor de servicios digitales de incluir en la notificación información que permita a la autoridad competente o al CSIRT determinar cualquier impacto transfronterizo de un incidente de seguridad.

Actualmente no hay legislación sectorial relativa a la categoría de proveedores de servicios digitales que establezca requisitos de seguridad y notificación comparables a los establecidos en el artículo 16 de la Directiva SRI que puedan considerarse en la aplicación del artículo 1, apartado 7, de la Directiva SRI[40].

En lo que respecta a los operadores de servicios esenciales, el sector financiero y, en particular, los sectores de la banca y las infraestructuras de los mercados financieros que figuran en los puntos 3 y 4 del anexo II están sujetos actualmente a requisitos de seguridad o notificación derivados de legislación sectorial de la UE. Esto se debe al hecho de que la seguridad y solidez de las TI y las redes y sistemas de información que utilizan las instituciones financieras es una parte esencial de los requisitos en materia de riesgos operativos que impone la legislación de la UE a las instituciones financieras.

Ejemplos

i) Directiva sobre servicios de pago 2

En el sector bancario y, más en concreto, respecto a la prestación de servicios de pago por parte de las entidades de crédito, tal como se definen en el artículo 4, punto 1, del Reglamento (UE) 575/2013, la Directiva sobre servicios de pago 2 (DSP 2)[41], establece, en sus artículos 95 y 96, requisitos de seguridad y notificación.

Más en concreto, el artículo 95, apartado 1, exige que los proveedores de servicios de pago adopten medidas paliativas y mecanismos de control adecuados para gestionar los riesgos operativos y de seguridad relacionados con los servicios de pago que prestan. Estas medidas deben implicar el establecimiento y mantenimiento de procedimientos eficaces de gestión de incidentes, en particular para la detección y la clasificación de los incidentes operativos y de seguridad de carácter grave. Los considerandos 95 y 96 de la DSP 2 precisan la naturaleza de tales medidas de seguridad. Cabe deducir de esas disposiciones que las medidas prescritas tienen por objetivo gestionar los riesgos de seguridad relacionados con las redes y sistemas de información que se utilizan en la prestación de servicios de pago. Por tanto, puede decirse que esos requisitos de seguridad tienen al menos un efecto equivalente al de la disposición correspondiente del artículo 14, apartados 1 y 2, de la Directiva SRI.

[40] Sin perjuicio de la notificación de una violación de la seguridad de los datos personales a la autoridad de control con arreglo al artículo 33 del RGPD.
[41] Directiva (UE) 2015/2366 (DO L 337 de 23.12.2015, p. 35).

En cuanto a los requisitos de notificación, el artículo 96, apartado 1, de la DSP 2 exige a los proveedores de servicios de pago que notifiquen sin dilación indebida los incidentes de seguridad a la autoridad competente. Además, a semejanza del artículo 14, apartado 5, de la Directiva SRI, el artículo 96, apartado 2, de la DSP 2 exige a la autoridad competente informar a las autoridades competentes de los Estados miembros para los cuales el incidente sea importante. Esta obligación implica al mismo tiempo que la notificación de incidentes de seguridad debe incluir información que permita a las autoridades evaluar el efecto transfronterizo de un incidente. El artículo 96, apartado 3, letra a), de la DSP 2 faculta en este contexto a la ABE para elaborar directrices sobre el contenido exacto y el formato de la notificación.

En consecuencia, cabe concluir que, en consonancia con el artículo 1, apartado 7, de la Directiva SRI, deben aplicarse los requisitos de seguridad y notificación de los artículos 95 y 96 de la DSP 2 en lugar de las disposiciones correspondientes del artículo 14 de la Directiva SRI cuando se trata de la prestación de servicios de pago por parte de entidades de crédito.

ii) Reglamento (UE) 648/2012 del Parlamento Europeo y del Consejo, de 4 de julio de 2012, relativo a los derivados extrabursátiles, las entidades de contrapartida central y los registros de operaciones

En lo que respecta a las infraestructuras de los mercados financieros, el Reglamento (UE) 648/2012, leído en relación con el Reglamento Delegado (UE) 153/2013 de la Comisión, contiene disposiciones sobre los requisitos de seguridad de las entidades de contrapartida central (ECC) que pueden calificarse de *lex specialis.* En concreto, dichos actos legislativos prevén una serie de medidas técnicas y de organización relacionadas con la seguridad de las redes y sistemas de información aún más detalladas que los requisitos del artículo 14, apartados 1 y 2, de la Directiva SRI y, por tanto, pueden considerarse acordes con los requisitos del artículo 1, apartado 7, de esta Directiva en lo que respecta a los requisitos de seguridad.

Más en concreto, el artículo 26, apartado 1, del Reglamento (UE) 648/2012 establece que las ECC deben disponer de *sólidos mecanismos de gobernanza, incluida una estructura organizativa clara, con líneas de responsabilidad bien definidas, transparentes y coherentes, así como de procedimientos eficaces de identificación, gestión, control y comunicación de los riesgos a los que estén o pudieran estar expuestas, junto con mecanismos adecuados de control interno, incluidos procedimientos administrativos y contables adecuados*. El apartado 3 del mismo artículo exige que la estructura organizativa garantice la continuidad y el correcto funcionamiento de la prestación de sus servicios y la realización de sus actividades, y emplear sistemas, recursos y procedimientos adecuados y proporcionados.

Por su parte, el apartado 6 del mismo artículo aclara que las ECC deben mantener *sistemas informáticos adecuados para gestionar la complejidad, la variedad y el tipo de servicios y actividades llevados a cabo, a fin de garantizar niveles elevados de seguridad y la integridad y confidencialidad de la información conservada*. El artículo 34, apartado 1, de dicho Reglamento exige el establecimiento, la aplicación y el mantenimiento de una estrategia adecuada de continuidad de la actividad y de recuperación en caso de catástrofe destinada a garantizar la oportuna recuperación de las operaciones.

Esas obligaciones se precisan en el Reglamento Delegado UE/153/2013 de la Comisión, de 19 de diciembre de 2012, por el que se completa el Reglamento (UE) n.° 648/2012 del Parlamento Europeo y del Consejo, en lo que se refiere a las normas técnicas de regulación relativas a los requisitos que deben cumplir las entidades de contrapartida central[42]. En concreto, el artículo 4 de este Reglamento obliga a las ECC a dotarse de herramientas adecuadas para la gestión de riesgos, de modo que puedan gestionar y notificar todos los riesgos pertinentes, especificando el tipo de medidas (p. ej.: empleo de sistemas de información y control de riesgos sólidos, disponibilidad de recursos y conocimientos técnicos y acceso a toda la información pertinente para ejercer la función de gestión de riesgos, disponibilidad de mecanismos de control interno adecuados, tales como procedimientos contables y administrativos eficaces, para asistir al consejo en su labor de control y evaluación de la adecuación y eficacia de las políticas, los procedimientos y los sistemas de gestión de riesgos).

Además, su artículo 9 remite de manera explícita a la seguridad de los sistemas informáticos e impone medidas técnicas y organizativas concretas relacionadas con el mantenimiento de un sistema sólido de seguridad de la información para la gestión de los riesgos de seguridad de los sistemas informáticos. Tales medidas deben incluir mecanismos y procedimientos que garanticen la disponibilidad de los servicios y la protección de la autenticidad, integridad y confidencialidad de los datos.

iii) Directiva 2014/65/UE del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, relativa a los mercados de instrumentos financieros y por la que se modifican la Directiva 2002/92/CE y la Directiva 2011/61/UE[43]

Respecto a los centros de negociación, el artículo 48, apartado 1, de la Directiva 2014/65/UE exige a los operadores que aseguren la continuidad de sus servicios en caso de disfunción de sus sistemas de negociación. Esta obligación general fue precisada y completada posteriormente por el Reglamento Delegado (UE) 2017/584 de la Comisión[44], de 14 de julio de 2016, por el que se completa la Directiva 2014/65/UE del Parlamento Europeo y del Consejo en lo relativo a las normas técnicas de regulación que especifican los requisitos organizativos de los centros de negociación[45]. En concreto, el artículo 23, apartado 1, de este Reglamento establece que los centros de negociación deben disponer de procedimientos y dispositivos de seguridad física y electrónica diseñados para proteger sus sistemas frente al uso indebido o el acceso no autorizado y para garantizar la integridad de los datos. Tales medidas deben prevenir o minimizar los riesgos de ataques contra los sistemas de información.

Además, el apartado 2 del mismo artículo establece que las medidas y dispositivos adoptados por los operadores deben detectar y gestionar rápidamente los riesgos relacionados con el acceso no autorizado, las interferencias en los sistemas que obstaculicen gravemente o interrumpan el funcionamiento de un sistema de información y las interferencias en los datos

[42] DO L 52 de 23.2.2013, p. 41.
[43] DO L 173 de 12.6.2014, p. 349.
[44] DO L 87 de 31.3.2017, p. 350.
[45] http://ec.europa.eu/finance/securities/docs/isd/mifid/rts/160714-rts-7_en.pdf

que pongan en peligro la disponibilidad, integridad o autenticidad de los datos. Por su parte, el artículo 15 del Reglamento exige a los centros de negociación que se doten de dispositivos efectivos de continuidad de las actividades que garanticen la suficiente estabilidad del sistema y permitan afrontar los incidentes perturbadores. En concreto, esas medidas deben permitir al operador reanudar la negociación antes de que transcurran dos horas desde que se haya producido el incidente perturbador y, al mismo tiempo, deben garantizar que la cantidad máxima de datos que puedan perderse sea próxima a cero.

El artículo 16, por su parte, establece que las medidas definidas para abordar y gestionar los incidentes perturbadores deben formar parte de un plan de continuidad de las actividades del centro de negociación y señala una serie de elementos específicos que debe considerar el operador al adoptar el plan de continuidad de las actividades (p. ej., establecimiento de un equipo específico de operaciones de seguridad, realización de una evaluación de impacto, sujeta a revisión periódica, que determine los riesgos).

A la luz del contenido de esas medidas de seguridad, queda claro que su objetivo consiste en gestionar y abordar los riesgos ligados a la disponibilidad, autenticidad, integridad y confidencialidad de los datos o los servicios prestados, como consecuencia de lo cual cabe concluir que la mencionada legislación específica de la UE contiene obligaciones de seguridad que tienen un efecto al menos equivalente al de las obligaciones correspondientes del artículo 14, apartados 1 y 2, de la Directiva SRI.

5.2. Artículo 1, apartado 3, de la Directiva SRI: Proveedores de telecomunicaciones y proveedores de servicios de confianza

De conformidad con el artículo 1, apartado 3, los requisitos de seguridad y de notificación previstos en la Directiva no son aplicables a las empresas que están sujetas a los requisitos de los artículos 13 *bis* y 13 *ter* de la Directiva 2002/21/CE. Los artículos 13 *bis* y 13 *ter* de la Directiva 2002/21/CE se aplican a las empresas que suministran redes públicas de comunicaciones o prestan servicios de comunicaciones electrónicas disponibles para el público. Por tanto, las empresas que suministran redes públicas de comunicaciones o prestan servicios de comunicaciones electrónicas disponibles para el público deben cumplir los requisitos de seguridad y notificación de la Directiva 2002/12/CE.

Ahora bien, si una misma empresa presta también otros servicios, como servicios digitales (p. ej., computación en la nube o mercado en línea) enumerados en el anexo III de la Directiva SRI, o servicios de DNS o de IXP con arreglo al anexo II, punto 7, de la Directiva SRI, la empresa quedará sujeta a los requisitos de seguridad y notificación de la Directiva SRI en lo que respecta a la prestación de esos servicios específicos. Debe señalarse que, habida cuenta de que los proveedores de servicios enumerados en el anexo II, punto 7, pertenecen a la categoría de operadores de servicios esenciales, los Estados miembros deben llevar a cabo un proceso de identificación con arreglo al artículo 5, apartado 2, e identificar a los operadores de DNS, IXP o TLD que deben cumplir los requisitos de la Directiva SRI. Esto significa que, tras esa evaluación, solo los proveedores de servicios de DNS, IXP o TLD que reúnan los criterios del artículo 5, apartado 2, de la Directiva SRI estarán sujetos a la obligación de cumplir los requisitos de la Directiva SRI.

Por otro lado, el artículo 1, apartado 3, especifica que los requisitos de seguridad y notificación previstos en la Directiva tampoco serán aplicables a los proveedores de servicios

de confianza sujetos a los requisitos análogos del artículo 19 del Reglamento (UE) n.º 910/2014.

6. Documentos publicados sobre las estrategias nacionales de ciberseguridad

	Estado miembro	Título de la estrategia y enlaces disponibles
1.	Austria	*Austrian Cybersecurity Strategy* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AT_NCSS.pdf (EN)
2.	Bélgica	*Securing Cyberspace* (2012) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/ncss-be-fr (FR)
3.	Bulgaria	*Cyber Resilient Bulgaria 2020* (2016) http://www.cyberbg.eu/ (BG)
4.	Croacia	*The national cyber security strategy of the republic of Croatia* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CRNCSSEN.pdf (EN)
5.	Chequia	*National cyber security strategy of the Czech Republic for the period from 2015 to 2020* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf (EN)
6.	Chipre	*Cybersecurity Strategy of the Republic of Cyprus* (2012) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CybersecurityStrategyoftheRepublicofCyprusv10_English.pdf (EN)
7.	Dinamarca	*The Danish Cyber and Information Security Strategy* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/DK_NCSS.pdf (EN)
8.	Estonia	*Cyber Security Strategy* (2014) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf (EN)
9.	Finlandia	*Finland´s Cyber security Strategy* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/FinlandsCyberSecurityStrategy.pdf (EN)
10.	Francia	*French national digital security strategy* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf (EN)
11.	Irlanda	*National Cyber Security Strategy 2015-2017* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_IE.pdf (EN)

12.	Italia	*National Strategic Framework for Cyberspace Security* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/IT_NCSS.pdf (EN)
13.	Alemania	*Cyber-security Strategy for Germany* (2016) http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/ModerneVerwaltung-OeffentlicherDienst/Informationsgesellschaft/cybersicherheitsstrategie-2016.pdf?__blob=publicationFile (DE)
14.	Hungría	*National Cyber Security Strategy of Hungary* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/HU_NCSS.pdf (EN)
15.	Letonia	*Cyber Security Strategy of Latvia 2014–2018* (2014) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss (EN)
16.	Lituania	*The programme for the development of electronic information security (cyber-security) for 2011–2019* (2011) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Lithuania_Cyber_Security_Strategy.pdf (EN)
17.	Luxemburgo	*National Cybersecurity Strategy II (2015)* https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Luxembourg_Cyber_Security_strategy.pdf (EN)
18.	Malta	*National Cyber Security Strategy Green Paper* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSSGreenPaper.pdf (EN)
19.	Países Bajos	*National Cyber Security Strategy 2* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS2Engelseversie.pdf (EN)
20.	Polonia	*Cyberspace Protection Policy of the Republic of Poland* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/copy_of_PO_NCSS.pdf (EN)
21.	Rumanía	*Cybersecurity Strategy of Romania* (2011) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf (RO)
22.	Portugal	*National Cyber Security Strategy* 2 (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/portuguese-national-cyber-security-strategy/view (EN)
23.	Eslovaquia	*Cyber Security Concept of the Slovak Republic for 2015 – 2020* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/cyber-security-concept-of-the-slovak-republic-1 (EN)

24.	Eslovenia	*Cyber Security Strategy establishing a system to ensure a high level of cyber security* (2016) http://www.uvtp.gov.si/fileadmin/uvtp.gov.si/pageuploads/Cyber_Security_Strategy_Slovenia.pdf (EN)
25.	España	*National Cyber Security Strategy* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_ESen.pdf (EN)
26.	Suecia	*The Swedish National Cybersecurity Strategy* (2017) http://www.government.se/49edf4/contentassets/b5f956be6c50412188fb4e1d72a5e501/fact-sheet-a-national-cyber-security-strategy.pdf (EN)
27.	Reino Unido	*National Cyber Security Strategy (2016-2021)* (2016) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national_cyber_security_strategy_2016.pdf (EN)

7. Lista de buenas prácticas y recomendaciones publicadas por ENISA

Respuesta a incidentes

- ✓ Estrategias de respuesta a incidentes y cooperación en caso de cibercrisis[46]

Gestión de incidentes

- ✓ Proyecto de automatización de la gestión de incidentes[47]
- ✓ Guía de buenas prácticas en gestión de incidentes[48]

Clasificación y taxonomía de incidentes

- ✓ Panorámica de las taxonomías existentes[49]
- ✓ Buenas prácticas de utilización de taxonomías en la prevención y detección de incidentes[50]

Madurez de los CSIRT

- ✓ Desafíos de los CSIRT nacionales de Europa en 2016: estudio sobre la madurez de los CSIRT[51]
- ✓ Estudio sobre la madurez de los CSIRT, proceso de evaluación[52]
- ✓ Directrices para los CSIRT nacionales y gubernamentales sobre cómo evaluar la madurez[53]

Creación de capacidades y formación de los CSIRT

- ✓ Guía de buenas prácticas en metodologías de formación[54]

Información sobre CSIRT existentes en Europa

Panorámica de los CSIRT por países[55]

[46] ENISA, *Strategies for incident response and cyber crisis cooperation* (2016). Disponible en: https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation
[47] Más información en: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/incident-handling-automation
[48] ENISA, *Good Practice Guide for Incident Management* (2010). Disponible en: https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management
[49] Más información en: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/existing-taxonomies
[50] ENISA, *A good practice guide of using taxonomies in incident prevention and detection* (2017). Disponible en: https://www.enisa.europa.eu/publications/using-taxonomies-in-incident-prevention-detection
[51] ENISA, *Challenges for National CSIRTs in Europe in 2016: Study on CSIRT Maturity* (2017). Disponible en: https://www.enisa.europa.eu/publications/study-on-csirt-maturity
[52] ENISA, *Study on CSIRT Maturity – Evaluation Process* (2017). Disponible en: https://www.enisa.europa.eu/publications/study-on-csirt-maturity-evaluation-process
[53] ENISA, *CSIRT Capabilities. How to assess maturity? Guidelines for national and governmental CSIRTs* (2016). Disponible en: https://www.enisa.europa.eu/publications/csirt-capabilities
[54] ENISA, *Good Practice Guide on Training Methodologies* (2014). Disponible en: https://www.enisa.europa.eu/publications/good-practice-guide-on-training-methodologies
[55] Más información en: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map