COMISIÓN
EUROPEA

Bruselas, 4.10.2017
COM(2017) 476 final

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

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO

Aprovechar al máximo 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

ES

Introducción

La Directiva (UE) 2016/1148 sobre la seguridad de las redes y sistemas de información de toda la Unión[1] (en lo sucesivo denominada la «Directiva SRI» o la «Directiva») adoptada el 6 de julio de 2016 es la primera legislación horizontal de la UE que aborda los desafíos de la seguridad y un verdadero factor de cambio para la resiliencia y la cooperación en materia de ciberseguridad en Europa.

La Directiva tiene tres objetivos principales:

- mejorar las capacidades de ciberseguridad nacionales;
- aumentar la cooperación a nivel de la UE; y
- fomentar una cultura de gestión de riesgos y notificación de incidentes entre los agentes económicos clave, en particular los operadores que prestan servicios esenciales para el mantenimiento de actividades económicas y de la sociedad y los proveedores de servicios digitales.

La Directiva SRI es una piedra angular en la respuesta de la UE a las crecientes amenazas y desafíos cibernéticos que acompañan la digitalización de nuestras existencias, tanto de la economía como de la vida social, y su aplicación es por ello una parte esencial del paquete de ciberseguridad presentado el 13 de septiembre de 2017. La efectividad de la respuesta de la UE queda inhibida hasta que la Directiva SRI no haya sido transpuesta en su integridad en todos los Estados miembros de la UE. Esto también ha sido reconocido como un punto crítico en la Comunicación de 2016 «Reforzar el sistema de ciberresiliencia de Europa y promover una industria de la ciberseguridad competitiva e innovadora»[2].

La novedad de la Directiva SRI y la urgencia de atajar un panorama de ciberamenazas en rápida evolución justifica que se preste especial atención a los problemas que afectan a todos los actores para garantizar que la transposición de la Directiva se realiza a tiempo y correctamente. A la vista de la fecha límite de la transposición el 9 de mayo de 2018 y del plazo para la identificación de los operadores de servicios esenciales el 9 de noviembre de 2018, la Comisión ha estado apoyando el proceso de transposición de los Estados miembros y su labor en el Grupo de cooperación para dicho fin.

La presente Comunicación con su anexo se basa en el trabajo preliminar y los análisis realizados por la Comisión hasta la fecha en relación con la aplicación de la Directiva SRI, en la aportación de la Europea de Seguridad de las Redes y de la Información (ENISA) y en los debates celebrados con los Estados miembros en la fase de transposición de la Directiva, en particular en el seno del Grupo de cooperación[3]. La presente Comunicación es el complemento de los grandes esfuerzos realizados hasta la fecha, en particular mediante:

[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.
[2] COM(2016) 410 final.
[3] Un mecanismo de cooperación estratégica entre Estados miembros en virtud de la Directiva SRI, artículo 11.

- El intenso trabajo del Grupo de cooperación, que ha aprobado un plan de trabajo centrado principalmente en la transposición de la Directiva SRI, y en particular en la cuestión de la identificación de los operadores de servicios esenciales y de sus obligaciones en relación con los requisitos de seguridad y las notificaciones del incidente. Aunque la Directiva contempla que la transposición de disposiciones relativas a operadores de servicios esenciales se realice a discreción, los Estados miembros reconocieron la importancia de un enfoque armonizado a este respecto[4].
- La creación y el ágil funcionamiento de la Red compuesta por equipos de respuesta a incidentes de seguridad informática (CSIRT) de conformidad con el artículo 12, apartado 1, de la Directiva. Desde entonces, esta red ha comenzado a sentar las bases de una cooperación operativa estructurada a nivel europeo.

Tanto para el nivel político como para el operativo, representados por estas dos estructuras, el compromiso total de todos los Estados miembros es esencial para lograr el objetivo de un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

La presente Comunicación y su anexo reforzarán dicho empeño al aunar y comparar las mejores prácticas de los Estados que sean pertinentes para la aplicación de la Directiva, aportando orientaciones complementarias sobre la forma en que debe aplicarse la Directiva y a través de explicaciones más detalladas sobre disposiciones específicas. El objetivo general es ayudar a los Estados miembros a lograr una aplicación efectiva y armonizada de la Directiva RSI en toda la UE.

La presente Comunicación se complementará además mediante el próximo Reglamento de Ejecución de la Comisión sobre la especificación de elementos y parámetros relacionados con la seguridad de las redes y sistemas de información y de requisitos para la notificación de incidentes para los proveedores de servicios digitales, de conformidad con el artículo 16, apartado 8, de la Directiva SRI. El Reglamento de Ejecución facilitará la aplicación de la Directiva respecto a las obligaciones que atañen a los proveedores de servicios digitales[5].

La Comunicación presenta las principales conclusiones del análisis de las cuestiones que se consideran puntos de referencia importantes e inspiración potencial desde el punto de vista de la transposición al Derecho nacional. Aquí el énfasis principal se pone en las disposiciones relativas a las capacidades y obligaciones de los Estados miembros respecto a las entidades comprendidas en el ámbito de aplicación de la Directiva. El anexo prevé un examen más detallado de esos ámbitos en los que la Comisión ve el máximo valor en la aportación de orientaciones prácticas sobre la transposición, mediante la explicación y su interpretación de

[4] El Grupo de cooperación está trabajando en documentos orientativos de referencia que se refieren a los siguientes elementos: los criterios para definir el grado de criticidad de un operador de conformidad con el artículo 5, apartado 2, de la Directiva; las circunstancias en las que los operadores de servicios esenciales están obligados a notificar los incidentes en virtud del artículo 14, apartado 7, de la Directiva; y los requisitos de seguridad para los operadores de servicios esenciales, con arreglo al artículo 14, apartados 1 y 2.

[5] El borrador del Reglamento de Ejecución puede ser consultado por el público en la siguiente dirección web: https://ec.europa.eu/info/law/better-regulation/have-your-say_en

determinadas disposiciones de la Directiva y por medio de la presentación de las mejores prácticas y de la experiencia acumulada con la Directiva hasta la fecha.

Hacia la aplicación efectiva de la Directiva SRI

El objetivo de la Directiva SRI es lograr un elevado nivel de seguridad de las redes y sistemas de información en la Unión. Para ello es preciso aumentar la seguridad de internet y de las redes y sistemas de información privados que respaldan el funcionamiento de nuestra sociedad y de nuestra economía. El primer elemento importante a este respecto es el grado de preparación de los Estados miembros, que debe garantizarse mediante la implantación de estrategias nacionales de ciberseguridad, tal como describe la Directiva, el trabajo de los CSIRT y el de las autoridades competentes nacionales.

Exhaustividad de las estrategias nacionales

Es importante que los Estados miembros aprovechen la oportunidad que brinda la transposición de la Directiva SRI para revisar su estrategia de ciberseguridad nacional a la luz de las lagunas, las buenas prácticas y los nuevos desafíos que se abordan en el anexo.

Aunque la Directiva, lógicamente, se centra en aquellas empresas y servicios que revisten una importancia crítica especial, la ciberseguridad de la economía y de la sociedad en su conjunto es la que necesita ser abordada de forma holística y coherente, dada la creciente dependencia de las TIC que tenemos. Por consiguiente, la adopción de estrategias nacionales exhaustivas que van más allá de los requisitos mínimos de la Directiva SRI (es decir, que cubren más que los sectores y servicios enumerados en los anexos II y III de la Directiva) incrementará el nivel general de seguridad de las redes y sistemas de información.

Como la ciberseguridad es un ámbito de orden público relativamente nuevo que está experimentando una rápida expansión, en la mayoría de los casos son necesarias nuevas inversiones, aunque la situación global de las finanzas públicas requiera recortes y ahorros. Por consiguiente, la adopción de decisiones ambiciosas a fin de garantizar unos recursos financieros y humanos adecuados que son indispensables para la aplicación eficaz de las estrategias nacionales, incluida la dotación de recursos suficientes para las autoridades competentes y los CSIRT a escala nacional, es fundamental para la consecución de los objetivos de la Directiva.

Eficacia de la aplicación y cumplimiento

La necesidad de designar las autoridades competentes nacionales y los puntos de contacto únicos respectivos está recogida en el artículo 8 de la Directiva y es un elemento clave a la hora de garantizar una aplicación eficaz de la Directiva SRI y la cooperación transfronteriza. Aquí han surgido planteamientos más centralizados y más descentralizados en los Estados miembros. Cuando los Estados miembros adoptan un planteamiento más descentralizado en relación con la designación de las autoridades competentes nacionales, ha demostrado ser primordial garantizar acuerdos de cooperación sólidos entre numerosas autoridades y los

puntos de contacto únicos (*véase el cuadro 1 de la sección 3.2 del anexo*). Esto mejoraría la eficacia de la aplicación y facilitaría el control del cumplimiento.

Basarse en la experiencia previa en relación con la protección de infraestructuras críticas de información (PICI) puede ayudar a diseñar un modelo óptimo de gobernanza para los Estados miembros, que garantice tanto la aplicación efectiva por sectores de la Directiva SRI, como un planteamiento horizontal coherente (*véase la sección 3.1 del anexo*).

Mejora de las capacidades de los CSIRT nacionales

Sin unos CSIRT nacionales eficaces y dotados de recursos adecuados en toda la UE, tal como contempla el artículo 9 de la Directiva SRI, la UE seguirá siendo demasiado vulnerable a las ciberamenazas transfronterizas. Por ello, los Estados miembros podrían plantearse la ampliación del ámbito de los CSIRT más allá de los sectores y servicios que están incluidos en el ámbito de aplicación de la Directiva (*véase la sección 3.3 del anexo*). Esto permitiría a los CSIRT nacionales prestar ayuda operativa a ciberincidentes que se produzcan en empresas y organizaciones que no estén en el ámbito de aplicación de la Directiva pero que también sean importantes para la sociedad y para la economía. Además, los Estados miembros podrían hacer pleno uso de las oportunidades adicionales de financiación que ofrece el programa de infraestructuras de servicios digitales (ISD) del Mecanismo «Conectar Europa» (MCE), concebido para mejorar las capacidades de los CSIRT nacionales y la cooperación entre ellos (*véase la sección 3.5 del anexo*).

Coherencia del proceso de identificación de los operadores de servicios esenciales

De conformidad con el artículo 5 de la Directiva SRI, los Estados miembros están obligados a identificar las entidades que se consideren operadores de servicios esenciales a más tardar el 9 de noviembre de 2018. En relación con dicho cometido, los Estados miembros podrán considerar la posibilidad de utilizar de forma coherente las definiciones y orientaciones que figuran en la presente Comunicación con el fin de asegurar que las entidades de tipo semejante que desempeñen una función parecida en el mercado interior sean identificadas sistemáticamente como operadores de servicios esenciales en los demás Estados miembros. Los Estados miembros podrán plantearse también ampliar el ámbito de aplicación de la Directiva SRI a las administraciones públicas, habida cuenta del papel que desempeñan para la sociedad y la economía en su conjunto (*véanse las secciones 2.1 y 4.1.3 del anexo*).

Resultaría muy útil ajustar en la mayor medida posible los planteamientos nacionales a la identificación de operadores de servicios esenciales, en particular siguiendo las orientaciones elaboradas por el Grupo de cooperación (*véase la sección 4.1.2 del anexo*), ya que ello daría lugar a una aplicación más armonizada de las disposiciones de la Directiva y por lo tanto reduciría el riesgo de fragmentación del mercado. En los casos en que los operadores de

servicios esenciales prestan servicios esenciales en dos o más Estados miembros, es fundamental intentar alcanzar un acuerdo entre los Estados miembros en el contexto del proceso de consulta en virtud del artículo 5, apartado 4, acerca de la identificación coherente de las entidades (*véase la sección 4.1.7 del anexo*), ya que ello evitaría un tratamiento normativo diferente de la misma entidad bajo las jurisdicciones de los distintos Estados miembros.

Presentación a la Comisión de la información relativa a la identificación de los operadores de servicios esenciales

De conformidad con el artículo 5, apartado 7, los Estados miembros están obligados a proporcionar a la Comisión información acerca de las medidas nacionales que permiten la identificación de los operadores de servicios esenciales, la lista de servicios esenciales, el número de operadores de servicios esenciales identificados y la pertinencia de dichos operadores para el sector. Además, los Estados miembros están obligados a facilitar, cuando existan, los umbrales utilizados para determinar el nivel de suministro pertinente o la importancia de ese operador concreto para el mantenimiento de un nivel de suministro suficiente. Los Estados miembros también podrán plantearse el compartir con la Comisión la lista de operadores de servicios esenciales identificados y si fuera necesario con carácter confidencial, ya que esto contribuiría a mejorar la precisión y la calidad de la evaluación de la Comisión (*véanse las secciones 4.1.5 y 4.1.6 del anexo*).

Planteamientos armonizados respecto a los requisitos de seguridad y notificación de incidentes para los operadores de servicios esenciales

En relación con las obligaciones relativas a los requisitos en materia de seguridad y notificación de incidentes para los operadores de servicios esenciales (artículo 14, apartados 1, 2 y 3), un planteamiento armonizado respecto a los requisitos de seguridad y notificación de incidentes destinado facilitar la conformidad de los operadores de servicios esenciales a través de las fronteras nacionales de la UE fomentaría en la máxima medida posible el efecto de un mercado único. La referencia en este caso sigue siendo el trabajo sobre un documento orientativo dentro del Grupo de cooperación (*véanse las secciones 4.2 y 4.3 del anexo*).

En caso de que un incidente cibernético afecte a varios Estados miembros es muy probable que una notificación de incidente obligatoria sea presentada por un operador de servicios esenciales o un proveedor de servicios digitales de conformidad con el artículo 14, apartado 3, y con el artículo 16, apartado 3, o por otra entidad que no esté en el ámbito de aplicación de la Directiva de forma voluntaria con arreglo al artículo 20, apartado 1. En línea con la recomendación de la Comisión para dar una respuesta coordinada a los incidentes y crisis de ciberseguridad de gran escala, los Estados miembros podrán plantearse armonizar sus planteamientos nacionales para poder facilitar lo antes posible información pertinente basada en dichas notificaciones a las autoridades competentes o a los CSIRT de los demás Estados miembros afectados. Para reducir el número de infecciones o resolver las vulnerabilidades antes de que sean explotadas es vital contar con información precisa y que permita actuar.

En un espíritu de cooperación para sacar el máximo partido a la Directiva SRI, la Comisión tiene la intención de ampliar las ayudas del Mecanismo «Conectar Europa» a todas las partes interesadas en el marco de esta normativa. Aunque se había prestado más atención a la creación de capacidad en materia de equipos de respuesta a incidentes de seguridad informática (CSIRT) y a una plataforma para una cooperación operativa rápida y efectiva, reforzando así la red CSIRT, la Comisión va a analizar ahora de qué forma la financiación del Mecanismo «Conectar Europa» puede beneficiar también a las autoridades nacionales competentes, así como a los operadores de servicios esenciales y a los proveedores de servicios digitales.

Conclusión

A la vista de la proximidad de la fecha límite para la transposición de la Directiva SRI a la legislación nacional, a más tardar el 9 de mayo de 2018, y a la vista de la fecha límite para la identificación de los operadores de servicios esenciales antes del 9 de noviembre de 2018, los Estados miembros deben tomar las medidas pertinentes para garantizar que las disposiciones y los modelos de cooperación de la Directiva SRI puedan facilitar las mejores herramientas posibles a nivel de la UE para lograr un elevado nivel común de seguridad de las redes y sistemas de información en toda la Unión. La Comisión pide a los Estados miembros que consideren dentro de este proceso la información pertinente, las orientaciones y las recomendaciones incluidas en la presente Comunicación.

La presente Comunicación podrán completarse mediante otras acciones, incluidas las generadas mediante el trabajo en curso en el marco del Grupo de cooperación.