Publicada la directiva sobre ciberseguridad: obligaciones para los gestores de infraestructuras críticas y servicios esenciales

José Miguel Lissén Arbeloa
Socio del Área de IP-IT de Gómez-Acebo & Pombo

Isabela Crespo Vitorique
Asociada senior *del Área de IP-IT de Gómez-Acebo & Pombo*

El 19 de julio del 2016 se ha publicado la Directiva sobre seguridad de las redes y de los sistemas de información de la Unión, pieza clave de la estrategia de ciberseguridad de la Unión Europea. La directiva impone a los Estados miembros la adopción de una estrategia nacional de seguridad y de medidas técnicas y organizativas para prevenir, gestionar y reaccionar ante ciberriesgos y ataques a las redes y sistemas de información de la Unión. La responsabilidad de velar por la seguridad recae en gran medida en las empresas y entidades gestoras de infraestructuras críticas y servicios esenciales (energía, transporte, banca y mercados financieros, sector sanitario, suministro de agua e infraestructura digital), que deberán implantar programas para crear una cultura de gestión, prevención de riesgos y ataques, así como de reacción en caso de producirse.

El 19 de julio del 2016, se ha publicado en el *Diario Oficial de la Unión Europea* la Directiva (UE) núm. 2016/1148, del Parlamento Europeo y del Consejo, de 6 de julio del 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, también conocida como *Directiva RSI*, o, por sus siglas en inglés, *Directiva NIS (Network and Information Systems)*, que entrará en vigor el 8 de agosto del 2016, estando los Estados miembros de la Unión Europea obligados a transponerla a más tardar el 9 de mayo del 2018.

La directiva se enmarca dentro de la estrategia de ciberseguridad de la Comisión Europea encaminada a la consecución de «[u]n ciberespacio abierto, protegido y seguro», representa la visión de conjunto de la Unión Europea sobre cómo prevenir y resolver mejor las perturbaciones de la red y los ciberataques, vela por un crecimiento seguro de la economía digital y contribuye a un mejor funcionamiento en el mercado interior.

1. Objeto y ámbito de aplicación

La directiva establece medidas que tienen como objeto lograr un elevado nivel común de seguridad de las redes y los sistemas de información dentro de la Unión y, a tal fin:

a) establece obligaciones para todos los Estados miembros de adoptar una estrategia nacional de seguridad de tales redes y sistemas;

b) crea un grupo de cooperación para apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados miembros y desarrollar la confianza y seguridad entre ellos;

N. de la C.: En las citas literales se ha rectificado en lo posible —sin afectar al sentido— la grafía de ciertos elementos (acentos, mayúsculas, símbolos, abreviaturas, cursivas...) para adecuarlos a las normas tipográficas utilizadas en el resto del texto.

c) crea una red de equipos de respuesta a incidentes de seguridad informática (en lo sucesivo, CSIRT, por sus siglas en inglés de *computer security incident response teams*);

d) establece requisitos en materia de seguridad y notificación para los operadores de servicios esenciales y para los proveedores de servicios digitales;

e) establece obligaciones para que los Estados miembros designen autoridades nacionales competentes, puntos de contacto únicos y CSIRT.

2. Estrategia nacional de seguridad

Cada Estado miembro adoptará una estrategia nacional de seguridad de las redes y los sistemas de información que establezca objetivos estratégicos y medidas políticas y normativas adecuadas para alcanzar y mantener un elevado nivel de seguridad y que cubra al menos los sectores y servicios que figuran en los anexos II y III de la directiva.

Los sectores identificados en el anexo II comprenden 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, mientras que los servicios identificados en el anexo III son los del mercado en línea, del motor de búsqueda en línea y los de computación en la nube.

Entre otras cuestiones, la estrategia nacional de seguridad de las redes y sistemas de información abordará las siguientes: *a*) los objetivos y prioridades de la estrategia nacional de seguridad de las redes y los sistemas de información; *b*) un marco de gobernanza para lograr esos objetivos y prioridades; *c*) la identificación de medidas sobre preparación, respuesta y recuperación, incluida la cooperación entre los sectores público y privado; *d*) una indicación de los programas de educación, concienciación y formación; *e*) una indicación de los programas de investigación y desarrollo relacionados; *f*) un plan de evaluación de riesgos para identificar riesgos, y *g*) una lista de los diversos agentes que participan en la ejecución de la estrategia de seguridad de las redes y sistemas de información.

3. Identificación de operadores de servicios esenciales

A más tardar el 9 de noviembre del 2018, los Estados miembros identificarán a los operadores de servicios esenciales establecidos en su territorio para cada sector y subsector mencionado en el anexo II. Dichos operadores son los que prestarán los servicios identificados a continuación, agrupados por sectores y subsectores de actividad:

- Energía/electricidad: los gestores de la red de distribución y los gestores de la red de transporte.

- Energía/crudo: los operadores de oleoductos de transporte de crudo, los operadores de producción de crudo, instalaciones de refinado y tratamiento, almacenamiento y transporte.

- Energía/gas: empresas suministradoras, gestores de la red de distribución, gestores de la red de transporte, gestores de almacenamiento, gestores de la red de gas natural licuado, compañías de gas natural, gestores de instalaciones de refinado y tratamiento de gas natural.

- Transporte aéreo: compañías aéreas, entidades gestoras de aeropuertos, operadores de control de tránsito aéreo;

- Transporte por ferrocarril: administradores de infraestructuras, empresas ferroviarias.

- Transporte marítimo y fluvial: empresas de transporte marítimo, fluvial y cabotaje (pasajeros y mercancías), organismos gestores de puertos, operadores de servicios de tráfico de buques.

- Transporte por carretera: autoridades viarias, operadores de sistemas inteligentes de transporte.

- Banca: entidades de crédito.

- Infraestructuras de los mercados financieros: gestores de centros de negociación, entidades de contrapartida central.

- Sector sanitario: prestadores de asistencia sanitaria.

– Suministro y distribución de agua potable: suministradores y distribuidores de aguas destinadas al consumo humano.

– Infraestructura digital: IXP, proveedores de servicios DNS, registros de nombres de dominio de primer nivel.

A la hora de determinar la importancia de un efecto perturbador, los Estados miembros tendrán en cuenta al menos los siguientes factores intersectoriales: *a*) el número de usuarios que confían en los servicios prestados por la entidad de que se trate; *b*) la dependencia de otros sectores que figuran en el anexo II sobre el servicio prestado por esa entidad; *c*) la repercusión que podrían tener los incidentes, en términos de grado y duración, en las actividades económicas y sociales o en la seguridad pública; *d*) la cuota de mercado de la entidad; *e*) la extensión geográfica con respecto a la zona que podría verse afectada por un incidente, y *f*) 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.

4. Grupo de cooperación y red de CSIRT

Se establece un grupo de cooperación a fin de apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados miembros, desarrollar confianza y seguridad, y alcanzar un elevado nivel común de seguridad de las redes y los sistemas de información. El Grupo de Cooperación ejercerá, entre otras, las funciones *a*) de intercambio de buenas prácticas en relación con la información sujeta a notificación de incidentes; *b*) de intercambio de información y buenas prácticas sobre investigación y desarrollo en materia seguridad de las redes y los sistemas de información, y *c*) de la recopilación de información de buenas prácticas sobre los riesgos e incidentes que afecten a dichas redes y sistemas.

A fin de contribuir a desarrollar la confianza y la seguridad entre los Estados miembros y a promover una cooperación operativa rápida y eficaz, se establece una red de CSIRT nacionales que estará formada por representantes de los correspondientes equipos de respuesta de los Estados miembros y desempeñará, entre otros, los siguientes cometidos: *a*) intercambiar información sobre servicios, operaciones y capacidades de cooperación de los CSIRT; *b*) intercambiar y discutir sobre información sensible de carácter no comercial relacionada con ese incidente y los riesgos asociados; *c*) intercambiar y proporcionar información no confidencial sobre incidentes concretos; *d*) discutir y, cuando sea posible, determinar una respuesta coordinada a un incidente que se haya identificado en un Estado miembro; *e*) prestar apoyo a los Estados miembros a la hora de abordar los incidentes transfronterizos, y *f*) discutir, explorar e identificar más formas de cooperación operativa y publicar directrices para facilitar la convergencia de prácticas operativas en lo que atañe a la cooperación operativa.

5. Requisitos en materia de seguridad y notificación

Los Estados miembros velarán por que los operadores de servicios esenciales 1) tomen las medidas técnicas y de organización adecuadas y proporcionadas para gestionar los riesgos que se planteen para la seguridad de las redes y los sistemas; 2) adopten medidas para prevenir y para reducir al mínimo los efectos de los incidentes que afecten a la seguridad de las redes y los sistemas de información en relación con la prestación de tales servicios esenciales, con el objeto de garantizar su continuidad, y 3) notifiquen sin dilación indebida a la autoridad competente o al CSIRT los incidentes que tengan efectos significativos en la continuidad de los servicios esenciales que prestan. Es de destacar que la notificación no sujetará al notificante a una mayor responsabilidad.

Además, los Estados miembros velarán por que los proveedores de servicios digitales 1) adopten medidas técnicas y organizativas adecuadas y proporcionadas para gestionar los riesgos existentes para la seguridad de las redes y sistemas de información que se utilizan en sus servicios ofertados; 2) adopten medidas para prevenir y reducir al mínimo el impacto de los incidentes que afectan a la seguridad de sus redes y sistemas de información en el ámbito de sus servicios, a fin de garantizar su continuidad, y 3) notifiquen sin dilación indebida a la autoridad competente o al CSIRT cualquier incidente que tenga un impacto significativo en la

prestación de uno de sus servicios. Igualmente, en este caso, la notificación no sujetará al notificante a una mayor responsabilidad.

6. Fomento de «una cultura de gestión de riesgos»

En los considerandos 44 y 46 de la directiva, el legislador de la Unión Europea enfatiza que su objetivo es que la responsabilidad de velar por la seguridad de las redes y los sistemas de información recaiga en gran medida en los operadores de servicios esenciales y en los proveedores de servicios digitales. A tal fin, hace hincapié en que, por parte de los Estados miembros, «[d]ebe fomentarse una cultura de gestión de riesgos que implique una evaluación del riesgo y la aplicación de medidas de seguridad adecuadas a los riesgos que hay que afrontar, y ésta se debe desarrollar a través de requisitos normativos adecuados y prácticas sectoriales voluntarias». Entre esas medidas de gestión de riesgos figuran aquellas cuya finalidad es determinar todo riesgo de incidentes, prevenir, detectar y gestionar incidentes y mitigar sus repercusiones.

7. Acciones que poner en práctica

Sin perjuicio de la forma en que se incorpore al Derecho español y al portugués el mandato del legislador de la Unión contenido en la directiva y de las prácticas sectoriales voluntarias que se vayan desarrollando por parte de los operadores de servicios esenciales, de los proveedores de servicios digitales y de los organismos reguladores de los Estados miembros, entendemos que, en sintonía con las recomendaciones y directrices propuestas el año pasado por organismos tales como la Securities and Exchange Commission (SEC) o la Office of Compliance Inspections and Examinations (OCIE) de Estados Unidos, ante la creciente proliferación de ataques, amenazas y riesgos para la seguridad de las redes y los sistemas de información, tanto los operadores de servicios esenciales como los proveedores de servicios digitales deben adoptar medidas destinadas a crear y consolidar una cultura de gestión de riesgos y protección de activos de la empresa.

Un buen programa de ciberseguridad y defensa descansa sobre dos pilares fundamentales: cumplimiento normativo e inteligencia sobre ciberriesgos. Para la efectiva consecución de este programa, se recomienda la adopción por parte de las empresas y de los gestores de infraestructuras y servicios críticos de las siguientes medidas:

1) *Cumplimiento normativo: políticas y procedimientos y buen gobierno.*

   a) La designación de un responsable de CSIRT dentro de cada organización.

   b) La implantación de buenas prácticas generales y sectoriales, en especial, en los departamentos más vulnerables.

   d) El desarrollo de políticas y procedimientos en un programa de ciberseguridad que incluyan lo siguiente:

   - La definición de mapas de riesgos relacionados con la ciberseguridad y protección de activos de la empresa, en especial, con respecto a las bases de datos y la información crítica.
   - La identificación de los ciberactivos de la empresa (activos con exposición a internet: bases de datos, sistemas de control industrial (ICS, SCADA…); información financiera, estratégica o sobre empleados o clientes, propiedad intelectual, secretos industriales y comerciales, etcétera).
   - Protocolo de respuesta ante incidentes.
   - Protocolos de notificación a nivel interno y ante las autoridades competentes en caso de brechas informáticas.
   - Políticas de actuación y responsabilidad de los empleados en el uso de herramientas informáticas de la empresa.

2) *Inteligencia sobre ciberriesgos: medidas operativas.*

   a) Implantación de un programa de inteligencia sobre ciberamenazas para gestionar riesgos y ataques.

b) Formación para empleados sobre ciberriesgos para asegurar niveles mínimos de preparación ante escenarios adversos.

c) Establecimiento de protocolos de control de acceso a redes y sistemas de información por parte de terceros (proveedores, clientes, socios comerciales, etcétera).

d) Puesta en marcha de medidas de seguridad física alrededor de ciberactivos críticos.