Spread the love

Lincoln, Ox

La protección de los servicios considerados esenciales para la sociedad son los objetivos sobre los que trabaja la Unión Europea y sus Estados.**

A tales efectos destaca la legislación y propuestas a las que aludimos.

En primer lugar la Directiva 2008/114/CE del Consejo, sobre Identificación y Designación de las Infraestructuras Críticas Europeas y la Evaluación de la Necesidad de Mejorar su Protección", que fue transpuesta en España con la "Ley 8/2011 por la que se establecen medidas para la Protección de las Infraestructuras Críticas".

En segundo la Directiva 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; y su primera transposición en España (Real Decreto-ley 12/2018 con tramitación parlamentaria como Proyecto de Ley de seguridad de las redes y sistemas de información (procedente del Real Decreto-ley 12/2018, de 7 de septiembre). Esta Directiva es objeto de desarrollo regulatorio, en el llamado «paquete NIS»).

En virtud de la Directiva (UE) 2016/1148, los países de la UE deben:

1. designar a **una o más autoridades nacionales competentes** y a uno o varios centros de respuesta a incidentes cibernéticos – **CSIRT-**, así como determinar un **punto de contacto único** (en caso de que haya más de una autoridad competente)
    - Los CSIRT son responsables de supervisar incidentes de

ciberseguridad y responder a ellos; efectuar análisis de riesgos e incidentes; participar en la red de CSIRTs; cooperar con el sector privado; fomentar la utilización de prácticas normalizadas para la clasificación de incidentes, riesgos e información, entre otras competencias

2. designar **operadores de servicios esenciales** en sectores fundamentales como la energía, el transporte, las finanzas, la banca, la salud, el agua y la **infraestructura digital**, en los cuales un ciberataque podría perturbar un servicio esencial.
3. adoptar una **estrategia nacional de ciberseguridad para las redes y sistemas de información**, que aborde la preparación y disposición para gestionar y reaccionar a los ciberataques; las funciones, responsabilidades y cooperación de la administración pública y de otros agentes; los programas de educación, concienciación y formación; los planes de investigación y desarrollo; y los planes de identificación de riesgos.
4. asegurar que sus autoridades nacionales competentes supervisan la aplicación de la Directiva *evaluando las políticas de ciberseguridad y seguridad de los operadores de servicios esenciale*s; *supervisando los proveedores de servicios digitales;* participando en el trabajo del **Grupo de cooperación** [formado por las autoridades competentes en materia de seguridad de las redes y de la información (SRI) de cada uno de los países de la UE, la Comisión Europea y la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA)]; informando al público cuando sea necesario a fin de evitar incidentes o gestionarlos cuando ya se hayan producido, respetando siempre los requisitos de confidencialidad; impartiendo instrucciones vinculantes para subsanar las deficiencias en ciberseguridad.

All Souls Bridge. OX

La Directiva se aplica a los operadores de servicios esenciales (designados) -OSE- como a los proveedores de servicios digitales -PSE-, aunque las obligaciones de unos y otros resulten algo distintas.

Sin embargo, la Directiva NIS *no se aplica a empresas que suministren redes públicas de comunicaciones o presten servicios de comunicaciones electrónicas disponibles para el público en el sentido de la Directiva 2002/21/CE del Parlamento Europeo y del Consejo (Directiva Marco de Comunicaciones Electrónicas)* que están sujetas a los requisitos específicos de seguridad e integridad, como *tampoco a los prestadores de servicios de confianza definidos en el Reglamento (UE) n.o 910/2014* del Parlamento Europeo y del Consejo (relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior) que están sujetos a los requisitos de seguridad establecidos en dicho Reglamento.

El Real Decreto Ley 12/2018 incorpora al ordenamiento español la Directiva NIS. Tiene por objeto regular la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y de los servicios digitales, y establecer un sistema de notificación de incidentes. También establece un marco institucional en las cuestiones relativas a su ámbito.

Se aplica a

- **Operadores de Servicios Digitales -OSE- dependientes de las redes y sistemas de información** c**omprendidos en los sectores estratégicos (infraestructuras críticas)** definidos en el anexo de la mencionada Ley 8/2011, sobre protección de infraestructuras críticas
    - Un operador de servicios esenciales está establecido en España cuando su r*esidencia o domicilio social* se encuentren en territorio español, *siempre que éstos coincidan con el lugar en que esté efectivamente centralizada la gestión administrativa y la dirección de sus negocios o actividades.*
    - Servicios esenciales que los operadores residentes o domiciliados en otro Estado ofrezcan a través de un *establecimiento permanente situado en España.*
    - La *Comisión Nacional para la Protección de las Infraestructuras Críticas aprobará una primera lista de servicios esenciales dentro de los sectores incluidos en el ámbito de aplicación de este real decreto-ley e identificará a los operadores que los presten que deban sujetarse a este real decreto-ley*
- **Prestadores o proveedores de servicios digitales – PSD-** conforme se determina en el artículo 3 e), es decir «*persona jurídica que presta un servicio digital.*» que además sean *mercados en línea, motores de búsqueda en línea y servicios de computación en nube.* Es decir, proveedores de servicios digitales que tengan su sede social en España y/o con establecimiento principal en la Unión Europea, así como los que, no estando establecidos en la Unión Europea, designen en España a su representante en la Unión para el cumplimiento de la Directiva (UE) 2016/1148 y se dediquen a alguna (o todas) de las 3 actividades

Exclusiones. El RD-l, no se aplica a

- a) Los operadores de redes y servicios de comunicaciones electrónicas, prestadores de servicios electrónicos de confianza que no sean designados como operadores críticos en virtud de la Ley 8/2011, de 28 de abril.
- b) Los proveedores de servicios digitales cuando se trate de microempresas o pequeñas empresas, de acuerdo con las definiciones recogidas en la Recomendación 2003/361/CE de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas.

Obligaciones de seguridad de los OSD y PSD:

Houses of Parliament

- **adoptar 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** utilizados en la prestación de los servicios sujetos a este real decreto-ley.
- **notificar incidentes** conforme al título V
- **tomar medidas adecuadas para prevenir y reducir al mínimo el impacto de los incidentes** que les afecten.

Los operadores de servicios esenciales designarán y comunicarán a la autoridad competente, **la persona, unidad u órgano colegiado responsable de la seguridad de la información, como punto de contacto y de coordinación técnica con aquella,** cuyas funciones específicas serán las previstas reglamentariamente.

    - Las autoridades competentes podrán establecer mediante *Orden ministerial obligaciones específicas* para garantizar la seguridad de las redes y sistemas de información empleados por los operadores de servicios esenciales. Así mismo, podrán *dictar instrucciones técnicas y guías orientativas* para detallar el contenido de dichas órdenes.
    - Al elaborar las disposiciones reglamentarias, instrucciones y guías, *tendrán en cuenta las obligaciones sectoriales,* las directrices relevantes que se adopten en el grupo de cooperación y los requisitos en materia de seguridad de la

información a las que estuviera sometido el operador en virtud de otras normas, como la Ley 8/2011, de 28 de abril, y el Esquema Nacional de Seguridad en el ámbito de la administración electrónica, aprobado por el Real Decreto 3/2010, de 8 de enero. Las autoridades competentes deberán coordinarse entre sí y con los diferentes órganos sectoriales con competencias por razón de la materia, con objeto de evitar duplicidades en las obligaciones exigibles y facilitar su cumplimiento a los operadores de servicios esenciales.

Los proveedores de servicios digitales determinarán las medidas de seguridad que aplicarán, teniendo en cuenta, como mínimo, los avances técnicos y los siguientes aspectos (atendiendo a los actos de ejecución de la Comisión Europea):

- La seguridad de los sistemas e instalaciones;
- La gestión de incidentes;
- La gestión de la continuidad de las actividades;
- La supervisión, auditorías y pruebas;
- El cumplimiento de las normas internacionales.

Turf Street (and Pub) Ox

Obligaciones de notificar

- (**Los operadores de servicios esenciales notificarán a la autoridad competente, a través del CSIRT de referencia**, los *incidentes que puedan tener efectos perturbadores significativos* en tales servicios, o, conforme se determine

reglamentariamente, incidentes relativos a los *sucesos o incidencias que puedan afectar a las redes y sistemas de información empleados para la prestación de los servicios esenciales, pero que aún no hayan tenido un efecto adverso* real sobre aquéllos.

- **Los proveedores de servicios digitales notificarán a la autoridad competente, a través del CSIRT de referencia (INCIBE en el caso de entidades privadas y empresarios individuales)** los incidentes que tengan efectos perturbadores significativos en dichos servicios.
    - A los efectos de valorar la gravedad del incidente, **los operadores de servicios esenciales medirán la relevancia teniendo en cuenta, como mínimo, los siguientes factores**: a) El número de usuarios afectados por la perturbación del servicio esencial. b) La duración del incidente. c) La extensión o áreas geográficas afectadas d) El grado de perturbación del funcionamiento del servicio. e) El alcance del impacto en actividades económicas y sociales cruciales. f) La importancia de los sistemas afectados o de la información afectada por el incidente para la prestación del servicio esencial. g) El daño a la reputación.
        - **Estos operadores deben realizar una notificación inicial, otra intermedia y otra final**
    - Los **operadores de servicios digitales, determinan la medición conforme a lo que establezcan los actos de ejecución** previstos en los apartados 8 y 9 del artículo 16 de la Directiva NIS. La obligación de la notificación del incidente únicamente se aplicará cuando el proveedor de servicios digitales tenga acceso a la información necesaria para valorar el impacto de un incidente.

- Los **operadores de servicios esenciales y los proveedores de servicios digitales así como cualquier otra parte interesada, que tengan noticia de incidentes que afecten de modo significativo a servicios digitales ofrecidos en España por proveedores establecidos en otros Estados miembros de la Unión Europea, *podrán* notificarlo a la autoridad competente aportando la información pertinente, al objeto de facilitar la cooperación** con el Estado miembro en el que estuviese establecido el citado proveedor.

- Las notificaciones tanto de operadores de servicios esenciales como de proveedores de servicios digitales se referirán a los incidentes que afecten a las **redes y sistemas de información** empleados en la prestación de los servicios, tanto si se trata de redes y servicios **propios como si lo son de proveedores externos**.
    - Las autoridades competentes y los **CSIRT de referencia utilizarán una plataforma común para facilitar y automatizar** los procesos de notificación, comunicación e información sobre incidentes.
    - El desarrollo reglamentario de este real decreto-ley preverá las medidas necesarias para el cumplimiento de lo preceptuado en este artículo por parte de los operadores de servicios esenciales.
        - Las autoridades competentes podrán establecer, mediante *Orden ministerial,* obligaciones específicas de notificación por los operadores de servicios esenciales. Así mismo, podrán dictar *instrucciones técnicas y guías orientativas* para detallar el contenido de dichas órdenes. Al elaborar las disposiciones reglamentarias, instrucciones y guías, se tendrán en cuenta las *obligaciones sectoriales,* las directrices relevantes que se adopten en el grupo de cooperación y los requisitos en materia de notificación de incidentes a los que estuviera sometido el operador en virtud de otras normas, como la Ley 8/2011, de 28 de abril, y el Esquema Nacional de Seguridad, aprobado por el Real Decreto 3/2010, de 8 de enero.
    - La obligación de notificación de incidentes no obsta al cumplimiento de los deberes legales de denuncia de aquellos hechos que revistan caracteres de delito .

Grove Qd, Lincoln, Ox

    - **Proteccion de notificantes:** Las notificaciones consideradas en este título no sujetarán a la entidad que las efectúe a una mayor responsabilidad. Además,

> los empleados y el personal que, por cualquier tipo de relación laboral o mercantil, participen en la prestación de los servicios esenciales o digitales, que informen sobre incidentes no podrán sufrir consecuencias adversas en su puesto de trabajo o con la empresa, salvo en los supuestos en que se acredite mala fe en su actuación.

Recuérdese a los efectos de la aplicación en España de la Directiva que los centros de respuesta a incidentes de seguridad cibernética, **en lo concerniente a las relaciones con los operadores de servicios esenciales son** 1º El CCN-CERT, del Centro Criptológico Nacional, al que corresponde la comunidad de referencia constituida por las entidades del ámbito subjetivo de aplicación de la Ley 40/2015, de 1 de octubre de Régimen Jurídico del Sector Público. 2.º **El INCIBE-CERT,** del Instituto Nacional de Ciberseguridad de España, al que corresponde la comunidad de referencia constituida por aquellas entidades no incluidas en el ámbito subjetivo de la Ley 40/2015, de 1 de octubre. (el INCIBE-CERT es operado conjuntamente por el INCIBE y el Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC) en todo lo que se refiera a la gestión de incidentes que afecten a los operadores críticos. 3.º El **ESPDEF-CERT,** del Ministerio de Defensa, que cooperará con el **CCN-CERT** (centro criptológico nacional) y el **INCIBE-CERT** en aquellas situaciones que éstos requieran en apoyo de los operadores de servicios esenciales y, necesariamente, en aquellos operadores que tengan incidencia en la Defensa Nacional y que reglamentariamente se determinen. **En lo concerniente a las relaciones con los proveedores de servicios digitales que no estuvieren comprendidos en la comunidad de referencia del CCN-CERT: el INCIBE-CERT. El INCIBE-CERT será, así mismo, equipo de respuesta a incidentes de referencia para los ciudadanos, entidades de derecho privado y otras entidades no incluidas anteriormente.**

Los CSIRT de referencia se coordinarán entre sí y con el resto de CSIRT nacionales e internacionales en la respuesta a los incidentes y gestión de riesgos de seguridad que les correspondan. En los supuestos de especial gravedad que reglamentariamente se determinen y que requieran un nivel de coordinación superior al necesario en situaciones ordinarias, el CCN-CERT ejercerá la coordinación nacional de la respuesta técnica de los CSIRT. Cuando las actividades que desarrollen puedan afectar de alguna manera a un operador crítico, los CSIRT de referencia se coordinarán con el Ministerio del Interior, a través de la Oficina de Coordinación Cibernética del Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC), de la forma que reglamentariamente se determine.

**Redactado con el apoyo del Proyecto de Investigación «Libertad de Mercado y

sobreendeudamiento de consumidores: estrategias jurídico-económicas para garantizar una segunda oportunidad» (Núm. Ref. DER2016-80568-R). Ministerio de Economía y Competitividad (España) del que la autora forma parte como investigadora.