Deloitte.

Transposición de la Directiva NIS

Pieza clave de la ciberseguridad en España

Contenido

Introducción

La protección de los servicios considerados esenciales para la sociedad es uno de los objetivos sobre los que tanto la Unión Europea a nivel general, como los distintos países que la componen a nivel local, llevan tiempo trabajando.

Para lograr este objetivo, desde hace tiempo se han establecido **regulaciones dedicadas a proteger las infraestructuras críticas que soportan los servicios esenciales**, comenzando con la publicación de 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 a través de la "Ley 8/2011 por la que se establecen medidas para la Protección de las Infraestructuras Críticas" (en adelante, LPIC).

De esta forma, la protección de los servicios esenciales hasta ahora se ha centrado en la protección de las infraestructuras asociadas a los mismos, siendo en estos momentos el objetivo **establecer los requisitos regulatorios para la protección de las redes y sistemas de información** que soportan dichos servicios. Para ello, a nivel europeo, en el año 2016 se publicó la "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 adelante, Directiva NIS). En septiembre de 2018, España ha incorporado la Directiva NIS a su ordenamiento jurídico a través del "Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información" (en adelante, la Ley), estableciéndose así por primera vez una ley española que se centra exclusivamente en la seguridad lógica de los sistemas y redes de información que soportan los servicios esenciales.

El presente artículo tiene como objetivo resumir los aspectos principales de la Ley, identificando sus principales impactos, especialmente para los Operadores de Servicios Esenciales (en adelante, OSE, u OES por sus siglas en inglés) y los Proveedores de Servicios Digitales (en adelante, PSD, o DSP por sus siglas en inglés). De esta manera, se pretende contestar a las siguientes preguntas:

- ¿A quién afecta la Ley?
- ¿Qué otros organismos son importantes dentro de la propia Ley?
- ¿Qué requerimientos de seguridad tendrán que cumplir OES y DSP?
- ¿Qué requerimientos de notificación tendrán que cumplir OES y DSP?
- ¿Cuáles son las sanciones a las que están expuestas las entidades?
- ¿Cuáles son los próximos pasos?

¿A quién aplica la Ley?

La Ley, al igual que la Directiva de la que emana, afecta a dos tipos distintos de entidades, los cuales quedan claramente diferenciados en el texto:

- **Los Operadores de Servicios Esenciales**, que serán designados por la autoridad competente, en función de si prestan un servicio esencial que dependa de redes y sistemas de información, y teniendo en cuenta además si un incidente sobre el servicio pudiera tener efectos perturbadores en la sociedad. A nivel nacional, los sectores estratégicos sobre los que se identificarán a estos operadores se han equiparado a aquellos reflejados en la LPIC.
- **Los Proveedores de Servicios Digitales**, que serán aquellas entidades que presten un servicio digital (en el sentido recogido en la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y comercio electrónico (LSSI), que sean (1) mercados en línea, (2) motores de búsqueda en línea, o (3) servicios de computación en la nube; siempre que no sean PYMEs.

Respecto a la aplicación de la Ley, debe destacarse por tanto que, si bien la identificación de los OES se realizará por los órganos y procedimientos previstos en la LPIC; los proveedores de servicios digitales serán los que, proactivamente, tendrán que comunicar su actividad a la autoridad competente en el plazo de tres meses desde que la inicien.

¿Qué otros organismos son importantes dentro de la propia Ley?

- **Autoridades competentes**, que serán quienes ejerzan las funciones de vigilancia y apliquen el régimen sancionador. Según el tipo de entidad, se distinguen los siguientes:
  - CNPIC: para todos aquellos OES que sean Operadores Críticos
  - CCN: para todos aquellos OES y DSP que no sean Operadores Críticos y formen parte del sector público.
  - Autoridad sectorial correspondiente por razón de la materia, según se determine reglamentariamente: para todos aquellos OES que no sean operadores críticos y no formen parte del sector público.
  - Secretaría de Estado para el Avance Digital, del Ministerio de Energía, Turismo y Agenda Digital: para todos aquellos DSP que no sean operadores críticos y no formen parte del sector público.
- **Equipos de respuesta a incidentes de seguridad informática de referencia** (CSIRT), que serán los encargados de analizar los riesgos y supervisar los incidentes a escala nacional, difundiendo alertas y aportando soluciones para mitigar sus efectos. Según el tipo de entidad, se distinguen los siguientes:
  - CCN-CERT: para los OES que formen parte del sector público, y aquellos DSP que forman parte de la comunidad de referencia del CCN-CERT
  - INCIBE-CERT: para los OES que no formen parte del sector público, y aquellos DSP que no forman parte de la comunidad de referencia del CCN-CERT.
  - ESPDEF-CERT: cooperará con CCN-CERT e INCIBE-CERT cuando lo requieran para apoyar a los OES, y siempre que tenga incidencia en la Defensa Nacional.
- **Punto de Contacto Único**, que será el encargado de garantizar una cooperación transfronteriza con las autoridades competentes y los CSIRT de otros estados miembros, y que será ejercido por parte del Departamento de Seguridad Nacional del Consejo de Seguridad Nacional.

¿Qué requerimientos de seguridad tendrán que cumplir los OES y DSP?

Según el artículo 16 de la Ley, "Los OES y los DSP deberán 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".

De la misma manera, la propia Ley indica que las medidas necesarias para cumplir con esto por parte de los OES se desarrollarán reglamentariamente, no haciendo dicha especificación para los DSP.

A continuación, se representa cuáles son los aspectos relacionados con requerimientos de seguridad reflejados en la Ley que afectarán a cada uno de los tipos de entidades.

Requisito de seguridad	OES	DSP
Designar y comunicar 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.	Sí	No
Establecimiento de desarrollos reglamentarios, órdenes ministeriales, instrucciones y guías que permitan detallar las obligaciones específicas	Sí	No
Determinación de medidas técnicas y de organización para gestionar los riesgos	Sí	Sí
Proporcionar toda la información necesaria para evaluar la seguridad de las redes y sistemas de información, incluyendo la política de seguridad	Sí	Sí*
Proporcionar información sobre la aplicación efectiva de la política de seguridad	Sí	Sí*
Ser auditado, o ser obligado a pasar una auditoría externa, solvente e independiente sobre la seguridad de las redes y sistemas de información	Sí	Sí*
Ser requerido para subsanar las deficiencias detectadas según la información recabada	Sí	Sí*

* Según el artículo 33, "la autoridad competente para la supervisión de los servicios digitales sólo inspeccionará el cumplimiento de las obligaciones derivadas de este real decreto-ley cuando tenga noticia de algún incumplimiento, incluyendo por petición razonada de otros órganos o denuncia".

¿Qué requerimientos de notificación tendrán que cumplir los OES y DSP?

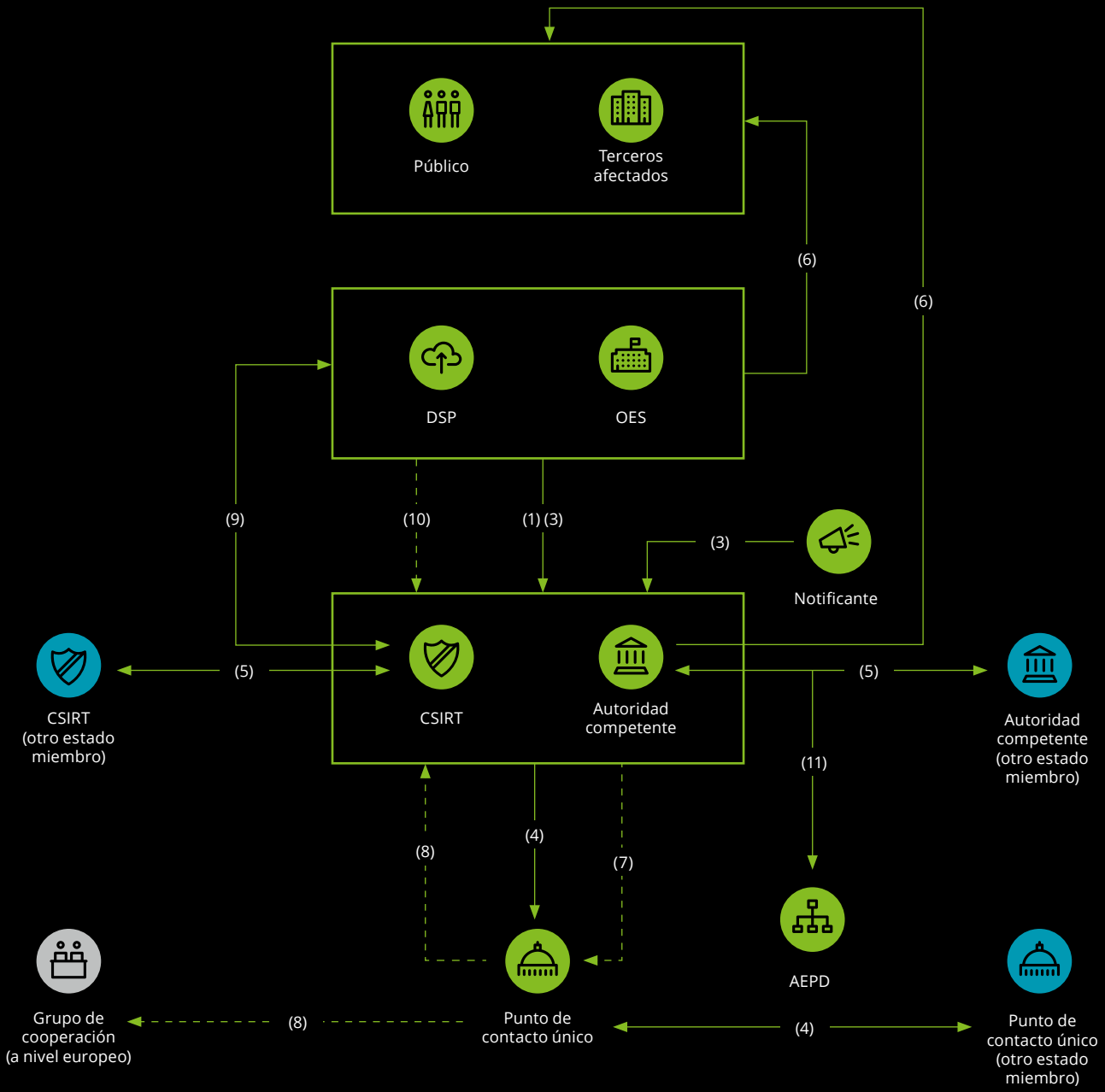
La Ley introduce un conjunto de requerimientos para identificar el impacto de un incidente, de forma que en función de los mismos puedan determinarse las obligaciones de notificación que deben cumplirse. A continuación se muestran los mismos, según la entidad afectada sea un OES o un DSP:

Criterios para determinar si un incidente es significativo	OES	DSP*
Número de usuarios afectados	Sí	Sí
Duración del incidente	Sí	Sí
Extensión o áreas geográficas afectadas	Sí	Sí
Grado de perturbación del funcionamiento del servicio	Sí	Sí
Alcance del impacto en actividades económicas y sociales cruciales	Sí	Sí
Importancia de los sistemas afectados o de la información afectada por el incidente para la prestación del servicio esencial	Sí	No
Daño a la reputación	Sí	No

*El propio texto de la Ley refleja que las consideraciones para determinar si un incidente es o no significativo deben ser las reflejadas en los actos de ejecución elaborados a nivel europeo, acto que ya ha sido elaborado y que incluso ha fijado unos umbrales a tener en cuenta ("Reglamento de Ejecución por el que se establecen normas para la aplicación de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo en lo que respecta a la especificación de los elementos que han de tener en cuenta los proveedores de servicios digitales para gestionar los riesgos existentes para la seguridad de las redes y sistemas de información, así como de los parámetros para determinar si un incidente tiene un impacto significativo").

En la propia Ley se definen obligaciones de notificación entre los diferentes actores involucrados, incluyendo OES, DSP, las autoridades competentes, los CSIRT, el Punto Único de Contacto, e incluso el público u otros organismos en otros estados miembros o a nivel europeo.

La siguiente figura muestra las diferentes notificaciones, comunicaciones e intercambios de información entre los distintos actores previstas por la Ley.



Asimismo, el detalle de cada una de las notificaciones reflejadas en la figura anterior se describe a continuación.

Requerimientos de notificación comunicación e intercambios de información relativa a incidentes	
(1)	Según el artículo 19.1 y 19.2, los operadores de servicios esenciales y los proveedores de servicios digitales notificarán a la autoridad competente, a través del CSIRT de referencia, los incidentes que puedan tener efectos perturbadores significativos en dichos servicios.
(2)	Según el artículo 20, se protege al notificante, no sujetándole a mayor responsabilidad por el mero hecho de notificar incidentes; y protegiendo contra consecuencias adversas a empleados y personal con relación laboral o mercantil que informen de incidentes.
(3)	Según el artículo 24, los OES y DSP, así como cualquier otra parte interesada, que tengan constancia de incidentes o de incumplimientos de requisitos de seguridad que afecten a servicios ofrecidos en España por proveedores establecidos en otros Estados Miembro, lo podrán notificar a la autoridad competente.
(4)	Según el artículo 25, las autoridades competentes y CSIRT informarán a través del punto de contacto único a los otros estados miembros, así como se remitirá por parte del contacto único a las autoridades y CSIRT de referencia la información necesaria en caso de que provenga de otro Estado Miembro.
(5)	Según el artículo 25.3, también se podrán realizar intercambios de información entre autoridades competentes de los estados miembro, y también entre los CSIRT de los estados miembro.
(6)	Según el artículo 26, la autoridad competente podrá exigir al OES o al DSP que informen al público o a terceros interesados sobre los incidentes, o bien que sea la misma autoridad competente la que lo realice.
(7)	Según el artículo 27.1, las autoridades competentes transmitirán al punto de contacto único un informe anual sobre los incidentes.
(8)	Según el artículo 27.2, el punto de contacto único remitirá al grupo de cooperación antes del 9 de agosto de cada año un informe anual recibido sobre las notificaciones recibidas, y lo remitirá a las autoridades competentes y CSIRT de referencia.
(9)	Según el artículo 28.1 los OES y DSP deberán solicitar ayuda a los CSIRT de referencia cuando no puedan resolver los incidentes por sí mismos, y atenderán a las indicaciones recibidas.
(10)	Según el artículo 28.2 los OES y DSP deben proporcionar al CSIRT y a la autoridad competente toda la información requerida para el desempeño de sus funciones.
(11)	Según el artículo 29, las autoridades competentes y CSIRT cooperarán con la Agencia Española de Protección de Datos cuando den lugar a violaciones personales.

Además, la propia Ley prevé una serie de aspectos significativos en lo que a la notificación de incidentes se refiere, como son:

- La utilización de una plataforma común por parte de las autoridades competentes y los CSIRT para facilitar y automatizar los procesos de notificación, comunicación e información sobre incidentes (según el artículo 19.4), y que además podrá ser empleada para la notificación de vulneraciones de seguridad de datos personales según el Reglamento General de Protección de Datos.

- La necesidad de fijar distintas comunicaciones durante todo el proceso (según el artículo 22), mediante una primera notificación sin dilación indebida, notificaciones intermedias de actualización, y una notificación final tras su resolución.

¿Cuáles son las sanciones a las que están expuestas las entidades?

De acuerdo al artículo 36, las sanciones pueden ser leves, graves o muy graves, con una cuantía que podrá llegar **hasta 1.000.000€** en función del tipo de sanción, teniendo en cuenta un conjunto de criterios establecidos en la Ley (grado de culpabilidad o la existencia de intencionalidad, continuidad o persistencia en la conducta infractora, naturaleza y cuantía de los perjuicios causados, etc.), aplicando los criterios de proporcionalidad que permitan que la sanción sea lo más justa posible.

Las sanciones serán impuestas por parte del órgano de la autoridad competente que se determinará reglamentariamente, salvo en el caso de infracciones muy graves, que correrá a cargo del Ministro competente correspondiente a cada autoridad competente.

Conclusiones y próximos pasos

A fecha de 9 de noviembre de 2018, España ha comenzado a identificar a los Operadores de Servicios Esenciales correspondientes a los sectores estratégicos de energía, transporte, salud, sistema financiero, agua, e infraestructuras digitales.

De la misma forma, a fecha de 9 de noviembre de 2019, se **cumplirá la fecha límite para identificar la lista de servicios esenciales e identificación de OES** en el resto de sectores estratégicos recogidos en el anexo de la LPIC.

Además de esta identificación de los servicios esenciales y los Operadores de Servicios Esenciales asociados, la Ley prevé el desarrollo reglamentario de la misma, así como la elaboración de órdenes ministeriales, instrucciones técnicas y guías orientativas que detallarán un conjunto de aspectos que no han sido especificados en la Ley actual.

Deloitte.

Diseñado y producido por el Dpto. de Comunicación, Marca y Desarrollo de Negocio, Madrid.