CNMC
COMISIÓN NACIONAL DE LOS MERCADOS Y LA COMPETENCIA

INFORME SOBRE EL PROYECTO DE REAL DECRETO POR EL QUE SE DESARROLLA EL REAL DECRETO-LEY 12/2018, DE 7 DE SEPTIEMBRE, DE SEGURIDAD DE LAS REDES Y SISTEMAS DE INFORMACIÓN

IPN/CNMC/036/19

SALA DE SUPERVISIÓN REGULATORIA

Presidenta
Dª. María Fernández Pérez

Consejeros
D. Benigno Valdés Díaz
D. Mariano Bacigalupo Saggese
D. Bernardo Lorenzo Almendros
D. Xabier Ormaetxea Garai

Secretario de la Sala
D. Joaquim Hortalà i Vallvé, Secretario del Consejo

En Madrid, a 14 de enero de 2020

La Sala de Supervisión Regulatoria de la Comisión Nacional de los Mercados y la Competencia, en su reunión de 14 de enero de 2020, ha aprobado el presente informe relativo al proyecto de Real Decreto por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

1. OBJETO DEL INFORME Y HABILITACIÓN COMPETENCIAL

1.1 Objeto y descripción del informe

Con fecha 12 de noviembre de 2019 la Secretaría General Técnica del Ministerio de Economía y Empresa remitió a la Comisión Nacional de los Mercados y la Competencia (en adelante, CNMC) el proyecto de Real Decreto por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, junto con la Memoria del análisis de impacto normativo, con el objeto de que la CNMC emita el informe de acuerdo con lo dispuesto en el artículo 5.2.a) de la Ley 3/2013, de 4 de junio, de creación de la CNMC.

El presente informe tiene por objeto analizar la citada propuesta y manifestar el parecer de la Sala de Supervisión Regulatoria sobre la misma.

1.2 Habilitación competencial

El artículo 5.2.a) de la Ley 3/2013, de 4 de junio, de creación de la Comisión Nacional de los Mercados y la Competencia (en adelante, Ley CNMC) establece que la CNMC participará, mediante informe, en el proceso de elaboración de normas que afecten a su ámbito de competencias en los sectores sometidos a su supervisión.

En este mismo sentido, el artículo 70.2.l) de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones (en lo sucesivo, LGTel), establece que, entre otras funciones, la CNMC será consultada por el Gobierno y el Ministerio de Industria, Energía y Turismo[1] en materia de comunicaciones electrónicas, particularmente en aquellas materias que puedan afectar al desarrollo libre y competitivo del mercado. Asimismo, se precisa que, en el ejercicio de esta función, la CNMC participará, mediante informe, en el proceso de elaboración de normas que afecten a su ámbito de competencias en materia de comunicaciones electrónicas.

En consecuencia, en aplicación de los anteriores preceptos, la CNMC es el organismo competente para elaborar el presente informe sobre el proyecto de Real Decreto por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, por afectar a sus competencias en materia de comunicaciones electrónicas.

La Sala de Supervisión Regulatoria resulta competente para su aprobación en virtud de lo previsto en el artículo 21.2 de la Ley CNMC y en el artículo 14.1.b) del Estatuto Orgánico de la CNMC aprobado por Real Decreto 657/2013, de 30 de agosto.

2. ANTECEDENTES

2.1 La Directiva NIS y el Real Decreto-Ley 12/2018

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 la Unión (en adelante, Directiva NIS –*Network and Information Security*-), establece los mecanismos necesarios para proporcionar una respuesta global en la Unión a los ataques contra las redes y sistemas de información de:

- Los operadores de servicios esenciales de actividades sociales o económicas cruciales en diferentes sectores estratégicos: energía, transporte, banca, sistema financiero, salud, agua e infraestructuras digitales.

[1] Entiéndase Ministerio de Economía y Empresa, según el Real Decreto 355/2018, de 6 de junio por el que se reestructuran los departamentos ministeriales.

- Proveedores de servicios digitales del tipo mercados en línea, motores de búsqueda y servicios de computación en nube.

La Directiva NIS ha sido transpuesta al ordenamiento jurídico español mediante el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, con el objeto de establecer un marco institucional para la coordinación entre las autoridades competentes en materia de seguridad y con los órganos de cooperación relevantes en el ámbito comunitario.

El Real Decreto-ley 12/2018 extiende su ámbito de aplicación más allá de los sectores estratégicos definidos en la Directiva NIS, al abarcar además otros sectores que estaban previamente recogidos en el anexo de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de infraestructuras críticas (en adelante, Ley PIC): administración, sector espacial, industria química, nuclear, instalaciones de investigación, alimentación y tecnologías de la información y las comunicaciones (TIC).

En la Directiva NIS, se consideran como operadores del sector de infraestructuras digitales únicamente a los Internet *eXchange Point* (IXP), proveedores de servicios de *Domain Name System* (DNS) y registros de nombres de dominio de primer nivel[2].

Así el Real Decreto-ley complementa y refuerza el marco normativo e institucional del Sistema de Protección de Infraestructuras Críticas establecido por la Ley PIC antes mencionada.

A su vez, los sistemas de información del sector público cuentan con la normativa especial del Esquema Nacional de Seguridad (Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica). En este sentido, la CNMC estaría sujeta a las obligaciones de dicho Real Decreto 3/2010 del Sector Público.

Según el artículo 16 del Real Decreto-ley 12/2018, las disposiciones reglamentarias tendrán en cuenta las obligaciones sectoriales, las directrices

[2] Un IXP o *"Internet eXchange Point"* es una instalación de red que permite interconectar más de dos sistemas autónomos independientes, principalmente para facilitar el intercambio de tráfico de Internet, sin requerir que pase por un tercer sistema autónomo, y sin modificar ni interferir de otra forma en dicho tráfico.

Un sistema de nombres de dominio «DNS», *"Domain Name System"*, por sus siglas en inglés, es un sistema distribuido jerárquicamente que responde a consultas proporcionando información asociada a nombres de dominio, en particular, la relativa a los identificadores utilizados para localizar y direccionar equipos en Internet. El proveedor de servicios de DNS es una entidad que presta servicios de DNS en Internet.

El registro de nombres de dominio de primer nivel es la entidad que administra y dirige el registro de nombres de dominio de Internet en un dominio específico de primer nivel.

relevantes que se adopten en el grupo de cooperación[3] y los requisitos en materia de seguridad de la información a las que estuviera sometido el operador en virtud de otras normas, como el citado Esquema Nacional de Seguridad.

Además de los operadores de servicios esenciales establecidos en España en los sectores estratégicos definidos en el anexo de la ley PIC, también están obligados al cumplimiento del Real Decreto-ley 12/2018 aquellos prestadores de servicios digitales que tengan su sede social en España y/o que constituyan su establecimiento principal en la Unión Europea, así como aquellos que designen en España a su representante en la Unión Europea.

Serán considerados servicios digitales aquellos servicios de la sociedad de la información (definidos en la Ley 34/2002, de 11 de junio, de servicios de la sociedad de la información y de comercio electrónico), que sean mercados en línea, motores de búsqueda en línea y/o servicios de computación en nube.

Sin embargo, el Real Decreto-ley 12/2018 no es de aplicación a:

- los operadores de redes y servicios de comunicaciones electrónicas y los prestadores de servicios electrónicos de confianza[4] que no sean designados como operadores críticos en virtud de la Ley PIC.
- los proveedores de servicios digitales cuando se trate de microempresas o pequeñas empresas[5].

La Comisión Nacional para la Protección de las Infraestructuras Críticas, dependiente de la Secretaria de Estado de Seguridad del Ministerio del Interior, es la encargada de aprobar la lista de servicios esenciales e identificar a los operadores que están sujetos a las obligaciones del Real Decreto-ley 12/2018.

[3] Establecido por el artículo 11 de la Directiva NIS.

[4] El Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE, en su artículo 3 define los servicios electrónicos de confianza como aquellos prestados habitualmente a cambio de una remuneración y consistentes en:

- La creación, verificación y validación de firmas electrónicas, sellos electrónicos o sellos de tiempo electrónicos, servicios de entrega electrónica certificada y certificados relativos a estos servicios.
- La creación, verificación y validación de certificados para la autenticación de sitios web.
- La preservación de firmas, sellos o certificados electrónicos relativos a estos servicios.

[5] 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.

De conformidad con el artículo 9 del Real Decreto-ley, las autoridades competentes en materia de seguridad de las redes y sistemas de información son las siguientes[6]:

- Para los operadores de servicios esenciales designados como operadores críticos conforme a la Ley PIC[7]: la Secretaría de Estado de Seguridad, del Ministerio del Interior, a través del Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC).

- Para los operadores del sector público de servicios esenciales no críticos y servicios digitales: el Ministerio de Defensa, a través del Centro Criptológico Nacional (CCN), siempre que no sean considerados como operadores críticos conforme a la Ley PIC.

- Para los operadores del sector privado de servicios esenciales no críticos, la autoridad sectorial correspondiente por razón de la materia, según se determine reglamentariamente (desarrollado en el proyecto de Real Decreto objeto del presente informe).

- Para los proveedores del sector privado de servicios digitales, la Secretaría de Estado para el Avance Digital (SEAD), del Ministerio de Economía y Empresa.

Finalmente, el Consejo de Seguridad Nacional, a través de su comité especializado en materia de ciberseguridad, es el responsable de establecer los mecanismos necesarios para la coordinación de las actuaciones de las autoridades competentes.

[6] La clasificación no sigue el orden establecido en el artículo 9 del Real Decreto-ley, centrándose el foco de atención en las diferentes autoridades competentes según el sector: público o privado.
[7] La Ley 8/2011 define a los operadores críticos como las entidades u organismos responsables de las inversiones o del funcionamiento diario de una instalación, red, sistema, o equipo físico o de tecnología de la información designada como infraestructura crítica.

Infraestructura crítica: las infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.

En la siguiente tabla se muestran de manera esquemática las diferentes autoridades competentes según el tipo de operador:

Tabla 1: Autoridades competentes definidas en el Real Decreto-ley 12/2018, de transposición de la Directiva NIS, para cada uno de los sectores y tipo de operador.

Tipo de operador	Autoridad competente	
Operador crítico	Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC)	Consejo de Seguridad Nacional
Resto de operadores esenciales y proveedores de servicios digitales del sector público	Centro Criptológico Nacional (CCN)	
Resto de operadores esenciales del sector privado	A determinar	
Proveedores de servicios digitales del sector privado	SEAD	

2.2 Redes y servicios de comunicaciones electrónicas

Las redes y servicios de comunicaciones electrónicas no están cubiertos por la Directiva NIS porque los mecanismos específicos para garantizar su seguridad e integridad están recogidos en las Directivas sectoriales y en la LGTel[8]. En su artículo 44, la LGTel establece un sistema de comunicación de incidentes paralelo al establecido en la Directiva NIS en el que los operadores que exploten redes o presten servicios de comunicaciones electrónicas disponibles al público están obligados a notificar al Ministerio de Industria, Energía y Turismo las violaciones de la seguridad o pérdidas de integridad que hayan tenido un impacto significativo en la explotación de las redes o los servicios. A su vez, el Ministerio comunicará dichos incidentes, violaciones de la seguridad o pérdidas de integridad a los siguientes organismos:

- A la Secretaría de Estado de Seguridad del Ministerio del Interior, aquellos incidentes que, afectando a los operadores estratégicos nacionales, sean de interés para la mejora de la protección de infraestructuras críticas, en el marco de la Ley PIC, de protección de infraestructuras críticas.

- A la CNMC, las violaciones de la seguridad o pérdidas de integridad a que se refiere el artículo 44 de la LGTel que afecten o puedan afectar a las obligaciones específicas impuestas por la CNMC en los mercados de referencia. Ciertamente, la integridad y seguridad de las redes y servicios afectaría a las obligaciones y condiciones de acceso que la CNMC puede establecer en el ejercicio de sus funciones de regulación sectorial ex ante

[8] El artículo 1.3 de la Directiva NIS establece que los requisitos de seguridad y notificación de la misma no aplican a las empresas sujetas a los requisitos de los artículos 13 bis y 13 ter de la Directiva Marco (Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas).

y de resolución de conflictos entre operadores, de conformidad con los artículos 13, 14 y 15 de la LGTel.

Del mismo modo el Código Europeo de Comunicaciones Electrónicas (CECE)[9] (pendiente de transposición), prevé en su artículo 40 que la Comisión Europea, teniendo en cuenta en la mayor medida posible el dictamen de la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA), pueda adoptar actos de ejecución en los que se detallen las medidas técnicas y organizativas de los proveedores de redes públicas de comunicaciones electrónicas o de servicios de comunicaciones electrónicas disponibles al público, que sean adecuadas y proporcionadas para gestionar adecuadamente los riesgos existentes para la seguridad de sus redes y servicios, así como las circunstancias, el formato y los procedimientos aplicables a los requisitos de notificación a la autoridad competente de los incidentes en materia de seguridad que hayan tenido consecuencias significativas en la explotación de las redes o los servicios.

Asimismo, una parte de los operadores de redes y servicios de comunicaciones electrónicas, en particular, aquellos que hayan sido designados como operadores críticos, también se encuentran en al ámbito de aplicación más extenso del Real Decreto-ley 12/2018, que incorpora sectores estratégicos adicionales según los definidos en la Ley PIC como, por ejemplo, el sector de las tecnologías de la Información y las Comunicaciones (TIC).

La Comisión Nacional para la Protección de las Infraestructuras Críticas (Comisión PIC) es la encargada de identificar el listado de servicios esenciales y operadores que los presten. Según la información publicada en la web del CNPIC[10], el 30 de octubre de 2018 la Comisión PIC designó a 132 operadores esenciales, referentes a 71 servicios esenciales aprobados[11], en los ámbitos estratégicos de energía, transporte, salud, sistema financiero, agua y TIC. Se señala que todos ellos son, a su vez, operadores críticos. Entre los servicios esenciales asociados al sector TIC se encuentran los servicios de acceso a Internet y los servicios de comunicaciones interpersonales[12].

[9] Directiva UE 2018/1972, del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por la que se establece el Código Europeo de Comunicaciones Electrónicas. Esta Directiva está vigente desde el día 20 de diciembre de 2018 pero está pendiente de transposición al ordenamiento jurídico español. El plazo de transposición finaliza el 20 de diciembre de 2020.
[10] http://www.cnpic.es/Biblioteca/Noticias/listado_servicios_esenciales.pdf
[11] Antes del 9 de noviembre de 2019, la CNPIC deberá aprobar los servicios esenciales y operadores esenciales correspondientes al resto de los sectores estratégicos, señalados en el anexo de la Ley 8/2011 PIC: administración, espacio, industria nuclear, industria química, instalaciones de investigación y alimentación.
[12] Los servicios esenciales declarados en el sector estratégico de las TIC son: servicios de acceso a internet, servicios de comunicaciones interpersonales, servicios de transporte de señales, servicios de comunicaciones audiovisuales de televisión digital terrestre, servicios de comunicaciones audiovisuales de radiodifusión sonora en OM y FM, servicios de la sociedad de la información, servicios de almacenamiento y procesamiento y seguridad TIC.

Por tanto, aquellos operadores de redes y servicios de comunicaciones electrónicas que presten estos servicios esenciales y que hayan sido considerados críticos estarán sometidos al ámbito de actuación del Real Decreto-ley, además de estar sometidos a los requisitos de seguridad estipulados en la normativa sectorial, concretamente, en el artículo 44 de la LGTel[13].

3. DESCRIPCIÓN DEL PROYECTO DE REAL DECRETO

El proyecto de Real Decreto objeto del presente informe, de desarrollo del Real Decreto-Ley antes explicado, consta de una Exposición de Motivos, 14 artículos organizados en 5 capítulos, 5 disposiciones adicionales, 4 disposiciones finales y un anexo.

El proyecto tiene la finalidad de desarrollar y concretar determinados aspectos no contemplados en el citado Real Decreto-ley 12/2018, que se resumen a continuación, y entre los que destacan:

- establecer las autoridades competentes en materia de seguridad de las redes y sistemas de información de los operadores del sector privado de servicios esenciales no críticos,
- instrumentar la cooperación y coordinación de las autoridades competentes a través de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes,
- señalar las funciones del punto de contacto único,
- establecer las medidas necesarias para el cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales,
- señalar las funciones del responsable de seguridad de la información de los operadores de servicios esenciales
- aprobar la Instrucción Nacional de Notificación y Gestión de Incidentes.

En el capítulo I, de disposiciones generales, se señala el objeto y ámbito de aplicación del real decreto (artículo 1) así como las definiciones de los términos utilizados en el proyecto (artículo 2).

El capítulo II, sobre el marco estratégico e institucional, se designa quiénes serán las autoridades competentes sectoriales de los operadores de servicios esenciales que no son operadores críticos a que se refiere el artículo 9.1.a) 2ª del Real Decreto-ley 12/2018 (artículo 3). El artículo 4 desarrolla la cooperación

[13] De hecho, esta singularidad ha sido puesta de manifiesto en el Informe de la Comisión Europea al Parlamento Europeo y al Consejo, Informe COM(2019) 546 de 28 de octubre de 2019, en el que se evalúa la coherencia de los enfoques adoptados por los Estados Miembros en la identificación de los operadores de servicios esenciales.

y coordinación de los CSIRT[14] de referencia a través de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes y determina qué operadores tienen incidencia en la Defensa Nacional. Del mismo modo define los supuestos de especial gravedad que requieran un nivel de coordinación superior al necesario en situaciones ordinarias. El artículo 5 desarrolla las funciones del Consejo de Seguridad Nacional, como punto de contacto único, para la coordinación de las actuaciones de las autoridades competentes.

El capítulo III, sobre los requisitos de seguridad, desarrolla en su artículo 6 las medidas para el cumplimiento de las obligaciones de seguridad en el caso de los operadores de servicios esenciales. El artículo 7 define la labor del responsable de seguridad de la información de los operadores de servicios esenciales, como punto de contacto y coordinación técnica con la autoridad competente respectiva.

El capítulo IV, de gestión de incidentes de seguridad, desarrolla en su artículo 8 la obligación de los operadores de servicios esenciales y los proveedores de servicios digitales de gestionar y resolver los incidentes de seguridad que afecten a las redes y sistemas de información utilizados para la prestación de sus servicios, tanto si se trata de redes y servicios propios como de proveedores externos. Los artículos 9 a 12 establecen el mecanismo de notificación por los operadores de servicios esenciales, mediante el que se determina que los incidentes con un nivel de peligrosidad alto, muy alto o crítico deben ser comunicados a la autoridad competente (a través del CSIRT de referencia), siguiendo la Instrucción Nacional de Notificación y de Gestión de Incidentes contenida en el anexo del proyecto y, utilizando, para ello, el procedimiento de notificación de incidentes que se articula a través de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes.

El capítulo V, sobre supervisión, dispone en un único artículo 14 la obligación de colaboración de los operadores de servicios esenciales y de los proveedores de servicios digitales con las autoridades competentes. Las autoridades competentes, asimismo, podrán requerir la colaboración de los CSIRT de referencia para el ejercicio de su función de supervisión, por medio de: i) ejercer actuaciones inspectoras o ii) requerir al operador de servicios esenciales la remisión de un informe de auditoría.

La disposición adicional primera establece que las referencias a los Ministerios, órganos y entidades previstos en el artículo 3 del proyecto de Real Decreto se entenderán realizadas a aquellos que en un futuro les pudieran sustituir o asumir sus competencias.

La disposición adicional segunda determina que los operadores de servicios esenciales tendrán la obligación de comunicar a la autoridad competente

[14] Los CSIRT (*Computer Security Incident Response Team*) son los equipos de respuesta a incidentes que analizan riesgos y supervisan incidentes a escala nacional, difunden alertas sobre ellos y aportan soluciones para mitigar sus efectos.

respectiva la identidad del responsable de la seguridad de la información del operador en el plazo de tres meses desde la entrada en vigor del real decreto.

La disposición adicional tercera prevé la posibilidad de que el Consejo de Seguridad Nacional apruebe orientaciones en relación con la Instrucción Nacional de Notificación y Gestión de Incidentes recogida en el anexo del Real Decreto que podrán recogerse en una Guía Nacional de Notificación y Gestión de Ciberincidentes.

Finalmente, la disposición adicional cuarta aclara el régimen específico del Banco de España, entendiéndose que las disposiciones del proyecto no entran en conflicto con las funciones asignadas al Banco de España, al Banco Central Europeo y el Sistema Europeo de Bancos Centrales.

El Anexo contiene la "Instrucción Nacional de notificación y gestión de ciberdelicuentes", que obliga a los operadores a comunicar los incidentes que se caractericen con un nivel de peligrosidad alto, muy alto o crítico.

Asimismo, se lleva a cabo una clasificación de la tipología de los incidentes (desde Spam o delitos de odio hasta ataques dirigidos a organizaciones concretas mediante mecanismos sofisticados –APT-), estableciendo la peligrosidad de cada tipología de la amenaza. Del mismo modo, se establece el nivel de impacto del ciberincidente en función de unos parámetros relacionados con la afectación a las redes y sistemas del operador.

Finalmente, se determina la información a notificar por los sujetos obligados en el momento en que tengan conocimiento del incidente, así como, los plazos para las notificaciones iniciales, intermedias y final.

A continuación, se describen algunos de los aspectos más destacados del proyecto de Real Decreto.

3.1 Autoridades competentes

El proyecto de Real Decreto completa la designación de autoridades competentes establecida en el Real Decreto-ley 12/2018 (ver Tabla 1) respecto de aquellos operadores de servicios esenciales que no tienen la consideración de operadores críticos, ni se encuentran comprendidos en el ámbito de aplicación de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Las nuevas autoridades competentes para servicios esenciales de operadores no críticos son las siguientes:

Tabla 2: Autoridades competentes de los correspondientes operadores servicios esenciales privados que no tienen la consideración de operadores críticos.

Sector	Autoridades competentes
Transporte	Ministerio de Fomento, a través de la Secretaría de Estado de Infraestructuras, Transporte y Vivienda.
Energía	Ministerio para la Transición Ecológica, a través de la Secretaría de Estado de Energía.
Tecnologías de la información	Ministerio de Economía y Empresa, a través de la Secretaría de Estado para el Avance Digital.
Sistema financiero y tributario	i. Ministerio de Economía y Empresa, a través de la Secretaría de Estado de Economía y Apoyo a la Empresa, para las entidades aseguradoras. ii. Banco de España, para las entidades de crédito. iii. Comisión Nacional del Mercado de Valores, para las entidades que prestan servicios de inversión y las sociedades gestoras de instituciones de inversión colectiva.
Espacio	Ministerio de Defensa, a través de la Secretaría General de Política de Defensa.
Industria química	Ministerio de Interior, a través de la Secretaría de Estado de Seguridad.
Instalaciones de investigación	Ministerio de Ciencia, Innovación y Universidades, a través de la Secretaría de Estado de Universidades, Investigación, Desarrollo e Innovación.
Salud	Ministerio de Sanidad, Consumo y Bienestar Social, a través de la Secretaría General de Sanidad y Consumo.
Agua	Ministerio para la Transición Ecológica, a través de la Secretaría de Estado de Medio Ambiente
Alimentación	i. Ministerio de Agricultura, Pesca y Alimentación, a través de la Secretaría General de Agricultura y Alimentación. ii. Ministerio de Sanidad, Consumo y Bienestar Social, a través de la Secretaría General de Sanidad y Consumo. iii. Ministerio de Industria, Comercio y Turismo, a través de la Secretaría de Estado de Comercio.
Industria nuclear	i. Ministerio para la Transición Ecológica, a través de la Secretaría de Estado de Energía. ii. Consejo de Seguridad Nuclear.

3.2 Coordinación de las diferentes autoridades competentes y notificación de incidentes

Los operadores de servicios esenciales y las redes de defensa de España, tienen a su disposición una serie de equipos de respuesta o CSIRT (*Computer Security Incident Response Team*) de referencia que son los encargados de informar a instancias superiores de los incidentes de seguridad y dar respuesta a los mismos. El destinatario de las notificaciones es la autoridad competente respectiva, como se ha visto en apartados anteriores.

Los CSIRT de referencia[15] 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:

1. 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).
2. En los supuestos de especial gravedad, el CCN-CERT ejercerá la coordinación nacional de la respuesta técnica de los CSIRT.

El proyecto de Real Decreto desarrolla los mecanismos de coordinación de los CSIRT con las autoridades competentes que, a grandes rasgos, comprenden las siguientes actuaciones:

- Los operadores de servicios esenciales (y los proveedores de servicios digitales[16]) notificarán a la autoridad competente respectiva los incidentes con un nivel de impacto crítico, muy alto o alto, tan pronto como dispongan de la información, a través del CSIRT de referencia.
- Tras una primera notificación del incidente, se prevén también notificaciones intermedias, así como una notificación final del incidente tras su resolución donde se informará, en su caso, de las medidas correctoras que eventualmente tiene previsto adoptar el operador.
- El procedimiento de notificación de incidentes se articula a través de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes, a fin de permitir el intercambio de información entre los operadores de servicios esenciales y proveedores de servicios digitales, las autoridades

[15] Los CSIRT de referencia en España son los siguientes:

a) En lo concerniente a las relaciones con los operadores de servicios esenciales:
1. El CCN-CERT, del Centro Criptológico Nacional, al que corresponde la comunidad de referencia constituida por las entidades del Sector Público.
2. El INCIBE-CERT, del Instituto Nacional de Ciberseguridad de España, al que corresponde la comunidad de referencia de las entidades privadas.
3. El ESPDEF-CERT, del Ministerio de Defensa, que cooperará con el CCN CERT y el INCIBE-CERT en aquellas situaciones que se requiera el apoyo de los operadores de servicios esenciales y, necesariamente, para aquellos operadores que tengan incidencia en la Defensa Nacional.

b) El INCIBE-CERT 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 será, asimismo, equipo de respuesta a incidentes de referencia para los ciudadanos y resto de entidades no contempladas en los apartados anteriores.

[16] Las medidas aplican a los proveedores de servicios digitales en tanto que no se regule de modo diferente en el acto de ejecución previsto en el artículo 16.9 de 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 la Unión.

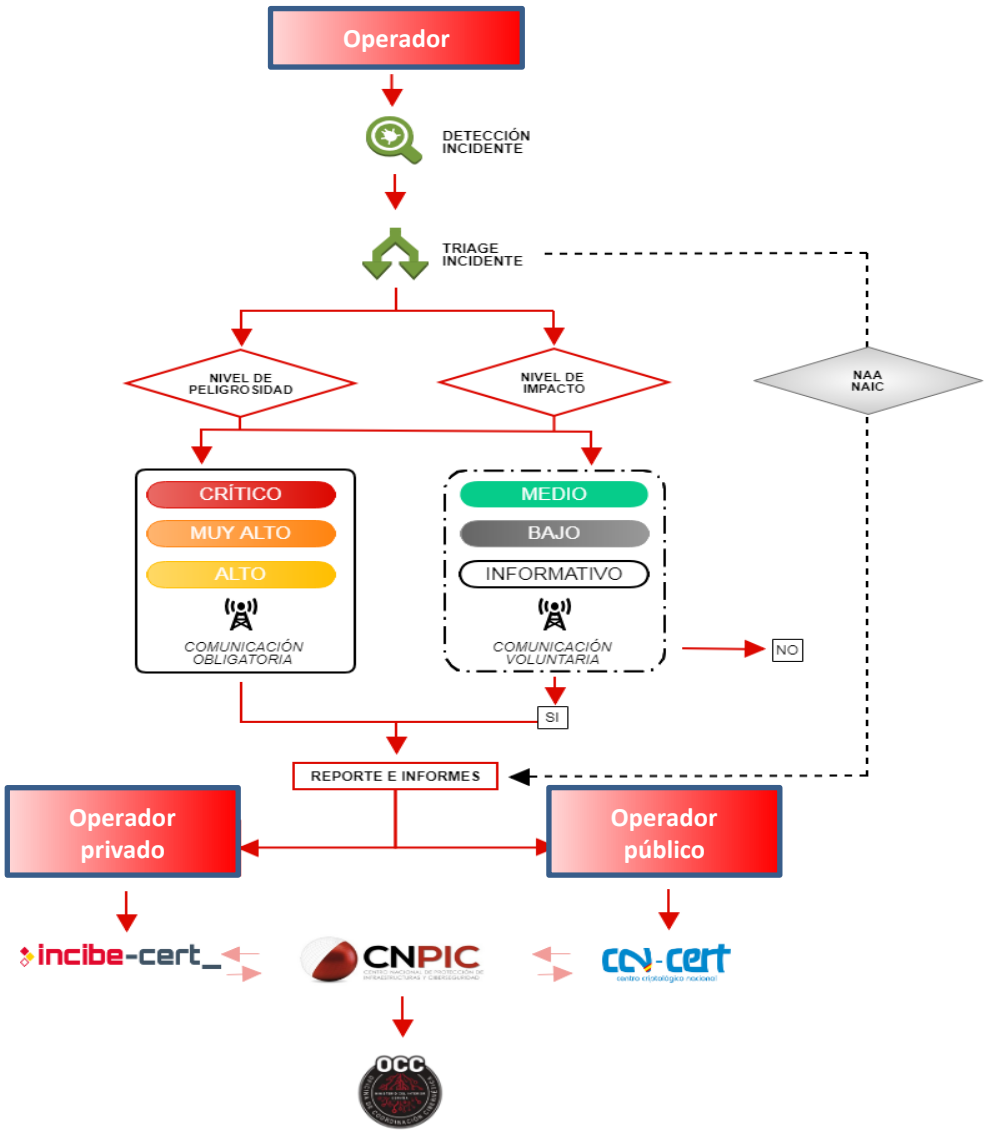
competentes y los CSIRT de referencia, garantizando la confidencialidad, integridad y disponibilidad de la información.

- Se atribuye al CCN-CERT la coordinación nacional de la respuesta técnica de los CSIRT en los supuestos de que se trate de un incidente con un impacto o nivel de peligrosidad muy alta o crítica, de acuerdo con lo establecido en el anexo (Instrucción nacional de notificación y gestión de ciberincidentes). Cuando el incidente pueda afectar 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).
- El CCN-CERT o CNPIC, según el caso, requerirán a los CSIRT de referencia determinada información, como la confirmación de que son correctos los datos asignados al incidente (clasificación, peligrosidad e impacto).
- El CSIRT de referencia, en colaboración con la autoridad competente, valorará si el incidente puede tener efectos perturbadores significativos para los servicios esenciales prestados en otros Estados miembros de la Unión Europea, informando en tal caso a los Estados miembros afectados, a través del punto de contacto único (el Consejo de Seguridad Nacional, a través del Departamento de Seguridad Nacional). El CSIRT debe elaborar un plan de acción para resolver el incidente con impacto transfronterizo.
- La guía nacional de notificación y gestión de ciberincidentes proporciona a los Responsables de Seguridad de la Información de los operadores (RSI) las directrices para el cumplimiento de las obligaciones de reporte de incidentes de ciberseguridad, consideradas como una referencia de mínimos en el que toda entidad, pública o privada, ciudadano u organismo, pueda encontrar un esquema y la orientación precisa acerca de a quién y cómo debe reportar un incidente de ciberseguridad acaecido en el seno de su ámbito de influencia.
- El Departamento de Seguridad Nacional es el encargado de aprobar orientaciones en relación con la Instrucción Nacional de Notificación y Gestión de Incidentes recogida en el anexo, así como la actualización de la Guía Nacional de Notificación y Gestión de Ciberincidentes[17].

En el siguiente esquema incluido en la Guía Nacional de Notificación y Gestión de Ciberincidentes se esboza el proceso de notificación y gestión de un incidente en el seno de su ámbito de influencia para toda entidad, pública o privada, ciudadano y demás organismos.

[17] Enlace a la Guía Nacional de Notificación y Gestión de Ciberincidentes. http://www.interior.gob.es/documents/10180/9771228/Gu%C3%ADa+Nacional+de+Notificaci%C3%B3n+y+Gesti%C3%B3n+de+Ciberincidentes.pdf/19676087-0253-4c58-bbb0-2fc58a5fd63b

Ilustración 1: proceso de notificación y gestión de un incidente, donde NAA se corresponde con el Nivel de Alerta Antiterrorista y NAIC es el Nivel de Alerta en Infraestructuras Críticas.



Fuente: Guía Nacional de Notificación y Gestión de Ciberincidentes

3.3 Funciones del punto de contacto único

El artículo 5 desarrolla las funciones de enlace del Consejo de Seguridad Nacional, a través del Departamento de Seguridad Nacional, como punto de contacto único a efectos de lo previsto en la Directiva NIS.

En particular, las funciones que se derivan del proyecto de Real Decreto son los siguientes:

- El Consejo de Seguridad Nacional comunicará a la Comisión Europea la lista de los operadores de servicios esenciales y, a los puntos de contacto únicos

de otros Estados, la intención de identificación de un operador de servicios esenciales de otro Estado miembro.

- Transmitirá a los puntos de contacto de otros Estados miembros la información sobre incidentes con impacto transfronterizo que les transmitan las autoridades competentes o CSIRT de referencia.
- A la inversa, notificará a los CSIRT y autoridades competentes los incidentes transfronterizos que puedan tener efectos perturbadores en los servicios esenciales.
- Dictará instrucciones a las autoridades competentes nacionales para que elaboren un informe sobre el tipo y número de incidentes de incidentes comunicados, sus efectos sobre los servicios y su carácter nacional o transfronterizo. Con la información recibida elaborará un informe anual resumido antes del 15 de febrero de cada año[18].

3.4 Medidas para el cumplimiento de las obligaciones de seguridad. Y funciones del responsable de seguridad de la información

El proyecto establece la obligación de los operadores de servicios esenciales y los proveedores de servicios digitales de adoptar las medidas técnicas y de organización adecuadas y proporcionadas para gestionar los riesgos que afecten a la seguridad de las redes y sistemas que utilicen, tanto propios como externos.

Los operadores de servicios esenciales deberán aprobar unas políticas de seguridad de las redes y sistemas de información, considerando, como mínimo, los siguientes aspectos: análisis y gestión de riesgos; gestión de riesgos de terceros o proveedores; catálogo de medidas de seguridad, organizativas, tecnológicas y físicas; gestión del personal y profesionalidad; adquisición de productos o servicios de seguridad: detección y gestión de incidentes: planes de recuperación y aseguramiento de la continuidad de las operaciones; mejora continua; interconexión de sistemas o registro de la actividad de los usuarios

En el proyecto se desarrolla también la figura de los responsables de seguridad. Los operadores de servicios esenciales deberán designar un responsable de seguridad de la información, cuyas funciones serán las siguientes:

- Elaborar las políticas de seguridad (técnicas y organizativas) para reducir al mínimo los efectos de los ciberincidentes, supervisar su efectividad y llevar a cabo los controles periódicos de seguridad.
- Preparar el documento denominado de Declaración de Aplicabilidad de medidas de seguridad que deberá remitirse a la autoridad competente, así como otra información que pueda ser solicitada (o por propia iniciativa) por parte del CSIRT o autoridad competente.

[18] Informe Anual de Seguridad Nacional 2018. Ver sección de ciberseguridad, pág. 61-73. https://www.dsn.gob.es/es/documento/informe-anual-seguridad-nacional-2018

- Remitir a la autoridad competente, a través del CSIRT de referencia, la notificación de incidentes que tengan efectos perturbadores en la prestación de servicios.
- Del mismo modo, recibir y supervisar las instrucciones y guías emanadas de la autoridad competente.

El responsable de seguridad debe contar con los siguientes requisitos:

- Contar con personal con conocimientos especializados y experiencia en sistemas de ciberseguridad.
- Contar con los recursos necesarios para el desarrollo de las funciones.
- Participar en todas las cuestiones de seguridad y con una comunicación directa con alta dirección.
- Mantener una independencia respecto a los responsables de las redes y sistemas de información.

3.5 Instrucción nacional de notificación y gestión de ciberincidentes (anexo)

Para la notificación de los incidentes de ciberseguridad se utilizará como criterio de referencia el nivel de peligrosidad que se asigne a un incidente, debiéndose comunicar los todos aquellos que se categoricen con un nivel alto, muy alto o crítico.

En la instrucción se lleva a cabo una clasificación de la taxononomía de los incidentes (contenido abusivo, dañino, obtención de información, intento de intrusión, disponibilidad, compromiso de la información, fraude, vulnerabilidad u otros) así como la asociación de cada uno de los incidentes a un nivel de peligrosidad (bajo, medio, alto, muy alto o crítico).

Del mismo modo, se lleva a cabo una enumeración de los criterios para la determinación del impacto de un cibercincidente por medio de la evaluación de las consecuencias que pueda tener en las funciones y actividades de la organización, en sus activos o en los individuos afectados. Asimismo, cada incidente se asociará a alguno de los niveles de impacto: sin impacto, bajo, medio, alto, muy alto o crítico.

Finalmente, en la Instrucción nacional de notificación y gestión de ciberincidentes se detallan los campos que deben remitir los operadores a la autoridad competente y los plazos para la notificación inicial, notificación intermedia y notificación final, según el nivel de peligrosidad o impacto.

4. VALORACION DEL PROYECTO DE ORDEN

Se valora positivamente la propuesta de Real Decreto por la que se desarrolla el Real Decreto-ley 12/2008, que incorpora al ordenamiento jurídico español la Directiva NIS, de cara a la puesta en marcha de los mecanismos de

coordinación, tanto nacional como internacional, que contribuirán a reducir el impacto de los ciberincidentes que ponen en peligro la seguridad pública y nacional.

Estas medidas son especialmente relevantes en un contexto en el que los ciberataques están en aumento. Según la información aportada por el CERT de Seguridad e Industria (INCIBE-CERT), operado por INCIBE bajo la coordinación con el Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC), se han resuelto un total de 123.064 incidentes de seguridad en 2017, un 6,77% más que en 2016.

Cabe destacar que las infecciones de programas que causan una denegación de servicio distribuido (ataque DDoS, *Distributed Denial of Service*) empiezan a afectar a dispositivos de control, medida o vigilancia remota que constituyen el denominado Internet de las Cosas (IoT).

A este respecto, cabe indicar que la CNMC prevé que el crecimiento de los dispositivos máquina a máquina (subconjunto de dispositivos IoT que requieren numeración para ser accesibles desde otras redes públicas) alcance un centenar de millones en el medio plazo (superior al número de líneas móviles), por lo que las medidas orientadas a prevenir incidentes de seguridad toman una relevancia significativa.

No obstante, se considera procedente hacer mención específica a las siguientes consideraciones:

1. El artículo 3 del proyecto de Real Decreto contiene una relación de las autoridades competentes en materia de seguridad de las redes y sistemas de información a los que están vinculados los operadores de servicios esenciales. Dicha relación cita expresamente a una serie de Ministerios tales como el Ministerio de Fomento para el sector transporte, el Ministerio para la Transición Ecológica en el sector de energía o el Ministerio de Economía y Empresa para el sector de tecnologías de la información.

   Asimismo, se incluye como autoridades competentes las diferentes autoridades nacionales independientes en sus respectivos sectores: el Banco de España o la Comisión Nacional del Mercado de Valores en el sector financiero y tributario. De manera específica, se hace una mención especial al Banco de España al señalarse en la disposición adicional cuarta que lo previsto en la normativa es de aplicación a este organismo en tanto en cuanto sea compatible con su naturaleza, funciones e independencia.

   No obstante, a pesar de que el artículo 3.1 (apartados “a”, “b” y “c”) se refiere como operadores de servicios esenciales que no sean operadores críticos a operadores de los sectores de transporte, energía y telecomunicaciones, no se hace mención a la CNMC, junto con los Ministerios correspondientes, como otro ejemplo de organismo independiente. Teniendo en cuenta las

funciones de supervisión y control de los mercados (y las nuevas competencias de energía), parecería lógico que se incluyera a este organismo en aras de asegurar que las medidas de seguridad que se aplican son compatibles con la normativa aplicable a los diferentes sectores cuya regulación está atribuida a la CNMC.

A estos efectos, se proponen los siguientes cambios en la redacción del citado artículo 3.1 (apartados a, b y c):

"Artículo 3. Autoridades competentes.

1. Son autoridades competentes de los operadores de servicios esenciales que no sean operadores críticos a que se refiere el artículo 9.1.a) 2.º del Real Decreto-ley 12/2018, de 7 de septiembre:

a) Respecto al sector del transporte:
i. El Ministerio de Transporte, Movilidad y Agenda Urbana, a través de la Secretaría de Estado de Transportes, Movilidad y Agenda Urbana.
ii. La Comisión Nacional de los Mercados y la Competencia.

b) Respecto al sector de la energía:
i. El Ministerio para la Transición Ecológica y Reto Demográfico, a través de la Secretaría de Estado de Energía.
ii. La Comisión Nacional de los Mercados y la Competencia.

c) Respecto al sector de las tecnologías de la información y las telecomunicaciones:

i. El Ministerio de Economía y Transformación Digital, a través de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales.
ii. *La Comisión Nacional de los Mercados y la Competencia.*
(…)"
"

2. El artículo 12 del proyecto de Real-Decreto contempla la gestión de los incidentes, con especial referencia a los intercambios de información que se produzcan entre los diferentes actores (autoridades competentes, CSIRT) y los operadores de servicios. Existe una mención a preservar, en la medida de lo posible, la confidencialidad de la información que recaben. Se sugiere hacer constar también que debe evitarse cualquier riesgo de intercambio de información entre los operadores que pudiera favorecer comportamientos de coordinación entre los mismos.

3. Por último, procede realizar la siguiente consideración formal. En la definición de redes y sistemas de información, que forma parte del Anexo del proyecto (apartado 7 del Anexo, actualmente, página 30), se declara que "*se entiende por este concepto uno de los tres siguientes puntos:*

- Una red de comunicaciones electrónicas ***en el sentido del artículo 2, letra a), de la Directiva 2002/21/CE****. (…)"*

El Real Decreto-ley 12/2018 se remite al Anexo II de la LGTel, para definir qué se entiende por redes de comunicaciones electrónicas. La LGTel transpone al derecho nacional, entre otras, la Directiva 2002/21/CE. Se recomienda incluir la misma referencia, ya que una vez la Directiva ha sido transpuesta al Derecho nacional, se aplica la norma nacional –debiendo ser esa la referencia-. Asimismo, la Directiva 2002/21/CE ha sido sustituida por la Directiva UE 2018/1972, del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por la que se establece el Código Europeo de Comunicaciones Electrónicas, pero está pendiente de transposición, por lo que actualmente ha de seguir aplicándose la LGTel.

5. CONCLUSIONES

Se valora positivamente la propuesta de Real Decreto por la que se desarrolla el Real Decreto-ley 12/2008, que incorpora al ordenamiento jurídico español la Directiva NIS, realizándose una serie de consideraciones específicas según se detallan en mayor medida en el apartado anterior sobre:

- La mención de la CNMC como autoridad independiente sectorial.
- El riesgo de intercambio de información entre operadores que pueda favorecer comportamientos de coordinación.
- El concepto de red de comunicaciones electrónicas.