MEMORIA DEL ANÁLISIS DE IMPACTO NORMATIVO DEL 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

FICHA DEL RESUMEN EJECUTIVO

Ministerio/Órgano proponente	Ministerio de Economía y Empresa Ministerio del Interior Ministerio de Defensa	**Fecha:** 12 de julio de 2019	
Título de la norma	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		
Tipo de Memoria	Normal☒ Abreviada ☐		
OPORTUNIDAD DE LA PROPUESTA			
Situación que se regula	La seguridad de las redes y sistemas de información utilizados en la provisión de servicios esenciales y de ciertos servicios digitales.		
Objetivos que se persiguen	Desarrollar el Real Decreto-ley 12/2018 que traspone al ordenamiento jurídico español 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 (la "Directiva 2016/1148"), en concreto, para: - Identificar a las autoridades sectoriales competentes de los operadores de servicios esenciales que no son operadores críticos, - Articular la cooperación y coordinación entre los CSIRT de referencia y de éstos con las autoridades competentes, - Desarrollar la obligación de los operadores de servicios esenciales de adoptar medidas para		

	gestionar los riesgos de seguridad de las redes y sistemas de información utilizados en la prestación de dichos servicios, - Regular la figura y funciones del responsable de seguridad de la información que designen los operadores de servicios esenciales, - Desarrollar las obligaciones de notificación de incidentes.
Principales alternativas consideradas	Ninguna. El desarrollo del Real Decreto-ley 12/2018 viene expresamente previsto su disposición final tercera, que habilita al Gobierno para el desarrollo reglamentario de la citada disposición. La opción de no hacer nada no es una alternativa, al ser necesario desarrollar el Real Decreto-ley 12/2018 que traspone la Directiva 2016/1148.
CONTENIDO Y ANÁLISIS JURÍDICO	
Tipo de norma	Real Decreto
Estructura de la Norma	El proyecto consta de Exposición de Motivos, 14 artículos organizados en 5 capítulos, 4 disposiciones adicionales, 4 disposiciones finales y un anexo.
Informes recabados	Deben recabarse los siguientes informes: - Informes de los Ministerios identificados como autoridades competentes en el artículo 3 del real decreto (artículo 26.5.1ª de la Ley 50/1997). - Informe preceptivo de la Secretaría General Técnica de los Ministerios proponentes: Mº de Economía y Empresa, Mº del Interior y Mº de Defensa (artículo 26.5.4ª de la Ley 50/1997). - Informe del Mº de Política Territorial y Función Pública (artículo 26.5. de la Ley 50/1997). - Informe del Consejo de Estado.

<table>
<tr><td></td><td colspan="2"></td></tr>
<tr><td>Trámite de audiencia</td><td colspan="2"></td></tr>
<tr><td colspan="3">ANÁLISIS DE IMPACTOS</td></tr>
<tr><td>ADECUACIÓN AL ORDEN DE COMPETENCIAS</td><td colspan="2">La Ley se dicta al amparo de las competencias exclusivas estatales en materia de telecomunicaciones y seguridad pública, previstas en el artículo 149.1.21ª y 29ª de la Constitución.</td></tr>
<tr><td rowspan="4">IMPACTO ECONÓMICO Y PRESUPUESTARIO</td><td>Efectos sobre la economía en general</td><td>La ley tendrá efectos positivos en la economía como consecuencia de la mejora en la seguridad de las redes y la información y la reducción del impacto de los incidentes de seguridad.</td></tr>
<tr><td>En relación con la competencia</td><td>☒ la norma no tiene efectos significativos sobre la competencia
☐ la norma tiene efectos positivos sobre la competencia
☐ la norma tiene efectos negativos sobre la competencia</td></tr>
<tr><td>Desde el punto de vista de las cargas administrativas</td><td>☐ supone una reducción de cargas administrativas.
☐incorpora nuevas cargas administrativas.
☒ no afecta a las cargas administrativas</td></tr>
<tr><td>Desde el punto de vista de los presupuestos, la norma
☐ Afecta a los presupuestos de la Administración del Estado
☐ Afecta a los</td><td>☐ implica un gasto

☐ implica un ingreso</td></tr>
</table>

	presupuestos de otras Administraciones Territoriales	
IMPACTO DE GÉNERO	La norma tiene un impacto de género	Negativo ☐ Nulo ☒ Positivo ☐
IMPACTO EN LA INFANCIA Y EN LA ADOLESCENCIA	La norma tiene impacto en la infancia y en la adolescencia	Negativo ☐ Nulo ☒ Positivo ☐
IMPACTO EN LA FAMILIA	La norma tiene impacto en la familia	Negativo ☐ Nulo ☒ Positivo ☐
OTROS IMPACTOS CONSIDERADOS	Impacto en la seguridad pública y en la seguridad nacional	El aumento en la seguridad de las redes y sistemas de información, así como la puesta en marcha de los mecanismos de coordinación, tanto nacional como internacional, contribuirán a reducir el impacto de los ciberincidentes que ponen en peligro la seguridad pública y que, en casos graves, podrían suponer riesgos para la seguridad nacional.
OTRAS CONSIDERACIONES		

La presente Memoria del Análisis de Impacto Normativo se emite de acuerdo con lo establecido en el artículo 26.3 de la Ley 50/1997, de 27 de noviembre, del Gobierno, y el Real Decreto 931/2017, de 27 de octubre, por el que se regula la Memoria del Análisis de Impacto Normativo.

Al no haberse aprobado la adaptación de la Guía Metodológica para la elaboración de la Memoria de Análisis de Impacto Normativo a que se refiere la disposición adicional primera del citado Real Decreto 931/2017, para la elaboración de esta Memoria se ha tenido en cuenta la Guía Metodológica aprobada por el Consejo de Ministros el 11 de diciembre de 2009.

ÍNDICE

A. OPORTUNIDAD DE LA PROPUESTA

1. MOTIVACIÓN

- *Causa de la propuesta.*

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 (la "Directiva") persigue dar una respuesta efectiva a los problemas de seguridad de las redes y sistemas de información mediante un planteamiento global en la Unión, integrando requisitos mínimos comunes en materia de desarrollo de capacidades y planificación, intercambio de información, cooperación y requisitos comunes de seguridad para los operadores de servicios esenciales y los proveedores de servicios digitales.

La Directiva 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 declarado de regular la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y los servicios digitales, estableciendo un sistema de notificación de incidentes por parte de los operadores, así como un marco institucional de cooperación entre autoridades, tanto a nivel nacional como comunitario.

De acuerdo con la Directiva, y dando un paso más en la transposición efectuada por el Real Decreto-ley 12/2018, el proyecto de real decreto pretende aumentar la seguridad lógica de los elementos empleados en la prestación de los servicios esenciales ofrecidos en los principales sectores de actividad económica y social, que cada vez se ven más afectados por incidentes que, en ocasiones, son de tal magnitud que afectan de modo significativo a la prestación de los servicios y suponen notables perjuicios a los usuarios afectados.

A título ilustrativo el número de incidentes gestionados por el CERT de Seguridad e Industria, del Instituto Nacional de Ciberseguridad (INCIBE), pasó de unos 18.000 en 2014 a 50.000 en 2015, 106.000 en 2016 y 123.000 en 2017.

Entre los incidentes de mayor repercusión, en el último año han tomado especial protagonismo las infecciones informáticas con programas de tipo ramsonware, que secuestran la información de los usuarios (por ejemplo, cifrando discos duros) solicitando un rescate para su recuperación. Estas infecciones se propagan en correos electrónicos que suplantan a usuarios legítimos ("phishing"), o alterando sitos web legítimos ("defacement") que infectan a los usuarios que las visitan.

También han sido relevantes incidentes que causan la indisponibilidad de sitios web desbordándolos con peticiones de acceso desde múltiples fuentes ("DDoS denegación de servicio distribuido") infectadas con programas que lanzan estos ataques de modo sincronizado, comenzando a afectar este tipo de infecciones a dispositivos de control, medida o vigilancia remota (que constituyen la llamada "Internet de las cosas" - IoT) que están empezando a desplegarse masivamente tanto por empresas como por particulares, y por sus especiales características en ocasiones no tienen las medidas de protección adecuadas.

- *Identificación de los colectivos afectados*

El Real Decreto-ley 12/2018 extiende su ámbito de aplicación, más allá de la relación mínima de sectores y subsectores prevista en la Directiva, a los sectores considerados en la Ley 8/2011 de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. De esta forma, se incluyen sectores adicionales a los contemplados en el anexo II de la Directiva (administración, sector espacial, industria química, nuclear, instalaciones de investigación y alimentación).

Estos operadores deben adoptar medidas técnicas y de organización adecuadas y proporcionadas para gestionar los riesgos, así como notificar sin dilación indebida los incidentes que tengan efectos significativos en la continuidad de los servicios esenciales que prestan.

De conformidad con lo previsto en la disposición adicional primera del Real Decreto-ley 12/2018, en el mes de noviembre de 2018 la Comisión Nacional para la Protección de las Infraestructuras Críticas aprobó una primera lista de los servicios esenciales y los operadores correspondientes a los sectores estratégicos energía, transporte, salud, sistema financiero, agua, e infraestructuras digitales.

De conformidad con la citada disposición, dicha Comisión deberá aprobar, con anterioridad al 9 de noviembre de 2019, la lista de servicios esenciales y operadores correspondientes al resto de los sectores estratégicos recogidos en el anexo de la Ley 8/2011, de 28 de abril.

Por otra parte, y de conformidad con lo previsto en su disposición adicional cuarta, los proveedores de servicios digitales no pertenecientes al sector público han procedido a comunicar su actividad a la Secretaría de Estado para el Avance Digital.

- *Interés público afectado*

El proyecto sirve al interés de garantizar la adecuada prestación de los servicios esenciales, así como de ciertos servicios digitales, en particular en lo concerniente a su continuidad y a la protección de la información empleada en su provisión.

Como consecuencia, tanto usuarios como empresas incrementarán su confianza en la utilización de las tecnologías de la información y de comunicaciones (TIC), lo que facilitará su aplicación más intensiva, y redundará en el desarrollo de nuevos servicios y funcionalidades, así como en mayores eficiencias en los existentes, especialmente en costes, contribuyendo al desarrollo económico y bienestar de los ciudadanos.

De modo secundario, la mejora generalizada en la seguridad de las redes y sistemas de información supondrá mayor robustez de estos sistemas ante ataques de tipo delictivo, contribuyendo a una mejora en la seguridad pública y, eventualmente, en la seguridad nacional, en la medida en que se consiga reducir la exposición a riesgos que pudieran resultar en situaciones de interés para la seguridad nacional y que obligarían a desencadenar mecanismos de gestión de crisis.

- *Por qué es el momento apropiado para hacerlo*

Una vez adoptada la relación inicial de servicios esenciales y los operadores que prestan dichos servicios, y habiendo comunicado los proveedores de servicios digitales su condición de tales, deben desarrollarse las disposiciones del Real Decreto-ley 12/2018 para el cumplimiento de la obligación de adoptar medidas de seguridad de las redes y sistemas de información por parte de los operadores de servicios esenciales, así como de notificación de incidentes.

Por otra parte, completada la trasposición de la Directiva por parte del conjunto de Estados miembros de la Unión Europea, emerge la oportunidad de aumentar las capacidades de cooperación en la materia con los países de nuestro entorno.

2. FINES Y OBJETIVOS PERSEGUIDOS

Los principales fines del proyecto al desarrollar las disposiciones del Real Decreto-ley 12/2018 coinciden con los marcados en la Directiva de impulsar el desarrollo del mercado interior a través de la mejora del nivel de seguridad en las redes y sistemas de información que sustentan la prestación de servicios en los sectores de mayor importancia para el desarrollo de actividades económicas y sociales.

De acuerdo con la Directiva, el desarrollo del Real Decreto-ley 12/2018 persigue impulsar el desarrollo del mercado interior a través de la mejora del nivel de seguridad en las redes y sistemas de información, aumentando la confianza de usuarios y prestadores de servicios y, por ende, la eficiencia y competitividad en su prestación, en particular, garantizando la continuidad en la prestación de servicios esenciales.

Se persigue, por tanto, aumentar la robustez de las redes y sistemas de información que sustentan la prestación de estos servicios, así como una mayor cooperación y coordinación en la gestión de incidentes de seguridad que puedan afectar a los mismos, tanto a nivel nacional como europeo, en línea con la estrategia nacional de ciberseguridad.

Se busca, asimismo, mejorar la eficacia en la lucha contra los delitos que involucran a las redes y sistemas de información, reduciendo sus efectos en la seguridad pública y, eventualmente, en la seguridad nacional.

Se persigue, en definitiva, articular un sistema general y coordinado de la ciberseguridad en España que garantice una respuesta ágil y eficaz ante los ciberincidentes.

En cuanto a los objetivos del proyecto, se considera necesario adoptar un real decreto de desarrollo del Real Decreto-ley 12/2018 para hacer posible su aplicación, en concreto, para:

- Identificar a las autoridades sectoriales competentes de los operadores de servicios esenciales que no son 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
- Articular la cooperación y coordinación entre los CSIRT de referencia y de éstos con las autoridades competentes
- Desarrollar la obligación de los operadores de servicios esenciales de adoptar medidas para gestionar los riesgos de seguridad de las redes y sistemas de información utilizados en la prestación de dichos servicios, sin perjuicio de la habilitación a las autoridades competentes para fijar mediante Orden Ministerial obligaciones específicas.
- Regular la figura y funciones del responsable de seguridad de la información que designen los operadores de servicios esenciales
- Desarrollar las obligaciones de notificación de incidentes, sin perjuicio de la habilitación a las autoridades competentes para fijar mediante Orden Ministerial obligaciones específicas.

3. ADECUACIÓN A LOS PRINCIPIOS DE BUENA REGULACIÓN Y ALTERNATIVAS

- *Adecuación a los principios de buena regulación*

El proyecto de real decreto es conforme con lo dispuesto en el artículo 129 apartado 1 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas en relación a los principios de buena regulación.

Responde a los principios de necesidad y eficacia, en tanto que se dicta en desarrollo de una disposición legal que es trasposición de una directiva europea.

También se satisface el principio de proporcionalidad, al no existir otras medidas menos gravosas para los operadores de servicios esenciales y proveedores de servicios digitales destinadas a cumplir la obligación de adoptar medidas técnicas y de organización para gestionar los riesgos para la seguridad de sus redes y sistemas de información, así como de notificar los incidentes que tengan efectos perturbadores significativos en los servicios que prestan.

De la misma manera, se cumple con el principio de seguridad jurídica, resultando el proyecto conforme a la Directiva europea que la origina y respetuosa con la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y su normativa de desarrollo, la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, así como la normativa comunitaria y nacional en materia de protección de datos.

Se ha cumplido igualmente con el principio de transparencia, al someterse al trámite de audiencia un texto que define claramente los objetivos de la iniciativa normativa y su justificación.

Por último, resulta conforme con el principio de eficiencia, dado que no se establecen cargas adicionales a las contempladas en el Real Decreto-ley.

- *Alternativas*

La única alternativa considerada ha sido la adopción de un real decreto de desarrollo del Real Decreto-ley 12/2018, según habilita expresamente su disposición final tercera.

La opción de no hacer nada no ha sido una alternativa, al ser necesario desarrollar el Real Decreto-ley 12/2018 que traspone la Directiva.

B. CONTENIDO Y ANÁLISIS JURÍDICO

1. CONTENIDO

El proyecto consta de una Exposición de Motivos, 14 artículos organizados en 5 capítulos, 4 disposiciones adicionales, 4 disposiciones finales, y un anexo.

El capítulo I, de disposiciones generales, señala en su artículo 1 el objeto y ámbito de aplicación del real decreto, este último por referencia al previsto en el Real Decreto-ley 12/2018. El artículo 2, de definiciones, aclara que las autoridades competentes son las identificadas tanto en el artículo 9 del Real Decreto-ley 12/2018 como en el artículo 3 del proyecto, y remite en cuanto al resto de conceptos utilizados a las definiciones previstas en el Real Decreto-ley.

El capítulo II, marco estratégico e institucional, designa en su artículo 3 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, por referencia a los sectores del transporte, energía, TIC, sector financiero, espacial, industria química, centros de investigación, sanitario e industria agroalimentaria y del agua.

También el artículo 3 prevé la posibilidad para las autoridades competentes de establecer, mediante orden ministerial, canales de comunicación oportunos con los operadores de servicios esenciales y con los proveedores de servicios digitales sujetos a su ámbito de supervisión.

El artículo 4 desarrolla la cooperación y coordinación de los CSIRT de referencia a través de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes. Este precepto desarrolla, conforme a la habilitación contenida en el artículo 11 del Real Decreto-ley 12/2018, qué operadores tienen incidencia en la Defensa Nacional, y determina los supuestos de especial gravedad que, cuando requieran un nivel de coordinación superior al necesario en situaciones ordinarias, atribuyen al CCN-CERT la coordinación nacional de la respuesta técnica de los CSIRT. Dichos supuestos hacen referencia a aquellos en los que, atendiendo a la naturaleza de las notificaciones inicial o sucesivas del incidente recibidas por el CSIRT de referencia, posean un impacto o nivel de peligrosidad muy alta o crítica de acuerdo con lo establecido en el anexo.

El artículo 5 regula 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, así como aquellas funciones de

coordinación de las actuaciones de las autoridades competentes que se derivan de lo previsto en el artículo 9.2 del Real Decreto-ley 12/2018, de 7 de septiembre.

El capítulo III, requisitos de seguridad, desarrolla en su artículo 6 las medidas para el cumplimiento de las obligaciones de seguridad a que se refiere el artículo 16 del Real Decreto-ley, que en el caso de los operadores de servicios esenciales se articulan a través de la política de seguridad de las redes y sistemas de información, atendiendo a los principios de seguridad integral, gestión de riesgos, prevención, respuesta y recuperación, líneas de defensa, reevaluación periódica y segregación de tareas. La relación de medidas adoptadas por el operador se formalizará en un documento denominado "Declaración de Aplicabilidad de medidas de seguridad", que será suscrito por el Responsable de Seguridad del sistema de información (cuya figura se desarrolla en el artículo siguiente), pudiendo ser complementadas, en particular, con las que, en su caso, establezcan las respectivas autoridades competentes.

El artículo 7 desarrolla, de conformidad con lo previsto en el artículo 16.3 del Real Decreto-ley, la figura del responsable de seguridad de la información, que deben designar los operadores de servicios esenciales con una función de punto de contacto y coordinación técnica con la autoridad competente respectiva.

El capítulo IV, gestión de incidentes de seguridad, incluye un artículo 8 que desarrolla 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 si lo son de proveedores externos. La citada obligación alcanza tanto a los incidentes detectados por el propio operador o proveedor como a los que les señalen el CSIRT de referencia o la autoridad competente.

El artículo 9 desarrolla las obligaciones de notificación por los operadores de servicios esenciales de los incidentes que puedan tener efectos perturbadores significativos en dichos servicios, así como de los incidentes que puedan afectar a las redes y sistemas de información empleados para la prestación de los servicios esenciales aun cuando no hayan tenido un efecto adverso real sobre aquéllos, por referencia a los niveles de impacto y peligrosidad, según sea el caso, previstos en la Instrucción Nacional de Notificación y de Gestión de Incidentes que se contiene en el anexo.

El procedimiento de notificación (artículo 10), que se efectuará a través del CSIRT de referencia, prevé una primera notificación del incidente, notificaciones intermedias y una notificación del incidente tras su resolución, informando del detalle de la evolución del suceso la valoración de la probabilidad de repetición del suceso, y las medidas correctoras que eventualmente tiene previsto adoptar el operador. Las notificaciones incluirán, en cuanto esté disponible, la información que permita determinar cualquier efecto transfronterizo del incidente.

El procedimiento de notificación de incidentes se articula a través de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes, regulada en el artículo 11, a fin de permitir el intercambio de información entre los operadores de servicios esenciales y proveedores de servicios digitales, las autoridades competentes y los CSIRT de referencia, garantizando la confidencialidad, integridad y disponibilidad de la información.

El artículo 12 desarrolla el artículo 14 del Real Decreto-ley sobre cooperación con otras autoridades con competencias en seguridad de la información y con las autoridades sectoriales, estableciendo que las consultas previstas en dicho artículo en materia de seguridad pública y seguridad ciudadana se realizarán a la Oficina de Coordinación Cibernética de CNPIC.

El artículo 13 regula el flujo de información sobre incidentes entre los CSIRT de referencia, los operadores de servicios esenciales (a través del responsable de seguridad de la información) y los prestadores de servicios digitales notificantes, y las autoridades competentes.

El capítulo V, sobre supervisión, desarrolla en su artículo 14 la obligación de colaboración de los operadores de servicios esenciales y los proveedores de servicios digitales con las autoridades competentes, que podrán requerir, asimismo, la colaboración de los CSIRT de referencia para el ejercicio de su función de supervisión.

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

La disposición adicional segunda señala, de conformidad con lo previsto en el artículo 6.1 del Real Decreto-Ley, que la identificación de los servicios esenciales y de los operadores que los presten se efectuará por los órganos y procedimientos previstos al efecto en el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

La disposición adicional tercera establece, para los operadores de servicios esenciales ya designados conforme a lo previsto en la disposición adicional primera del Real Decreto-ley 12/2018, la obligación de comunicar a la autoridad competente 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 cuarta prevé la posibilidad de adoptar, por parte del Consejo de Seguridad Nacional, una guía de cumplimiento de la Instrucción Nacional de Notificación y Gestión de Incidentes contenida en el anexo.

Por último, el proyecto contiene cuatro disposiciones finales sobre (i) habilitación para el desarrollo normativo, (ii) habilitación para la modificación del anexo del real decreto, (iii) título competencial y (iv) entrada en vigor.

El anexo contiene la Instrucción Nacional de Notificación y Gestión de Incidentes.

2. ANÁLISIS JURÍDICO

- Relación con las normas de rango superior:

  El proyecto de real decreto desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, que incorpora al ordenamiento jurídico español la Directiva (EU) 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.

  El rango formal del proyecto se justifica por lo previsto en la disposición final tercera del Real Decreto-ley 12/2018 que habilita al Gobierno para desarrollar reglamentariamente lo previsto en él sin perjuicio de la competencia de los Ministros para fijar las obligaciones específicas mediante Orden Ministerial en los supuestos previstos en su articulado.

  En concreto, las habilitaciones que comprende el Real Decreto-ley y que se desarrollan en este real decreto son las siguientes:

  - Art. 9.1 letra a 2º del Real Decreto-Ley: identificación de las autoridades sectoriales competentes de los operadores de servicios esenciales que no son operadores críticos.
  - Art. 9 Art. 11.1 letra a) 3º del Real Decreto-Ley: determinación de los operadores con incidencia en la Defensa Nacional.
  - Art. 11.2 primer párrafo del Real Decreto-Ley: determinación de los supuestos de especial gravedad que, cuando requieran un nivel de coordinación superior al necesario en situaciones ordinarias, atribuyen al CCN-CERT la coordinación nacional de la respuesta técnica de los CSIRT.
  - Art. 11.2 segundo párrafo del Real Decreto-Ley: coordinación de los CSIRT de referencia con el Ministerio del Interior, a través de la Oficina de Coordinación Cibernética del CNPIC, cuando las actividades que aquellos desarrollen puedan afectar de alguna manera a un operador crítico.

- Art. 16.2 del Real Decreto-Ley: obligación de los operadores de servicios esenciales de adoptar medidas para gestionar los riesgos de seguridad de las redes y sistemas de información utilizados en la prestación de dichos servicios.
- Art. 16.3 del Real Decreto-Ley: determinación del plazo para que los operadores de servicios esenciales designen y comuniquen a la autoridad competente la persona, unidad u órgano colegiado responsable de la seguridad de la información, y desarrollo de sus funciones específicas.
- Art. 19.1 segundo párrafo del Real Decreto-Ley: notificaciones sobre 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.
- Art. 19.5 del Real Decreto-Ley: obligaciones de notificación de incidentes por parte de los operadores de servicios esenciales.

La aprobación de la propuesta mediante una norma con rango de real decreto es coherente con los términos de las propias habilitaciones contenidas en el Real Decreto-ley 12/2018, que por defecto se interpreta que debe realizarse mediante la norma de rango reglamentario con mayor rango, es decir, mediante real decreto; toda vez que corresponde al Gobierno ejercer la potestad reglamentaria de acuerdo con la Constitución y las leyes (así, artículo 97 de la Constitución y artículo 1.1 de la Ley 50/1997, de 27 de noviembre).

Desde una perspectiva formal, con arreglo al artículo 24.1.c) de la Ley 50/1997, de 27 de noviembre, deben adoptar la forma de reales decretos acordados en Consejo de Ministros, las decisiones que aprueben normas reglamentarias de la competencia de éste.

- Relación con la Unión Europea:

- *Comunicación conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, de 7 de febrero de 2013, "Estrategia de ciberseguridad de la Unión Europea: un ciberespacio abierto, protegido y seguro"*
- *Directiva (EU) 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.*
- *Reglamento de ejecución (UE) 2018/151 de la Comisión de 30 de enero de 2018 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.

- Relación con otras normas:

- *Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas*
- *Ley 36/2015, de 28 de septiembre, de Seguridad Nacional*
- *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*

- Normas que se modifican:

  Ninguna. No obstante, según señala la disposición adicional segunda, la identificación de los servicios esenciales y de los operadores que los presten se efectuará por los órganos y procedimientos previstos al efecto en el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas, cuya modificación se está tramitando de forma paralela a este proyecto de real decreto.

- Normas que quedan derogadas:

  Ninguna.

- Futuras normas:

  El Real Decreto-ley 12/2018 y el proyecto de real decreto se completarán con la futura aprobación de las órdenes ministeriales que, para los respectivos ámbitos sectoriales, corresponde aprobar a las autoridades competentes para: (i) el establecimiento de factores específicos del sector para determinar si un incidente puede tener efectos perturbadores significativos (art. 6.1 del Real Decreto-Ley), (ii) el establecimiento de canales de comunicación oportunos con los operadores (art. 10 b) del Real Decreto-Ley), (iii) la coordinación con los CSIRT de referencia a través de protocolos de actuación (art.10 c) del Real Decreto-Ley), (iv) el establecimiento de obligaciones específicas para garantizar la seguridad de las redes y sistemas de información empleados por los operadores de servicios esenciales (art. 16.4 del Real Decreto-Ley), y (v) el establecimiento de obligaciones específicas de notificación por los operadores de servicios esenciales (art. 19.5 del Real Decreto-Ley).

C. ADECUACIÓN AL ORDEN DE DISTRIBUCIÓN DE COMPETENCIAS

El proyecto de real decreto no afecta a las competencias de las Comunidades Autónomas al dictarse en virtud de las competencias exclusivas en materia de telecomunicaciones y seguridad pública atribuidas al Estado por el artículo 149.1.21ª y 29ª de la Constitución.

D. IMPACTO ECONÓMICO Y PRESUPUESTARIO

- *Impacto económico general*

1. *Efectos en los precios de los servicios.*

   Las medidas tendrán un impacto neutral en los precios de servicios.

   El coste, para los prestadores de servicios afectados, de cumplir con las obligaciones de adoptar medidas de seguridad de las redes y sistemas de información debería ser marginal en el conjunto de costes del desarrollo de su actividad, ya que la obligación sólo recae sobre operadores de dimensión relevante dentro de cada uno de los sectores considerados, de los que cabe esperar ya tengan medidas de protección adecuadas, que sólo deberán adaptar a los requisitos previstos normativamente.

   Por otra parte, el esfuerzo económico dedicado a medidas de seguridad debe considerarse como una inversión, puesto que genera rendimientos positivos como resultado de la reducción del impacto de los incidentes de seguridad, siendo esto también aplicable a las medidas de seguridad de la información que afectan a las redes y sistemas considerados.

2. *Efectos en la productividad*

   Las medidas tendrán un efecto positivo sobre la productividad.

   El incremento de medidas de seguridad de las redes y sistemas de información empleados en la prestación de los servicios, junto con la mayor eficacia en la gestión de los riesgos de incidentes de seguridad de la información, reducirá el impacto perjudicial de estos incidentes en los servicios, redundando en una mayor productividad en su prestación.

3. *Efectos en el empleo*

Las medidas tendrán un efecto neutral sobre el empleo.

Los medios personales que deben destinar los prestadores de servicios para el cumplimiento de sus obligaciones vienen referidos, esencialmente, a la figura del responsable de seguridad de la información, que deben designar los operadores de servicios esenciales como punto de contacto y de coordinación técnica con la autoridad competente respectiva.

4. *Efectos sobre la innovación*

   Las medidas tendrán un efecto positivo sobre la innovación.

   La incorporación de las tecnologías de la información y las comunicaciones a los procesos productivos y de provisión de servicios está siendo uno de los principales mecanismos para la innovación en la totalidad de sectores de actividad económica y social. Sin embargo, las incertidumbres y amenazas ciertas que constituyen los incidentes de seguridad de la información, que afectan a las redes y sistemas de información empleados en dichos procesos, suponen un freno para la incorporación de estas tecnologías.

   Por tanto, el efecto positivo que tendrán las medidas previstas en el proyecto en la reducción del impacto de estos incidentes tendrá, como consecuencia indirecta, una reducción en este efecto freno y un efecto positivo en la innovación como consecuencia de la incorporación más intensiva de las tecnologías de la información y las comunicaciones.

5. *Efectos sobre los consumidores*

   Las medidas tendrán un efecto positivo sobre los consumidores.

   Los incrementos de productividad e innovación en la prestación de los servicios contribuirán a dinamizar los mercados de los diferentes sectores considerados, con el consiguiente aumento de la demanda de dichos servicios por parte de los consumidores (así como de las PyMEs que, en muchos casos, tienen necesidades similares a las de los consumidores).

   Este incremento de la demanda se verá reforzado, asimismo, por la mayor confianza de los consumidores en la aplicación de las tecnologías de información y comunicaciones a la prestación de servicios en los diferentes sectores considerados.

6. *Efectos en relación con la economía europea y otras economías*

   Las medidas tendrán un efecto positivo en relación con la economía europea.

   Dado que el proyecto desarrolla la norma nacional de transposición de la Directiva (UE) 2016/1148, que tienen entre sus objetivos el impulso

al mercado interior, contribuye igualmente a este objetivo, a través de tres elementos diferenciados:

- Reducción de lastre que suponen los incidentes de seguridad de las redes y sistemas de información en la prestación de los servicios de los sectores considerados, tanto en costes de prestación como en el freno a la innovación para incorporar tecnologías de información y comunicaciones.
- Reducción de las cargas administrativas para los prestadores que ofrecen servicios en varios países de la U.E., como consecuencia de la aproximación de las legislaciones en materias de requisitos de seguridad de las redes y sistemas de información.
- Fomento de la industria europea de ciberseguridad, al reducirse la fragmentación del mercado en este subsector como consecuencia de la citada aproximación de requisitos nacionales.

7. *Efectos sobre las PyMEs*

   Las medidas no tendrán impacto en costes para las PyMEs que, con carácter general, no estarán sometidas a las obligaciones en materia de seguridad de las redes y sistemas de información previstas para los operadores de servicios esenciales.

   Mención aparte merecen los proveedores de servicios digitales (buscadores en línea, mercados en línea y proveedores de servicios en nube) que, con excepción de las microempresas y pequeñas empresas, sí están sometidos a obligaciones de seguridad y de notificación de incidentes, pero de mucha menor intensidad que las aplicables a los operadores de servicios esenciales, en línea con lo previsto en la Directiva (UE) 2016/1148.

- *Efectos en la competencia y la unidad de mercado*

  El proyecto tiene un efecto neutral en la competencia en los diferentes mercados afectados y se adecúa a lo dispuesto en la Ley 20/2013, de 9 de diciembre, de Garantía de la Unidad de Mercado.

  Por otra parte, las obligaciones para los operadores se definen de acuerdo con el principio de proporcionalidad, afectando por igual a todos los operadores de cada sector que cumplan determinados criterios objetivos (ligados, fundamentalmente, a la importancia relativa de cada operador en el conjunto del sector), y correspondiendo a las autoridades competentes sectoriales la concreción de dichos criterios en el ámbito de que se trate.

- *Impacto presupuestario*

- Desde el punto de vista de los ingresos:

  Las medidas adoptadas no supondrán ingresos adicionales para el Estado.

- Desde el punto de vista del gasto:

  Tanto el desarrollo de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes, como las medidas de supervisión incluidas en este proyecto de real decreto, serán atendidas con las disponibilidades presupuestarias existentes en cada ejercicio y con los medios personales existentes y no supondrán incremento de dotaciones ni de retribuciones ni de otros gastos de personal.

E. CARGAS ADMINISTRATIVAS

A efectos de la Memoria, se consideran cargas administrativas todas aquellas tareas de naturaleza administrativa que deben llevar a cabo las empresas y los ciudadanos para cumplir con las obligaciones derivadas de la norma.

El proyecto no incrementa las cargas administrativas dado que, tanto la obligación de los operadores de servicios esenciales de realizar auditorías de seguridad de las redes y sistemas de información que utilicen, como la obligación de notificar los incidentes de seguridad de las redes y sistemas de información con efectos perturbadores significativos en los servicios esenciales o en los servicios digitales, fueron introducidas por el Real Decreto-ley 12/2018.

F. IMPACTO DE GÉNERO, EN LA INFANCIA, EN LA ADOLESCENCIA Y EN LA FAMILIA

El proyecto tiene un impacto de género nulo**,** debido a que su contenido no incluye ningún tipo de medida que pueda atentar contra la igualdad de oportunidades entre hombres y mujeres.

Por otra parte, tampoco se aprecia ningún impacto en la infancia, en la adolescencia y la familia.

G. OTRAS CONSIDERACIONES

El proyecto no tiene impacto en aspectos de carácter social y medioambiental, ni en materia de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad.

Se estima, por el contrario, que sí tiene impacto en la seguridad pública y en la seguridad nacional.

Al respecto, cabe señalar que la mayoría de incidentes que sufren las redes y sistemas de información se deben a fallos fortuitos, errores de configuración, uso o deficiencias de los sistemas. Sin embargo, un número significativo son causados por ataques deliberados, en muchos casos de tipo delictivo.

El impacto de las acciones criminales cibernéticas puede ser muy elevado ya que pueden lanzarse a distancia de modo anónimo y masivo, especialmente a través de Internet, y pueden tener efectos secundarios y repercusiones cruzadas en sistemas distintos a los atacados a causa de la alta interdependencia de los sistemas de información.

Por ello, el aumento en la seguridad de las redes y sistemas de información que se derivará de la aplicación de las disposiciones del proyecto, así como de los mecanismos de coordinación, tanto nacional como internacional desarrollados en ella, contribuirán a reducir el impacto de las actuaciones que ponen en peligro la seguridad pública y que, en casos graves, podrían suponer riesgos para la seguridad nacional.

H. TRAMITACIÓN Y CONSULTAS

El proyecto de real decreto ha sido elaborado por un equipo interministerial (Grupo de Trabajo) formado por el Ministerio de Economía y Empresa, designado como departamento responsable de la transposición, y los Ministerios de Interior (Centro Nacional de Protección de Infraestructuras y Ciberseguridad, CNPIC) y Defensa (Centro Criptológico Nacional, CCN), así como el Departamento de Seguridad Nacional (DSN), designados todos ellos como competentes en la transposición.

El proyecto debe ser sometido a los siguientes trámites:

1. **Trámite de audiencia** e información públicas previsto en el apartado 6 del artículo 26 de la Ley 50/1997, de 27 de noviembre, del Gobierno.

   De acuerdo con lo previsto en el apartado 2 del citado artículo, se ha prescindido del trámite de consulta pública al ser un proyecto de desarrollo del

Real Decreto-ley 12/2018 que no impone obligaciones adicionales a los destinatarios.

2. Informe de los **Departamentos Ministeriales** afectados en el ámbito de sus competencias, de acuerdo con el **artículo 26.5.1ª** de la Ley 50/1997.

En particular, debe recabarse el informe de los Ministerios afectados por la designación de autoridades competentes efectuada en el artículo 3 del proyecto.

3. De acuerdo con lo dispuesto en el **artículo 26.5.4º de la Ley 50/1997**, de 27 de noviembre, del Gobierno, resulta preceptivo el informe de la **Secretaría General Técnica de los Ministerios proponentes (Ministerio de Economía y Empresa, Ministerio del Interior, Ministerio de Defensa).**

4. Informe previsto en el **artículo 26.5.6ª de la Ley 50/1997, del Ministerio de la Presidencia y para las Administraciones Territoriales**, en tanto que el proyecto pudiera afectar a la distribución de competencias entre el Estado y las Comunidades Autónomas.

5. Se recabará informe de la **Agencia Española de Protección de Datos** .

6. Se someterá el proyecto al **Consejo de Ministros**, a fin de que este decida, de conformidad con lo dispuesto en el artículo 26.4 de la Ley 50/1997, sobre la realización de cualesquiera otros trámites que considere oportunos.

7. El proyecto de ley se publicará en el **Portal de Transparencia**, en virtud de lo previsto en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno (ex. artículo 7).

8. De acuerdo con lo previsto en el artículo 26.5.5ª de la Ley 50/1997, del Gobierno, se solicitará aprobación previa del **Ministerio de Política Territorial y Función Pública**.

9. En todo caso, se solicitará el dictamen del **Consejo de Estado** (artículo 21.2 Ley Orgánica 3/1980, de 22 de abril, del Consejo de Estado).