MEMORIA DE IMPACTO NORMATIVO SOBRE EL ANTEPROYECTO DE LEY DE SEGURIDAD DE LAS REDES Y SISTEMAS DE INFORMACIÓN

FICHA DEL RESUMEN EJECUTIVO

Ministerio/Órgano proponente	Ministerio de Energía, Turismo y Agenda Digital. Secretaría de Estado para la Sociedad de la Información y la Agenda Digital.	**Fecha**	
Título de la norma	Ley ……/2017 de ….de….., Seguridad de las Redes y Sistemas de Información		
Tipo de Memoria	Normal ☒ Abreviada ☐		
OPORTUNIDAD DE LA PROPUESTA			
Situación que se regula	Las actividades económicas y sociales se basan de modo creciente en el empleo de las redes y sistemas de información, cuya seguridad toma en consecuencia una importancia que justifica la actuación legislativa. Por otra parte, la interconectividad que caracteriza a las redes y sistemas de información causa interdependencias entre ellos, que se manifiestan singularmente en el caso los riesgos y amenazas a su seguridad, por lo que las distintas actuaciones destinadas a aumentar esta seguridad son más eficaces cuando se adoptan de forma coordinada, tanto entre los distintos países como entre los diferentes sectores y autoridades involucradas. En este contexto, la Ley propuesta regulará la seguridad de las redes y sistemas de información utilizados en la provisión de servicios esenciales y de ciertos servicios digitales, adoptando un enfoque común para diferentes sectores de actividad económica y social.		

Objetivos que se persiguen	La Ley persigue en primer lugar los objetivos marcados en 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, que transpone mediante esta Ley al ordenamiento jurídico Español. Se persigue 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, aumentando la confianza de usuarios y prestadores de servicios en la utilización de tecnologías de la información, lo que animará a su uso mejorando la eficiencia y competitividad en la prestación de servicios. También facilitará la prestación de servicios con alcance transeuropeo al establecer sobre sus prestadores requisitos similares en todos los Estados miembros en materia seguridad de las redes y sistemas de información, reduciendo la fragmentación nacional en estos requisitos, impulsando la industria europea 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. Las mejoras se conseguirán al aumentar la robustez de las redes y sistemas de información que sustentan estos servicios ante incidentes, ya sean provocados o fortuitos, asegurando que los prestadores adoptan medidas adecuadas ante los riesgos afrontados y al estado del arte, así como por mayor coordinación en la gestión de incidentes de seguridad de las redes y sistemas de información, tanto a nivel nacional como con los otros Estados de la Unión Europea. Para ello, partiendo de la identificación de los sectores considerados, prevé mecanismos para identificar los servicios esenciales de cada uno de ellos y para designar a sus principales prestadores, atendiendo para ello al impacto que podría tener en el servicio un incidente de seguridad sufrido por las redes y sistemas de información de cada prestador.

	Se definen mecanismos para asegurar que los prestadores designados adoptan medidas adecuadas para afrontar los riesgos de seguridad que afectan a las redes y sistemas de información que utilizan, fijando como objetivo prioritario de estas medidas el garantizar la continuidad en la prestación de los servicios esenciales. También se definen mecanismos para establecer sobre los prestadores designados la obligación de notificar los incidentes de seguridad que puedan tener impacto significativo en sus servicios previéndose asimismo la posibilidad de informar sobre estos incidentes a la población cuando sea adecuado para prevenir incidentes, actuar sobre uno en curso o cuando su divulgación redunde en el interés público. Se consideran diferenciadamente los denominados "servicios digitales": aquellos pertenecientes al ecosistema de Internet con los que usuarios finales tienen mayor contacto y que, por tener un carácter esencialmente transnacional, se justifica que se regulen asimismo con una perspectiva internacional. Para ellos la Ley se remite a las obligaciones establecidas de modo común para los prestadores de estos servicios a escala de la Unión Europea, a través de los actos de ejecución específicos previstos en la Directiva (UE) 2016/1148, recogiendo la Ley los instrumentos necesarios para hacer efectiva la aplicación de estas obligaciones sobre los prestadores que actúen bajo jurisdicción española. Para aumentar la eficacia de las medidas adoptadas se refuerzan los mecanismos de cooperación en materia de seguridad de las redes y sistemas de información con el resto de estados de la Unión Europea, y asimismo se prevé la existencia a nivel nacional de un marco institucional para su aplicación, que daría continuidad a la estrategia nacional de ciberseguridad. Por último se prevén mecanismos para garantizar la coordinación de las disposiciones de la Ley con otras normativas relevantes para estas materias, tanto de carácter transversal (fundamentalmente las relativas a la protección de infraestructuras críticas y a la protección de datos de carácter personal) como con las normativas

	sectoriales relacionadas con la seguridad de las redes y sistemas de información.
Principales alternativas consideradas	La principal alternativa considerada ha sido modificar la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, que presenta coincidencias en su ámbito material de aplicación y objetivos con los del anteproyecto presentado. Sin embargo la Ley 8/2011 tiene un alcance limitado en ciertos aspectos, ya que su objeto es mejorar la protección del Estado frente a atentados terroristas u otro tipo de amenazas, buscando para ello la protección contra ataques deliberados de las infraestructuras, ubicadas en territorio nacional, que son indispensables y no permiten soluciones alternativas para prestar determinados servicios. No entrarían pues en el alcance de la Ley 8/2011 la protección frente a eventos que no supongan una amenaza para el Estado, como son en particular los incidentes fortuitos y otros riesgos de seguridad que no tengan su origen en ataques deliberados de tipo delictivo o terrorista, de modo consecuente con el título competencial en materia de seguridad pública al amparo del que se dictó dicha ley. Tampoco entrarían en el alcance de esa ley las medidas destinadas a garantizar la continuidad en la prestación de servicios en supuestos en que, pese a existir alternativas, su disrupción pueda tener impactos significativos, ni tampoco permite obligar a adoptar medidas de protección sobre elementos ubicados fuera del territorio nacional que resulten sin embargo necesarios para la prestación de servicios en España. El alcance de la Ley 8/2011 es por otra parte más amplio en otros aspectos, ya que dedica gran parte de su contenido a garantizar la seguridad física de las infraestructuras empleadas para la prestación de servicios, y también considera aspectos que no son objeto de la presente Ley, como garantizar el eficaz funcionamiento de las Instituciones del Estado. Por ello se ha optado por establecer una ley de nueva planta que incorpora disposiciones que garantizan la

	coordinación de las actuaciones con las que se vienen desarrollando en el marco de la normativa de protección de infraestructuras críticas, minimizando así las cargas administrativas derivadas de la aplicación de la nueva ley.
CONTENIDO Y ANÁLISIS JURÍDICO	
Tipo de norma	Ley General.
Estructura de la Norma	El anteproyecto consta de Exposición de Motivos, 42 artículos organizados en 7 títulos, tres disposiciones adicionales, una disposición transitoria y tres disposiciones finales
Informes recabados	El texto del anteproyecto de Ley ha sido informado por el Consejo Nacional de Ciberseguridad
Trámite de audiencia	Para la elaboración del anteproyecto se han tomado en cuenta los comentarios recabados en el proceso de consulta previa, previsto en el artículo 26.2 Ley 50/1997, de 27 de noviembre, desarrollado entre los días 2 y 21 de diciembre de 2016.
ANÁLISIS DE IMPACTOS	
ADECUACIÓN AL ORDEN DE COMPETENCIAS	La Ley se dicta al amparo de la competencia exclusiva estatal en materia de telecomunicaciones, prevista en el artículo 149.1.21ª de la Constitución, y de competencia atribuida al Estado en virtud del artículo 149.1.29.ª de la Constitución Española en materia de seguridad pública.
IMPACTO ECONÓMICO Y PRESUPUESTARIO	Efectos sobre la economía en general: Las Tecnologías de la Información y de las Comunicaciones (TIC) constituyen en sí mismas uno de los sectores más dinámicos de la economía, y al mismo tiempo se están introduciendo de modo creciente en el resto de sectores económicos a través de las redes y sistemas de información que los sustentan.

		Por otra parte, la elevada complejidad, interdependencias e interconexiones, inherentes a estas redes y sistemas de información, las hacen especialmente vulnerables ante los incidentes que pongan en riesgo la seguridad de la información que tratan o las constituyen. Por ello toda actuación que conduzca a mejorar la seguridad de la información repercute positivamente en la economía, directamente en el sector en el que se aplique e indirectamente en los demás sectores como consecuencia de las interdependencias mencionadas. Es difícil cuantificar el coste de los incidentes de seguridad por diversas razones: su naturaleza cambiante, la falta de visibilidad por el riesgo reputacional para las entidades o los efectos indirectos e inducidos que ciertos incidentes pueden provocar en otras actividades, internas o externas a las organizaciones, pero que no se posible relacionan de modo directo con el incidente. No obstante es indudable que los incidentes de seguridad de la información tienen un impacto considerable en la economía. A título ilustrativo, el informe anual de ciberseguridad de Cisco de 2017, basado en una encuesta a más de 2900 profesionales de 13 países, señala que un 29% de las organizaciones sufrieron pérdidas de ingresos causadas por ataques contra la seguridad de la información, con pérdidas superiores al 20% de los ingresos en un 38% de los casos, siendo estas cifras significativamente

		superiores a las de informes precedentes. También un informe de IBM de 2016, que cubre 383 compañías de 12 países, que sólo considera incidentes en registros médicos, financieros o de tarjetas de crédito, estima en 4 millones de dólares el coste medio de cada incidente, con un coste anual per cápita promedio cercano a 200 $.
	En relación con la competencia	☒ 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
	Desde el punto de vista de las cargas administrativas	☐ supone una reducción de cargas administrativas. ☒ incorpora nuevas cargas administrativas. ☐ no afecta a las cargas administrativas

	Desde el punto de vista de los presupuestos, la norma ☒ Afecta a los presupuestos de la Administración del Estado ☐ Afecta a los presupuestos de otras Administraciones Territoriales	☒ implica un gasto ☐ implica un ingreso
IMPACTO DE GÉNERO	La norma tiene un impacto de género	Negativo ☐ Nulo ☒ Positivo ☐
OTROS IMPACTOS CONSIDERADOS	Impacto en la seguridad pública y en la seguridad nacional	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 la Ley así como de los mecanismos de coordinación, tanto nacional como internacional previstos 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.
OTRAS CONSIDERACIONES		

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, incluye una serie de preceptos que deben transponerse al derecho nacional a más tardar el 9 de mayo de 2018.

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 busca pues aumentar la seguridad lógica de los elementos empleados en la prestación de los servicios esenciales ofrecidos 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 en todos los casos suponen 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 y más de 106.000 en 2016.

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.

La seguridad lógica de los principales sectores económicos y sociales se considera en cierta medida en la Ley 8/2011 de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, que sin embargo pone un mayor acento en la seguridad física de las infraestructuras citadas, y carece de elementos como el desarrollo de capacidades e intercambio de información en materia de seguridad lógica con otros estados miembros, o un régimen sancionador que garantice el cumplimiento de las obligaciones.

- *Identificación de los colectivos afectados*

En cuanto a requisitos comunes de seguridad, la directiva identifica una relación mínima de sectores y subsectores en los que los Estados miembros deben identificar:

- los servicios que consideran esenciales para el mantenimiento de actividades sociales o económicas cruciales, y
- los operadores que ofrecen dichos servicios y para los que un incidente en sus redes y sistemas de información pueden tener un efecto perturbador significativo en el servicio,

Deben asimismo velar por que estos operadores tomen medidas técnicas y de organización adecuadas y proporcionadas para gestionar los riesgos, y que notifiquen sin dilación indebida los incidentes que tengan efectos significativos en la continuidad de los servicios esenciales que prestan.

Estas motivaciones son igualmente aplicables a nivel nacional, tanto en los sectores señalados en la directiva como en otros en los que la seguridad de las redes y sistemas de información son un elemento importante, como sucede en particular con 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, que consecuentemente se consideran en la Ley de transposición nacional.

Consecuentemente se extiende el ámbito de aplicación a sectores adicionales a los contemplados en el anexo II de la directiva (Administración, Espacio, Industria química, Nuclear, Instalaciones de investigación y Alimentación).

Se consideran en esta Ley los sectores de comunicaciones electrónicas y de servicios de confianza de modo particular dado que, como se indica en la Directiva, los operadores de estos sectores ya están sujetos a requisitos de seguridad e integridad, equivalentes a los previstos en la Directiva, en normativa comunitaria que tiene reflejo en la normativa nacional correspondiente, particularmente en la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, en la Ley 59/2003, de 19 de diciembre, de firma electrónica,

y en el Reglamento (UE) 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. Consecuentemente únicamente se incluyen a los operadores ambos sectores hayan sido designados como operadores críticos.

Con todo ello se persigue la máxima coherencia entre esta ley y la citada 8/2011, con la que además del ámbito de aplicación comparte varios aspectos, tales como los órganos y procedimientos para la identificación de servicios esenciales y de los operadores de servicios esenciales, la identificación de autoridades competentes y CSRIT de referencia para los operadores críticos.

- *Interés público afectado.*

El principal interés es la adecuada prestación de los servicios esenciales en los sectores considerados en el anteproyecto de Ley, 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, lo que redunda en el desarrollo de nuevos servicios y facilidades así como en mayores eficiencias en los existentes, especialmente en costes, lo que contribuye 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 eventos que pudieran resultar en situaciones de interés para la seguridad nacional, que obligarían a desencadenar mecanismos de gestión de crisis.

- *Por qué es el momento apropiado para hacerlo*

La Directiva (UE) 2016/1148 establece el 9 de mayo de 2018 como fecha límite para su transposición.

Esta obligación formal, al afectar a todos los Estados miembros de la Unión Europea, supone asimismo una oportunidad para aumentar las capacidades de cooperación en la materia con los países de nuestro entorno, dado que además de las obligaciones sobre los operadores de los sectores señalados la Directiva

considera mecanismos de coordinación y compartición de información entre Estados, que encuentran su reflejo en el anteproyecto de Ley.

De otra parte, la importancia creciente que tienen las redes y sistemas de información en la prestación de servicios en los sectores considerados en el anteproyecto de ley, induce a establecer requisitos sectoriales específicos en materia de seguridad de la información, que podrán encauzarse a través de los mecanismos previstos en el anteproyecto, de modo que se propicia un enfoque coherente entre todos ellos.

2. OBJETIVOS

Los principales objetivo del anteproyecto de Ley coinciden con los marcados en 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, que transpone mediante esta Ley al ordenamiento jurídico Español.

Se persigue pues 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.

El impulso al mercado interior vendrá, por una parte, de la mayor confianza, tanto de usuarios como de prestadores de servicios, en la utilización de tecnologías de la información y comunicaciones en la prestación de estos servicios, que animará a incorporarlas en los procesos de provisión mejorando su eficiencia y competitividad.

Por otra parte facilitará la prestación de servicios con alcance transeuropeo en los sectores considerados en la directiva al establecerse sobre sus prestadores requisitos similares en todos los Estados miembros en materia seguridad de las redes y sistemas de información, promoviendo por último el desarrollo de la industria europea de ciberseguridad al reducirse la actual fragmentación nacional en el establecimiento de estos requisitos.

Como objetivos secundarios se persigue la mejora de la eficacia en la lucha contra los delitos que involucran a las redes y sistemas de información, ya sea como objetivo o como instrumento de comisión, reduciendo sus efectos nocivos en la seguridad pública así como, eventualmente, en la seguridad nacional.

Esta mejora se conseguirá, en primer lugar, por la mayor robustez de las redes y sistemas de información ante ataques, al asegurarse que los prestadores de servicios adoptan medidas para su protección adecuadas a los riesgos afrontados y al estado del arte, y en segundo lugar al mejorar los mecanismos de

coordinación en la definición y operación de mecanismos de gestión de los incidentes que pueden afectar a la seguridad de las redes y sistemas de información, tanto a nivel nacional como con los otros Estados de la Unión europea.

Para ello, partiendo de una enumeración de dichos sectores, prevé mecanismos para identificar los servicios esenciales de cada sector, así como para designar a sus principales prestadores, atendiendo para ello al impacto que podría tener en el servicio un incidente de seguridad sufrido por las redes y sistemas de información de cada prestador.

Se definen mecanismos para asegurar que los prestadores designados adoptan medidas adecuadas para afrontar los riesgos de seguridad que afectan a las redes y sistemas de información que utilizan, fijando como objetivo prioritario de estas medidas el garantizar la continuidad en la prestación de los servicios esenciales.

También se definen mecanismos para establecer sobre los prestadores designados la obligación de notificar los incidentes de seguridad que puedan tener impacto significativo en sus servicios, previéndose asimismo la posibilidad de informar sobre estos incidentes a la población cuando sea adecuado para prevenir incidentes, actuar sobre uno en curso o cuando su divulgación redunde en el interés público.

Se consideran diferenciadamente los denominados “servicios digitales”, aquellos pertenecientes al ecosistema de Internet con los usuarios finales tienen mayor contacto, cuyo carácter esencialmente transnacional justifica que se regulen asimismo con una perspectiva internacional. La Ley se remite a las obligaciones establecidas de modo común en la Unión Europea para los prestadores de estos servicios, en los actos de ejecución específicos previstos en la Directiva (UE) 2016/1148, recogiendo los instrumentos necesarios para hacer efectiva la aplicación de estas obligaciones sobre los prestadores que actúen bajo jurisdicción española.

Para aumentar la eficacia de las medidas adoptadas se refuerzan los mecanismos de cooperación en materia de seguridad de las redes y sistemas de información con el resto de estados de la Unión Europea, y asimismo se prevé la existencia a nivel nacional de un marco institucional para su aplicación, que daría continuidad a la estrategia nacional de ciberseguridad.

Por último se prevén mecanismos para garantizar la coordinación de las disposiciones de la Ley con otras normativas relevantes para estas materias, tanto de carácter transversal, como las relativas a la protección de infraestructuras críticas y a la protección de datos de carácter personal, como con

las normativas sectoriales, ya sean nacionales o comunitarias, que establezcan requisitos relacionados con la seguridad de las redes y sistemas de información.

Se aprovecha la oportunidad que brinda la transposición de la Directiva para clarificar las funciones que diversos órganos y entidades vienen desempeñando en el área de la ciberseguridad, tanto en el plano estratégico como en el operativo, tomando para ello como base y referencia principal el sistema articulado por la Ley 8/2011, de 28 de abril, sobre protección de infraestructuras críticas, previéndose incluso un mecanismo de coordinación excepcional para situaciones de crisis al amparo del Sistema nacional de seguridad.

Se persigue con todo ello articular un sistema general y coordinado de la ciberseguridad en España que garantice una respuesta ágil y eficaz ante los ciberincidentes, que cada vez son más frecuentes y dañinos, por su carácter intersectorial, excediendo por ello la ley el propósito de la mera transposición de la Directiva en determinados aspectos:

- Para facilitar la supervisión y observancia de las obligaciones que recaen sobre los proveedores de servicios digitales, se establece en el artículo 7 la obligación de que los proveedores establecidos en España así como los que, no estando establecidos en la UE designen en España a su representante en la Unión, notifiquen su actividad a la Autoridad Competente en el plazo de tres meses desde su inicio. La disposición transitoria única establece idéntico plazo para que los proveedores que estuvieran realizando esta actividad a la entrada en vigor de la ley realicen dicha notificación.

- Se precisan en el artículo 11 las responsabilidades de los diferentes CERTs nacionales afectados por las disposiciones de la Ley, previendo asimismo mecanismos de colaboración y coordinación para situaciones específicas, en particular ante eventos de especial gravedad.

- El artículo 14 extiende la obligación de cooperación entre las autoridades competentes y las autoridades policiales, considerada en la Directiva a las autoridades de seguridad nacional y de seguridad pública.

- Junto a la previsión de la Directiva de considerar, en la designación de los operadores de servicios esenciales, factores sectoriales específicos al determinar la potencial importancia de los incidentes, el artículo 14 establece la obligación genérica de que las autoridades competentes cooperen con los órganos sectoriales competentes, el artículo 15 exige que las obligaciones que se establezcan tengan en cuenta las obligaciones sectoriales existentes y contempla la posibilidad de introducir obligaciones de seguridad específicas para cada sector, y el artículo 18 prevé la introducción de obligaciones sectoriales de notificación.

- En relación con la promoción en el uso de normas y especificaciones técnicas aceptadas a nivel europeo o internacionalmente, que contempla la Directiva, el artículo 16 añade la promoción de las normas técnicas elaboradas en el marco del Reglamento europeo de normalización así como las elaboradas por los organismos internacionales de normalización.

- La prevalencia que establece la Directiva para las obligaciones sectoriales en materia de seguridad y notificación de incidentes establecidas en normas derivadas de actos jurídicos de la Unión, se extiende en el artículo 17 a las obligaciones que en estas materias establezcan en las normativas nacionales.

- Se establece en el artículo 18 la obligación de notificar todo incidente que pueda tener un impacto significativo en los servicios, contemplándose la posibilidad de establecer reglamentariamente obligaciones de notificación de incidentes que aún no hayan tenido un impacto significativo.

- Este artículo 18 establece un marco homogéneo para todas las entidades con obligaciones de notificar incidentes, al sumar a los tres parámetros que según la Directiva deben considerarse al valorar la importancia de los efectos de los incidentes de los operadores de servicios digitales, los parámetros adicionales que considera para los servicios digitales (grado de perturbación del servicio e importancia de los sistemas o información afectados por el incidente) y, adicionalmente, el daño reputacional.

- El artículo 19 otorga protección a quienes, siendo empleados o guarde relación con los prestadores de servicios digitales y operadores de servicios esenciales, informen sobre incidentes sufridos por éstos. Ello se hace en pos de una cultura de gestión de riesgos, objetivo que también persigue la Directiva.

- Como complemento a las obligaciones de adoptar medidas para prevenir y reducir los efectos de los incidentes, el artículo 28 añaden las obligaciones de resolver los incidentes y de atender a las indicaciones recibidas del CSIRT de referencia responsables de la gestión de incidentes y riesgos, alcanzando estas obligaciones tanto a operadores de servicios esenciales como a proveedores de servicios digitales.

- El artículo 30 recoge una relación de supuestos para los que se autoriza la cesión de datos personales de conformidad con la normativa de protección de datos.

- Se extienden los supuestos de notificaciones voluntarias que la Directiva limita a los incidentes de entidades no designadas como operadores de servicios esenciales con impacto significativo en la continuidad de los

servicios que prestan, posibilitando el artículo 31 que operadores de servicios esenciales y prestadores de servicios digitales notifiquen incidentes que no alcancen el nivel de impacto significativo que motiva la obligación de notificar.

3. ALTERNATIVAS.

La principal alternativa considerada ha sido modificar la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, que presenta coincidencias en su ámbito material de aplicación y objetivos con los del anteproyecto presentado.

Sin embargo la Ley 8/2011 tiene en ciertos aspectos un alcance limitado, ya que su objeto es mejorar la protección del Estado frente a atentados terroristas u otro tipo de amenazas, buscando para ello la protección contra ataques deliberados de las infraestructuras, ubicadas en territorio nacional, que son indispensables y no permiten soluciones alternativas para prestar determinados servicios.

No entrarían pues en el alcance de la Ley 8/2011 la protección frente a eventos que no supongan una amenaza para el Estado, como son en particular los incidentes fortuitos y otros riesgos de seguridad que no tengan su origen en ataques deliberados de tipo delictivo o terrorista, de modo consecuente con el título competencial en materia de seguridad pública al amparo del que se dictó dicha ley.

Tampoco entrarían en el alcance de esa ley las medidas destinadas a garantizar la continuidad en la prestación de servicios en supuestos en que, pese a existir alternativas, su disrupción pueda tener impactos significativos, ni tampoco permite obligar a adoptar medidas de protección sobre elementos ubicados fuera del territorio nacional que resulten sin embargo necesarios para la prestación de servicios en España.

El alcance de la Ley 8/2011 es por otra parte más amplio en otros aspectos, ya que dedica gran parte de su contenido a garantizar la seguridad física de las infraestructuras empleadas para la prestación de servicios, y también considera aspectos que no son objeto de la presente Ley, como garantizar el eficaz funcionamiento de las Instituciones del Estado.

Otra alternativa hubiera sido modificar las normativas sectoriales que regulan de modo específico los diferentes sectores considerados en la Directiva (así como los sectores adicionales que se ha decidido incorporar en el anteproyecto de ley) incorporando en todos ellos los requisitos de seguridad de las redes y sistemas de información que se exigen en la Directiva, llevando de este modo a todos los sectores a una situación equivalente a la que disfrutan los sectores de

comunicaciones electrónicas y de servicios de confianza, que como se ha señalado hizo innecesario considerarlos en la Directiva así como, de modo correspondiente, en el anteproyecto de ley.

Esta opción se enfrentaba en primer lugar con el problema de la diversidad de situaciones de las diferentes normativas sectoriales, tanto en lo referente a su estructura normativa y organización sectorial, como en relación con el nivel de madurez en materia de seguridad de la información tanto de los operadores como de los reguladores sectoriales, así como en lo tocante a la distribución competencial de la regulación, dependiendo de si ésta depende o no de las comunidades autónomas así como de la existencia o no de una agencia reguladora independiente para cada sector.

Esta diversidad de situaciones suponía obstáculos notables para alcanzar el objetivo de coordinación y aplicación homogénea de medidas de seguridad de las redes y sistemas de información, de especial importancia dado el alto grado de interdependencias entre los sectores y la utilización en muchos casos de elementos o suministradores comunes a varios sectores. Asimismo esta opción introducía indudables incertidumbres en el calendario de modificación de las diferentes regulaciones sectoriales, que podría poner en riesgo la fecha límite de transposición establecida en la Directiva UE) 2016/1148.

Por ello se ha optado por establecer una ley de nueva planta que incorpora disposiciones que garantizan la coordinación de las actuaciones con las que se vienen desarrollando en el marco de la normativa de protección de infraestructuras críticas, a fin de reducir las cargas administrativas derivadas de la aplicación de la nueva ley.

Por otra parte el anteproyecto de ley considera la participación de los departamentos ministeriales con competencia por razón de la materia en cada uno de los sectores considerados, en la definición de los criterios para la identificación de servicios y operadores de servicios esenciales, así como los requisitos de las medidas de seguridad y de notificación de incidentes que han de cumplir estos operadores, con el fin de facilitar la integración de estos requisitos con el resto de requisitos que establezca la regulación sectorial en cada caso.

B. CONTENIDO, ANÁLISIS JURÍDICO Y DESCRIPCIÓN DE LA TRAMITACIÓN.

1. CONTENIDO.

El anteproyecto consta de Exposición de Motivos, 42 artículos organizados en 7 títulos, tres disposiciones adicionales, una disposición transitoria y tres disposiciones finales.

Título I. Disposiciones generales

El artículo 1 establece el objeto de la Ley, fijándose su ámbito de aplicación en el artículo 2, que queda perfectamente delimitado con las definiciones de los términos clave empleados en la Ley, recogidas en el artículo 3.

En el artículo 4 se promueve que la Directiva (UE) 2016/1148 se aplique de modo coherente en España con el resto de países de la Unión Europea introduciendo como referencia para la aplicación de la Ley, así como en la elaboración de reglamentos y guías previstos en ella, los resultados de los trabajos de los grupos que prevé dicha directiva: actos de ejecución, recomendaciones y directrices del Grupo de cooperación y las buenas prácticas identificadas en este grupo y en la red de CSIRT

Finalmente, el artículo 5 salvaguarda de lo establecido en la Ley a las acciones emprendidas por razón de seguridad nacional y salvaguarda de funciones estatales esenciales.

Título II. Servicios esenciales y servicios digitales

Este título se dedica a la identificación de los sujetos obligados por la Ley: operadores de servicios esenciales y proveedores de servicios digitales.

Para ello el artículo 6 se dedica a los operadores de servicios esenciales, estableciendo el proceso para su identificación, que encomienda a los órganos y procedimientos previstos por la Ley 8/2011 y su normativa de desarrollo, y establece su revisión con periodicidad bienal en conjunción con la de los planes estratégicos sectoriales previstos en dicha ley.

El artículo identifica una relación de criterios generales que deben valorarse para identificar a los operadores de servicios esenciales, relacionados con las repercusiones que pueden tener los incidentes que sufran, contemplando la posibilidad de añadir criterios sectoriales, y se fija el criterio para la designación como operadores de servicios esenciales a los que previamente hubieran sido designado como operadores críticos en virtud de la Ley 8/2011.

También se establece el mecanismo de coordinación con otros Estados miembros de la UE en la designación de operadores que ofrezcan servicios en varios países.

Por su parte el artículo 7 establece la obligación, a los meros efectos de su conocimiento, de que los operadores de servicios esenciales comuniquen su actividad a la autoridad competente en el plazo de tres meses desde su inicio.

Título III. Marco estratégico e institucional

Este título identifica a las entidades encargadas de la aplicación de la Ley y sus funciones correspondientes, así como los mecanismos para coordinar sus actuaciones tanto con sus contrapartes de otros Estados miembros de la UE como con otras autoridades nacionales con competencias en seguridad de la información.

Como punto de partida el artículo 8 encuadra la aplicación de la Ley en la Estrategia de Ciberseguridad Nacional, y encomienda al Consejo de Seguridad Nacional su promoción e impulso, de acuerdo con lo establecido en la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.

Seguidamente el artículo 9 identifica las autoridades competentes encargadas de supervisar la aplicación de la Ley por los operadores de servicios esenciales designados y proveedores de servicios digitales, en función de la naturaleza de éstos.

Así se designa al Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC) como autoridad competente para los operadores de servicios esenciales que además hayan sean designados como operadores críticos en virtud de la Ley 8/2011, y al Ministerio de la Presidencia y para las Administraciones Territoriales, a través del Centro Criptológico Nacional, para las entidades del sector público que no sean operadores críticos, siendo la autoridad competente para el resto de operadores de servicios esenciales la autoridad sectorial correspondiente. Para los proveedores de servicios digitales se designa como autoridad competente a la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital, del Ministerio de Energía, Turismo y Agenda Digital.

Se busca con ello la máxima coherencia con los mecanismos de supervisión de la seguridad de los sistemas de información establecidos por una parte en la Ley 8/2011, en materia de infraestructuras críticas, y por otra en la Ley 40/2015 para las entidades del sector público, encomendándose al Consejo de Seguridad

Nacional la coordinación de las actuaciones de las diferentes autoridades competentes, a través de su comité especializado en materia de ciberseguridad.

El artículo 10 identifica las funciones de las autoridades competentes por remisión a los títulos o artículos de la Ley que describen cada una de ellas, y se contemplan adicionalmente las funciones de "establecer canales de comunicación oportunos con los operadores de servicios esenciales y con los proveedores de servicios digitales" y "coordinarse con los CSIRT de referencia a través de los protocolos de actuación" que, en ambos casos, podrán desarrollarse reglamentariamente.

Se sigue una mecánica similar con los CSIRT de referencia, identificando el artículo 11 cuáles son los que corresponden a cada operador de servicios esenciales o proveedor de servicios digitales en función de su naturaleza. Se designa así al CCN-CERT del Centro Criptológico Nacional, como CSIRT de referencia para las entidades del ámbito subjetivo de aplicación de la Ley 40/2015, y al INCIBE-CERT para el resto de entidades, precisándose que será operado conjuntamente por el INCIBE y por el CNPIC en lo referente a la gestión de incidentes que afecten a los operadores críticos.

También se prevén mecanismos de coordinación de CSIRT para actividades que puedan afectar de alguna manera a los operadores designados como críticos en virtud de la Ley 8/2011, y para situaciones que requieran actuaciones coordinadas o conjuntas.

Finalmente también establece este artículo que los ciudadanos, las entidades de derecho privado y aquellas otras entidades no citadas previamente en el artículo forman parte de la comunidad de referencia del INCIBE-CERT.

El artículo 12 establece los requisitos que deben reunir estos CSIRT de referencia en materia de disponibilidad de sus servicios y canales de comunicación, instalaciones y continuidad de sus instalaciones, identifica las funciones que deben desempeñar en la gestión de incidentes, su participación en la red de CSIRT establecida en la Directiva (UE) 2016/1148, en otras redes de cooperación internacional, así como su cooperación con el sector privado, fomentando en particular la adopción y utilización de prácticas comunes de clasificación y gestión de riesgos e incidentes.

El artículo 13 designa al Consejo de Seguridad Nacional, a través del Departamento de Seguridad Nacional, como el punto de contacto único nacional encargado de garantizar la cooperación transfronteriza de las autoridades competentes con las de otros Estados miembros de la UE, así como con el grupo de cooperación y la red de CSIRT establecidos en la Directiva (UE) 2016/1148.

Finalmente, el artículo 14 trata de la cooperación y colaboración entre las entidades identificadas en los artículos anteriores y otras entidades con competencias en seguridad de la información: órganos con competencias en materia de seguridad nacional, seguridad pública, seguridad ciudadana y protección de datos de carácter personal, órganos con competencias por razón de la materia en cada uno de los sectores incluidos en el ámbito de aplicación de la ley, y Ministerio Fiscal para el caso de incidentes con caracteres de delito.

Título IV. Obligaciones de seguridad

En este título se establecen de mecanismos destinados a garantizar que los operadores de servicios esenciales y proveedores de servicios digitales disponen de procedimientos y medidas adecuadas de gestión de la seguridad de la información, teniendo en cuenta los requisitos que pudieran derivarse de la aplicación de normativas sectoriales así como las normas técnicas relevantes.

El artículo 15 establece que operadores de servicios digitales y proveedores de servicios digitales deben adoptar medidas adecuadas para gestionar los riesgos y para prevenir y reducir el impacto de los incidentes, y otorga a las autoridades competentes la capacidad de fijar reglamentariamente obligaciones específicas destinadas a tal fin, así como instrucciones y guías técnicas, teniendo para ello en cuenta tanto las directrices relevantes que adopte el grupo de cooperación establecido en la Directiva (UE) 2016/1148 como las obligaciones a las que estuvieran sometidos los operadores en virtud de su normativa sectorial o de otras normas relacionadas con la seguridad de la información.

No se prevé tal desarrollo para los proveedores de servicios digitales ya que la Directiva (UE) 2016/1148, bajo el principio de armonización máxima, les otorga la capacidad de determinar qué medidas de seguridad adoptan. Por tanto el artículo se remite a los parámetros que la Directiva establece que deben tener en cuenta dichas medidas así como a las obligaciones concretas que recojan los actos de ejecución que detallen dichos parámetros.

El artículo 16 orienta a las autoridades competentes a que las obligaciones, guías e instrucciones técnicas que adopten conforme al artículo anterior promuevan la utilización de las normas o especificaciones técnicas elaboradas en el marco del Reglamento europeo sobre normalización y, en su defecto, las aprobadas por organismos internacionales de normalización y las aceptadas a nivel europeo o internacional que sean pertinentes en la materia.

Por último el artículo 17 establece la prevalencia de las obligaciones de seguridad derivadas de normativa sectorial específica frente a las que se adopten conforme a lo previsto en este título cuando aquellas obligaciones tengan efectos

al menos equivalentes a los de ésta, extendiendo asimismo esta fórmula a las obligaciones de notificación de incidentes, a las que se dedica el título siguiente.

Título V. Notificación de incidentes

Este título recoge las disposiciones relativas las notificaciones y a la resolución de los incidentes que afectan a los operadores de servicios esenciales y a proveedores de servicios digitales, considerando por una parte los incidentes que deben notificarse obligatoriamente por tener una importancia tal que pueda tener efectos significativos en los servicios esenciales, y por otra las notificaciones voluntarias de incidentes que no alcanzan tales efectos, así como las notificaciones voluntarias de incidentes de entidades que presten servicios esenciales y no hayan sido designados como operadores de servicios esenciales.

El artículo 18 establece la obligación de los operadores de servicios esenciales de notificar los incidentes que sufran que puedan tener efectos significativos en dichos servicios, contemplando la posibilidad de extender reglamentariamente la obligación a sucesos o incidencias que aún no hayan tenido un efecto adverso real sobre los servicios. También contempla la posibilidad de desarrollar reglamentariamente obligaciones específicas, guías o instrucciones técnicas relativas a las notificaciones, teniendo en cuenta en todo caso otras obligaciones a las que estuvieran sometidos los operadores, como las sectoriales, el Esquema Nacional de Seguridad o las derivadas de la normativa sobre protección de infraestructuras críticas, así como las directrices relevantes que pudiera adoptar el Grupo de Cooperación establecido por la Directiva (UE) 2016/1148.

El artículo 19 aclara que los operadores no incurren en mayor responsabilidad por las notificaciones que realicen, y establece un régimen de protección para que los empleados y otras personas relacionadas con los operadores de servicios esenciales no vean mermados sus derechos laborales si notifican incidentes sufridos por éstos últimos.

El artículo 20 recoge los factores que han de considerarse para determinar la importancia de los posibles efectos de los incidentes sufridos por los operadores de servicios esenciales, que desencadena la obligación de notificación, y el 21 recoge las fases del procedimiento de notificación, desde la identificación inicial del incidente hasta su resolución, contemplando el artículo 22 las circunstancias en las que procede aplicar flexibilidad en dicho procedimiento.

El artículo 23 prevé mecanismos para facilitar que las autoridades competentes tengan noticia de incidentes que afecten a proveedores que ofrezcan servicios digitales en España, con vistas a facilitar la coordinación con la autoridad competente del país de establecimiento del proveedor que, según establece la Directiva (UE) 2016/1148, es quien debe responsabilizarse de la supervisión de su aplicación para toda la Unión.

El artículo 24 contempla mecanismos relativos a los incidentes con impacto transfronterizo, previéndose el intercambio de la información relevante con los Estados miembros afectados a través del punto de contacto único, tanto cuando el incidente se haya producido en España como cuando haya tenido lugar en otro Estado y se reciba la notificación por esta vía.

El artículo 25 contempla la posibilidad de que las autoridades competentes decidan que debe informarse al público información de incidentes cuyo conocimiento redunde en interés público, pudiendo informar la propia autoridad competente al público de modo directo o instar a hacerlo al operador de servicios esenciales o proveedor de servicios digitales, garantizando el artículo 26 que se respeta la confidencialidad de la información sensible, al igual que cuando se informa de incidentes a otras autoridades competentes, a los CSIRT, o a otros Estados miembros.

El artículo 27 recoge la obligación, establecida en la Directiva (UE) 2016/1148, de que las autoridades competentes informen anualmente al punto de contacto único sobre las notificaciones de incidentes recibidas, incluyendo información sobre los efectos de los incidentes en otros servicios o su posible impacto transfronterizo, debiendo el punto de contacto único remitir al grupo de cooperación un informe anual resumido sobre estas notificaciones,

El artículo 28 establece la obligación de los operadores de servicios esenciales y de los proveedores de servicios digitales de resolver los incidentes, solicitando para ello la asistencia de los CSIRT cuando sea necesario y atendiendo las indicaciones que éstos realicen.

En materia de datos personales, el artículo 29 establece la obligación de autoridades competentes y CSIRT de referencia de colaborar con la AEPD en la resolución de incidentes que afecten a datos de carácter personal, identificándose por su parte en el artículo 30 una relación de supuestos en los que se entenderá autorizada la cesión de datos personales relacionados con los incidentes a efectos de su gestión.

Finalmente el artículo 31 contempla las notificaciones de carácter voluntario, que pueden efectuar tanto las entidades potencialmente afectadas por obligaciones de notificación, cuando sufran incidentes que no revistan la importancia que motive tal obligación como por entidades que ofrezcan servicios esenciales pero no estén sujetas a obligaciones de notificación al no haber sido designados como operadores de servicios esenciales según lo previsto en el artículo 6.

Título VI. Supervisión

Este título recoge las disposiciones relativas a la supervisión, por las autoridades competentes, de las obligaciones de seguridad y de notificación de incidentes establecidas en los dos títulos precedentes, incluyendo la cooperación transfronteriza entre autoridades competentes en las situaciones oportunas.

El artículo 32, dedicado a la supervisión de los operadores de servicios esenciales, contempla la posibilidad de que la autoridad competente les requiera información sobre sus medidas y políticas de seguridad, la auditoría de éstas y el dictado de instrucciones para subsanar los incumplimientos detectados.

El artículo 33, dedicado a los proveedores de servicios digitales, sólo contempla la posibilidad de supervisión cuando la autoridad competente tenga noticia de incumplimiento de las obligaciones, pudiendo en tales casos solicitar al proveedor la información para evaluar la seguridad y políticas adoptadas e instarle a subsanar los incumplimientos detectados, pero sin indicar el modo exacto en que debe hacerlo, conforme a los principios de regulación mínima y supervisión a posteriori establecido en la Directiva (UE) 2016/1148.

Por último el artículo 34 establece principios para la cooperación transfronteriza entre autoridades competentes cuando las redes y sistemas de información de los operadores o proveedores de servicios digitales se encuentren en otros Estados miembros o, de modo recíproco, se ubiquen en España las de operadores o proveedores que ofrezcan servicios en otros países.

Título VII. Régimen sancionador

El artículo 35 establece la responsabilidad de los operadores de servicios esenciales y de los proveedores de servicios digitales.

En el artículo 36 se tipifican las infracciones, que se clasifican en tres categorías: muy graves, graves y leves, estableciéndose en el artículo 37 las escalas correspondientes para las sanciones, así como la posibilidad de publicación, a costa del sancionado, de las infracciones muy graves y graves,

En el artículo 38 se identifican los criterios que debe tener en cuenta el órgano sancionador al establecer las sanciones, contemplándose en el artículo 39 los supuestos en los que el órgano sancionador moderará la cuantía de las sanciones o puede acordar no iniciar la apertura de expediente sancionador, apercibiendo en su lugar al sujeto responsable.

El artículo 40 establece un régimen específico para las infracciones cometidas por órganos o entidades de las Administraciones públicas.

En el artículo 41 se establece que la competencia para imponer sanciones corresponde al Ministro competente de acuerdo con el artículo 9 en caso de infracciones muy graves y al órgano de la autoridad competente que se determine reglamentariamente en el caso de infracciones graves y leves.

El artículo 42 prevé la actuación en supuestos de concurrencia de infracciones de los preceptos de la ley cuando se trate de hechos tipificados en normativas sectoriales, dando preeminencia a éstas, y prevé también que cuando, en las actuaciones sancionadoras, se tenga conocimiento de hechos que pudieran ser constitutivos de infracciones tipificadas en otras leyes, éstos se notifiquen al órgano competente que corresponda.

La disposición adicional primera establece fechas límite para la identificación, de acuerdo con el artículo 6, de las relaciones iniciales de servicios esenciales y de operadores de servicios esenciales.

La disposición adicional segunda precisa que los operadores de redes y servicios de comunicaciones electrónicas y de servicios electrónicos de confianza designados como críticos no obsta para la aplicación de su normativa específica en materia de seguridad, estableciendo en estos casos la actuación coordinada del Ministerio del Interior y del Ministerio de Energía, Turismo y Agenda Digital.

La disposición transitoria única da un plazo de tres meses a los proveedores de servicios digitales que estuvieran activos en el momento de entrada de la ley para que notifiquen su actividad.

Por último, la disposición final primera establece en el artículo 149.1.21º y 29º el fundamento constitucional de la Ley, declarando la disposición final segunda que la Ley incorpora al ordenamiento jurídico interno la Directiva (UE) 2016/1148.

2. ANÁLISIS JURÍDICO

- Antecedentes

- *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) 2015/1148 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*

- Relación con otras normas

- *Ley orgánica 15/1995, de 13 diciembre, de protección de datos de carácter personal*

- *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*

Otras normas proyectadas

- Listado de la normas que quedan modificadas

  Ninguna

- Listado de la normas que quedan derogadas.

  Ninguna

3. DESCRIPCIÓN DE LA TRAMITACIÓN.

El anteproyecto de ley se elaboró tomando en cuenta el resultado de la consulta previa prevista en el artículo 26.2 Ley 50/1997, que se desarrolló entre los días 2 y 21 de diciembre de 2016 a través de la página web del MINETAD como departamento responsable de la transposición, y fue publicitada en las del Ministerio del Interior, Departamento de Seguridad Nacional y Centro Criptológico Nacional.

En ella se recibieron una quincena de contribuciones, procedentes de asociaciones y empresas de los sectores financiero, energético, TIC y transportes, de instituciones públicas (autoridades portuarias, confederaciones hidrográficas), así como de particulares.

Varias contribuciones incidían en la necesidad de respetar aspectos recogidos en la Directiva, que necesariamente ha recogido el anteproyecto, tales como como la cooperación internacional (artículos 24 y 27), respeto de la información confidencial (artículo 26), promoción en la utilización de estándares internacionales (artículo 16), o la necesidad de adoptar un enfoque de regulación liviana para los proveedores de servicios digitales (artículo 15).

Otras cuestiones planteadas en las contribuciones fueron:

- Obligaciones aplicables a los proveedores de comunicaciones, solicitando su refuerzo las empresas usuarias (sector financiero) y reclamando no aplicar

nuevas obligaciones las operadoras y asociaciones sectoriales. No se tuvo en consideración al no incluirse este sector en el ámbito de aplicación de la Ley, en consonancia con la exclusión recogida en el artículo 1.3 de la Directiva.

- Refuerzo de las obligaciones de notificación de los proveedores de servicios digitales. No es posible considerarlo, pues se rigen por el principio de armonización máxima.

- No imponer más obligaciones a los operadores que las previstas en la Directiva. No se atendió, pues la posibilidad de añadir obligaciones sectoriales (artículo 15) facilita la convergencia regulatoria.

- Clarificar el reparto de responsabilidades entre operadores de servicios esenciales y proveedores de servicios digitales que les suministren servicios. No es necesario: la Directiva sólo incluye aclaraciones en los considerandos, ya el régimen de responsabilidades de los operadores de servicios esenciales es idéntico para cualquiera de sus suministradores, sean o no proveedores de servicios digitales.

- Buscar coherencia y coordinación con regulaciones concurrentes, en particular la de Infraestructuras Críticas, y en la notificación de incidentes. Se acercan ambas regulaciones en la adopción de definiciones comunes (artículo 3), delimitación de ámbito de aplicación (artículo 2) y utilización de mecanismos comunes para la identificación de los servicios esenciales (artículo 6) y la designación de los operadores de servicios esenciales. Asimismo se incluyen disposiciones para promover la cooperación con otras autoridades con competencias en seguridad de la información (artículo 14) y garantizar que las obligaciones impuestas tienen en cuenta las adoptadas en virtud de normativas sectoriales (artículos 15 y 16), y para facilitar las obligaciones de notificación de incidentes de seguridad que puedan establecerse en virtud de varias normativas (artículos 18, 29 y 30).

- Utilizar CERT actuales, sus comunidades de referencia, facilitar el intercambio de información entre ellos, facilitar acceso a información de incidentes para su tratamiento, y crear un CERT específico para los servicios digitales. Las primeras peticiones se recogen en el artículo 11, y en el 28 el suministro de información de incidentes a los operadores, pero no se considera necesario crear nuevos CERT, pues los actuales pueden dar respuesta a las necesidades de los servicios digitales.

- Establecer con detalle las obligaciones de seguridad. Estas cuestiones serán objeto del desarrollo ulterior de la norma.

- Dotar recursos o incentivos para la adopción de requisitos por los operadores, y fomentar la creación de grupos de trabajo para compartir experiencias. No

se han considerado por no ser materias propias de la transposición de la Directiva, sino de la ejecución de políticas del Gobierno en materia de ciberseguridad.

C. ANALISIS DE IMPACTOS.

1. ADECUACIÓN DE LA NORMA AL ORDEN DE DISTRIBUCIÓN DE COMPETENCIAS.

- *Distribución de competencias entre el Estado y las Comunidades Autónomas.*

  No afecta a las competencias de las CCAA al dictarse en virtud de las competencias atribuidas al Estado por el artículo 149.1.21ª y 29ª de la Constitución.

- *Distribución competencial entre Departamentos ministeriales:*

  Se establece un reparto de competencias entre el Ministerio de Hacienda y Función Pública, el Ministerio del Interior, el Departamento de Seguridad Nacional, el Ministerio de Energía, Turismo y Agenda Digital y los ministerios con competencias en los sectores considerados por razón de la materia en:
  - la identificación de los servicios esenciales y de los operadores de servicios esenciales (artículo 6),
  - el establecimiento de específicos sobre seguridad y notificación de incidentes (artículos 15, 17 y 18)
  - la supervisión y observancia de estos requisitos (título VI)
  - la coordinación nacional e internacional (artículos 13, 24 y 27)

2. 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 de la normativa.

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 en esta norma.

Por otra parte el coste de las obligaciones de notificación de incidentes significativos será poco relevante, dado que se prevén en el artículo 18 mecanismos que faciliten la coordinación de estas notificaciones con las de naturaleza similar que, por razón de las normativas sobre protección de datos de carácter personal, de protección de infraestructuras críticas, o de garantías de seguridad de los sistemas, datos, comunicaciones y medios electrónicos utilizados por laas entidades del sector público.

Finalmente, las cargas administrativas de supervisión de las obligaciones señaladas no resultan relevantes, dada la dimensión de los prestadores de servicios sobre los que recaen, como se detalla en la sección correspondiente de la memoria.

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 a la mayor eficacia en la gestión de los riesgos de incidentes de seguridad de la información que conllevarán las mejoras en la coordinación que se deriva de las medidas adoptadas en la Ley llevará a menores impactos 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 recursos humanos que deben dedicar los prestadores de servicios al cumplimiento de obligaciones que establece la ley son poco relevantes.

De otra parte los incrementos de productividad derivados indirectamente del menor impacto esperado de los incidentes de seguridad en las redes y sistemas de información, que podrían derivarse en la reducción de empleos, pueden verse compensados por la mayor demanda de los servicios ofrecidos como consecuencia de los incentivos que supone para sus consumidores, como se indica más adelante.

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 anteproyecto de ley 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 derivados de las medidas adoptadas contribuirán a dinamizar los mercados de los diferentes sectores considerados en el anteproyecto de ley, con el consiguiente aumento de la demanda de dichos servicios por parte de los consumidores (y de las PyME, 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 en el anteproyecto de ley.

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 con el proyecto de ley se transpone al derecho nacional la Directiva (UE) 2016/1148, que tienen entre sus objetivos el impulso al mercado interior, el anteproyecto de ley 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 los servicios de los sectores considerados por la ley, tanto en costes de prestación como en el freno a la innovación incorporando tecnologías de información y comunicaciones a su prestación.
- 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 PyME*

Las medidas no tendrán impacto en costes para las PyME, que en general no estarán sometidas a las obligaciones previstas en la Ley al no alcanzar las condiciones requeridas para ser designadas como operadores de servicios esenciales.

Mención aparte merecen los prestadores de servicios digitales (buscadores en línea, mercados en línea y prestadores de servicios en nube), que con excepción de las microempresas y pequeñas empresas están sometidos a obligaciones de seguridad y de notificación de incidentes, como exige la Directiva (UE) 2016/1148. Sin embargo también en este caso cabe considerar que el peso de estas obligaciones será liviano, incluso para las PyME, como consecuencia del “enfoque ligero” que la directiva establece para las obligaciones que pesan sobre estos prestadores y su supervisión a nivel nacional.

- *Efectos en la competencia en el mercado*

  Las medidas tendrán un efecto neutral en la competencia en los diferentes mercados afectados.

  Las medidas adoptadas suponen obligaciones para operadores de los diferentes sectores considerados en la Ley que 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 la importancia relativa de cada operador en el conjunto del sector) participando los ministerios competentes por razón de la materia (o los reguladores sectoriales, en el caso de que existan) en la concreción de dichos criterios para cada sector.

Impacto presupuestario.

1. *Impacto en los Presupuestos Generales del Estado.*

   - 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

     Las medidas de seguridad adoptadas por los operadores de servicios esenciales y prestadores de servicios digitales han de ser supervisadas por la Administración de conformidad con lo establecido en los artículos 32 (que contempla la posibilidad de encomendar y remitir a la autoridad competente auditorías de seguridad) y 33.

     Asimismo las obligaciones de notificación de incidentes con impacto significativo contempladas en el artículo 18 implican la dedicación de recursos de la administración para afrontar las actuaciones que puedan derivarse de tales notificaciones. Debe considerarse asimismo la atención a las notificaciones de incidentes de carácter voluntario que se contempla en el artículo 31.

     Dado que en uno y otro caso los requisitos de seguridad y actuaciones derivadas de la notificación de incidentes pueden comportar aspectos significativamente diferentes en función del sector concreto en el que se establezcan, habrá que dedicar recursos igualmente específicos por sector, pudiendo estimarse en 3 puestos de trabajo de funcionario de grupo A2 por cada sector (o su equivalente en medios externos) más un puesto de trabajo de funcionario de grupo A1 por sector, encargado de la

coordinación de las actuaciones y ejercicio de las funciones de autoridad pública (no sustituible por medios externos).

Estos recursos de personal serán adicionales a los actualmente destinados por los departamentos competentes, en cada caso, para la supervisión de obligaciones de los operadores de servicios esenciales en relación con la seguridad en la provisión de sus servicios, así como a los dedicados para la prestación, por parte de los CSIRT nacionales, de atención a la gestión de incidentes de seguridad de las redes y sistemas de información.

Por último, en relación con la notificación de incidentes, será necesario el desarrollo de la plataforma considerada en el artículo 18 cuyo coste no será relevante dado que facilitará la integración de las obligaciones de notificación de incidentes establecidos en la normativa de protección de datos, de infraestructuras críticas y en esquema de seguridad nacional.

3. IMPACTO POR RAZÓN DE GÉNERO

A los efectos de lo previsto en la letra b), apartado primero del artículo 24, de la Ley 50/1997, de 27 de noviembre, del Gobierno, en la redacción dada por la ley 30/2003 de 13 de octubre, sobre medidas para incorporar la valoración del impacto de género en las disposiciones normativas que elabore el Gobierno, se señala que el Anteproyecto tiene un impacto de género nulo**,** en la medida en que su contenido no incluye ningún tipo de medida que pueda atentar contra la igualdad de oportunidades entre hombres y mujeres.

Por otro lado, teniendo en cuenta que los principales destinatarios son los operadores, tanto públicos como privados, éstos tendrán forma empresarial, sin que las obligaciones o “cargas” que para ellos se derivan del anteproyecto estén ni vinculadas ni relacionadas, ni siquiera tangencialmente, con la posibilidad de atentar contra las medidas previstas en la Ley Orgánica 3/2007, de 22 de marzo, para la Igualdad efectiva entre hombres y mujeres.

4. OTROS IMPACTOS

A los efectos de lo previsto en el artículo 2.2 del Real Decreto 1083/2009, se señala que el Anteproyecto no tiene impacto en aspectos de carácter social y medioambiental y al impacto en materia de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad, ni en ningún otro aspecto adicional a los identificados en dicho artículo.

5. IDENTIFICACIÓN DE CARGAS ADMINISTRATIVAS.

INCORPORACIÓN DE CARGAS

El anteproyecto de Ley introduce 3 nuevas cargas administrativas:

- Obligación de los prestadores de servicios digitales establecidos en España de notificar su actividad a la autoridad competente.
- Obligación de los operadores de servicios esenciales de realizar auditorías de seguridad de las redes y sistemas de información que utilicen.
- Obligación de notificar los incidentes significativos de seguridad de las redes y sistemas de información que utilicen.

REDUCCIÓN DE CARGAS.

- El mecanismo de notificación de incidentes a través de la plataforma informática contemplada en el artículo 18 permitirá simplificar las obligaciones de notificación establecidas en la normativa de protección de datos, infraestructuras críticas y esquema de seguridad nacional al establecer un sistema de ventanilla única para las notificaciones de incidentes establecidas en dichas normativas.