MINISTERIO
DE ENERGÍA, TURISMO
Y AGENDA DIGITAL

SECRETARÍA DE ESTADO PARA LA SOCIEDAD
DE LA INFORMACIÓN Y LA AGENDA DIGITAL

SUBDIRECCIÓN GENERAL DE SERVICIOS
DE LA SOCIEDAD DE LA INFORMACIÓN

Consulta pública sobre sobre la transposición de la Directiva (UE) 2016/1148 del Parlamento europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión

Las respuestas a esta consulta pública podrán remitirse hasta el día 21 de diciembre de 2016 a la siguiente dirección de correo electrónico: sgssi@minetad.es.

Sólo serán consideradas las respuestas en las que el remitente esté identificado.

Con carácter general las contribuciones recibidas se considerarán susceptibles de difusión pública. Las partes de la información remitida que, a juicio del interesado, deban ser tratadas con carácter confidencial y en consecuencia no proceda su libre difusión, deberán ser específicamente señaladas en el propio texto de la contribución, no considerándose a estos efectos los mensajes genéricos de confidencialidad de la información.

Muchas gracias por su colaboración.

Madrid, 1 de diciembre de 2016

De acuerdo con el artículo 26.2 de la Ley 50/1997, de 27 de noviembre, del gobierno, mediante este documento se sustancia la consulta pública sobre la transposición de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

1. Problemas que se pretenden solucionar con la nueva norma.

La Directiva que se transpone pretende implantar una cultura de ciberseguridad en las empresas y entidades que gestionan servicios esenciales para la sociedad y la economía de los distintos países y, por ende, para el buen funcionamiento del mercado interior.

La prestación de esos servicios está cada vez más ligada a las redes y sistemas de información por el tratamiento cada vez más intenso de los datos (personales o no) mediante técnicas de “Big Data” y por la creciente automatización de los procesos internos de producción y gestión económica. Ello implica, a su vez, una mayor exposición a los riesgos que entraña el empleo de una red abierta y global, como Internet, por donde también se difunden virus y programas maliciosos que pueden llegar a interferir en la prestación de servicios esenciales, provocar fugas de datos personales, comprometer información confidencial de valor comercial y afectar, en fin, al funcionamiento de dicho mercado interior. Como demuestran las estadísticas de los CERTs españoles, el número de incidentes gestionados ha ido en aumento en los últimos años.

La Directiva impone, por ello, a las entidades gestoras de servicios esenciales, así como a los prestadores de ciertos servicios digitales considerados clave en el funcionamiento de Internet, la obligación de establecer sistemas de gestión de la seguridad de la información en sus organizaciones y de notificar a las autoridades los incidentes que tengan especial gravedad. Así mismo, obliga a los Estados miembros a supervisar el cumplimiento de estas obligaciones y a velar por que existan equipos de respuesta a incidentes de seguridad con capacidad para proteger a las empresas de la propagación de estos incidentes. Así mismo, impulsa la cooperación entre autoridades nacionales y el intercambio de información como medio para elevar el nivel de seguridad en la Unión Europea frente a amenazas de carácter transfronterizo.

2. Necesidad y oportunidad de su aprobación.

La necesidad y oportunidad de una norma sobre la seguridad de los sistemas de información y redes de comunicaciones de que dependen los servicios esenciales o en que se basan los servicios típicamente digitales vienen determinadas por la obligación del Estado español de transponer la Directiva (UE) 1148/2016 del Parlamento Europeo y del Consejo, de 6 de julio de 2016 (artículo 288 del Tratado de funcionamiento de la Unión Europea). La Directiva se publicó en el DOUE el 19 de julio de 2016 y fija como plazo límite para su incorporación al Derecho nacional el 9 de mayo de 2018, es decir, 22 meses.

Además, exige la aplicación desde el 10 de mayo de 2018 de las disposiciones de transposición de la Directiva en cada Estado; la adaptación de las Estrategias nacionales de seguridad de las redes y sistemas de información a los contenidos mínimos establecidos en su artículo 7, y la determinación de las entidades obligadas a cumplir la Directiva, por prestar servicios esenciales, antes del 9 de noviembre de 2018.

3. Objetivos de la norma.

a) Transposición de la Directiva (UE) 1148/2016:

El primer objetivo de la norma es transponer de manera íntegra y fiel la Directiva (UE) 1148/2016 y establecer con ello un régimen jurídico específico sobre la seguridad de las redes y sistemas de información que sirven de soporte a los servicios esenciales, incluidos los servicios de naturaleza y origen típicamente digital.

b) Engarzar las obligaciones de los prestadores y las competencias públicas derivadas de la Directiva (UE) 1148/2016 con las obligaciones y competencias establecidas en normas concurrentes:

Pese a no existir una regulación previa equivalente, el Ordenamiento jurídico español sí cuenta con normas generales sobre seguridad, en particular, las Leyes 8/2011, de 28 de abril, por la que se establecen medidas para la Protección de las Infraestructuras Críticas, y 36/2015, de 28 de septiembre, de Seguridad Nacional, con las que es conveniente lograr un buen encaje, para completar adecuadamente el esquema institucional de aplicación de dichas leyes y no duplicar ni crear obligaciones innecesarias a las empresas y sujetos obligados.

Este mismo objetivo es el que debe animar la coordinación entre las obligaciones de notificación de incidentes previstas en la Directiva (UE) 1148/2016 y en el Reglamento (UE) 2016/679 del Parlamento europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, cuando den lugar a una violación de datos personales. El Reglamento (UE) 2016/679 también entrará en vigor en mayo de 2018.

c) Fijar el esquema institucional público de la ciberseguridad en España:

Así mismo, es un objetivo de la norma de transposición atribuir las funciones de supervisión de las obligaciones previstas en la Directiva (UE) 1148/2016; establecer los sistemas de coordinación y cooperación entre autoridades con competencias en materia de seguridad y con las autoridades con competencias sectoriales; determinar la autoridad que actuará como punto de contacto con la Comisión y los demás Estados miembros, y designar uno o varios equipos de respuesta a incidentes de seguridad para llevar a cabo las funciones descritas en el anexo I de la Directiva.

4. Posibles soluciones alternativas, regulatorias y no regulatorias.

No hay una alternativa no regulatoria para la transposición de la Directiva (UE) 1148/2016. Como toda Directiva, obliga a España a dictar una norma para incorporar sus contenidos al Ordenamiento jurídico nacional o a identificar las normas mediante las que ya se entiende incorporada ésta.

Al crear nuevas obligaciones y derechos, y determinar la organización institucional y operativa de la ciberseguridad en España, es apropiado que la norma de transposición tenga rango de ley.

La Directiva (UE) 1148/2016 ofrece flexibilidad a los Estados para adaptar sus preceptos al Derecho nacional. A continuación, se enumeran algunos de los puntos que deberán ser concretados:

- El ámbito de aplicación de la norma: pueden incluirse, si se estima conveniente, además de los sectores relacionados en el anexo II, otros sectores económicos.
- El régimen sancionador de los prestadores de servicios.

- Las competencias para la supervisión de las obligaciones: pueden recaer en una o varias autoridades. La Directiva sólo obliga a designar una de ellas como punto de contacto para la cooperación transfronteriza.
- Las funciones de respuesta a incidentes: pueden atribuirse a uno o varios CERTs. La Directiva sólo exige que cumplan los requisitos y realicen las funciones enumeradas en el anexo I.
- La notificación de incidentes: puede hacerse a la autoridad competente o al CERT.