Breves Dpto. Intangibles

Agosto de 2016

pwc

En el presente número de Breves:

Informamos de las últimas normativas e iniciativas de cooperación en materia de Ciberseguridad, entre las que destacan la Directiva 2016/1148 del Parlamento Europeo y del Consejo, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, la publicación de un Código de Derecho de la Ciberseguridad y el acuerdo suscrito entre la Comisión Europea y la industria para la creación de una asociación público-privada sobre Ciberseguridad, bajo el siguiente esquema:

1. *Necesidad*
2. *Aspectos clave de la Directiva*
3. *Acuerdo sobre Ciberseguridad*
4. *Código de Derecho de la Ciberseguridad*

Directiva y Código de Ciberseguridad

1. Necesidad de una normativa homogénea

Las redes y los sistemas de información desempeñan un papel crucial en la sociedad, el cambio tecnológico, la digitalización de las funciones de las empresas, y la utilización masiva de información son ya un hecho en gran parte de las organizaciones, de forma que su ***fiabilidad y seguridad son vitales para el desarrollo de las actividades económicas y sociales,*** *y para el funcionamiento del mercado interior.*

El uso de la tecnología ha comportado a su vez, un aumento en los incidentes de seguridad, ataques informáticos, sustracción y utilización inconsentida de información y, ciberdelincuencia en general. Estas acciones son cada vez más frecuentes y mayor su intensidad e impacto económico y reputacional para quienes las sufren.

A pesar de ser relevante y recomendable que las compañías implementen sistemas de prevención y detección de dichos incidentes y/o ataques, se ha demostrado que los mismos resultan en ocasiones ineficaces o cuanto menos insuficientes.

Bajo una perspectiva europea, las capacidades existentes no bastan para garantizar un elevado nivel de seguridad de las redes y sistemas de información de la Unión. Los niveles de preparación de los Estados miembros son muy distintos y generan niveles desiguales de protección de los consumidores y usuarios. A su vez, la ***falta de una normativa única y homogénea*** *en materia de Ciberseguridad, y la escasa coordinación entre entes públicos y privados, dificulta la persecución y solución de este tipo de amenazas.*

Conscientes de ello, tanto los organismos supranacionales, como los Gobiernos de los distintos estados, están emprendiendo ***estrategias de coordinación, y desarrollando iniciativas legislativas*** *para dar una respuesta efectiva a los problemas de seguridad de las redes y de los sistemas de información.*

2. Aspectos clave de la Directiva sobre Ciberseguridad

La Directiva 2016/1148 *del Parlamento Europeo y del Consejo, de 6 de julio, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión cuya entrada en vigor tuvo lugar el pasado 8 de agosto, viene a establecer un marco global en la Unión que integre los requisitos mínimos comunes de seguridad para los operadores de servicios esenciales y los proveedores de servicios digitales.*

Estos requisitos mínimos pasan por la obligación de los Estados miembros de ***establecer una estrategia nacional*** *de seguridad de las redes y sistemas de información; facilitar la* ***cooperación estratégica y el intercambio de información*** *entre los Estados a través del Grupo de cooperación creado al efecto;* ***notificar los incidentes de seguridad informática*** *a través de la red de CSIRT (Computer Security Incident Response Team, equipo de respuesta a incidentes de seguridad informática), y* ***designar autoridades nacionales competentes*** *y puntos de contacto únicos y CSIRT con funciones relacionadas con la seguridad de las redes y sistemas de información*

La Directiva recoge los requisitos de seguridad y notificación aplicables tanto a ***los operadores de servicios esenciales como a los prestadores de servicios digitales****, exceptuando su aplicación a las empresas que suministren redes públicas de comunicaciones o presten servicios de comunicaciones electrónicas disponibles para el público, como tampoco a los prestadores de servicios de confianza.*

Son los Estados miembros los que deberán ***identificar cuáles son*** *los operadores de servicios esenciales y los proveedores de servicios digitales establecidos en su territorio, de acuerdo con los criterios contemplados en el Anexo II de la propia Directiva y tienen para ello hasta el 9 de noviembre de 2018.*

Se considerarán operadores esenciales aquellas entidades que presten un servicio esencial para el mantenimiento de actividades sociales o económicas cruciales; que la prestación del servicio dependa de las redes y sistemas de información; y en los que un incidente tendría ***efectos perturbadores significativos****.*

En su art. 6, la Directiva define qué entiende por efecto perturbador significativo, como por ejemplo el número de usuarios que confían en dicho servicio, la dependencia de otros sectores o la repercusión del incidente, grado y duración.

En su art. 14, enumera los parámetros que se tendrán en cuenta para determinar cuando un incidente debe considerarse significativo, y por tanto, estar sujeto a notificación de los incidentes: número de usuarios afectados por la perturbación, duración y extensión geográfica.

El espíritu de la Directiva es la de fomentar ***una cultura de gestión de riesgos*** *que implique la evaluación de dichos riesgos y las medidas de seguridad pertinentes, que deben ser abordados mediante los* ***desarrollos normativos adecuados*** *y códigos o practicas sectoriales voluntarias.*

La Directiva no afecta a las acciones que cada Estado miembro, pueda adoptar para ***salvaguardar y garantizar la protección en intereses esenciales de su seguridad****, preservar el orden publico y la seguridad publica, y permitir a investigación, detección y enjuiciamiento de infracciones penales.*

Los Estados disponen hasta el próximo 9 de mayo de 2018 para trasponer la Directiva.

3. Acuerdo público-privado sobre Ciberseguridad

El pasado 5 de julio, la Comisión Europea, como parte de la estrategia de Mercado Único Digital de 2015, suscribió también un acuerdo con la industria, miembros de las administraciones nacionales, regionales y locales y centros de investigación y académicos para el fomento de la cooperación en materia de ciberseguridad.

El objetivo de esta asociación es el fomento de la cooperación e investigación entre las entidades implicadas de cada uno de los Estados miembro con el fin de encontrar soluciones de ciberseguridad en sectores como energía, salud, transporte y finanzas, así como lograr un marco de certificación común europeo a los que las empresas puedan someterse de forma armonizada para los productos de seguridad de las Tecnologías de la Información y Comunicación.

Se pretende también una mejora en la cooperación transfronteriza en los casos de ciberdelincuencia grave y se procederá, además, a llevar a cabo una evaluación sobre el funcionamiento de la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), con el fin de reforzar su propia ciberresilencia, o capacidad de sus sistemas para soportar y recuperarse frente a incidentes de seguridad.

4. Código de Derecho de la Ciberseguridad

Sin perjuicio de las anteriores iniciativas, debe asimismo mencionarse la reciente publicación por parte de Instituto Nacional de Ciberseguridad de España (INCIBE), de una compilación de toda la normativa nacional (leyes, decretos, órdenes, etc.) relacionada con la ciberseguridad, a fin de mejorar su conocimiento, y promover su aplicación y actualización.

Dicho código, publicado en el BOE y al que se puede acceder a través de la siguiente URL: www.boe.es/legislacion/codigos/, se estructura mediante capítulos que contienen la totalidad de la normativa nacional relacionada con ciberseguridad y, en concreto, en relación a las siguientes materias:

- *Seguridad nacional*
- *Infraestructuras críticas*
- *Seguridad (seguridad ciudadana y seguridad privada)*
- *Equipo de respuesta a incidentes de seguridad*
- *Telecomunicaciones y usuarios (servicios de la sociedad de la información y comercio electrónico, firma electrónica, conservación de datos, etc.)*
- *Ciberdelincuencia (Código Penal, LeCrim)*
- *Protección de Datos*