ECIJA | Torre de Cristal Pº de la Castellana, 259C
28046 Madrid · Tel: +34 917 816 160
www.ecija.com

Nota informativa - Real Decreto - Ley 12/2018: Seguridad de las redes y sistemas de información.

Madrid, 13 de septiembre de 2018

El pasado 8 de septiembre se publicó en el BOE el Real Decreto - Ley 12/2018 que supone la transposición de la Directiva (UE) 2016/1148 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.**

Esta norma (y su futuro desarrollo reglamentario) se une a la **ley 8/2011**, de 28 de abril, para la **protección de las infraestructuras críticas**, a la **ley 36/2015**, de 28 de septiembre, de **Seguridad Nacional**, al **Real Decreto 3/2010**, de 8 de enero, por el que se regula el **Esquema Nacional de Seguridad,** y al reciente **Reglamento (UE) 2016/679 general europeo de protección de datos,** para formar el principal marco normativo español en materia de ciberseguridad.

La nueva norma tiene como objetivo mejorar la seguridad de los sujetos obligados en su alcance, así como dar una respuesta coordinada a incidentes especialmente graves.

Dentro del ámbito de aplicación de esta nueva norma se encuentran:

- **Los servicios esenciales dependientes de las redes y sistemas de información** comprendidos en los sectores estratégicos definidos en el anexo de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

- En el caso de las **actividades de explotación de las redes, prestación de servicios de comunicaciones electrónicas y los recursos asociados, así como de los servicios electrónicos de confianza**, expresamente excluidos en la Directiva, el real decreto-ley se aplicará únicamente en lo que respecta a los operadores críticos.

- **Prestadores de servicios digitales como buscadores, prestadores de servicios de cloud o determinados servicios en línea (mercados en línea) que empleen a más de 50 trabajadores y cuyo volumen de negocios anual o cuyo balance general anual supere los 10 millones de euros** (es decir, se incluyen aquellos portales web donde puedan adquirirse productos o servicios, siempre que dicho prestador de servicios no sea considerado microempresa o pequeña empresa).

La norma está a la espera de un desarrollo reglamentario que establezca los extremos e interpretaciones de la misma, sin embargo, los requisitos y obligaciones pueden categorizarse en tres tipos:

- **Realización de un análisis de riesgos en materia de seguridad de la información.**
- **Implementación de medidas de seguridad en base al análisis de riesgos realizado.**
- **Notificar posibles incidentes de seguridad en determinados supuestos.**

En lo relativo a los **incidentes de seguridad**, cabe destacar que **estos tendrán que notificarse siempre *que puedan tener efectos perturbadores significativos* a un CSIRT determinado** (Equipo de respuesta a incidentes en sus siglas en inglés). La norma nombra tres CSIRT de referencia a quien notificar según la tipología del sujeto obligado: CCN-CERT, INCIBE-CERT y ESPDEF-CERT. La finalidad de esta notificación es que estos equipos puedan coordinarse entre

sí, así como con otros CSIRT nacionales e internacionales en la respuesta ante incidentes de especial gravedad

La norma prevé la posibilidad **de tener que notificar a los interesados dicho incidente de seguridad** si así lo decidiese la autoridad competente.

Con respecto a las **medidas de seguridad** a implementar, si bien, habrá que esperar al reglamento de desarrollo de esta norma para mayor concreción, el propio texto incide en la necesidad de dar cobertura (como mínimo) a los siguientes aspectos:

- **seguridad de los sistemas e instalaciones**;
- **gestión de incidentes**;
- **gestión de la continuidad de las actividades**;
- **supervisión, auditorías y pruebas**;
- **cumplimiento de las normas internacionales.**

Aunque se trata de un catálogo de medidas abierto (como sucede con el Reglamento General de Protección de Datos) la norma cita los **estándares de seguridad** como el Esquema Nacional de Seguridad, normas y guías internacionales (ISO, NIST, catálogo de ENISA, etc) como puntos de referencia.

En lo relativo a las posibles sanciones por el incumplimiento del contenido de este Real Decreto Ley, las mismas podrán ir desde una **amonestación**, pasando por una multa de hasta 100.000 € (en el caso de una infracción leve) **hasta una multa de 1.000.000 €**, en el caso de infracciones muy graves.

Quedamos a su disposición para cualquier duda o cuestión que pudiera surgir.

Un cordial saludo.

Área de Tecnologías de la Información y Ciberseguridad de ECIJA
info@ecija.com
91.781.61.60