Ciberseguridad: nuevas obligaciones para las empresas

El Gobierno trabaja en un borrador que desarrolla la normativa sobre seguridad de las redes para los operadores de servicios esenciales.

Las pérdidas económicas provocadas por los ciberataques ascendieron al 0,8% del PIB mundial, es decir, a unos 74,15 billones de euros en 2018. Esta cifra incluida en el informe Panorama actual de la ciberseguridad en España de Google no ha parado de aumentar en 2019 y su previsión de crecimiento es aún peor para 2020.

Por este motivo, es lógico que los gobiernos de todo el mundo estén ahondando en diferentes legislaciones que favorezcan un aumento de la ciberseguridad. No en vano, un ataque a una empresa que preste servicios esenciales para un país puede meter en problemas graves a toda la nación por falta de suministros de primera necesidad.

En este sentido, el documento que tiene entre manos el Gobierno español es el borrador del real decreto que desarrolla precisamente el real decreto 12/2018, de seguridad de las redes y sistemas de información para los operadores de servicios esenciales y sus proveedores.

Para aclarar la situación actual, Vicente Moret, of counsel del área de ciberseguridad de Andersen Tax & Legal, ha elaborado una guía para despejar las principales dudas sobre las nuevas obligaciones que tendrán que atender las empresas una vez se apruebe el texto definitivo.

¿En qué estado se encuentra el borrador con el nuevo Gobierno? ¿Es posible que se introduzcan nuevas modificaciones?

En la misma situación que hace dos meses. Está pendiente de su aprobación en Consejo de Ministros y de la correspondiente publicación.

¿Será obligatorio un responsable de seguridad de la información (RSI) para todas las compañías?

El RSI deberá ser nombrado por las empresas que hayan sido designadas como operadores de servicios esenciales, independientemente de dónde esté situado su domicilio social. Los sectores clave son energía, salud, TIC, industria nuclear, financiero o transporte, entre otros.

Respecto a los prestadores de servicios digitales, se incluirían mercados en línea, motores de búsqueda online o servicios de computación en la nube.

¿Cuáles son sus responsabilidades ?

Son muchas y variadas. Destacan, entre otras, elaborar y proponer las políticas de seguridad de redes y sistemas de la organización que incluyan las medidas concretas; desarrollar procedimientos; llevar a cabo auditorías periódicas de seguridad; notificar los incidentes a la autoridad competente; actuar como capacitador de buenas prácticas;o interpretar y aplicar las guías de la Administración.

Además, deberá hacerlo manteniendo la debida independencia respecto a los responsables de sistemas de información y ostentando una posición en la organización que facilite el desarrollo de esas funciones y una comunicación real y efectiva con la alta dirección, según establece el borrador de reglamento, insiste el of counsel de Andersen Tax & Legal.

¿Están las empresas españolas preparadas para las nuevas obligaciones?

Las que tienen más capacidades y volumen y en ciertos sectores, como el financiero o el energético, probablemente sí.

¿Están cumpliendo con las ya establecidas en el RD 12/2018?

Las empresas obligadas ya han empezado a adaptarse para llevar a cabo un debido cumplimiento normativo, que además les permite mitigar posibles responsabilidades en caso de incidente grave.

¿A qué sanciones se pueden llegar a enfrentar las empresas si no cumplen?

Hay un completo régimen sancionador, siendo responsables los operadores de servicios esenciales y los proveedores de servicios digitales. Por la comisión de infracciones muy graves, la multa será de 500.001 euros hasta un millón de euros; las graves de 100.001 euros hasta 500.000 euros; y las leves se castigarán con amonestación o multa de hasta 100.000 euros.

Fuente: Expansión