

# La nueva normativa de ciberseguridad obliga a las empresas a adaptarse

Los incidentes a través de la red detectados en España se duplicaron hasta los 115.000

**X. G. P.** MADRID.

El próximo 28 de mayo entrará en vigor en España el nuevo Reglamento de Protección de Datos de la Unión Europea, normativa de indudable influencia en la lucha contra la ciberdelincuencia, que precede a la fecha máxima de transposición, prevista para el 8 de mayo de 2018, de la Directiva 2016/1148 del Parlamento Europeo y del Consejo, relativa a medidas para garantizar un elevado nivel común de seguridad de las redes y de la información en la UE (Directiva NIS).

Ambas normativas obligan a las empresas a adaptarse a partir de ahora con el objetivo de evitar ser víctimas de ataques malintencionados y para evitar problemas y sanciones en que se pueda incurrir por responsabilidad civil o penal, por no haber adoptado las medidas necesarias para cumplir con las exigencias legislativas. Enfrentarse a las ciberamenazas ya no es una cuestión del departamento de informática, sino que requiere la intervención del conjunto de toda la empresa, desde el consejo de administración hasta el último integrante de la plantilla.

Entre los delitos contemplados en el artículo 31 bis del Código Penal, que regula la responsabilidad penal de la persona jurídica, se incluye el informático y el de descubrimiento, revelación de secretos y allanamiento informático.

## Desprestigio para la marca

En la medida en que las empresas implementen controles internos de seguridad informática, estarán

contribuyendo a la mitigación de los mismos y a la eficacia de su programa de compliance. Los incidentes en materia de ciberseguridad se duplicaron en España en 2016 y los gestionados por el Instituto Nacional de Ciberseguridad (Incibe), organismo dependiente del Ministerio de Industria, pasaron de los 50.000 detectados en 2015 a unos 115.000 el año pasado. Sin embargo, el peligro es muy superior, porque no todos los incidentes que sufren las empresas se denuncian, porque algunas entienden que un ciberataque puede suponer un desprestigio para su marca.

Para María Gutiérrez, directora de Seguridad de Fujitsu, "la pri-

Los expertos recomiendan vigilar la información personal que maneja la entidad

vacidad se ha convertido en un lujo, por eso es tan importante". Uno de los primeros elementos que debe resguardar la empresa son los datos propios y de terceros que maneja, particularmente los personales y la información sensible, que puede generarle responsabilidad conforme lo dispuesto en la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal.

El Reglamento europeo de Protección de Datos incluye principios que se deben respetar, como son la licitud, la lealtad y la transparencia. Se incluyen, asimismo, los principios de limitación de la finalidad; minimización de datos, exactitud; limitación del plazo de conservación; integridad; y responsabilidad proactiva.