elEconomista

05/06/2017

Tirada: 50.000 Categoría: Económicos
Difusión: 30.000 Edición:
Audiencia: 78.000 Página: 37

Abogacía Española CONSEJO GENERAL

AREA (cm2): 542,2 OCUPACIÓN: 48,1% V.PUB.: 5.100 € NOTICIAS DE LA ABOGACÍA||JUSTICIA Y TRIBUNALES

GETTY

La empresa responde por el ciberdelito de sus empleados

Los expertos subrayan, durante las Juntas de la Abogacía, los vínculos entre la protección de datos y el 'compliance'

Pedro del Rosal GRANADA

Los delitos cometidos por un empleado contra la privacidad de los datos personales y contra la seguridad de los sistemas de información pueden generar responsabilidad penal de la empresa para la que trabaje, si ésta no ha adoptado las medidas de prevención necesarias para evitar su comisión.

Así lo puso de manifiesto la fiscal jefa de Sala del Tribunal Supremo y coordinadora nacional contra la Criminalidad Informática, Elvira Tejada, durante las VII Juntas de Gobierno del Consejo General de la Abogacía Española (CGAE) que concluyeron ayer en Granada.

"Hay una normativa de protección de datos que hay que cumplir y si su incumplimiento implica responsabilidades delictivas, podría derivarse de él la responsabilidad penal de la persona jurídica", relató Tejada en una de las ponencias que más interés generó a lo largo de los dos días de las jornadas (especialmente tras los ciberataques masivos de las últimas semanas).

La última reforma del Código Penal incorporó al título que ya incluye la protección de los delitos contra la protección de datos dos nuevos tipos que sancionan los ataques a los sistemas de información.

"Acceder a un sistema, aunque no lleguemos a los datos que contiene, ya está tipificado como delito. También la interceptación de las comunicaciones entre sistemas", explicó la fiscal, quien subrayó que estos tipos se encuentran dentro de la lista cerrada de delitos que generan responsabilidad penal de las personas jurídicas.

La "negligencia" en la adopción de las medidas de prevención necesarias (dentro de los programas de *compliance*) puede derivar, si uno de sus empleados comete estos delitos, en una condena para la empresa.

> El segundo negocio ilegal más lucrativo en el mundo es en la actualidad la ciberdelincuencia

Los expertos que intervinieron junto a Tejada pusieron especial énfasis en las medidas de prevención y de respuesta en materia de ciberseguridad y en su estrecha vinculación con las nuevas exigencias que introduce el Reglamento General del Protección de Datos (que estará vigente el 25 de mayo de 2018) y los programas de *compliance*.

Sanciones millonarias

En la actualidad, se estima que la ciberdelincuencia es el segundo negocio ilegal más lucrativo, solo por detrás de la venta de armas, y multiplicando por tres el dinero que mueve el tráfico de drogas.

"La denuncia es un medio más, pero no la solución. La solución es tener protocolos de respuesta, saber exactamente qué hacer las 24 horas siguientes a un ataque. Hay que tener un plan de reacción. Luego sí, denunciar e investigar, pero esa no puede ser la única solución", incidió la jefa de la Sección Técnica de la Unidad de Investigación y Tecnología de la Policía Nacional, Silvia Barrera.

A los riesgos económicos y reputacionales que implica ser más vulnerable ante un posible ciberataque, hay que añadir la posibilidad de ser sancionado por no haber adoptado las medidas de protección exigidas por el Reglamento de protección de datos. Las multas, con esta norma, podrán alcanzar los 20 millones de euros o el 4 por ciento del volumen anual de negocio.

@ Más información en **www eleconomista es/ecoley**