LegalToday.com
Por abogados, para abogados

Blog ECIJA 2.0

8

de
Noviembre

Marta Aldea

Asociada de IT, Risk & Compliance de ECIJA

¿Pueden los despachos de abogados evitar las fugas de información?

Las fugas de información son uno de los principales quebraderos de cabeza de las empresas en materia de seguridad, y los despachos de abogados son uno de sus principales afectados. Pero, ¿cómo puede un despacho evitar este tipo de fugas?

La respuesta a esta pregunta nos la pretende proporcionar la Guía TIC, publicada por el Consejo General de la Abogacía Española en colaboración con el Instituto Nacional de Ciberseguridad y la Agencia Española de Protección de Datos, cuyo objetivo es el análisis, desde un punto de vista eminentemente práctico, de la prevención de las fugas de información en un despacho de abogados así como de su gestión, en el caso que efectivamente llegase a producirse.

No cabe duda que la información que se gestiona en un despacho de abogados es de carácter altamente confidencial y sensible, **por lo que su protección resulta necesaria de cara a evitar que personal no autorizad**o pudiera acceder a información privilegiada del despacho.

De acuerdo a lo establecido en la Guía, un despacho de abogados se encuentra expuesto a fugas de información tanto por ataques internos como externos. En este sentido, **podrían robar información confidencial** desde empleados

descontentos hasta terceros ajenos que buscan dañar la imagen del despacho.

Las causas que pueden provocar que se llegue a producir una fuga de información, principalmente son:

Organizativas: Falta de clasificación de la información confidencial, no delimitación del ámbito de difusión de la información, inexistencia de acuerdos de confidencialidad con los empleados o ausencia de formación y protocolos de actuación.

Causas técnicas: Puede ocasionar una fuga de información diversas causas técnicas, como puede ser ataques de troyanos, **el uso generalizado de la nube o bien el uso de las tecnologías móviles personales** para el trabajo diario (Bring Your Own Device o BYOD).

En este sentido, una de las medidas que la Guía considera esenciales y que deben ser implantadas para prevenir fugas de información es la adopción del principio del mínimo privilegio: los usuarios en cualquier organización sólo deben t**ener acceso a la información** estrictamente necesaria para el desarrollo de sus funciones.

El limitar acceso a la información confidencial pasa por la adopción de diferentes soluciones técnicas, **desde las más habituales que es limitar las carpetas de red al personal estrictamente necesario,** hasta productos específicos destinados a la gestión del ciclo de vida de la información, o la gestión de dispositivos externos, u otros específicos cuyo fin es evitar la fuga de información.

Lo cierto es que la ciberseguridad se ha convertido en uno de los grandes retos **no solo de los despachos de abogados, sino de cualquier empresa** que considere la información que gestiona como uno de sus activos más importantes a proteger. Por tanto, resulta de vital importancia aplicar todas las medidas necesarias para que evitar fugas de información que puedan poner en riesgo la seguridad y confidencialidad de dicha información.