Las investigaciones por robo de información confidencial en las empresas aumentan un 30%

Las empresas pueden perder por este fraude desde 30.000 euros hasta 2 millones de euros.

Zenit Detectives, compañía española experta en investigaciones aplicadas en el ámbito empresarial, apunta que, desde la llegada de la crisis, el número de investigaciones por robo de información confidencial en las empresas se ha incrementado en un 30%.

Las pérdidas económicas provocadas por este tipo de estafa hacen que los departamentos de RRHH acudan a la contratación de detectives privados. Estas pueden alcanzar desde los 30.000 euros hasta los 2 millones de euros por empresa en cualquier tipo de sector. Desde 2009, el porcentaje se ha acentuado fundamentalmente por el mal uso de nuevos dispositivos tecnológicos propiedad de la empresa, como portátiles, smartphones y tablets.

“La tecnología forma parte ya del trabajo diario dentro de las empresas, pero además está siendo utilizada para el robo de información confidencial. La portabilidad de estos terminales y su utilización fuera de la empresa, hace más fácil su uso indebido por parte de algunos empleados que comercian con información corporativa y hacen un uso fraudulento de ella”, explica José María Alonso, Director Operativo de Zenit Detectives.

Según Alonso, “la herramienta básica para detectar este tipo de fraudes es la ciberforensis. El uso de la informática para realizar determinados fraudes, como la fuga de información, está propiciando un crecimiento en la utilización de la ciberforensis para detectarlos. Desde Zenit Detectives hemos notado un incremento del 41% en este tipo de investigaciones”.

Según los datos de Zenit, el uso de la ciberforensis -metodología para obtener y aportar información, así como las pruebas sobre conductas, hechos privados y delitos perseguidos a instancia de parte ocurridos en medios informáticos y digitales- apunta un crecimiento del 75% para detectar fraudes realizados con herramientas informáticas.

“A la hora de realizar la ciberforensis el detective realiza un back up de los datos del ordenador del trabajador investigado, así como de sus dispositivos móviles siempre con un representante de los trabajadores y un notario como testigos”, concluye Alonso.