

# Gestión

Pymes  
Emprendedores  
Autónomos

## El 'espionaje industrial' está ahí para sustraer lo más valioso de su empresa

El 20% de los expedientes que se investigan de forma privada tienen que ver con este espionaje

Las pequeñas empresas también están expuestas por la subcontratación de fabricación tecnológica

Verónica Rodríguez

MADRID. Suele ser un tema tabú en cualquier conversación de empresa, ya que implica muchos factores sensibles como la confianza, la responsabilidad, la prevención o seguridad, pero lo cierto es que las fugas de información, la sustracción de documentos confidenciales o la venta de secretos empresariales existen.

No pensemos en Watergates ni en Philip Marlowes. Lo que puede darse en llamar espionaje empresarial suele ser más prosaico, pero no por ello menos letal. Damián Fuentes, jefe de Sección de Propiedad Intelectual e Industrial de la Policía Nacional, pone el acento en los numerosos casos de "accesos no autorizados a sistemas informáticos, empleando para ello aplicaciones de espionaje informático o spyware".

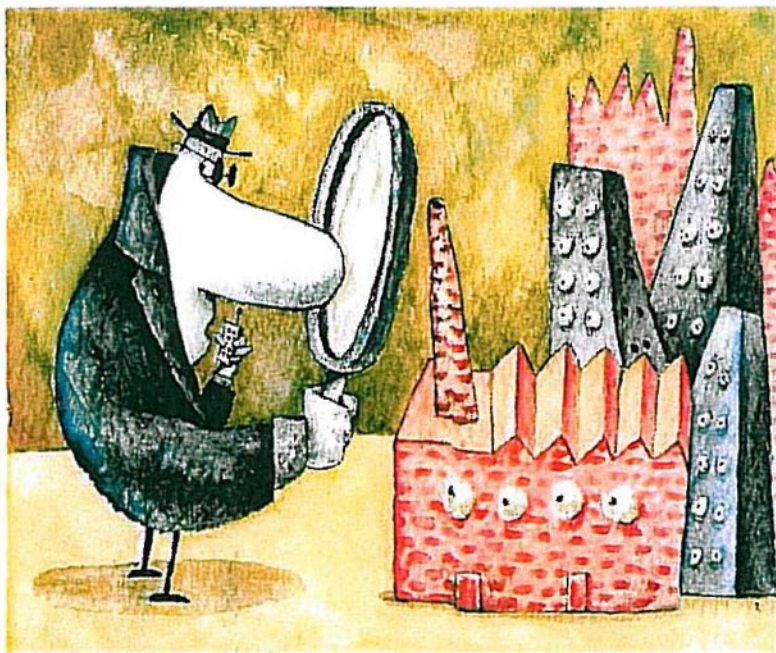
Un *espía informático* es un programa que se introduce en los sistemas de las empresas mediante virus o troyanos y se distribuye por correo electrónico. Puede usurpar diseños industriales, fórmulas, sistemas de fabricación y *know how* estratégico (conocimiento de la empresa) y ser aprovechado por empresas competidoras o divulgado de forma no autorizada.

### Saber quien entra

Lo cierto es que esto se puede evitar si se aplican una medidas elementales de control en la empresa. El primer paso es el establecimiento de una correcta política de contratación de personal: "Algo tan sencillo como saber quién entra en la empresa, desde personal, hasta becarios pasando por encargados de limpieza o sustitutos en época vacacional", señala Damián Fuentes.

También resulta de utilidad determinar la política de acceso a la red informática. "Muchos de estos programas espía llegan a la empresa por archivos de tonterías, ejecutables o correos ajenos al trabajo".

Otro ámbito en el que quizá no se repare lo suficiente es el de las "típicas reuniones de trabajo en restaurantes, o las conversaciones que



TUCCIUS

se mantienen en la barra del bar habitual tomando el café de media mañana, algo muy típico de nuestra cultura", dice Fuentes. Existen multitud de ejemplos en los que la información puede escaparse: archivos sin cerradura, claves compartidas e incluso recordadas con un *post-it*, directorios o agendas con notas explícitas, etcétera.

Algo más: ¿Alguna vez se ha planteado si el fantástico hotel o centro de convenciones donde celebra su acto de empresa reúne las características necesarias en materia de seguridad? Por ejemplo, si las salas incorporan los requisitos de insonorización necesarios como para que no se escuche todo sobre lo que allí se diserta.

Marita Fernández es directora general de la agencia de detectives Método 3, y el contraespionaje industrial es una de sus especialida-

des. "Somos cada vez más un país no sólo de servicios sino de tecnología punta, con empresas que fabrican componentes informáticos para sectores especializados como la aviación, algo que cuesta mucho dinero". Explica que la empresa que contrata sus servicios está interesada en indagar quiénes tienen interés en *desvelar* los secretos de la compañía, pero también cómo han logrado infiltrarse o acceder a ellos, "con el objetivo de evitar que lo hagan de nuevo".

Los expedientes relacionados con ataques a la propiedad industrial de las empresas suelen ocupar el 20 por ciento del total de los que cada año resuelven los despachos privados de investigación. Según esta investigadora privada, no sólo las grandes empresas deben extremar precauciones, "hay muchas pequeñas, de no más de veinte traba-

jadores, que son subcontratadas por grandes para la fabricación de alguna línea de producto y disponen por tanto de información relacionada con los desarrollos de estas corporaciones: el último modelo de airbag ó cinturón de seguridad".

### Destrucción confidencial

Y es que el tema de la seguridad puede llegar también a requerir la destrucción de documentos confidenciales, sobre todo cuando éstos afectan a otras partes implicadas. Daniel Rodríguez, de la empresa Dataeraser, recuerda que las sanciones por uso indebido de este tipo de información, que forma parte de muchas bases de datos, pueden ascender hasta 600.000 euros. Empresas de recursos humanos, despachos de abogados, laboratorios, son algunas de las que más demandan estos servicios.

### Las claves

#### CÓMO 'TAPAR' TODAS LAS 'RENDIJAS'

##### Plan integral de seguridad

**1** Conviene crear un departamento más en la propia empresa, encargado única y exclusivamente de temas de seguridad: desde la instalación de un plan de evacuación hasta intrusiones en los equipos informáticos, salas de acceso restringido, etcétera.

##### Destrucción de documentos

**2** Gestionar la destrucción de documentos de carácter confidencial, internamente si es un despacho pequeño o contratando externamente este servicio a otra empresa.

##### Control directo

**3** Cuando una empresa toma la decisión de instalar líneas de producción en el exterior, conviene reforzar los mecanismos de control directo trasladando el personal directo de confianza a la zona para evitar fugas de información.

##### Reuniones 'peligrosas'

**4** Evite conversaciones de trabajo mientras toma su café o come en el restaurante habitual. Son ocasiones perfectas para que los *loggers* recolecten información sensible.

##### Investigación privada

**5** Las empresas también pueden recurrir a la contratación de detectives privados para descubrir quiénes están detrás de un intento de robo de documentos y cómo los han conseguido.