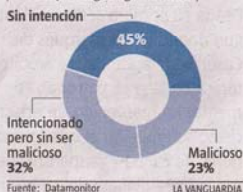


## GESTIÓN

## Inconsciencia y problemas

| Porcentaje de fugas según intención |



Fuente: Datamonitor

LA VANGUARDIA

## La imagen está en peligro

Un 33% de las empresas encuestadas por Datamonitor creen que una fuga de información puede acabar con su negocio y un 70% que perjudicaría su imagen. Sólo un 23% de las fugas lleva mala fe, pero todas son peligrosas...

## CULTURA DE SEGURIDAD

## ¿Empleados inconscientes?

En momentos de crisis aumentan los riesgos de salida incontrolada de datos confidenciales

Jordi Goula

Muchos empresarios andan preocupados estos días por un problema que, a decir verdad, ni tan siquiera se habían planteado, acuciados como están por la falta de pedidos, la sequía crediticia o los negros augurios económicos para el año recién estrenado. Se trata del peligro de que alguna persona que abandone la empresa pueda llevarse información confidencial para hacer de ella el uso que crea conveniente, que con toda seguridad supondrá un trastorno para la compañía. Este es un caso extremo -pero no inusual en estos tiempos- al que no hace falta llegar para ser consciente de que la información que manejan los empleados no siempre está a salvo de potenciales depredadores... o simples inconscientes. Por si las moscas, basta con pensar que alguien de la competencia siempre podría estar dispuesto a pagar por saber qué estrategia se prepara para el 2009, qué productos se lanzarán, qué sueldos se están pagando... ¿Algún sector puede verse afectado en especial? En principio, todos están expuestos a ello, dicen los especialistas.

Es evidente que el riesgo siempre ha existido. Tanto como que ahora es mucho más fácil caer en la tentación. Un ejemplo lo simplifica. ¿Sabe que hoy puede llevar en el bolsillo el equivalente a 700 toneladas de papel, simplemente almacenadas en un lápiz (USB) de 16 gigas? Este minúsculo dispositivo se ha convertido en el nuevo *maletín* en el que muchos trabajadores guardan secretos de la empresa, como identificaciones de clientes, datos de la plantilla... ¿Son todos ellos conscientes de su responsabilidad?

Un estudio de Cisco con la colaboración de Insight Express refleja que tanto en las pymes como en las grandes corporaciones "la plantilla no asume la seguridad como un elemento más de la cultura corporativa, por lo que tres de cada cuatro empleados son responsables de la fuga de datos de la empresa". Por ello, según Marie Claire Pfeifer, consejera delegada de Giga Trust Spain, partner de Microsoft y líder de software de seguridad para contenidos y correo electrónico, "el equipo humano debe conocer la normativa vi-

## ¡Ojo con cuatro grandes riesgos!

Veamos que dicen los expertos de Giga Trust sobre los cuatro grandes riesgos existentes ante el

control de la información, que deben solventarse en la gestión y el trabajo diario de los empleados

**1. Cambios de plantilla.** Casi la mitad de los empleados que van a otra empresa acaban por filtrar información de su anterior puesto de trabajo. Pueden transportar datos fácilmente, ya que en su 'lápiz' pueden almacenar todo tipo de información confidencial y hacérsela llegar a la competencia. Si no hay un sistema que controle cómo se difunden los datos, los secretos de la compañía pueden dejar de serlo cuando se proceda a despedir a un trabajador.

**2. Planes anuales.** Hay que evitar que caigan en manos de los empleados. No es que se trate de ocultar información, sino de

determinar quien puede acceder a ella y, por tanto, compartirla. En la actualidad, los antiguos 200 folios de información que se necesitaban para plasmar nuevas estrategias o el plan de reestructuración y toda la información puede ir en un CD.

**3. Oficina en casa.** Ya sea por cuestiones de flexibilidad, por la conciliación o por alguna de las nuevas formas de interacción, el caso es que hoy son normales las 'oficinas móviles' o el teletrabajo. Estos nuevos puestos de trabajo permiten a los empleados manejar los datos de un nuevo cliente desde cualquier lugar. Mucha información sale de

la empresa para continuar el trabajo desde casa. Es el primer eslabón de la cadena para perder el control de los datos.

**4. Información sensible.** La formación y la concienciación son las dos claves para aunar una buena gestión de los recursos humanos y del riesgo. Si, por ejemplo, en una compañía, el plan de reestructuración de los empleados llega por accidente al portátil de uno de ellos, el equipo directivo tendrá que dar explicaciones mucho antes de lo previsto. La implantación de sistemas de seguridad debe llevar aparejada una formación paralela a los empleados

gente y la política de difusión de información de su compañía".

En esta línea, muchos departamentos de recursos humanos están formando a sus trabajadores para que no solamente se familiaricen con las aplicaciones informáticas sino que conozcan las repercusiones de violar la Ley Orgánica de Protección de Datos -la más dura de Europa- o la Propiedad Industrial y, sobre todo, cómo evitarlo.

"Lo cierto es que en las empresas, los empleados están muy preocupados por la seguridad de su ordenador -virus, spam...- y de sus contraseñas, para que no en-

## Casi la mitad de los empleados reconoce que ha enviado información sensible a personas equivocadas

tre nadie en él. En cambio, no son tan cuidadosos con la información de la empresa que facilitan a través del correo electrónico a personas que, a su vez, pueden rebotarla a otras... incurriendo en un riesgo enorme al perderse totalmente el control de la información".

Según un informe de Giga Trust, casi la mitad de los empleados reconoce que ha enviado alguna vez información sensible a personas equivocadas a través de un mail. "Por ello, es necesario controlar cualquier archivo con un software que gestione los permisos de uso, como reenviar, guardar, copiar, imprimir... para proteger contenidos creados en Outlook, Word, Excel, PDF y más de 50 formatos", prosigue Pfeifer.

Además del instrumento de control que debe llevar todo archivo, Pfeifer insiste en no desdeñar la importancia que tiene la formación del empleado. "A través de la formación interna de las empresas, hay que enseñarle qué información se puede mandar, a quién se puede mandar y, sobre todo, a gestionar sus usos". En definitiva, se trata de que los equipos humanos sean capaces de gestionar estos procesos para restringir y autorizar los permisos de uso sobre la información de la empresa. En GigaTrust asignan para esta tarea un papel decisivo al departamento de recursos humanos, que "debe ser el encargado de facilitarles el camino con el uso de aplicaciones informáticas de seguridad".



JOMA

## Casos que han trascendido

Por su trascendencia y la importancia de las entidades se han conocido algunas situaciones realmente grotescas. Son sólo la punta del iceberg de una red de problemas que restan en la intimidad de muchísimas compañías. Recordemos dos de los casos más conocidos.

**Banco de Irlanda:** perdió el control de datos personales de más de 10.000 clientes (seguros de

vida, cuentas bancarias, peticiones de presupuestos, historiales médicos...). Los datos no estaban encriptados y se encontraban en dispositivos portátiles que fueron sustraídos a varios gestores de ventas del banco que no tenían encriptados los datos ni contaban con sistemas de seguridad en sus herramientas de trabajo (en sus portátiles). Los empleados trabajaban con información confidencial sin ningún tipo de protección.

**American Express, NatWest y Royal Bank of Scotland** perdieron datos de clientes, más de 1 millón, (números de cuentas y firmas de clientes del banco) que se encontraban en un dispositivo móvil que no contaba con sistema de seguridad. El dispositivo fue vendido por un empleado del banco que desconocía la importancia de proteger este tipo de información, almacenarla y, sobre todo, de guardarla y compartirla de forma segura.