

Tirada: 41.995

Difusión: 33.000  
(OJD)

Audiencia: 73.000  
(EGM)

**i&n**  
ideas&negocios

Fecha: enero de 2008  
Sección: Análisis

Superficie: 1.155 cm2

Ocupación: 300 %

Págs.: 52-53-54



## 10 | Análisis

Protección de información

# La seguridad es clave en la Red



Más allá de la Ley de Protección de Datos, conviene instalar en las empresas algunos sistemas informáticos que permitan controlar el envío de información



MARIE-CLAIRE PFEIFER,  
CONSEJERA DELEGADA  
DE GIGATRUST EN ESPAÑA



**L**a ley manda cuando hablamos de seguridad en las empresas. La Ley Orgánica de Protección de Datos (LOPD) o la normativa sobre Propiedad Intelectual obligan tanto a las pequeñas y medianas empresas como a las grandes entidades a establecer e

→→ En las entidades financieras o sanitarias hay gran cantidad de información confidencial

implantar sistemas de control no sólo en el acceso a la información sino también en su difusión. Sin embargo, la mayoría de ellas no tiene integrada en su cultura corporativa la protección de sus datos como elemento central en sus políticas de gestión, administración y comunicación. En cualquier empresa existe riesgo de una fuga de datos pero en entidades públicas, financieras, industriales y sanitarias son especialmente peligrosas. Cada día, operan con gran cantidad de información que es

confidencial o de uso restringido como informes médicos, transacciones bancarias, firmas de clientes o planes estratégicos. La principal preocupación, en este sentido, es no perder el control de esa información una vez que se difunde a través de las numerosas herramientas de comunicación con las que contamos actualmente como el correo electrónico, las intranets/extranets, el teléfono móvil, una Blackberry, un ordenador portátil o un USB.

Su implantación provoca fallos en los sistemas de seguridad de las empresas ya que pueden perder el control de la información una vez enviada. Pongamos un ejemplo; muchos empleados reconocen haber mandado accidentalmente algún email con información sensible a destinatarios equivocados. En este tipo de situaciones, podemos llegar a saber a quién le hemos enviado por error datos confidenciales pero difícilmente podremos saber qué hará con ellos y con quién los compartirá. Sólo seremos capaces de controlarlo a través de siste-

mas informáticos que vigilen y protejan los contenidos. Son las conocidas soluciones de gestión de permisos de usos, que se pueden instalar en cualquier empresa con independencia de su tamaño, el volumen de información con el que trabaje y las herramientas de comunicación que utilice.

¿Cómo funciona la gestión de permisos? Este tipo de aplicaciones gestionan la protección de información para controlar su uso, es decir, autoriza si los contenidos que se envían pueden ser copiados, impresos, guardados o reenviados a unos destinatarios de con-

→→ Hay aplicaciones informáticas que son capaces de controlar los envíos de datos

fianza. También permitirá ampliar o extender esta autorización con fechas determinadas, por ejemplo, que sólo se permita imprimir un informe durante un

periodo de siete días. De esta forma, controlaremos a quién se envía la información y que podrá hacer con ella, por lo que evitamos o reducimos el riesgo de una fuga de datos ya sea de forma accidental o intencionada. Ya sabemos en qué consiste este tipo de sistemas, ahora veremos cómo se implementan. El procedimiento es sencillo: la empresa accede a la aplicación a través de un servidor y, una vez conectada a ese programa, podrá gestionar los envíos de información y determinar que usos quiere autorizar.

Cumplir con la normativa, tanto dentro como fuera de la empresa, es una obligación legal proteger y restringir el acceso a determinadas informaciones para garantizar que no llegue a manos

desconocidas y puedan utilizarse contra la propia empresa o sus clientes. Por eso es importante que sepamos que las pérdidas para las compañías pueden alcanzar los 1,5 millones de euros al año según Datamonitor con el peligro añadido de violar la LOPD o la propiedad intelectual, con las multas que conlleva.

→→ Por no cumplir la normativa, las empresas pierden 1,5 millones de euros al año

Una de las herramientas que nos permitirá auditarlo, son las llamadas listas o logs que reflejan quién ha hecho qué con un correo o con los datos adjuntos. Con este sistema, podremos realizar un

seguimiento sobre nuestra información y evitamos el riesgo gracias a la gestión de permisos de uso.

## Solución al riesgo

Ésta es la solución de gestión de permisos, una solución fácil que responde a la preocupación de las compañías ante una fuga de datos no sólo por las repercusiones económicas sino también de imagen, de credibilidad y confianza. Frente al riesgo de perder información, tenemos la solución de prevención y protección. Ante el desafío de la fuga de datos, contamos con aplicaciones suficientes para evitarlo. Sólo es necesario un compromiso real por parte de los empresarios para implantar políticas de seguridad que protejan sus secretos comerciales.

