



¿Cómo evitar las fugas de información?

Una práctica habitual en cualquier empresa, y al mismo tiempo necesaria, es invertir en tecnología para adaptar los modelos de negocio a los cambios del mercado; un mercado donde la innovación y el fomento de la I+D están a la orden del día.

Marie-Claire Pfeifer,
Consejera Delegada de GigaTrust en España

La automatización de los procesos, la agilización de las labores de administración o la rapidez en los envíos de documentación son algunas de las ventajas de implantar las últimas versiones de programas de edición o contabilidad. Sin embargo, como la tecnología ya forma parte de la cultura de las empresas, hay un aspecto ligado a ella y que va ganando terreno, siendo ya imprescindible: la seguridad.

Paralelamente a la utilización de las nuevas tecnologías, también son mayores los riesgos que se corren al integrarse y formar parte del mundo de Internet. La Red no sólo ha cambiado las formas de trabajar e interrelacionarse dentro de las compañías, sino que ha abierto sus puertas a cualquier usuario. Y es aquí donde se encuentra el riesgo.

El correo electrónico se ha convertido en una herramienta de

comunicación indispensable; a través de él es posible ponerse en contacto con clientes, socios o colaboradores prácticamente a diario. Además, con los nuevos dispositivos, como la *Blackberry* o los móviles, es posible acceder a los contenidos y correos desde cualquier lugar y en cualquier momento.

En este punto conviene plantearse unas cuestiones clave: ¿tenemos protegidos esos contenidos que mandamos por correo?, ¿cumplimos la ley cuando los difundimos a través de Internet?, ¿sabemos lo que el receptor hará con la información enviada? Desde nuestra experiencia podemos decir que las empresas están tomando conciencia de la importancia de proteger sus archivos cuando los comparten, y empiezan a tener integrada la seguridad en su política corporativa, teniendo en

cuenta las consecuencias de difundir información sin estar protegida.

CONTROL DE LA DIFUSIÓN

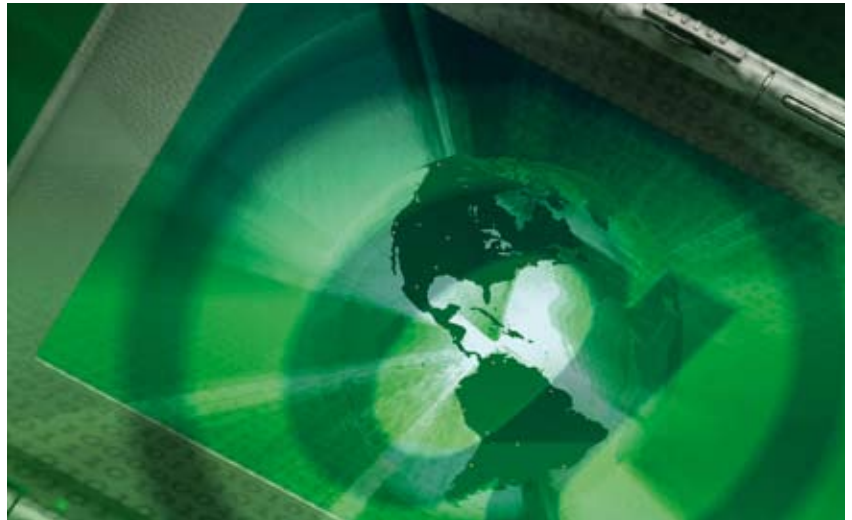
Una norma general en las empresas es controlar el acceso a los documentos y los archivos; pero esto no es suficiente. Controlar su difusión es tan importante como proteger su acceso. ¿Por qué? Porque la información puede llegar a manos desconocidas y ser utilizada para perjudicar. A esto hay que añadir el riesgo de estar compartiendo datos sin cumplir con la normativa, por ejemplo la Ley Orgánica de Protección de Datos (LOPD) o las leyes que regulan la Propiedad Intelectual. Hay determinados contenidos que son de acceso restringido y uso limitado, por lo que es esencial garantizar su seguridad para evitar, o al menos reducir, el riesgo de una fuga de información.

Según un estudio de *Datamonitor*, las pérdidas en las grandes compañías pueden alcanzar los 1,5 millones de euros al año en concepto de pérdida de clientes, socios o accionistas, caídas en Bolsa (si es el caso), inversiones en marketing y comunicación para recuperar la credibilidad, acciones publicitarias con el objetivo de generar confianza de nuevo en el mercado y cuantiosas multas por violar la normativa.

Y es que las fugas de datos no se pueden mantener en secreto porque las empresas están obligadas por ley a comunicarlo. Ya hemos visto casos de compañías como ING Direct, American Express o Royal Bank of Scotland que han hecho frente a fugas de información.

Las empresas están tomando conciencia de la importancia de proteger sus archivos cuando los comparten

Planteado el problema, la solución es sencilla. La propuesta que recomendamos es contar con un *software* que proteja los contenidos, tanto si están siendo enviados como si están simplemente archivados, ya sea en el móvil, en un portátil o en el escritorio del ordenador. La clave es controlar su utilización, es decir, autorizar los permisos de uso de contenidos sensibles como informes médicos, transacciones financieras o identificaciones de clientes. Para ello, contamos con aplicaciones informáticas (como el *Intelligent Rights Management* – IRM, Gestión Inteligente de Permisos) que actúan como filtro y permiten autorizar si los recep-



tores de los datos que se envíen podrán reenviarlos, imprimirlos, copiarlos o guardarlos. Además, se podrán realizar seguimientos para saber quién ha hecho qué con un determinado mail y su contenido. Con estas sencillas soluciones, garantizamos la protección de datos confidenciales o restringidos.

POLÍTICA DE SEGURIDAD

La información de la empresa es su principal valor: planes estratégicos, organización de la plantilla, previsión de ventas, resultados, planificación de inversiones, informes sobre clientes y un largo etcétera. Las consecuencias de compartirlas y difundirlas sin estar protegidas no sólo se traducirán en pérdidas económicas, sino también en repercusiones negativas en la imagen y en la posición en el mercado. Evitarlo es tan sencillo como implantar una política de seguridad corporativa a nivel teórico y, en un plano práctico, un *software* de seguridad que controle la difusión de las comunicaciones y una planificación de la estrategia de almacenamiento de información para mejorar la estructura de contenidos y los sistemas de gestión y operaciones. El objetivo es organizar

y optimizar el entorno de la empresa de una forma rápida y con el menor impacto posible.

Como se ha visto, tan importante es el contenido que se difunde como los canales a través de los que se envía y a quién se le manda. Por eso, empresas como la nuestra indican a las entidades y organizaciones hasta dónde pueden llegar, qué datos pueden difundir o cómo proteger sus documentos, ya que el valor de las compañías depende de su gestión, pero también de la protección de secretos comerciales, listas de precios y otros archivos digitales. Se trata de proporcionar soluciones de seguridad de contenidos a las empresas sin perder la transparencia y accesibilidad a sus datos, tal y como se recoge en las normas de un buen gobierno corporativo.

La información se mueve rápidamente, sobre todo a través de Internet, recorriendo miles de kilómetros en cuestión de segundos. Esa información pasa por distintos programas, servidores y correos electrónicos, por lo que se puede perder el control sobre ella. En este contexto, la pregunta esencial a la que las empresas deben dar respuesta es: ¿está protegida nuestra información electrónica? ■