

ALMACENAMIENTO Y GESTIÓN DE LA INFORMACIÓN EN LAS PYME

Gran parte de la actividad empresarial diaria en los países desarrollados depende, en mayor o menor medida, de sistemas y redes informáticas. Hasta las organizaciones cuya actividad nada tiene que ver con la tecnología, hacen uso de los ordenadores y de Internet en algún momento: comunicación con clientes, emisión de facturas, trámites con la Administración, etc.).

Es por este motivo por el que la seguridad de la información tiene cabida en el seno de la organización de las comunicaciones de las empresas. En ellas deben primar la integridad y la disponibilidad de los datos. Ambos elementos junto con la preservación de la confidencialidad, forman parte de la definición de la Seguridad de la Información, según diversas normativas y estándares internacionales (como por ejemplo, ISO 27001).

No obstante, el papel de la seguridad en las organizaciones no es algo nuevo. Ya fue contemplado por los teóricos de organización y dirección de empresas a principios del siglo XX, llegando a concluir que se trataba de una función empresarial, al mismo nivel que otras: producción, comercial, financiera, etc. Hoy en día la seguridad es de vital importancia para garantizar el cumplimiento con la normativa vigente (Ley Orgánica de Protección de Datos de Carácter Personal¹, Ley de Servicios de Sociedad de la Información², Ley General de Telecomunicaciones³, Ley de Firma Electrónica⁴, etc.) y en último extremo la continuidad del negocio.

En relación con la normativa, la seguridad centra sus esfuerzos no sólo en los métodos para prevenir o mitigar la pérdida de datos, sino en cumplir lo exigido por la ley. El caso más reciente, debido a la publicación del nuevo Reglamento de Desarrollo⁵, es el de la LOPD donde se definen una serie de obligaciones legales que deben cumplir personas físicas y jurídicas con los ficheros de carácter personal, y que están estrechamente relacionadas con las medidas expuestas en el presente artículo.

¹ Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Disponible en <http://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf>

² Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico. Disponible en <http://www.boe.es/boe/dias/2002/07/12/pdfs/A25388-25403.pdf>

³ Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones. Disponible en: <http://www.boe.es/boe/dias/2003/11/04/pdfs/A38890-38924.pdf>

⁴ Ley 59/2003, de 19 de diciembre, de firma electrónica. Disponible en: <http://www.boe.es/boe/dias/2003/12/20/pdfs/A45329-45343.pdf>

⁵ Real Decreto 1720/2007, de 21 de Diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal. Disponible en: <http://www.boe.es/boe/dias/2008/01/19/pdfs/A04103-04136.pdf>

La LOPD diferencia tres niveles de seguridad: básico, medio, alto en función de los datos que los ficheros tengan. Se consideran **tipos de datos de nivel básico**:

- los nombres y apellidos,
- las direcciones de contacto (físicas y electrónicas),
- los teléfonos y
- los números de cuentas corrientes entre otros.

Ahora bien, ¿qué PYME no guarda alguno de estos datos (ya sea de sus clientes, distribuidores, etc.)? Pues bien, el mero hecho de almacenar esta información supone la obligación por ley, a la empresa de disponer de un documento de seguridad, un régimen de funciones y obligaciones del personal, un registro de incidencias, control de acceso, gestión de soportes y copias de respaldo.

En este contexto, este artículo pretende descubrir aspectos tradicionalmente más obviados sobre la gestión de la información. Lejos de los antivirus, cortafuegos y demás herramientas, existen herramientas de recuperación de datos, gestión de soportes y la protección de datos que son medidas básicas de seguridad, que corresponden al nivel de madurez básico en materia de seguridad de la información de organizaciones y entre las que se encuentran las copias de seguridad y las unidades de almacenamiento.

I Causas de la pérdida de datos

Para que una PYME pueda identificar y conocer las fuentes de la pérdida de datos debe hacerse la siguiente pregunta: ¿cuáles son las amenazas y los enemigos que dan lugar a la necesidad de una política de gestión de la información para mi empresa?

Con independencia de que posteriormente se identifique cada una de las principales causas, el denominador común a todas ellas es que **“las amenazas son impredecibles”**. No se conoce cuando van suceder, ni si aquellas personas que pueden solucionar el problema, estarán presentes en el momento que los incidentes ocurran. Por consiguiente, aunque los profesionales de los sistemas de información tomen precauciones para proteger los datos empresariales, no siempre se puede evitar la pérdida; aunque sí se puede reducir considerablemente el riesgo de que suceda y sus consecuencias.

Habitualmente aunque se pueden diferenciar entre causas internas y externas, en función del origen de las mismas:

- **Anomalías en el hardware:** interrupción del suministro eléctrico, fallo del soporte donde se almacenan los datos, fallo del controlador, etc.

- **Error humano:** supresión o formateo de la unidad de forma accidental y daño causado por una caída o golpe, desconocimiento de la política de copias. En el recientemente publicado *Estudio sobre la seguridad y e-confianza en las pequeñas y microempresas españolas* realizado por INTECO el 47,5% de las entidades no dispone de ningún procedimiento que le indique cómo realizar las copias de seguridad. Además el 4,6% de las entidades afirma haber sufrido una pérdida de datos o robo de la información.
- **Anomalías en el software:** daños causados por las herramientas de diagnóstico o reparación, errores de las copias de seguridad, complejidad de la configuración, errores que provocan el cierre de la aplicación, etc.
- **Malware:** virus, troyanos, gusanos, etc. Según datos de INTECO⁶ el porcentaje de empresas con menos de 50 trabajadores que en 2009 afirmaban haber sufrido un incidente de seguridad fue el 77,4%. Los incidentes que sufren principalmente y que tienen relación con los datos son: los virus (afirman sufrirlos el 49,2% de las empresas), los fallos técnicos (el 22,8%) y los troyanos (21,7%).
- **Desastres naturales:** incendios, inundaciones, etc. En 2008, según el Center for Research on the Epidemiology of Disasters (CRED)⁷, ocurrieron 354 desastres que afectaron a 214 millones de personas en el mundo.
- **Leve formación específica del personal:** en tecnologías de la información, en los programas de recuperación, etc.

La importancia de conocer el fundamento de las incidencias y la identificación del origen en el seno de las propias empresas puede resultar garantía suficiente para poder minimizar las consecuencias.

II Consecuencias de la pérdida de datos

No se puede entender la necesidad de una buena gestión de la información ni las alternativas disponibles para conseguirla, si no se comprende la problemática que conlleva el ignorar este pilar fundamental de la Seguridad de la Información.

Un estudio realizado en 2002 por la Asociación Española para la Dirección Informática (AEDI), con la colaboración de Microsoft⁸, identificaba el porcentaje de empresas que

⁶ INTECO (2009): Estudio sobre la seguridad y e-confianza en las pequeñas y microempresas españolas. Disponible en http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Estudios_e_Informes_1/Estudio_seguridad_microempresas

⁷ Center for Research on the Epidemiology of Disasters (CRED) (2009): Annual disaster statistical review.

⁸ Asociación Española para la Dirección Informática (AEDI) y Microsoft (2002): Política empresarial de seguridad de la información. Disponible en: <http://www.aedi.es/asp/Estudio5-web.pdf>. El estudio realizado sobre una muestra de 283

eran conscientes de que no podían sobrevivir más de 4 días sin la información de sus ordenadores era de un 74%.

Ahora bien, un reciente estudio de Symantec⁹ del 2009, sobre preparación ante desastres, muestra una gran discrepancia entre la forma en que las PYME perciben su nivel de preparación (ataques informáticos, interrupciones eléctricas o catástrofes naturales, entre otros) y el real. Mientras que el 82% de las empresas dicen que están satisfechos o muy satisfechos con sus planes y, un número similar (84%), dicen que se sienten protegidos en caso de que ocurra un desastre. No obstante, la realidad revela que, de media, las PYME han sufrido tres interrupciones en los últimos doce meses y que casi el 50% no tiene un plan para poder afrontar tales interrupciones.

Dicho esto, no sólo se trata de los daños que puedan ocasionarse a la información guardada y la consecuente pérdida de los activos e inversiones que de ella dependan. Otros perjuicios son:

- Tiempo perdido (y consecuentemente dinero) para tratar de restaurar o regenerar la información perdida.
- Pérdidas ocasionadas por la indisponibilidad de esta información.
- Robo y revelación de información sensible y/o confidencial, lo cual puede suponer violaciones de la legislación vigente y, por tanto, sanciones.
- Impacto en términos de imagen de la empresa ante terceros: clientes, proveedores, etc.
- Retrasos en los procesos de producción.
- Posibles daños a la salud de los empleados y clientes.

Queda patente que, por mucho que la implantación de determinadas medidas de seguridad puedan resultar incómodas, para muchos usuarios del sistema, éstas son absolutamente necesarias. En los siguientes epígrafes se presentan las medidas y herramientas básicas para alcanzar los niveles mínimos de seguridad y poder gestionar de forma segura la información.

empresas se realizó a responsables de la dirección informática de empresas y organizaciones, consumidoras y usuarias de Tecnologías de la Información.

⁹ Symantec (2009): SMB Disaster Preparedness Survey. Disponible en http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=dpsurvey

III Medidas y herramientas para alcanzar niveles mínimos de seguridad

Realización de copias de seguridad

Por copia de respaldo o de seguridad o backup se entiende una copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación. Estas copias buscan salvaguardar la integridad y disponibilidad de los datos, y deben estar acompañadas de un procedimiento o política, preferiblemente por escrito, para su realización y recuperación en caso de fallo informático.

Así para una PYME lo fundamental es disponer de una correcta Política de Copias de Seguridad que planifique las copias que se deberían realizar, en función del volumen y el tipo de información generada por el sistema informático, especificando el tipo de copias (completa, incremental o diferencial) y el ciclo de esta operación (diario, semanal, mensual, etc.).

Dicha política debe tener en cuenta, como mínimo, los siguientes puntos:

- Realización y supervisión de las copias por personal debidamente autorizado.
- Procedimiento escrito de inventariado y etiquetado de las cintas y soportes que alojan las copias.
- Almacenamiento de los soportes empleados en lugares seguros, a ser posible en un local distinto a aquel donde se encuentra la información que generó la copia.
- Aplicación de técnicas criptográficas para asegurar la privacidad de los datos guardados.
- Comprobación periódica del estado en el que se encuentran los soportes y del proceso de generación de copias de seguridad.
- Registro de destrucciones, pérdidas y recuperaciones de datos.

Además de estas medidas, hay que tener bien claro qué es lo que se ha de guardar. Obviamente, se deben realizar copias de seguridad de los archivos que sean únicos al sistema; esto debe incluir directorios “Mis Documentos” y la carpeta o partición del disco donde guardemos nuestro datos (en sistemas Windows); o “/etc/” y “/usr/local/” o “/home” y la partición o carpeta donde guardemos nuestros datos (en sistemas Linux). Lo que no tiene ninguna utilidad es realizar una copia de seguridad de directorios como “c:\windows\system32” (en equipos con Windows) o “/dev/” o “/proc/” (en sistemas Linux).

Obstáculos en el contexto de las PYME

Aunque muchas PYME sí entienden la importancia de realizar copias de seguridad de sus datos, es difícil para una compañía de recursos limitados desarrollar un sistema fiable. Para este tipo de empresas, cualquiera de los siguientes obstáculos puede hacer que las copias de seguridad de datos sean ineficaces o demasiado difíciles de mantener:

- **Copias de seguridad inadecuadas:** si los sistemas de copia de seguridad no se testean periódicamente, es probable que surjan problemas inesperados durante su restauración, arruinando su validez. Por supuesto, restaurar una copia completa para comprobar que todo es correcto, puede ser demasiado trabajo para los métodos habituales de operación, por lo que lo que se suele hacer es tratar de recuperar varios ficheros aleatorios del backup, asumiendo que si estos funcionan, toda la copia se considera correcta.
- **Tiempo entre cada copia de seguridad:** sin copias de seguridad periódicas, una entidad podría perder todos los datos recientes, que pueden diferir significativamente de los datos disponibles en las copias de seguridad.
- **Complejidad de las opciones de las copias de seguridad:** sin personal informático específico (TI), los conocimientos técnicos y el tiempo necesarios para hacer funcionar un sistema de alta calidad pueden resultar complejos constituyendo un elemento de disuasión para una empresa pequeña.

Limitaciones de la medida

Todo esquema de copia de seguridad tiene cierto impacto, en términos de dedicación de personal y recursos, en el sistema que ha sido copiado. Si este impacto es significativo, la copia de seguridad debe ser acotada en el tiempo. Estableciéndose si fuese necesario otro tipo de ciclo temporal para la realización de las copias.

Además, todos los soportes de almacenamiento tienen una capacidad finita y un coste real. Buscar la cantidad correcta de capacidad acorde con las necesidades de la copia de seguridad es una parte importante del diseño de la Política de Copias de Seguridad.

Finalmente aun cuando el escenario sea idílico, las copias de seguridad únicamente rescatan la copia más reciente, y no necesariamente los ficheros más recientes. Para restaurar documentos que estaban siendo modificados y de los que no se mantiene una copia de seguridad lo suficientemente actualizada, existe una alternativa que se presenta más adelante: la recuperación de datos.

Unidades de almacenamiento de datos

Son dispositivos que leen o escriben los datos en los medios o soportes de almacenamiento, y que permiten conformar la memoria secundaria o almacenamiento secundario del ordenador. Muchos de estos dispositivos por lo general se emplean para albergar las copias de respaldo/seguridad antes mencionadas.

Existen multitud de dispositivos diferentes donde almacenar copias de seguridad, desde el arcaico disco flexible hasta unidades de cinta de última generación. Evidentemente, cada uno tiene sus ventajas y sus inconvenientes pero, se utilice el medio que se utilice, este ha de cumplir una norma básica: ha de ser estándar.

Muchos administradores presumen de disponer de dispositivos de última generación, pero esto puede ser un arma de doble filo, ¿qué sucede si se necesita recuperar datos y no se dispone de esa unidad lectora tan avanzada? Imagínese que se produce un incendio y desaparece una máquina, y con ella el dispositivo que se utiliza para realizar copias de seguridad. En esta situación, o se dispone de otra unidad idéntica a la perdida, o recuperar la información va a resultar complicada.

Dado que existen muchos, **tipos de dispositivos sobre los que realizar las copias de seguridad**, lo que deben realizar los administradores es una elección en función de cuál es que mejor se adapta a las necesidades que su organización necesite. Los principales son:

- **Discos duros:** estos dispositivos permiten la posibilidad de utilizar una unidad de disco duro completa (o una partición) para realizar copias de seguridad; pudiendo crearse un sistema de ficheros sobre la unidad o la partición correspondiente, montarla posteriormente y copiar todos los ficheros que interese guardar en ella. Algo muy interesante en algunas situaciones, debido a la sencillez que supone, es utilizar como dispositivo de copia un disco duro idéntico al que está instalado en el sistema, y del que se desea hacer el backup.
- **Cintas magnéticas:** han sido durante años (y siguen siendo en la actualidad) el dispositivo de backup por excelencia. La principal diferencia entre el almacenamiento en cintas y en discos es que las primeras son un medio de acceso secuencial, mientras que el disco es un medio de acceso aleatorio. El acceso a la información es más lento, pero es ideal para almacenar cantidades ingentes de datos pues únicamente se hace uso de estas para restaurar datos en situaciones ocasionales. Hoy en día la cinta de mayor almacenamiento puede almacenar 800GB de datos sin compresión.
- **CD-ROM/DVD:** en la actualidad todas las máquinas poseen grabadoras de CD-ROM y/o DVD, pudiéndose guardar hasta 4,7GB en un DVD de capa simple por

algo menos de 30 céntimos. Por estos motivos muchos administradores, especialmente de PYME, se decantan por realizar sus copias de seguridad en uno o varios DVD.

- **NAS (Network Attached Storage):** son sistemas que están diseñados para almacenar datos y hacerlos accesibles a los equipos conectados a una red, mostrándose en la red local como un simple nodo. Por ese motivo no requieren pantalla, ratón o teclado, sino que poseen interfaz Web. NAS es muy útil para proporcionar almacenamiento centralizado a ordenadores clientes en entornos con grandes cantidades de datos, ya que puede habilitar sistemas fácilmente y con bajo costo con balance de carga, tolerancia a fallos y servidor web para proveer servicios de almacenamiento. Un dispositivo hardware simple, llamado NAS box o NAS head, actúa como interfaz entre el NAS y los clientes. Los clientes siempre se conectan al NAS head (no a los dispositivos individuales de almacenamiento) a través de una conexión de red o Ethernet¹⁰.
- **Llavero USB:** se trata de un pequeño dispositivo de almacenamiento que utiliza la memoria flash para guardar la información sin necesidad de pilas. Su capacidad suele ser inferior a la de los dispositivos previamente mencionados, pero suficiente para replicar ficheros y documentos de uso cotidiano. Cuentan con la ventaja de que siguen funcionando a pesar del polvo y rayones. Aunque su uso normal es para transportar información, también se pueden emplear como copia de respaldo de documentos importantes.

Tomando en consideración la diversidad de dispositivos identificados lo que tienen que tener en cuenta las PYME son, en primer lugar, los datos que se van a almacenar y posteriormente otras características como:

- Fiabilidad: toda pieza mecánica en movimiento es susceptible de fallar, de igual forma, el polvo o los rayones pueden afectar negativamente a algunos de los soportes mencionados. Los discos duros, por ejemplo, son sistemas cerrados y su núcleo magnético no está expuesto, por lo que los convierte en más fiables que las unidades de cinta.
- Ciclo de trabajo: esta noción mide el porcentaje de tiempo que una unidad de respaldo está leyendo, escribiendo y verificando datos. Como todo dispositivo ha sido concebido para un ciclo de trabajo concreto, si alguno de los datos van a ser leídos con poca frecuencia, entonces no será tan necesario un dispositivo diseñado para lectura intensiva.

¹⁰ Entiéndase por dirección Ethernet, aquella dirección que identifica a nuestro dispositivo de red en una red local.

- Tasa de transferencia: mide la velocidad a la que una unidad puede leer y escribir datos. Este es un factor que determinará llegado el caso, la dilación entre un incidente y la recuperación de un conjunto de datos.
- Flexibilidad: un dispositivo puede ser flexible de diferentes formas, pero las que interesan en este contexto son la capacidad de responder a diferentes tasas de datos y la capacidad de usarlos de distintas formas. Por ejemplo, las unidades de cinta son las menos flexibles ya que sólo pueden hacer dos cosas: escribir datos de forma secuencial y leerlos de la misma manera. Así, estas unidades sólo se pueden utilizar con aplicaciones que entienden como leer y escribir a cinta.
- Tiempo de acceso a los datos guardados: disponer de un dispositivo rápido facilita el almacenamiento y la recuperación de grandes cantidades de datos, ahora bien, muchas de las recuperaciones serán de archivos individuales o conjuntos pequeños de ficheros. Cuando este es el caso, importa más el tiempo que se tarda en cargar un volumen, buscar el lugar concreto de este y comenzar a leer los datos. Las unidades de cinta, dada su característica secuencial, suelen tener tiempos de acceso a datos mucho más elevados y por consiguiente lentos.
- Capacidad: se trata de la cantidad del volumen de datos que la unidad puede almacenar. En muchas ocasiones serán más adecuadas las unidades que permiten albergar en un único dispositivo la copia completa del sistema que se quiere respaldar.
- Portabilidad: la facilidad de trasladar la unidad de un lugar a otro es un aspecto muy a tener en cuenta, pues uno de los principales puntos de una adecuada política de backups es la separación física de los sitios de respaldo. Ahora bien, teniendo en cuenta que hoy día se pueden realizar transferencias por red a lugares remotos con suma facilidad, la portabilidad ha perdido algo de protagonismo.
- Coste: por regla general, las unidades más fiables, flexibles, con mayor capacidad y tasa de transferencia y con valores pequeños de acceso a dato costarán más.

Obstáculos en el contexto de las PYME

El precio va a ser el mayor condicionante para una PYME de cara a escoger una u otra alternativa. Nótese que no sólo se trata del coste directo de la compra del dispositivo, sino que la gestión de la inteligencia subyacente en un sistema de backups también va a ser determinante. En muchas ocasiones serán necesarias tareas de automatización y verificación que tendrán un coste asociado, este coste será distinto para cada uno de los medios explicados.

Al mismo tiempo, muchas PYME carecen de personal dedicado exclusivamente a la labor de administración de sistemas. Por ese motivo cabe pensar que el personal que se encargará de la realización de copias de seguridad podría ser personal no técnico que no disponga de los conocimientos necesarios para manejar y automatizar las tareas de copia con algunos de estos dispositivos.

Limitaciones de la medida

Sea cual sea la unidad de almacenamiento escogida, podría llegar a ser totalmente inútil si se guarda en el mismo lugar en que se encuentran los datos originales que fueron replicados (casos de incendios, inundaciones, etc.).

De igual forma, la capacidad o la velocidad de estos dispositivos no van a garantizar la confidencialidad de los datos que almacenan, para ello será necesario emplear soluciones de cifrado e implementar políticas de acceso a datos.

Tampoco hay que obviar que, como se ha dicho con anterioridad, estos dispositivos son susceptibles de fallos y ante tales acontecimientos sólo queda una opción que tal vez no tenga plenas garantías de éxito como es la recuperación de datos.

Recuperación de datos

La recuperación de datos hace referencia a las técnicas empleadas para recuperar archivos que han sido perdidos o eliminados de algún medio de almacenamiento.

Hay dos formas básicas de perder información de un medio:

- pérdida física de datos o
- pérdida lógica de datos.

La primera de ellas, la pérdida física de datos, es la que presenta más complicaciones, dado que implica un problema real sobre la superficie donde están almacenados los datos. Por ejemplo, un rayón en un CD.

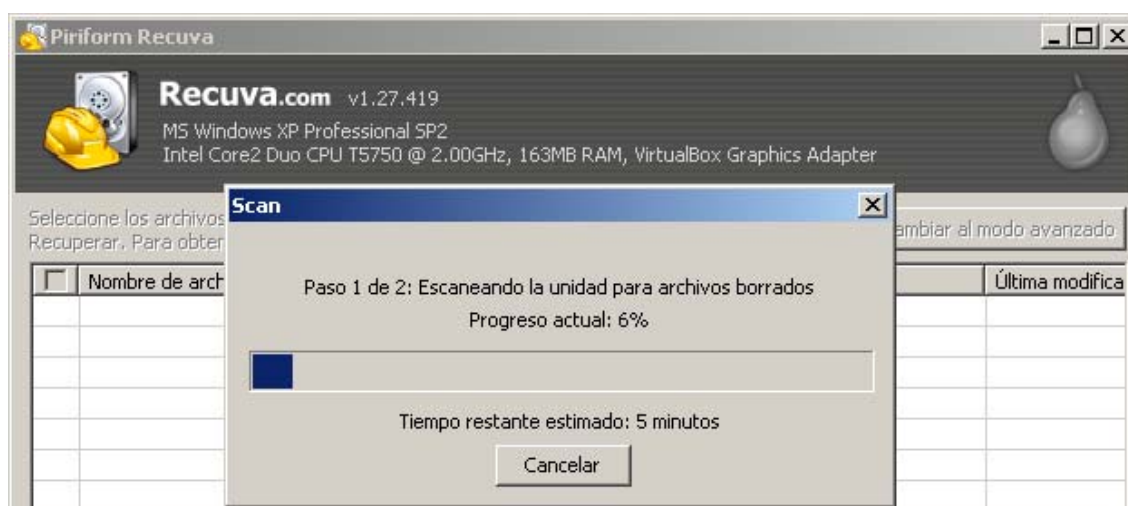
En cambio, en la pérdida lógica de datos lo que ocurre es la eliminación de archivos de forma voluntaria (mediante la opción de borrar archivo de cualquier sistema operativo) o de manera involuntaria (por la existencia de un virus). Sin embargo, en los discos duros y otros medios de almacenamiento, los archivos no son borrados realmente del disco, sino que son marcados como eliminados. El sistema operativo interpreta que estos lugares del disco marcados como eliminados son en realidad espacio libre y, por lo tanto, podrá escribir sobre ellos. Muchas veces la información así marcada no es sobrescrita de inmediato, y por esta razón se puede recuperar si las PYME disponen de un software intuitivo para llevar dicha acción.

Ahora bien, hay que destacar que si no se poseen los conocimientos adecuados y se intenta ir más allá de los asistentes de las herramientas básicas de recuperación, se podría llegar a destruir de forma permanente los datos que se desean restaurar.

Por otra parte, la pérdida física de datos muchas veces requerirá la intervención de un experto que pueda identificar errores mecánicos y sustituir piezas defectuosas. Un ejemplo de recuperación física es la sustitución de un circuito impreso defectuoso de un disco duro por uno de una unidad funcional.

Ahora bien, en la mayoría de las ocasiones la pérdida de datos suele deberse a un fallo del sistema operativo en sí. En tales casos siempre se puede montar el disco duro con un sistema operativo de inicio sin necesidad de instalación (llamados “live”) y copiar los datos importantes que albergaba la unidad.

Ilustración 1: Ejemplo de herramienta gratuita de recuperación de datos por pérdida lógica



Fuente: INTECO

Obstáculos en el contexto de las PYME

Los servicios profesionales de recuperación de datos suelen tener costes elevados. En muchas ocasiones una PYME no va a estar dispuesta a hacer frente a tal gasto. Dicho esto, probablemente el principal obstáculo de cara a su adopción no será el dinero, sino el propio desconocimiento de la existencia de estas técnicas.

Limitaciones de la medida

La recuperación de datos no es viable para todas las empresas, ni para todas las situaciones, siempre habrá que contrastar el coste de la recuperación con el coste de recrear los datos perdidos.

Gestión de soportes

Las unidades de almacenamiento y las copias de seguridad previamente mencionadas se han de gestionar adecuadamente para que sólo personal autorizado tenga acceso a ellas y estén disponibles e íntegras en caso de necesitarlas. Esto es lo que se entiende por gestión de soportes.

Una correcta gestión de soportes debe contemplar la existencia una política o procedimiento que establezca:

- Un registro de entradas y de salidas de estos, con el fin de poder trazar los movimientos de datos y ficheros de la organización. Se trata de una medida obligatoria en España para los ficheros con datos de carácter personal de nivel medio o alto, de acuerdo con lo dispuesto por la Ley Orgánica de Protección de Datos.
- Una autorización (incluso por escrito) del responsable del sistema informático en el caso de la salida de soportes que contengan datos sensibles o de carácter personal fuera de los locales de la entidad.
- La protección de los soportes durante sus traslados y almacenamiento (medidas físicas y lógicas), dejando claro cuales son las responsabilidades de los transportistas que custodien los soportes. Esto incluye los soportes que han adquirido un especial protagonismo en los últimos años (unidades de memoria extraíbles USB, tarjetas de memoria, etc.), a los que se les ha de exigir un estricto control y una limitación de su uso con el fin de evitar fugas de información y traslados no conformes con la política de gestión implantada. De hecho, los soportes extraíbles no sólo representan un potencial problema de fugas de información, sino que también podrían facilitar la entrada de código malicioso en el entorno empresarial. Para evitar esto se puede deshabilitar o limitar la conexión de dispositivos externos en los puertos USB y FireWire¹¹ de todos o parte de los equipos informáticos, o bien implementar una estrategia de permisos y restricciones para su uso.
- Finalmente, la destrucción segura de soportes, dado que con técnicas análogas a las que se describieron en el epígrafe de recuperación de datos, es posible acceder a información sensible de una empresa empleando los discos duros que esta decide desechar o vender. Un ejemplo de algunas de las formas de proceder que existen figuran en la siguiente tabla.

¹¹ Tipo de puerto de comunicaciones de alta velocidad desarrollado por la compañía Apple. La denominación real de esta interfaz es la IEEE 1394. Se trata de una tecnología para la entrada/salida de datos en serie a alta velocidad y la conexión de dispositivos digitales.

Tabla 1: Procedimientos para la destrucción de soportes en función de su contenido

Contenido y uso futuro	Cómo actuar
Soportes que hayan contenido datos y ficheros sensibles y que vayan a ser reutilizados	Borrado físico de forma segura.
Soportes magnéticos que hayan contenido datos sensibles y que vayan a ser reutilizados	Utilización de herramientas para el borrado seguro de soportes magnéticos (<i>Wipe</i>), basadas en la sobre-escritura con distintos patrones binarios de los datos a eliminar
Equipo de trabajo de un usuario	Además del borrado de datos y ficheros personales, eliminación de carpetas temporales, <i>cookies</i> , copias de seguridad, certificados digitales, libreta de direcciones, configuraciones (Internet, correo electrónico, etc.)
Soportes con documentos y ficheros de sensibilidad crítica	Desmagnetización o destrucción total del soporte de almacenamiento

Fuente: INTECO

Obstáculos en el contexto de la PYME

La presencia de diversos actores (transportistas, responsables de sistemas informáticos, personal encargado del inventariado, etc.) en la gestión de soportes, puede suponer un problema, dado que no todas las PYME disponen de estas figuras, lo cual en muchas ocasiones conduce a un vacío de responsabilidad, que dificulta la aplicación de estas recomendaciones que figuran en la política o procedimiento de gestión.

Los conocimientos técnicos también van a ser un obstáculo importante, por ejemplo, difícilmente una empresa le va a dar la importancia requerida a la destrucción segura de soportes si no se comprende que un borrado simple de archivos en muchas ocasiones permite la recuperación de estos.

Dicho esto, el desconocimiento no sólo será técnico, en caso de que los datos que se estén tratando sean datos personales, sino que las medidas que hay que tomar a la hora de establecer un procedimiento de copia de seguridad y de gestión de soportes son más estrictas, y están, en algunos casos reguladas por la ley orgánica de protección de carácter personal y el reglamento de medidas de seguridad de ficheros de datos personales. Esto podría ocasionar para las empresas multas o sanciones que van desde leves a muy graves conforme a lo especificado en título VII de la LOPD y el capítulo III del RDLOPD.

Limitaciones de la medida

Una correcta gestión de soportes no va a impedir todo acceso no autorizado a la información que estos contienen. La política que la entidad elabore deberá estar acompañada de un bastionado¹² multicapa de la infraestructura de red de la empresa para minimizar los accesos no autorizados fruto de la explotación de vulnerabilidades en los distintos actores de la subred.

Protección de datos y documentos sensibles

La protección de datos comienza por la clasificación en sí de los documentos y de los datos de la organización en función de su nivel de confidencialidad. De esta forma se puede discernir entre la información que pueda ser conocida por personas ajenas a la empresa, la que pueda ser utilizada sólo por empleados, la que sólo sea accesible por un subconjunto de empleados, etc.

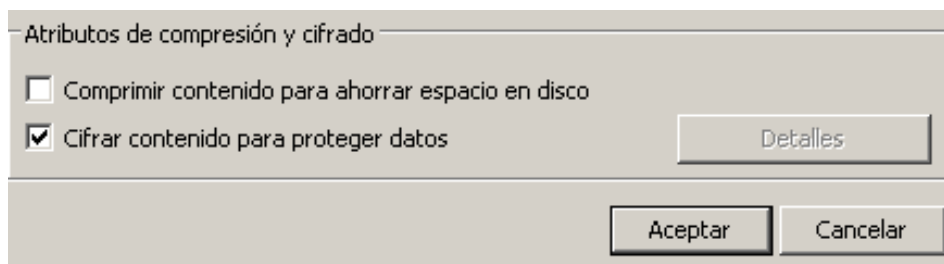
Una correcta protección de datos debe contemplar la existencia una política o procedimiento que establezca:

- La **clasificación de los documentos** en función del nivel de confidencialidad y de las personas que pueden acceder a los datos. Esto permitirá discernir entre la que pueda ser conocida por personas ajenas a la empresa, la que pueda ser utilizada sólo por empleados, la que sólo sea accesible por un subconjunto de empleados, etc. Una posible clasificación de documentos y datos de una PYME es: sin clasificar o desclasificada, de uso interno, confidencial y secreta o reservada.
- El **ciclo de vida** (creación, utilización, modificación y destrucción) de los documentos más sensibles debería estar registrado en una base de datos para tal fin.
- El **cifrado de datos y documentos** más sensibles mediante el uso de criptografía. Esta ciencia permite garantizar la confidencialidad, la integridad y la autenticidad de los mensajes y documentos guardados en un sistema o red informático.

Esta función de cifrado puede ser realizada por los propios sistemas operativos hoy día (EFS en Windows), por aplicaciones específicas como Truecrypt o por dispositivos hardware de almacenamiento secundario que cifran automáticamente los ficheros que en ellos se guardan.

¹² Consiste en implementar todas las medidas de seguridad posibles para proteger un sistema.

Ilustración 2: Ejemplo de aplicación de cifrado EFS en Windows



Fuente: INTECO

Centrándose exclusivamente en los datos guardados en discos duros, existen tarjetas criptográficas que se añaden a la placa de un ordenador, que se pueden configurar para realizar la encriptación automática de todos los ficheros guardados en estos dispositivos.

- El **almacenamiento, recuperación y transmisión de claves** a los distintos usuarios que garanticen una buena gestión de los documentos y/o datos de la organización.

Obstáculos en el contexto de la PYME

A la hora de implementar los algoritmos criptográficos las PYME pueden o disponer de personal especializado o desconocer la complejidad de las operaciones que se tienen que realizar con los datos. Esto hace que, a veces, se decanten por hardware especializado que puede resultar más caro o con mayor número de complementos y funcionalidades de los que necesitan.

Ahora bien, hay que señalar que el precio de estos aparatos no siempre justifica la mejora en rendimiento con respecto a soluciones software gratuitas. Es más, las soluciones lógicas, en muchas ocasiones, tienen la ventaja de una mayor flexibilidad, y portabilidad del algoritmo criptográfico, que se podría ejecutar de este modo en un mayor número de sistemas, lo cual es muy atractivo en el contexto de una PYME

Limitaciones de la medida

Antes de la puesta en marcha de cualquier política o procedimiento de protección de datos las empresas deben considerar las implicaciones que una mala gestión de la base de datos de las claves tienen para el futuro de la compañía.

Para finalizar, **INTECO** quiere recordar que **la mejor forma que tienen las PYME para garantizar la implantación de dichos planes y políticas es la utilización de un Sistema de Gestión de la Seguridad de Información (SGSI)**. Si desean conocer en detalle en qué consiste y cómo INTECO puede ayudarles, pueden consultar la videoguía *SGSI: Una importante ayuda para la gestión de la seguridad de las organizaciones*,

disponible en nuestra web¹³. Con ella se quiere sensibilizar a la PYME sobre la utilidad del uso de esta medida como apoyo para la gestión de la seguridad de las organizaciones.

¹³ Disponible en: <http://cert.inteco.es/extfrontinteco/img/File/intecocert/sgsi/>