

Un asunto que tradicionalmente se ha descuidado en las pymes es la gestión de los riesgos, a pesar de que estas compañías son especialmente sensibles a que por causa de un riesgo mal gestionado se produzcan pérdidas inesperadas, que en este tipo de empresas son difíciles de gestionar.

Especialmente relevante es la pérdida de datos, los cuales pueden poner en peligro la viabilidad de la empresa. La mayoría de las pymes no suelen tener recursos propios para gestionar los riesgos y por lo tanto están muy expuestas a la pérdida de datos informáticos, clave para su funcionamiento.

Pérdida y Recuperación de datos en las pymes



Hoy en día la creciente dependencia de los datos y la proliferación del almacenamiento de información, clave en equipos informáticos en empresas y en ordenadores personales, aumenta la necesidad de disponer de soluciones de recuperación de datos.

Hasta hace poco los datos que se perdían debido a anomalías del hardware y

el software, equipos que no arrancan, infecciones de virus, errores humanos y particiones suprimidas o perdidas, eran irrecuperables. En la actualidad la mayoría de los datos perdidos se pueden recuperar.

Existen tres principales costes cuantificables asociados a cada incidente de pérdida de datos: el coste del

soporte técnico de la recuperación, la pérdida de productividad debido a la inactividad del usuario y el coste asociado a los datos que no podrán recuperarse.

Las facturas y listado de clientes y pedidos en curso son los datos que más a menudo se pierden y esta circunstancia puede incidir de forma grave en la viabilidad de la empresa.

Tendencias asociadas a la pérdida de datos

La pérdida de datos está experimentando un crecimiento exponencial. Las principales causas que contribuyen al incremento de la pérdida de datos, especialmente en las pymes, son el incremento de los datos almacenados electrónicamente, los módulos de almacenamiento de mayor capacidad, el aumento de los datos clave, las técnicas y herramientas de copia de seguridad poco fiables o no suficientemente verificadas, la inexistencia de planes de seguridad y contingencia ante desastres, la escasez de profesionales en el área de proceso de datos y la actitud "a mí eso no me puede pasar".

Causas de la pérdida de datos

¿Dónde, cómo y en que porcentajes se produce la pérdida de datos?

- Por anomalías del hardware o del equipo en un 44% de los datos por interrupción del suministro eléctrico, fallo del soporte/cabezal y fallo del controlador.
- Por errores humanos en el 32%, es decir: supresión o formato de unidad accidental y daño causado por una caída o golpe.
- Anomalías del programa de software: 14%.
—Daños causados por las herramientas de diagnóstico o reparación, errores de las copias de

seguridad y complejidad de la configuración—.

- Los virus afectan en 7% de los casos. —Virus polimorfos, de sector de arranque e infectantes de archivos—.
- Y los desastres naturales en un 3% como los incendios, inundaciones y fallos del sistema de alimentación.

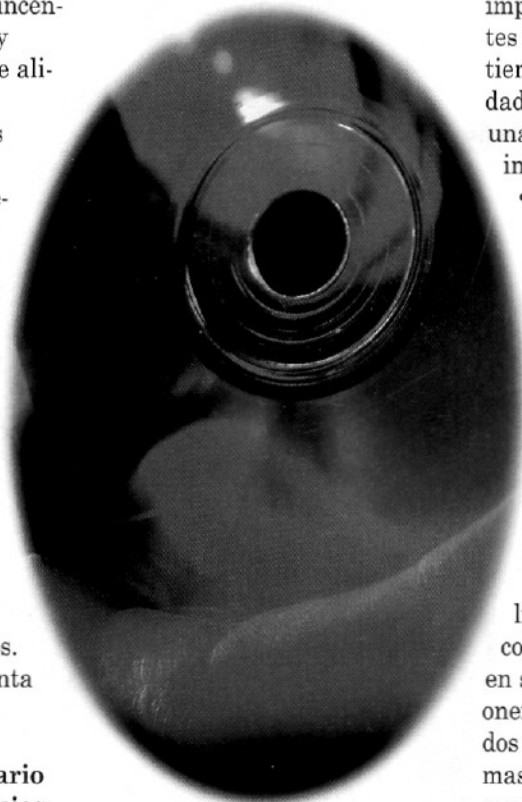
Estas cinco grandes amenazas para los datos informáticos tienen dos aspectos en común: son impredecibles y, la mayoría de las veces, incontrolables. Por consiguiente, aunque los profesionales de los sistemas de información tomen precauciones para proteger los datos empresariales, no siempre se podrá evitar la pérdida de datos. Hay que tener en cuenta que nada es infalible.

¿Cuándo es necesario contar con los servicios de un especialista en recuperación de datos?

A continuación ofrecemos algunos ejemplos de situaciones que exigen la intervención de profesionales del servicio de recuperación de datos:

- Sistema de copia de seguridad poco fiable: si no se dispone de un sistema de copia de seguridad fiable y probado de forma regular, las pérdidas de datos de cualquier tamaño pueden ser muy graves, o incluso irreversibles, para una empresa.

- Anomalías en la copia de seguridad y la restauración: los procesos de copia de seguridad y restauración pueden verse afectados si las cintas no pueden leerse, los datos están dañados o se reali-



zan procedimientos de copia de seguridad inapropiados. Aunque las copias de seguridad se lleven a cabo correctamente, siempre existe un lapso de tiempo entre los datos más actuales y la última copia de seguridad realizada.

- Se requiere una gran cantidad de tiempo y de esfuerzo para realizar los procesos de copia de seguridad y restauración: en muchos casos, el tiempo necesario para restaurar los datos de un

proceso de copia de seguridad puede mermar la productividad y suponer importantes pérdidas financieras.

- Reconstrucción de datos difícil o imposible: la reconstrucción de datos implica numerosos costes como la pérdida de tiempo, ingresos y calidad, que la convierten en una opción difícil o incluso imposible.

- Sistema que no arranca: aunque los daños de las estructuras del sistema operativo sean mínimos, es posible que el sistema no arranque.

- Anomalía del sistema RAID —tecnología de almacenamiento masivo de información que utiliza conjuntos de discos duros económicos en sustitución de los onerosos modelos utilizados por los grandes sistemas— o de duplicación: muchas organizaciones copian datos simultáneamente en dos ubicaciones de almacenamiento distintas. Sin embargo si los datos ya están dañados antes de copiarse, o si uno de los dos sistemas —o ambos— falla, es posible que los datos se destruyan o que no se puedan recuperar. En los sistemas RAID la seguridad de los datos también pueden peligrar si dos o más unidades del mismo dispositivo lógico fallan al mismo tiempo o si la reconstrucción de una

unidad perdida en un sistema RAID no se realiza correctamente.

Además, los sistemas RAID y de duplicación no pueden proteger el sistema frente a virus, daños del software y errores humanos.

- Datos alterados o destruidos intencionadamente: los datos son susceptibles de ser suprimidos o eliminados intencionadamente por virus nocivos, violaciones de seguridad o empleados disgustados.
- Datos alterados o destruidos accidentalmente: prácticamente todos los usuarios de datos electrónicos pueden suprimir o destruir datos por error.
- Archivos dañados o suprimidos de las bases de datos MS SQL o MS Exchange: las anomalías de sistemas, los fallos del suministro eléctrico y las supresiones intencionadas o accidentales son algunos ejemplos de situaciones en las que la información clave del sistema resulta inaccesible.

¿Qué debe exigirse a un especialista en recuperación de datos?

La recuperación de datos es un proceso tecnológicamente complejo que requiere amplios conocimientos y experiencia. Elija una compañía que ofrezca servicios

de diagnóstico conclusivos y de recuperación de datos, así como soluciones de software.

La empresa de recuperación de datos debe poder recuperar datos de todo tipo de sistemas, incluidos los portátiles y PC de escritorio; y tipos de soportes —incluidos todos los tipos de discos duros, discos ópticos, discos extraíbles, soportes flash, volúmenes con varias unidades y sis-



temas RAID, así como todos los tipos de cintas—. Debe estar capacitado tecnológicamente para tratar sus sistemas y cumplir con los requerimientos de los principales fabricantes.

- Para proteger los datos empresariales importantes, una compañía de recuperación de datos debe contar con potentes sistemas de protección de

la seguridad de los datos, como protocolos de propiedad, cifrado de datos e instalaciones protegidas.

- Para recuperar los datos de forma rápida y rentable es necesario poder realizar recuperaciones de datos de servidores, equipos de escritorio o portátiles a través de una conexión de módem o Internet, con la calidad de las recuperaciones internas y sin necesidad de extraer piezas ni desmontar el sistema. Igualmente, debe poder reconstruir los datos corruptos.

Consejos para proteger sus datos

En muchas ocasiones se trata de seguir y respetar unas normas sencillas y elementales pero muy eficaces para la protección de los datos informáticos. Abrir un disco sin tener los recursos y experiencia necesarios puede causar un daño muy grave y poner en peligro una eventual recuperación.

Anomalías lógicas o estructurales de software pueden producir daños graves y afectar negativamente la recuperación de datos. Por lo tanto, hay que tener muy presente los siguientes consejos, e idealmente, ante un problema de este tipo, no hacer nada y llamar a un especialista:

- Cuidados para su Disco Duro

1. Proteja su unidad de traqueteos y golpes.
 2. Cuidado con la energía electrostática.
 3. Aclimatación de la sala en la que se almacena el equipo. Lleve a cabo revisiones periódicas de sus unidades de disco duro.
 5. Ubique su hardware en un lugar seguro.
 6. Portátiles. No son tan resistentes como a muchos les gusta pensar.
- Cuidados para sus cintas
1. Mantenga sus cintas en su correspondiente caja hasta que las emplee.
 2. No trate de cargar una cinta en la unidad si detecta abolladuras, roturas o humedad en las fundas de las cintas, en las puertas o en los selectores de protección de archivos.
 3. Almacene sus cintas de manera adecuada.
 4. Cuidado con las temperaturas extremas.
 5. Evite los campos magnéticos.
- Proteja sus Datos Valiosos
1. Configure su ordenador en un entorno seguro.
 2. Haga *backup* de sus datos de forma regular.
 3. Use un sistema de alimentación ininterrumpido (UPS)
 4. Pase el antivirus de forma regular y actualícelo cuatro veces al año.
 5. Vigile los ruidos extraños.
 6. No emplee software tras una pérdida de datos sin estar seguro de que no hace cambios automáticos perjudiciales en la estructura

Nicolas Green
Director general de Ontrack