

LAS CINCO MEJORES PRÁCTICAS PARA PROTEGER TUS COPIAS DE SEGURIDAD

El cifrado de backup debe formar parte de la estrategia de seguridad. En muchos entornos, el almacenamiento se ha realizado fuera de la supervisión de los responsables de seguridad, ya que éstos se suelen centrar en áreas como la seguridad perimetral, la detección y prevención de intrusiones y la protección de sistemas. Como resultado, es probable que la infraestructura de almacenamiento (el almacenamiento principal y, especialmente, las copias del mismo) represente un talón de Aquiles en lo que se refiere a seguridad. Así, las políticas de seguridad de datos se convierten en un problema corporativo cuando deberían ser un elemento fundamental de la estrategia de seguridad de una empresa. Estas políticas pueden dar lugar a acciones tácticas y operativas mediante el esfuerzo conjunto de las organizaciones de seguridad y de almacenamiento. Para ello, el almacenamiento debe convertirse en una parte integral de la estrategia de seguridad de la empresa.

Para lograr estos objetivos, la empresa debe crear una práctica alrededor de cinco áreas fundamentales:

- 01** Asignar responsabilidad y autoridad
- 02** Evaluar riesgos
- 03** Desarrollar un programa de protección de la información
- 04** Comunicar el proceso
- 05** Ejecutar y probar el proceso

01 ASIGNAR RESPONSABILIDAD Y AUTORIDAD

Convierte la seguridad del almacenamiento en una función dentro de la arquitectura y las políticas globales de seguridad de la información. Incluso, aunque la empresa decida que la seguridad de las copias o del almacenamiento deben asignarse al equipo de almacenamiento, éstas deben integrar cualquier medida de seguridad de almacenamiento y backup con las que proteger el resto de la infraestructura. La integración de medidas de seguridad en la custodia y el backup ayuda a crear una protección más eficaz.

Divide las obligaciones cuando los datos sean especialmente confidenciales. Es importante asegurar que la persona que autoriza el acceso no sea la misma persona responsable de la ejecución.

El 90%
de las empresas que sufren una pérdida de datos importante desaparece del mercado en dos años.

FUENTE: CÁMARA DE COMERCIO DE LONDRES

02 EVALUAR EL RIESGO DE ALMACENAMIENTO YA QUE ÉSTE SE APLICA A LA SEGURIDAD DE LA INFORMACIÓN

REALIZAR UN ANÁLISIS DE RIESGOS DE TODO EL PROCESO DE BACKUP

Los responsables deben examinar todos los pasos en la metodología para la realización de backups en busca de vulnerabilidades en la seguridad. ¿Podría un administrador crear de forma secreta copias de seguridad? ¿Se dejan abiertas las cajas con soportes magnéticos? ¿Existe una estricta cadena de custodia de los backup? Si el backup y transporte de datos se realiza sin cifrar, puede originar que los datos críticos estén en riesgo.

EJECUTAR UN ANÁLISIS DE COSTES Y BENEFICIOS DEL CIFRADO DE DATOS DE BACKUP

Si un análisis de riesgos descubre numerosas vulnerabilidades, las organizaciones deben considerar seriamente si el cifrado está garantizado. Este proyecto debería ser más exhaustivo y no ceñirse únicamente al coste exclusivo de las licencias de software o dispositivos, e incluir los costes de tareas operativas relacionadas con el cifrado en procesos de backup y recuperación ante posibles incidencias, así como el impacto del cifrado en el tiempo de recuperación. El coste total del cifrado debería compararse con los riesgos potenciales y la probabilidad de una infracción de seguridad para determinar si tiene sentido, económicamente hablando, la implementación de un cifrado más amplio o más reducido, o no lo tiene en ningún caso. El cifrado de cintas con datos confidenciales es una inversión que merece la pena.

IDENTIFICAR LOS DATOS SENSIBLES

Conoce qué archivos, bases de datos y columnas se consideran suficientemente confidenciales por las unidades de negocio para garantizar el coste adicional de la protección. Asimismo, debes saber dónde se encuentran los datos. En muchas ocasiones, los datos se encuentran duplicados en el entorno. Es importante disponer de políticas y procedimientos que permitan saber exactamente dónde se encuentran los datos en todo momento. Por ejemplo, las empresas tienen información en portátiles que también puede estar duplicada en un disco de red o en un repositorio de backup utilizado en el PC.

03 DESARROLLAR UN PROGRAMA DE PROTECCIÓN DE LA INFORMACIÓN

ADOPTAR UN MÉTODO DE SEGURIDAD MULTICAPA

Adopta un método multicapa de protección de datos mediante la aplicación de las mejores prácticas para la red de datos de la red de almacenamiento, mientras que se añaden capas "a medida" del tipo de datos a custodiar. Entre éstas se incluyen las áreas de:

- **AUTENTICACIÓN.** Aplicación de técnicas de autenticación y anti-spoofing.
- **AUTORIZACIÓN.** Aplicación de privilegios en base a las funciones y responsabilidades en lugar de dar acceso administrativo completo. Cuando estén disponibles, uso de capacidades administrativas basadas en funciones de aplicaciones de gestión del almacenamiento, especialmente backup.
- **CIFRADO.** Todos los datos confidenciales deben estar cifrados cuando se almacenen o copien. Además, todos los datos de interfaz de gestión transmitidos a través de cualquier red que no sea privada deben estar cifrados. Los datos confidenciales se definen como la información que contiene datos personales o secretos comerciales.
- **AUDITORÍA.** Deben mantenerse los registros de las operaciones administrativas de cualquier usuario para garantizar la rastreabilidad y responsabilidad.

REALIZAR COPIAS DE LAS CINTAS DE BACKUP

Depender de una única copia de los datos no es nunca una buena idea. A pesar de que los soportes pueden tener una vida útil larga, son susceptibles de daños ambientales y físicos. La práctica recomendada consiste en realizar las copias de seguridad en soportes magnéticos y enviar dicha copia a un lugar externo. El método recomendado para los soportes de backup es escribir una cinta nueva mediante la lectura de la original. Este método tiene la ventaja de verificar que los datos del backup se puedan leer eliminando en la medida de lo posible el punto único de fallo de la cinta de backup.

La razón más frecuente por la cual no se cuenta con una política de duplicación de copias de seguridad es la falta de tiempo. Desde un punto de vista práctico, la realización de copias de seguridad conlleva mucho tiempo, lo que dificulta la duplicación de datos de forma puntual. Existen varios métodos para hacer frente a este problema. El primer método comienza con la optimización del sistema de backup para reducir el tiempo empleado en realizar el backup original. A continuación, pueden usarse varias unidades de cinta de alta velocidad para crear la segunda copia con fines de almacenamiento externo. Otro método consiste en usar la capacidad de algunos paquetes de software de backup para crear simultáneamente un original y una copia.



Aunque este método no tiene la ventaja de verificación tratada en el párrafo anterior, ahorra el tiempo necesario para realizar copias, y cualquier tipo de copia es mejor que no disponer de ninguna. Independientemente del tamaño del entorno, una combinación de dispositivos de cinta de alta velocidad, bibliotecas de cintas virtuales y servicios profesionales pueden ayudar a satisfacer este importante requisito.

IMPLEMENTAR UNA CADENA ESTRICTA E INTEGRAL DEL PROCESO DE CUSTODIA PARA LA GESTIÓN DE SOPORTES

La cadena de custodia se refiere a la actuación, método, gestión, supervisión y control de soportes o información (normalmente soportes magnéticos, aunque no siempre). El objetivo último de una cadena de custodia correcta es conservar la integridad de los recursos. Los siguientes aspectos sobre la cadena de custodia deben tenerse en cuenta.

Se debe realizar un seguimiento de los soportes mediante códigos de barras y generar informes que detallen su ubicación actual. Una práctica recomendada es realizar un informe diario de las copias de seguridad que se hayan enviado fuera y de las que hayan caducado, mandando a destruir aquellas que ya no son necesarias. Deben existir procedimientos operativos estándar documentados para garantizar que se lleven a cabo estas medidas. Deben analizarse la seguridad y el acceso a las instalaciones externas. Los soportes deben colocarse en contenedores cerrados antes de sacarlos del centro de datos. Asimismo, debe realizarse un seguimiento posterior de los mismos, mediante el análisis de códigos de barras cada vez que se traslada un contenedor, incluidos los que se encuentran en el centro de datos y en ubicaciones externas. Los contenedores de soportes deben estar sellados y no quedar nunca expuestos a que alguien pueda cogerlos.

Combina el inventario de soportes custodiados de forma externa periódicamente (al menos una vez al mes) con cintas que puedan guardarse internamente. Al final de cada mes, debe realizarse un control de inventario de todo lo externalizado y compararse con los registros de la aplicación de backup/archivado con el objetivo de descubrir posibles incoherencias. Si los soportes no están contabilizados se deben tomar las medidas oportunas.

Cuando los soportes hayan quedado obsoletos o ya no pueda confiarse en su integridad, estos deberán destruirse de forma adecuada. La destrucción de los soportes magnéticos se logra normalmente mediante la aplicación de un proceso de destrucción del cartucho, ya sea mediante la eliminación de los datos de la cinta o la destrucción de la cinta en su conjunto, con lo que quedaría inutilizable. La destrucción de datos puede realizarse en las propias instalaciones con un equipo de desmagnetización adecuado, o a través de los servicios de un tercero. (Si la destrucción de los datos tiene lugar en tus instalaciones, asegúrate de que el equipo de desmagnetización está calibrado para el soporte correcto). La destrucción de datos se realiza de una forma más óptima a través de una organización que proporcione un certificado de destrucción.

CONOCER LA CADENA DE CUSTODIA

Otro elemento crítico en la gestión segura de soportes es garantizar que los proveedores de custodia externa sigan las prácticas recomendadas. A continuación, se indican algunos elementos que deben tenerse en cuenta:

- VULNERABILIDAD.

No dejes las cintas en un contenedor abierto, por ejemplo, una caja de cartón en el mostrador de recepción a la espera de ser recogida. La recogida debe seguir un procedimiento operativo estándar en el que un responsable del departamento de informática entregue y reciba la firma de un representante conocido e identificado del proveedor.

- PROCESO DE SELECCIÓN.

Cuando una empresa externa custodia los datos críticos de tu compañía, debes estar seguro de que el proveedor realiza un minucioso proceso de selección de su personal.

- LA EMPRESA DEBE SEGUIR UN PROCESO COMPLETO DE LA CADENA DE CUSTODIA.

Tu proveedor debe explicarte todo el proceso relacionado con la gestión de los soportes de principio a fin. Haz hincapié en la seguridad física, junto con mecanismos de auditoría y control para garantizar que se sigue el proceso. Resulta poco aconsejable trasladar datos confidenciales en vehículos que puedan identificarse fácilmente.

- **CUSTODIA EN MALETINES.**

Con la custodia en maletines se realiza el seguimiento de cubos o cajas, pero no de su contenido. La mayoría de los proveedores admiten este tipo de custodia.

- **CONTROLES DE SEGURIDAD FÍSICOS.**

Las instalaciones deben protegerse de forma adecuada. Ninguna persona no autorizada debe tener acceso al área de seguridad.

- **CONTROLES MEDIOAMBIENTALES.**

Las cintas y otros soportes no deben almacenarse nunca en el maletero de un vehículo ni en ninguna otra ubicación con un entorno no controlado. Para la custodia de soportes magnéticos, el entorno debe controlarse de forma estricta, incluyendo la temperatura, la humedad y el control estático. El polvo es el peor enemigo para la mayoría de soportes y dispositivos de grabación. El entorno de backup y custodia debe permanecer limpio y libre de polvo. Debes utilizar un trapo suave y antiestático para limpiar el exterior de los cartuchos, y eliminar el polvo de las ranuras de una biblioteca utilizando aire comprimido de un pulverizador. Las cintas deberán transportarse en un soporte electrostático y no apilarse en un cubo o una caja de cartón. Aunque parezcan bastante duraderas, las cintas pueden dañarse fácilmente si se manipulan de forma incorrecta.

TENER EN CUENTA LA CUSTODIA DE DATOS DIGITALES

Un aspecto a tener en cuenta es la custodia de datos digitales y el transporte de información de soportes físicos en un vehículo. Actualmente, existen diversas compañías que ofrecen a los profesionales de IT la posibilidad de realizar copias de seguridad de los datos a través de Internet. Los datos pueden cifrarse y trasladarse a través de Internet hasta una instalación de datos de backup seguros. La custodia de datos digitales puede no ser una solución práctica para todos los datos de la empresa, pero sí puede resultar práctica para los datos distribuidos en servidores de archivos o en ordenadores personales. Los datos distribuidos pueden representar el 60% de la información de una empresa y resulta difícil para los encargados de IT poder controlarlos en su totalidad.

Asegúrate de que el proveedor que ofrece estos servicios cifra los datos mientras se transfieren y cuando están en espera. Además, habla con el proveedor sobre cómo mantener disponible la información. ¿Se ha realizado una copia de seguridad en un soporte magnético? ¿Se ha replicado en otro sitio? Asegúrate de que las prácticas de recuperación de datos ante posibles incidencias del proveedor cumplan un estándar excepcional. Habla con el proveedor sobre cómo mantener la información disponible para su recuperación o la asistencia en procesos judiciales.

Cuando una empresa externa custodia la información crítica de tu compañía, debes asegurarte de que realiza un minucioso proceso de selección de sus empleados.

04 COMUNICAR LOS PROCESOS DE PROTECCIÓN DE LA INFORMACIÓN Y SEGURIDAD

Una vez definido el proceso para garantizar que los datos confidenciales están protegidos y gestionados de forma adecuada, es importante asegurar que las personas responsables de la seguridad estén bien informadas y hayan recibido la formación adecuada. Las políticas de seguridad representan el aspecto más importante de la asignación de responsabilidad y autoridad.

INFORMAR A LOS DIRECTORES EMPRESARIALES DE LOS RIESGOS, LAS CONTRAMEDIDAS Y LOS COSTES

La pérdida de datos y el robo de propiedad intelectual son un problema de la empresa, no del departamento de informática. Como tal, el Responsable de la Seguridad de la Información (CISO, por sus siglas en inglés) debería comenzar a aplicar la seguridad de los datos mediante formación a los ejecutivos de la empresa en lo que se refiere a los riesgos, amenazas y posibles pérdidas debidas a infracciones de seguridad, más el coste de contramedidas de seguridad. De esta forma, los directores corporativos pueden tomar decisiones fundadas sobre el coste y las ventajas de las inversiones en seguridad de datos.

VALORAR LOS RIESGOS Y FORMAR AL PERSONAL

Los datos procedentes de estudios de seguridad demuestran que "más vale prevenir que curar". Es más probable que las organizaciones que se dedican a valorar los riesgos apliquen políticas, procedimientos y tecnologías de seguridad que protegen los activos vitales. Por otro lado, una infraestructura vulnerable y un personal sin formación representan un problema en potencia: indican una retribución real por realizar el "trabajo repetitivo y agotador" de la seguridad.

05 EJECUTAR Y PROBAR EL PLAN DE SEGURIDAD DE PROTECCIÓN DE LA INFORMACIÓN

La protección de datos seguros no se basa en la tecnología, sino que representa todo un proceso. Ése es el motivo por el que es importante validar el proceso. A medida que una empresa crece, la protección de la información y los datos necesitan cambiar, por lo que las prácticas de seguridad de la información deben adaptarse. Una vez desarrollado y definido el plan integral, y tras informar de él a las personas apropiadas, es hora de llevarlo a la práctica. Asegúrate de contar con las herramientas, tecnologías y metodologías que necesitas para la clasificación de la información.

Prueba el proceso una vez implementado. Recuerda, la prueba debe incluir los procesos de backup y recuperación. Intenta incluir en el proceso una amenaza, incluida la pérdida de un servidor y de un soporte, problemas de red, problemas con un dispositivo, problemas de clasificación de datos y cualquier otro escenario que pudiera afectar al negocio. Realiza pruebas con el personal que pudiera estar menos familiarizado con el proceso. Este test ayuda a garantizar que el proceso resulta fácil de seguir y que puede ejecutarse incluso si el responsable no está en la oficina.

Se tardan **19 días**
en volver a escribir
20 Mb de datos
perdidos.

FUENTE: REALTY TIMES

Cada **15 segundos**
se rompe un
disco duro.

FUENTE: HARRIS INTERACTIVE

2.000 portátiles
se roban o se pierden
cada día.

FUENTE: HARRIS INTERACTIVE

LA INFORMACIÓN TIENE VIDA PROPIA. TE AYUDAMOS A GESTIONARLA.

Podemos ayudarte a gestionar tu información durante todo el ciclo de vida, reducir costes y mejorar la eficiencia.



**ANÁLISIS Y
ORIENTACIÓN**



**ALMACENAMIENTO
Y PROTECCIÓN**



DIGITALIZACIÓN



**ACCESO
FLEXIBLE**



**DESTRUCCIÓN
SEGURA**

UN SOCIO EN EL QUE CONFIAR

Independientemente del tamaño de la empresa o el sector, ofrecemos servicio especializado basado en estos principios clave:

CONFIANZA

Durante casi 60 años hemos sido el socio de confianza de empresas de todos los tamaños. Trabajamos desde más de 1.000 instalaciones de todo el mundo.

SEGURIDAD

Gracias a nuestras instalaciones seguras, los equipos y los procesos optimizados, tu información siempre estará en buenas manos.

EXPERIENCIA

Nuestro amplio y profundo conocimiento se basa en nuestro personal, procesos y tecnologías. La comprensión de los requerimientos relacionados con la normativa legal nos permite colaborar con los clientes para que puedan sacar mayor partido a su información, al mismo tiempo que reducen los costes.

ORIENTACIÓN AL CLIENTE

Nuestro compromiso con un servicio de máxima calidad ofrece asistencia 24 horas al día, todos los días.

SOSTENIBILIDAD

Al ayudarte a reducir la información que necesitas mantener y reciclar lo que no se necesita, ayudamos a las empresas a cumplir con los compromisos de sostenibilidad.

LLÁMANOS

Para obtener más información y asesoramiento sobre cómo Iron Mountain puede ayudarte con la gestión de la información, visita www.ironmountain.es o llama al 900 22 23 24.

