COPIAS DE SEGURIDAD
– GUÍA DE USUARIO –

Xavi Conde
Gerard Soteras

Índice

Introducción

En el mundo digital actual, la pérdida de datos debido a errores humanos, fallos técnicos o ataques cibernéticos puede tener consecuencias devastadoras. Por esta razón, el uso de copias de seguridad es esencial para garantizar la protección y recuperación de la información en caso de cualquier incidente.

Copia de seguridad, backup, respaldo de datos… Són algunos de los muchos nombres, que se le da a la acción de duplicar y almacenar la información en un medio alternativo para prevenir su pérdida. Existen muchos métodos, estrategias y softwares para realizar copias de seguridad, cada uno adaptado a las necesidades específicas de las empresas y usuarios individuales.

Esta guía proporciona información detallada sobre los diferentes tipos de copias de seguridad, su importancia, estrategias recomendadas y la mejor manera de implementarlas en diversos entornos. Al final, el objetivo que se persigue, es garantizar la integridad y disponibilidad de los datos reduciendo riesgos y asegurando la continuidad del negocio ante cualquier pérdida.

Copias de seguridad

Una copia de seguridad es un proceso que realiza una duplicación de la información almacenada en un sistema o dispositivo a otro soporte externo, al host o servidor donde se encuentran los datos. Su finalidad principal es garantizar la recuperación de datos en caso de pérdida, corrupción o eliminación accidental de los mismos. En el ámbito empresarial, las copias de seguridad son esenciales para la protección de la información sensible y la continuidad operativa de la empresa.

Existen diversos métodos para realizar copias de seguridad, desde soluciones automatizadas hasta medios manuales, dependiendo de las necesidades de cada empresa o usuario, se aplicará un tipo u otro. Implementar una estrategia de respaldo adecuada puede marcar la diferencia entre la recuperación efectiva de datos y la pérdida irreversible de estos. Además, es recomendable establecer protocolos de verificación para comprobar la integridad de los datos respaldados.

Según la incibe (Instituto Nacional de Ciberseguridad de España) en el contexto empresarial, las copias de seguridad forman parte del Plan Director de Seguridad y del Plan de Contingencia y Continuidad del Negocio, definiendo la información a respaldar, los soportes a utilizar y la periodicidad de las copias.

Importancia de las copias de seguridad

Las copias de seguridad juegan un papel crucial en la seguridad informática y la gestión de los datos. Su importancia radica en diversos aspectos, que mencionaremos a continuación:

Protección contra pérdida de datos: Fallos en el hardware, errores humanos, ataques cibernéticos y desastres naturales pueden provocar la pérdida de información valiosa.

Continuidad del negocio: En caso de incidentes, disponer de copias de seguridad permite restaurar rápidamente los sistemas y minimizar el tiempo de inactividad, además garantiza una menor pérdida económica para el negocio.

Cumplimiento normativo y legal: Muchos marcos legales, exigen la conservación de ciertos datos durante períodos específicos. Tener respaldos adecuados facilita el cumplimiento de estas normativas y nos evita sanciones.

Defensa ante ataques cibernéticos: Como ya hemos visto en numerosas ocasiones, enfrentarse a amenazas como ransomware puede ser devastador. Un respaldo actualizado permite restaurar los datos sin ceder ante los atacantes.

Optimización de recursos: Contar con respaldos de información permite una rápida recuperación en caso de fallos, evitando la necesidad de invertir en recuperación de datos o reconstrucción de sistemas.

Además, es importante tener en cuenta que los dispositivos de almacenamiento (como todos los dispositivos electrónicos) tienen una vida útil limitada y pueden fallar con el tiempo, lo que hace aún más importante la implementación de copias de seguridad adaptadas a las necesidades de la persona o la empresa.

Tipos de copias de seguridad y periodicidad

Copia de seguridad en espejo (RAID 1)
Se basa en la duplicación en tiempo real de la información hacia otro disco duro.

Ventajas: Recuperación inmediata de datos sin necesidad de procesos adicionales, ya que se encuentran en un dispositivo hardware, a nuestro alcance.
Desventajas: No protege contra eliminación accidental, ya que los cambios se replican en ambos discos.
Periodicidad: Se actualiza constantemente en tiempo real.
Recomendaciones: Normalmente, suele ir acompañado con otro tipo de copias de seguridad para mayor protección.

Copia de seguridad completa
Realiza un respaldo íntegro de todos los datos almacenados en el sistema.

Ventajas: Restauración sencilla y rápida, ya que toda la información está en una única copia, ya que además suelen estar centralizadas.
Desventajas: Requiere un gran espacio de almacenamiento y consume más tiempo.
Periodicidad: A causa de su peso y tiempo para realizarse, se suele recomendar hacerlo de manera semanal o mensual, dependiendo del volumen de datos y la criticidad.
Recomendaciones: Ideal para complementar con copias diferenciales o incrementales.

Copia de seguridad diferencial
Copia únicamente los datos que han cambiado desde la última copia completa, se consigue mediante una comparativa de los archivos de la última copia y la actual.

Ventajas: Ocupa menos espacio que una copia completa y reduce el tiempo de respaldo.
Desventajas: A medida que se generan más copias diferenciales, el tamaño del respaldo crece.
Periodicidad: Suelen hacerse diariamente, para mantener versiones recientes de los archivos.
Recomendaciones: Puede usarse en combinación con copias completas para reducir tiempos de recuperación en caso necesario.

Copia de seguridad incremental
Guarda solo los archivos que han sido modificados desde la última copia (incremental o completa), atendiendo a las necesidades del negocio o usuario.

Ventajas: Optimiza el uso del almacenamiento y reduce el tiempo de respaldo.
Desventajas: La restauración puede ser más lenta, ya que depende de varias copias.
Periodicidad: Suele ser diaria o varias veces al día, dependiendo del volumen de cambios y la criticidad.
Recomendaciones: Es muy recomendable un buen control de versiones para evitar pérdidas de datos.

Estrategias de copias de seguridad

Estrategia 3-2-1
Suele ser la estrategia referente, ya que te garantiza una protección efectiva de los datos:
3 copias de cada archivo crítico (una original y dos de respaldo).
2 almacenamientos en diferentes medios (por ejemplo, disco duro y almacenamiento en la nube).
1 copia almacenada fuera del sitio principal (offsite) para protección ante desastres físicos (ataques hardware, desastres naturales…).

Estrategia de copia 4-3-2
Muy parecido a la 3-2-1, pero adaptando los valores, para mejorar la seguridad de los datos, pero aumentando significativamente el almacenamiento.
4 copias de cada archivo crítico.
3 almacenamientos diferentes (nube, disco local y NAS).
2 copias almacenadas fuera de la organización.

Estrategia de respaldo continuo
Esta estrategia se basa en realizar la copia de seguridad en tiempo real, cada vez que detecte algún cambio en los datos.
Ventaja: Minimiza la pérdida de datos al instante.
Desventaja: Puede generar alta carga en los sistemas y requiere infraestructura robusta.

Almacenamiento

Opciones de almacenamiento
Dependiendo del volumen de datos y la necesidad de accesibilidad de la persona o negocio que esté llevando a cabo la copia de seguridad, existen diversas opciones para almacenar copias de seguridad y definir cuál se adapta más a cada situación:

Dispositivos NAS: Permiten la gestión centralizada de copias de seguridad en pequeñas y medianas empresas.
Cintas magnéticas: Ideales para almacenamiento de grandes volúmenes a largo plazo, con bajo costo por terabyte.
Discos duros externos (HDD y SSD): Útiles para copias locales con acceso rápido.
Almacenamiento en la nube: Ofrece acceso remoto y protección contra desastres físicos, ya que se los datos se almacenan de manera distribuida.
Soluciones híbridas: Combinación de almacenamiento local y en la nube para una mayor flexibilidad, implica un mayor desarrollo pero también són las más seguras.

Datos a respaldar

Criterios de selección
Para optimizar el proceso de respaldo, es importante definir qué datos requieren protección prioritaria:
Información crítica del negocio: Documentos estratégicos, bases de datos y sistemas esenciales.
Registros legales y financieros: Información contable, contratos y datos obligatorios por ley.
Datos operativos: Registros de clientes, proyectos y archivos de trabajo en curso.
Sistemas y configuraciones: Programas, archivos de instalación y configuraciones clave.

Tipos de información a respaldar
Los tipos de datos más relevantes que deben incluirse en las copias de seguridad son:

Bases de datos empresariales: Información estructurada fundamental para operaciones.
Archivos administrativos y de gestión: Reportes, documentos de planificación y contratos.
Correos electrónicos corporativos: Mensajes importantes que contengan datos comerciales.
Sistemas de software y configuraciones: Programas y ajustes críticos para el funcionamiento de la empresa.

Conclusión

La realización de copias de seguridad es una de las medidas más importantes para garantizar la protección y recuperación de datos. Sin una estrategia adecuada, la pérdida de información puede ocasionar graves consecuencias operativas, económicas y legales.

Hemos visto que existen diversos métodos y estrategias para realizar copias de seguridad, cada uno con sus propias ventajas y desventajas. La elección del mejor método dependerá de las necesidades y características de cada empresa o usuario. Implementar la estrategia 3-2-1, junto con otras metodologías como la 4-3-2 o el respaldo continuo, puede proporcionar una seguridad adicional y minimizar riesgos.

Es fundamental realizar copias de seguridad de manera periódica, asegurando que los datos respaldados sean verificados y almacenados en ubicaciones seguras. Como también, es recomendable llevar a cabo simulaciones de restauración para garantizar la integridad de la información y la efectividad de los procedimientos.

Finalmente, la protección de los datos es una responsabilidad compartida. Tanto las empresas como los usuarios individuales deben adoptar buenas prácticas para mitigar posibles pérdidas y garantizar la continuidad operativa ante cualquier eventualidad. Invertir en copias de seguridad es una decisión inteligente que proporciona tranquilidad y seguridad ante cualquier incidente.

Bibliografía

Microsoft. (2023). *"Plan de copias de seguridad en Windows"*

Kaspersky. (2022). *"Estrategias de respaldo y recuperación ante desastres"*

Veeam Software. (2023). *"Estrategia de backup 3-2-1 y mejores prácticas"*

Red Hat. (2022). *"Guía sobre copias de seguridad y recuperación en entornos empresariales"*

IBM. (2023). *"Data Backup and Recovery Best Practices"*

Cisco. (2022). *"Backup and Disaster Recovery Strategies for IT Infrastructure"*