Resumen sobre Backups

Es una copia de información importante, un duplicado de datos e información que dispone de una organización, esto con el objetivo de guardar y tener a mano esta información en casos de emergencia, donde se pierda la información o datos.

Tipos de copia de seguridad

Existe una gran cantidad de tipos de copias de seguridad, que se diferencian por su manera de copiar los datos, velocidad y requerimientos de espacio.

- **Completa.**

Crea una copia completa de todos los datos de un sistema. Este puede ser una copia de los datos de un ordenador portátil o un ejemplo seria una copia de todas las nóminas digitales del año.

VENTAJAS: La restauración de una copia de seguridad completa es rápida

DESVENTAJAS: cada ejecución es lenta y ocupa más espacio con respecto a las otras tipologías.

- **Incremental**.

Primero se realiza una copia de seguridad completa y las siguientes copias incluyen únicamente los cambios realizados desde la última copia de seguridad.

VENTAJAS: Es mucho más rápida que una copia de seguridad completa y requiere menos espacio

DESVENTAJAS: la restauración es más lenta que con una copia de seguridad completa o diferencial.

- **Diferencial**.

Se realiza una copia de seguridad de todos los cambios realizados desde la última copia de seguridad completa.

VENTAJAS: Es mucho más rápida y requiere menos espacio de almacenamiento que una copia de seguridad completa,

DESVENTAJA: Las restauraciones son más lentas que con una copia de seguridad completa, pero más rápidas que con copias de seguridad incrementales.
Además de la velocidad de realización y de restauración y la seguridad, el espacio es un requisito fundamental a la hora de planificar una estrategia de copias de seguridad

• **Espejo**.

Es un reflejo fiel de la fuente que se está respaldando, lo que implica que un archivo eliminado en el origen, también se eliminará en la copia de seguridad.

• **Sintética completa.**

Reconstruye la imagen de copia de seguridad completa usando todas las copias incrementales o diferenciales. Puede almacenarse en cintas en localizaciones externas, con la ventaja de que se reduce el tiempo de restauración.

• **Backup incremental inverso.**

Es una copia de seguridad incremental de los cambios realizados entre dos instancias de una copia espejo. Después de la copia completa inicial, cada copia sucesiva aplica los cambios a la anterior completa, creando una nueva copia de seguridad sintética completa cada vez, mientras se mantiene la capacidad de volver a las versiones anteriores

• **Protección de datos continua (CDP).**

es un proceso en el que cada cambio realizado en un documento, archivo o carpeta almacenado activa automáticamente una copia de seguridad de esa fuente de datos.

Tipos de copias de seguridad según su destino

•Locales

cuando el medio de almacenamiento se mantiene a mano o en el mismo edificio que la fuente. Puede tratarse de discos duros o unidades de almacenamiento conectado en red (NAS).

• Externas

cuando el medio de almacenamiento se mantiene en una ubicación geográfica diferente de la fuente (otra oficina, otro edificio o ubicaciones externas). De esta manera se consigue protección adicional contra robos, incendios, inundaciones y otros desastres naturales.

• Remotas

cuando, además de ser externas, es posible acceder, restaurar o administrar las copias de seguridad sin estar físicamente presente en la instalación de almacenamiento de respaldo.

• En línea

cuando se realizan en un medio de almacenamiento que siempre está conectado de forma segura a una red o conexión a Internet. Es un servicio ofrecido hoy en día por muchos centros de datos. Es también llamado copia de seguridad en la nube, si es proporcionado como un servicio en la nube.

Dispositivos utilizados para copias de seguridad

Discos Duros Externos:

Los discos duros externos son unidades de almacenamiento que se conectan a través de puertos USB o Thunderbolt a una computadora o servidor. Vienen en diferentes capacidades, desde gigabytes hasta varios terabytes.

Usuarios comunes: Tanto empresas como usuarios individuales utilizan discos duros externos. Son populares para copias de seguridad personales y para pequeñas empresas debido a su accesibilidad y costo asequible.

Uso para backup: Los discos duros externos son ideales para realizar copias de seguridad de datos importantes, ya que ofrecen una forma rápida y sencilla de hacerlo. Sin embargo, no son la mejor opción para la retención a largo plazo debido a la posibilidad de daños físicos o pérdida.

Tipo de Backup Favorecido: Copias de seguridad incrementales y diferenciales.

Ventajas:

Capacidad de almacenamiento significativa.

Acceso rápido a los datos.

Relativamente económicos.

Desventajas:

Vulnerables a daños físicos y fallas.

No ideales para la retención a largo plazo.

Pueden ser robados o extraviados.

Unidades de Cinta:

Las unidades de cinta utilizan cintas magnéticas para almacenar datos. Están diseñadas para una retención a largo plazo y se utilizan principalmente en entornos empresariales.

Usuarios comunes: Las empresas grandes y organizaciones gubernamentales son los principales usuarios de unidades de cinta debido a su capacidad de almacenamiento masivo y confiabilidad.

Uso para backup: Las unidades de cinta son ideales para copias de seguridad empresariales y archivado de datos a largo plazo debido a su capacidad y resistencia a la degradación con el tiempo. Sin embargo, son menos adecuadas para copias de seguridad frecuentes debido a la velocidad de acceso más lenta.

Tipo de Backup Favorecido: Copias de seguridad completas

Ventajas:

Excelente para almacenamiento a largo plazo.

Gran capacidad de almacenamiento.

Menor costo por gigabyte en comparación con otros medios.

Desventajas:

Velocidad de acceso lenta.

Requiere hardware especializado.

No es adecuado para copias de seguridad frecuentes.

Dispositivos de Almacenamiento en Red (NAS):

Descripción: Un NAS es un dispositivo de almacenamiento conectado a una red que permite el acceso compartido a datos y la configuración de copias de seguridad automáticas. Puede contener múltiples discos duros.

Usuarios comunes: Empresas de todos los tamaños y usuarios avanzados en el hogar que necesitan un almacenamiento centralizado y compartido.

Uso para backup: Los NAS son ideales para copias de seguridad empresariales y personales debido a su capacidad de acceso remoto, redundancia y escalabilidad.

Tipo de Backup Favorecido: diferenciales

Ventajas:

Acceso compartido a través de la red.

Redundancia de datos para mayor seguridad.

Escalabilidad fácil al agregar discos adicionales.

Desventajas:

Requiere configuración y mantenimiento.

Vulnerable a fallas de red y ataques.

Costoso en comparación con soluciones individuales.

Servicios de Almacenamiento en la Nube:

Descripción: Los servicios de almacenamiento en la nube son plataformas en línea que permiten a los usuarios almacenar y acceder a sus datos a través de Internet. Los datos se almacenan en servidores remotos gestionados por proveedores de servicios en la nube.

Usuarios comunes: Tanto individuos como empresas utilizan servicios de almacenamiento en la nube. Son muy populares para respaldos personales y empresariales debido a su facilidad de uso y flexibilidad.

Uso para backup: Los servicios en la nube ofrecen copias de seguridad automáticas y programables, lo que los hace ideales para usuarios que desean acceso desde cualquier lugar y una mayor seguridad de los datos. También son útiles para colaboración en línea y recuperación ante desastres.

Tipo de Backup Favorecido: Copias de seguridad Incrementales y Diferenciales, pero también puede manejar Copias de seguridad Completas si es necesario.

Ventajas:

Acceso desde cualquier lugar con conexión a Internet.

Alta escalabilidad y flexibilidad.

Copias de seguridad automáticas y programables.

Desventajas:

Dependencia de proveedores externos.

Posibles problemas de seguridad y privacidad.

Costos recurrentes a largo plazo.

Unidades de Estado Sólido (SSD):

Descripción: Las unidades de estado sólido utilizan memoria flash para almacenar datos y no tienen partes móviles. Son rápidas y resistentes a golpes.

Usuarios comunes: Principalmente, usuarios avanzados y empresas que necesitan alta velocidad de acceso a datos.

Uso para backup: Los SSD se utilizan para copias de seguridad que requieren velocidad y resistencia, como copias de seguridad de servidores o aplicaciones críticas. Sin embargo, debido a su costo por gigabyte más alto, a menudo se combinan con otros dispositivos de respaldo.

Tipo de backup favorecido: completa e incremental

Ventajas:

Velocidades de lectura y escritura extremadamente rápidas.

Resistentes a golpes y vibraciones.

Baja latencia.

Desventajas:

Costo por gigabyte más alto que otros dispositivos.

Vida útil limitada en comparación con algunos medios.

Dispositivos de Almacenamiento Óptico (por ejemplo, Discos Blu-ray):

Descripción: Los discos ópticos utilizan láseres para grabar y leer datos en discos. Son resistentes a daños físicos y ofrecen una forma de archivar datos a largo plazo.

Usuarios comunes: Usuarios individuales y algunas empresas que desean archivar datos importantes de forma segura.

Uso para backup: Los discos ópticos son ideales para el almacenamiento a largo plazo y la protección contra daños físicos. Sin embargo, son menos adecuados para copias de seguridad frecuentes debido a su lentitud en la grabación y recuperación de datos.

Tipo de Backup Favorecido: Completa

Ventajas:

Resistencia a daños físicos y al agua.

Ideal para archivar datos importantes a largo plazo.

Portabilidad.

Desventajas:

Capacidad de almacenamiento limitada en comparación con otros medios.

Lentitud en la grabación y recuperación de datos.

Requiere hardware compatible.

Políticas de respaldo de información

Las políticas de respaldo son un conjunto de normas con el objetivo de proteger la información contra una amplia gama de amenazas para asegurar la continuidad del servicio y minimizar los daños, procurando la preservación de la confidencialidad, disponibilidad e integridad de la información. Estas políticas son esenciales para prevenir la pérdida de datos debido a fallas tecnológicas, errores humanos, desastres naturales o ataques cibernéticos. Las políticas de respaldo de información pueden variar significativamente de una empresa a otra. Esto se debe a que las necesidades, recursos, objetivos y entornos tecnológicos de cada organización son diferentes. Algunos de los factores que influyen en las diferencias entre las políticas de respaldo de una empresa a otra incluyen:

- Tamaño y tipo de empresa: Las pequeñas empresas pueden tener políticas de respaldo más simples en comparación con las grandes corporaciones.

- Recursos disponibles: Las empresas con mayores recursos pueden invertir en tecnologías y soluciones de respaldo más avanzadas, mientras que las empresas más pequeñas pueden depender de soluciones más asequibles.

- Tecnología y sistemas utilizados: El entorno tecnológico de una empresa, incluyendo el tipo de sistemas operativos, bases de datos y aplicaciones utilizados, puede influir en la elección de las soluciones de respaldo.

- Riesgos y amenazas: Las empresas pueden enfrentar diferentes riesgos y amenazas, como ciberataques, desastres naturales o errores humanos, lo que puede influir en la estrategia de respaldo.

- Cambios en la infraestructura y la tecnología: Las empresas que adoptan nuevas tecnologías o cambian su infraestructura pueden necesitar ajustar sus políticas de respaldo en consecuencia.

- Criticidad de los datos: La importancia de los datos varía según la empresa y puede influir en la frecuencia y los métodos de respaldo. Por ejemplo, una empresa de servicios financieros puede considerar sus datos financieros como críticos y respaldarlos con mayor frecuencia.

Dado que las necesidades y circunstancias varían, es fundamental que cada empresa desarrolle una política de respaldo de información que se adapte a sus características específicas. Sin embargo, todas las empresas deben asegurarse de que sus políticas de respaldo cumplan con los estándares de seguridad y buenas prácticas de gestión de datos para proteger adecuadamente sus activos digitales. Algunas de las políticas que se pueden encontrar en varias empresas son:

1.COBIT: Es un conjunto de reglas y guías para que las empresas administren su tecnología de manera efectiva. Ayuda a asegurarse de que las personas obtengan lo que necesitan de la tecnología y de que se use de manera segura.

- **Definir una política de respaldo:** Debería haber una política clara que establezca los requisitos de respaldo para la organización, incluyendo la frecuencia de respaldos, la retención de datos, la ubicación de los respaldos, etc.
- **Documentar procedimientos de respaldo:** Los procedimientos para realizar respaldos, así como la recuperación de datos, deben documentarse y seguirse de manera consistente.
- **Automatizar cuando sea posible:** Se debe utilizar la automatización para programar respaldos de manera regular y garantizar su cumplimiento.
- **Proteger los respaldos:** Los datos de respaldo son valiosos y deben protegerse adecuadamente contra el acceso no autorizado y los desastres, como incendios o inundaciones.
- **Realizar pruebas de recuperación:** Deben realizarse pruebas periódicas para garantizar que los respaldos sean recuperables y que los tiempos de recuperación sean aceptables.
- **Gestionar la retención de datos:** COBIT sugiere que las organizaciones establezcan políticas claras de retención de datos para determinar cuánto tiempo deben mantenerse los respaldos y cuándo deben ser eliminados de manera segura.
- **Revisión y mejora continua:** Los procesos de respaldo deben revisarse regularmente y mejorarse según sea necesario para mantenerse alineados con los objetivos de la organización y los cambios en el entorno de TI.

2.ISO/IEC 27001: La norma ISO 27001 es una norma internacional que establece los requisitos para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información (SGSI) en una organización. Esta norma se utiliza para ayudar a las organizaciones a proteger sus activos de información y garantizar la confidencialidad, integridad y disponibilidad de la información.

- **Alcance del SGSI para Copias de Seguridad**: La organización debe definir claramente el alcance del SGSI para incluir la gestión de copias de seguridad. Esto implica identificar los activos de información relevantes que requieren respaldo y las partes interesadas relacionadas.
- **Política de Seguridad de la Información para Copias de Seguridad**: La organización debe establecer una política de seguridad de la información que incluya objetivos y compromisos específicos relacionados con la gestión de copias de seguridad. Esto asegura que se aborden los

aspectos críticos, como la frecuencia de las copias, los procedimientos de recuperación y la retención de datos.

- **Análisis de Riesgos para Copias de Seguridad**: Se debe realizar una evaluación de riesgos enfocada en las amenazas y vulnerabilidades que pueden afectar la integridad y disponibilidad de las copias de seguridad. Esto incluye considerar posibles fallos en el proceso de respaldo y ataques cibernéticos dirigidos a los datos de respaldo.

- **Tratamiento de Riesgos para Copias de Seguridad:** Un plan de tratamiento de riesgos debe ser desarrollado para las copias de seguridad. Esto implica la implementación de controles adecuados, como cifrado de datos de respaldo y sistemas de autenticación, para mitigar o aceptar los riesgos identificados.
- **Cumplimiento Legal y Regulatorio para Copias de Seguridad:** La organización debe identificar y cumplir con todos los requisitos legales y regulaciones relacionados con la gestión de copias de seguridad, como las leyes de privacidad de datos y retención de registros.
- **Objetivos y Controles de Seguridad para Copias de Seguridad:** Establecer objetivos específicos para la gestión de copias de seguridad, tales como tiempos de recuperación, y aplicar controles técnicos y procedimentales para alcanzar esos objetivos.
- **Procesos de Gestión de la Seguridad para Copias de Seguridad:** La norma ISO 27001 incluye procesos de gestión como la planificación de respaldos, monitoreo de copias y recuperación ante desastres, que son fundamentales para garantizar la seguridad de las copias de seguridad.
- **Auditoría y Revisión para Copias de Seguridad:** Realizar auditorías internas periódicas para evaluar el cumplimiento de los requisitos y revisar la eficacia de los procedimientos de copias de seguridad y recuperación.

- **Mejora Continua para Copias de Seguridad:** La organización debe buscar constantemente la mejora en la gestión de copias de seguridad, corrigiendo deficiencias, implementando acciones correctivas y preventivas, y revisando regularmente los resultados.

- **Documentación para Copias de Seguridad:** Mantener documentación adecuada que respalde el SGSI en relación con las copias de seguridad, incluyendo políticas, procedimientos y registros de respaldo.

3.NIST: Es un instituto que establece estándares para la seguridad de la información y la tecnología. Ofrece pautas para proteger sistemas informáticos, contraseñas y enseña sobre seguridad en línea. Algunas de estas son:

- **Copia de seguridad (Backup**): La copia de seguridad se refiere al proceso de hacer copias de los datos y la información crítica de una organización para su preservación y recuperación en caso de pérdida, daño o eliminación accidental. Las copias de seguridad se utilizan para garantizar la disponibilidad y la integridad de los datos.
- **Restauración (Restore):** La restauración es el proceso de recuperar datos y sistemas desde las copias de seguridad almacenadas. Cuando ocurre una pérdida de datos o un incidente, la restauración se utiliza para devolver los sistemas y datos a un estado operativo normal.

- **Política de Copias de Seguridad:** Una política de copias de seguridad es un conjunto de directrices y procedimientos que una organización establece para gestionar las copias de seguridad de sus datos. Esto incluye la frecuencia de las copias de seguridad, la retención de datos, la ubicación de almacenamiento y otros aspectos relacionados con la gestión de la información respaldada.
- **Copia de Seguridad Completa:** Una copia de seguridad completa implica la copia de todos los datos y archivos en un sistema o dispositivo en un momento dado. Estas copias de seguridad son útiles para restaurar completamente un sistema, pero pueden ser intensivas en tiempo y recursos.
- **Copia de Seguridad Incremental:** Una copia de seguridad incremental solo copia los datos que han cambiado desde la última copia de seguridad, lo que ahorra espacio de almacenamiento y tiempo de respaldo. Para restaurar completamente un sistema, es necesario combinar múltiples copias de seguridad incrementales.
- **Copia de Seguridad Diferencial:** Una copia de seguridad diferencial copia todos los datos que han cambiado desde la última copia de seguridad completa. Esto significa que solo se necesitan dos conjuntos de copias de seguridad (la completa y la diferencial más reciente) para restaurar completamente un sistema.
- **Plan de Continuidad del Negocio:** Un plan de continuidad del negocio incluye estrategias y procedimientos para garantizar la continuidad de las operaciones de una organización en caso de interrupciones, desastres o incidentes que afecten la disponibilidad de datos y sistemas. Las copias de seguridad y la restauración son componentes clave de estos planes.
- **Pruebas de Restauración:** Las pruebas de restauración son pruebas regulares que se realizan para verificar que las copias de seguridad sean efectivas y que los datos se puedan restaurar correctamente en caso de necesidad. Estas pruebas son esenciales para garantizar la capacidad de recuperación de una organización.

4.EITIL: Es una biblioteca de mejores prácticas para administrar servicios de tecnología. Ayuda a las empresas a gestionar y entregar servicios tecnológicos de manera organizada y eficiente, enfocándose en la satisfacción del cliente y la mejora continua.

- **Enfocarse en el valor:** Asegúrate de que los backups se realicen de manera que agreguen valor real a la organización al garantizar la disponibilidad y la recuperación de datos críticos en caso de pérdida o desastre.
- **Empezar desde donde ya estamos:** Utiliza las infraestructuras y sistemas de backup existentes para mejorar y optimizar la gestión de respaldo en lugar de comenzar desde cero.
- **Avanzar iterativamente y retroalimentarse:** Implementa mejoras continuas en tus procesos de respaldo. Realiza revisiones periódicas de la efectividad de los backups y ajusta tus estrategias en función de los resultados y los comentarios recibidos.
- **Colaborar y promover la visibilidad:** Trabaja en colaboración con los equipos de TI y los usuarios finales para comprender sus necesidades de respaldo. Asegúrate de que los procedimientos y políticas de respaldo sean transparentes y comprensibles para todos los involucrados.
- **Visión Holística:** Considera todos los aspectos de la gestión de backups, desde la planificación y la implementación hasta la monitorización y la recuperación. Asegúrate de que los backups se ajusten a la estrategia general de gestión de servicios de TI de la organización.

- **Mantenerlo simple y práctico:** Diseña y administra tus políticas y procedimientos de respaldo de manera que sean simples y fáciles de seguir. Evita la complejidad innecesaria que pueda dificultar la recuperación de datos.
- **Optimizar y automatizar:** Utiliza herramientas y soluciones de backup automatizadas para optimizar la eficiencia de tus procesos de respaldo. Esto puede ayudar a reducir errores humanos y garantizar la consistencia en las copias de seguridad.

CASOS DE ÉXITO

T-Mobile 2020

T Mobile sufrió una pérdida de datos debido al error de un empleado el cual por accidente eliminó el directorio raíz causando así la completa eliminación de los datos de producción, esto causó interrupción del servicio y fallos en la red de los usuarios. Al tener una buena implementación de backup se lograron recuperar los datos.

Play Station Network 2011

Play Station durante 2011 sufrió un ataque de Ransomware debido a una brecha de seguridad, pero al ser demasiada información no era enviada a los atacantes por lo cual se pudo restaurar la información eliminando la información actual, las consecuencias de este inconveniente fueron la interrupción de servicios, para enmendar su problema Play Station Network regaló 2 juegos de su plataforma.

CASOS DE FRACASO

British Airways 2017

British Airways durante 2017 sufrió un accidente debido a una falla en la línea eléctrica lo cual causó una eliminación en la información principal y el backup se encontraba realizándose en ese momento quedando comprometido también, como resultado no se pudo recuperar la información.

Gitlab 2017

Gitlab en 2017 debido a un error por parte de uno de los empleados el cual eliminó el directorio raíz borrando así toda la información, como ultimo recurso les quedaba recurrir a la copia de seguridad, pero para su mala suerte el equipo encargado del backup no había verificado que el backup se haya realizado correctamente, por lo cual se perdieron todos los datos.

CASO DE ÉXITO Y FRACASO

Pixar 1999

Durante la producción de Toy Story 2 una de las encargadas de modelado 3D de personajes se encontraba en proceso de embarazo el equipo le preparó una computadora con la copia entera del proyecto para que pudiera trabajar desde su casa, un día de producción uno de los empleados ejecutó un comando en la terminal lo cual hizo que borrara todos los archivos del proyecto, en ese momento no se tenia el backup actualizado y la única copia con el trabajo más próximo a la fecha era el de la compañera que estaba embarazada, en ese momento la computadora que le prepararon paso a valer mil millones de dólares y luego de recuperar la información se continuó con normalidad, decimos que es un caso de éxito porque se logro recuperar la información pero de fracaso porque no estaban bien implementado el respaldo de información.

Implementación de respaldo de la información

se refiere al proceso de poner en práctica una estrategia de copias de seguridad (backups) para proteger y respaldar los datos críticos de una organización. Implica la configuración y ejecución de los procedimientos y sistemas necesarios para asegurar que los datos se copien, almacenen y puedan recuperarse de manera eficiente y segura en caso de pérdida, corrupción, fallos del sistema, ataques cibernéticos u otros incidentes.

A continuación, se detallan algunos aspectos clave de la implementación de respaldo de la información:

1. **Selección de tecnologías y herramientas**: Esto implica elegir el hardware y el software adecuados para realizar copias de seguridad. Esto puede incluir la elección de dispositivos de almacenamiento como discos duros externos, cintas magnéticas, servidores de almacenamiento en red (NAS) o soluciones de copia de seguridad en la nube. También se seleccionan aplicaciones y software de copia de seguridad que se ajusten a las necesidades de la organización.

2. **Políticas de respaldo**: Se definen políticas específicas que establecen qué datos se deben respaldar, con qué frecuencia se deben realizar las copias de seguridad y cuánto tiempo se deben retener. Estas políticas deben estar alineadas con las necesidades de la organización y las regulaciones aplicables.

3. **Programación de copias de seguridad**: Se establece un horario para la realización de las copias de seguridad. Esto puede incluir copias de seguridad diarias, semanales o mensuales, según los requisitos de la organización y la importancia de los datos.

4. **Seguridad de datos**: Se implementan medidas de seguridad para proteger los datos de copia de seguridad contra el acceso no autorizado. Esto puede incluir la encriptación de datos de copia de seguridad y el control de acceso a los sistemas de copias de seguridad.

5. **Pruebas y verificación**: Se realizan pruebas periódicas para asegurarse de que las copias de seguridad se estén realizando correctamente y que los datos se puedan recuperar según lo planeado en caso de necesidad.

6. **Monitoreo y gestión**: Se establecen procedimientos para supervisar el estado de las copias de seguridad, detectar problemas y tomar medidas correctivas si es necesario. Esto puede incluir la supervisión de registros de copias de seguridad y la implementación de alertas.

7. **Capacitación del personal**: Se capacita al personal responsable de la gestión de las copias de seguridad para que comprendan los procedimientos y las políticas, y puedan responder adecuadamente en caso de incidentes.

Enlaces de los simuladores:

Simulador 1

http://lasdpc.icmc.usp.br/~ssc640/grad/ec2015/backup_simulator/

Simulador 2

https://pbs.proxmox.com/docs/prune-simulator/

Simulador 3

https://calculator.veeam.com/vbr/