UT 5: Copias de seguridad e imágenes de respaldo

2ºSMR – Seguridad Informática

Copias de Seguridad

Necesario hacer copias de seguridad de datos por varios motivos:

- Para prevenir amenazas lógicas (virus, perdidas de información, robos…)
- Desastres de diversa índole (incendios, inundaciones…).
- Fallos en hardware/software
- Errores humanos: borrados, formateos "accidentales"
- LOPD

Ya hemos visto que ni RAID 1 ni el RAID 5 son seguros, ya que protegen ante el fallo de uno de los discos, pero no, si fallan los dos.

Las copias de seguridad garantizan:

- La integridad y disponibilidad de la información
- Son útiles para restaurar sistemas operativos, datos de configuración de redes, software de aplicaciones, datos de aplicaciones…
- Son un mecanismo de seguridad pasiva

Componentes Copias de Seguridad

Al realizar copia seguridad deberá determinarse la información a copiar

- **Copia de los datos** → copia de seguridad de los datos del usuario o empresa que están almacenados en un ordenador.
- **Imagen del Sistema** → copia de seguridad de los programas (sistema operativo y aplicaciones) que están instalados en un ordenador.
  - La imagen de un sistema es un volcado del contenido del disco duro con todo: ejecutables, datos del sistema operativo, todas las aplicaciones instaladas.
    - Generalmente se comprime en un único fichero que ocupan varios gigabytes
    - El fichero suele estar cifrado y se almacena lejos del sistema original.
    - La imagen no es un método adecuado para hacer copias de seguridad en la empresa

Dispositivo en que se realizará la copia:

- Discos ópticos
- Discos duros (soportes SSD, servidores NAS, red SAN)
- Memorias Flash
- Cabinas de cintas
- Servidores en la nube: Cloud Storage

Tipos Copias Seguridad

En función del **instante** en que se realiza la copia, hay dos tipos de copia:

- **Offline (en frío):** Implica que en los datos de los que se realiza la copia no están en un periodo de actividad, es decir no existen usuarios o procesos accediendo a los mismos. Es el método más seguro. Problema: muchos sistemas actuales no se pueden parar (24x7)

- **Online (en caliente):** La copia de seguridad se realiza mientras los datos sobre los que se realiza la copia está en un periodo de actividad, es decir pueden existir usuarios o procesos accediendo al mismo. Software de copia de seguridad deberá garantizar (bloqueando los archivos) la integridad de los datos copiados

Tipos Copias Seguridad

En función de la **cantidad información copiada** hay tres tipos de copia:

- **Completa:** incluye toda la información identificada. Si es una unidad de disco, todos los archivos y carpetas que contiene; si es una base de datos, la exportación de todas sus tablas.

- **Diferencial:** incluye toda la información que ha cambiado desde la última vez que se hizo una copia de seguridad completa.

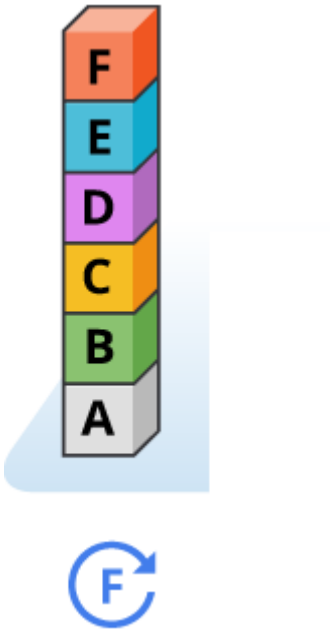
- **Incremental:** incluye toda la información que ha cambiado desde la última copia de seguridad, sea completa o incremental.

En una empresa mediana es habitual el esquema de diez cintas:

- Una para un backup completo (los viernes).
- Cuatro para un backup parcial diario (diferencial o incremental) de lunes a jueves.
- Cinco para backups completos anteriores: quincenal, mensual, trimestral, semestral y anual.

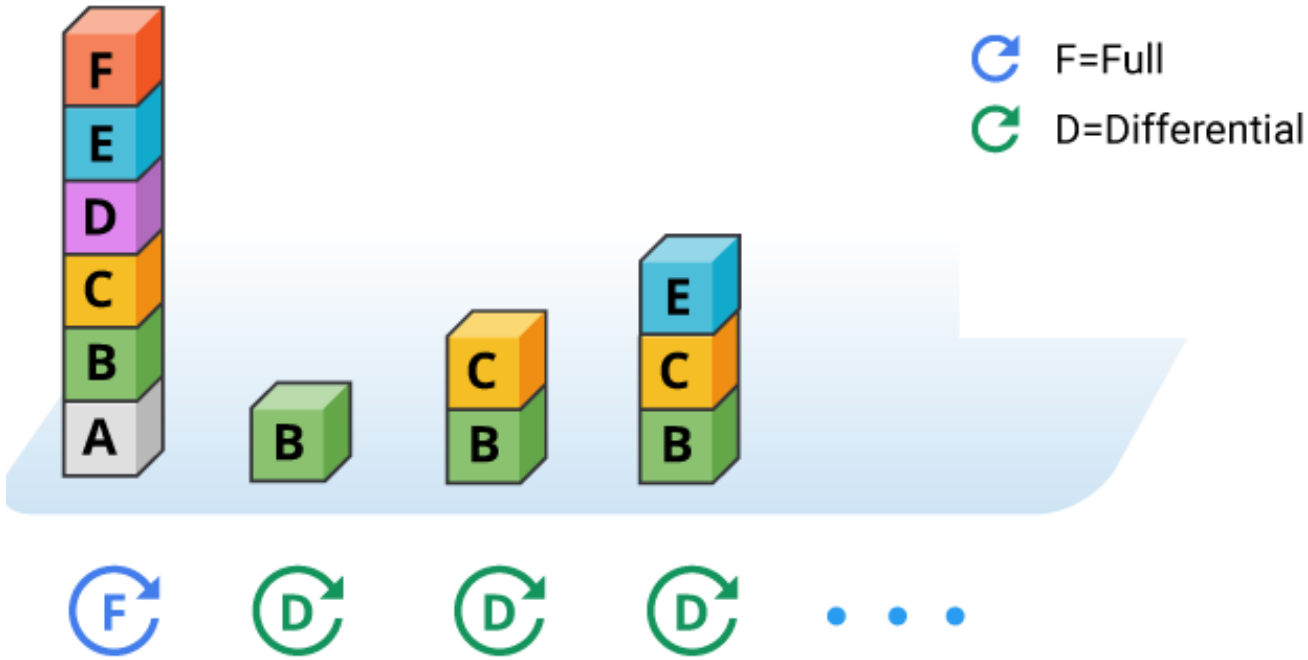
Tipos Copias Seguridad

Copia Completa



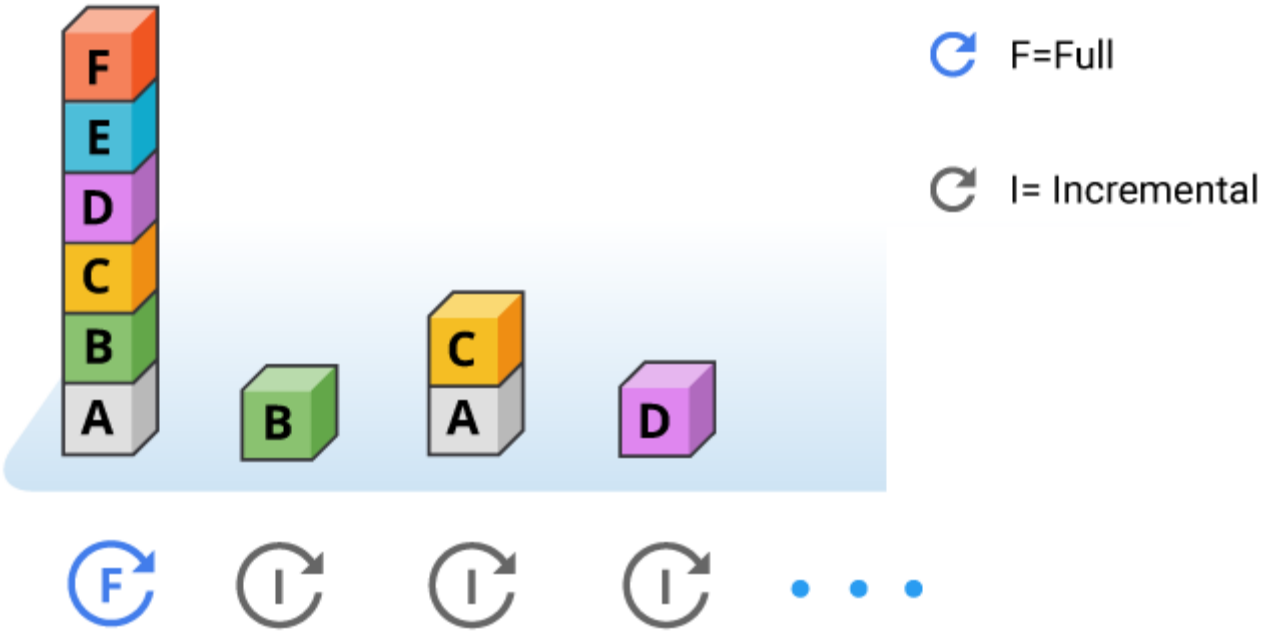
Tipos Copias Seguridad

Copia Diferencial



Tipos Copias Seguridad

Copia Incremental



Tipos Copias Seguridad

¿Diferencial o Incremental?

- Si hay poca actividad diaria, se puede permitir el diferencial, porque aporta la ventaja de que cada cinta diaria tiene toda la información necesaria para recuperar ese día (en el incremental, si perdemos la cinta de un día, puede que tenga ficheros que no estén en las cintas siguientes).

- Pero si hay mucha actividad, estamos de nuevo ante el problema de mantener la consistencia de la copia.

Tipos Copias Seguridad

Método	Espacio Almacenamiento	Velocidad Copia	Restauración	Copia Recomendada
Completo	Máximo	Muy lento	Muy simple	Pocos datos a copiar
Completo + Incremental	Mínimo	Rápido	Compleja	Muchos datos que cambian frecuentemente
Completo + Diferencial	Intermedio	Lento	Sencilla	Datos con velocidad cambio moderada

Tipos Copias Seguridad

En función de la **ubicación de la copia** hay dos tipos:

- **On-site:** la copia se guarda físicamente cerca de la información original.

- **Off-site:** la copia se guarda físicamente lejos de la información original. Garantiza que hay una copia fuera de las dependencias donde está la información original y que puede restaurar la información en caso de desastre total.

Tipos Copias Seguridad

En función de la **intención de la copia** hay tres tipos:

- **Backup:** llamamos así a las copias de los archivos realizadas periódicamente, con intención de poder deshacer una posible pérdida de integridad en los datos originales, y revertir los datos a como estaban en un momento anterior en el tiempo.

- **Archiving:** copiar los archivos para almacenar por un largo período de tiempo, sea por cuestiones legales como la contabilidad o por motivo de espacio, para retirar información antigua. Si se necesitan, se pueden restaurar.

- **Disaster recovery**: recuperar desde una situación en la que el sistema original está fuera de servicio. Se requiere entonces que la copia de seguridad permita restaurar totalmente los datos del sistema.

Tipos Copias Seguridad

En función de la **intención de la copia** hay tres tipos:

- **Backup:** llamamos así a las copias de los archivos realizadas periódicamente, con intención de poder deshacer una posible pérdida de integridad en los datos originales, y revertir los datos a como estaban en un momento anterior en el tiempo.

- **Archiving:** copiar los archivos para almacenar por un largo período de tiempo, sea por cuestiones legales como la contabilidad o por motivo de espacio, para retirar información antigua. Si se necesitan, se pueden restaurar.

- **Disaster recovery**: recuperar desde una situación en la que el sistema original está fuera de servicio. Se requiere entonces que la copia de seguridad permita restaurar totalmente los datos del sistema.

Encriptación Copias Seguridad

Es importante utilizar sistemas de cifrado robustos si vamos a copiar o almacenar información sensible o privada, para impedir su lectura a otras personas.

El cifrado es un método por el que convertimos en ilegible una determinada información o mensaje para que sólo acceda a ella la persona autorizada haciendo uso de una contraseña, código o PIN necesario para descifrarlo.

Software de copia seguridad incorpora algoritmos de crifrado: AES, 3DES …

Ventajas uso cifrado:

- Mayor seguridad

Desventajas uso cifrado:

- Ralentiza los procesos de copia/restauración

Encriptación Copias Seguridad

Los procesos de cifrado pueden realizarse principalmente sobre dos ámbitos de contenido:

- El **dispositivo de almacenamiento**: se cifra todo un medio de almacenamiento, como un disco duro. No será posible acceder a ninguna información contenida en él sin conocer el sistema de descifrado. Este método nos puede llevar mucho tiempo si el número de archivos a cifrar es elevado. También veremos reducida la velocidad de funcionamiento del disco duro, por lo que solo será una opción recomendable si utilizamos dicho disco esencialmente como dispositivo de copia de seguridad.

- Los **archivos y carpetas**: podemos proteger una parte de la información contenida en un medio de almacenamiento, sea un disco duro o la nube. Solo aquellas carpetas o archivos que escojamos para el cifrado serán ilegibles para quien no conozca la clave, y el resto de información será accesible normalmente.

Comprensión Copias Seguridad

Las copias de seguridad ocupan una gran cantidad de espacio, por lo que puede ser costoso al momento de invertir en el medio a utilizar.

Para reducir el espacio necesario la copias de seguridad pueden ser comprimidas. Existen varias formas de hacerlo, pero una de la mas práctica es utilizar directamente programas con soporte para compresión.

Software copia seguridad lleva herramientas incorporadas para reducir el tamaño de los ficheros generados.

Ventajas:

- Reduce el tamaño del backup.

Desventajas:

- El proceso de compresión/descomprensión reduce la velocidad copia/restauración del backup.

Políticas Copias Seguridad

Conjunto de reglas, criterios y procedimientos que deben seguir todos los usuarios de los sistemas para proveer métodos de recuperación de la información.

Las políticas deben definir al menos:

- Tipos de copias
- Frecuencia con la que se realizan las copias de seguridad.
- Franja horaria en la que se hace la copia
- Soporte donde deben realizarse
- Ubicación de la copia o de los centros de respaldo
- Persona o departamento responsable

Políticas Copias Seguridad

Aplicar sentido común a la hora de diseñar unas políticas de respaldo con los medios disponibles. Reglas básicas:

- **Rotación** - No usar el mismo medio para dos copias que vayan seguidas. Si el sistema falla durante el proceso de back-up, se perderán los datos originales y los del back-up, y no habrá otra copia para restaurar. Es necesario disponer de varios medios, de igual tecnología o distinta, e ir rotando las copias sucesivas entre ellos.

- **Copias off-site** - Siempre hay que asegurarse de guardar un backup, de no más de una semana de antigüedad, fuera del sitio donde está su sistema. Si las instalaciones de su organización sufren un incidente global, la copia off-site permitirá la recuperación del desastre.

- **Back-up diario** - Realizar un back-up cada día toma poco tiempo. La mayoría de los datos se vuelven obsoletos rápidamente.

Políticas Copias Seguridad

Una política de copia de seguridad debe cumplir los siguientes requisitos:

- Identificar los datos que requieren ser preservados. Son aquellos cuya pérdida afectaría a la continuidad del negocio.

- Establecer la frecuencia con la que se van a realizar los procesos de copia. Esta frecuencia influye en la cantidad de información que se puede perder con respecto a la fuente original. Este parámetro es de suma importancia y requiere de un análisis exhaustivo.

- Disponer el almacén físico para las copias. Este almacén se determina en función de la seguridad que requiere la información entre almacenes en el mismo edificio o remotos en edificios externos.

Políticas Copias Seguridad

Una política de copia de seguridad debe cumplir los siguientes requisitos:

- Buscar una probabilidad de error mínima, asegurándose de que los datos son copiados íntegramente del original y en unos soportes fiables y en buen estado. No se deben utilizar soportes que estén cerca de cumplir su vida útil para evitar que fallen cuando vaya a recuperarse la información que contienen.

- Controlar los soportes que contienen las copias, guardándolos en un lugar seguro y restringiendo su acceso sólo a las personas autorizadas.

Políticas Copias Seguridad

Una política de copia de seguridad debe cumplir los siguientes requisitos:

- Planificar la restauración de las copias:
  - Formando a los técnicos encargados de realizarlas
  - Disponiendo de soportes para restaurar la copia, diferentes de los de producción
  - Estableciendo los medios para disponer de dicha copia en el menor tiempo posible
- Probar el sistema de forma exhaustiva para comprobar su correcta planificación y la eficacia de los medios dispuestos.

Software Copias Seguridad

Diferentes tipo software:

- Software genérico para realizar copias de seguridad

  - ✓ Software para crear imágenes
  - ✓ Software para sincronizar directorios
  - ✓ Software para copiar cualquier tipo de fichero

- Software específico para determinados sistemas/servidores

  - ✓ Software para copias sistemas
  - ✓ Software para copias bases datos
  - ✓ Software para servidores correo …

Software Copias Seguridad

Diferentes tipo software:

- Software genérico para realizar copias de seguridad

  - ✓ Software para crear imágenes
  - ✓ Software para sincronizar directorios
  - ✓ Software para copiar cualquier tipo de fichero

- Software específico para determinados sistemas/servidores

  - ✓ Software para copias sistemas
  - ✓ Software para copias bases datos
  - ✓ Software para servidores correo …

Creación y recuperación. LiveCD.

- Existen varias herramientas en los distintos sistemas operativos para crear y recuperar imágenes (Norton Ghost, Acronis True Image), pero tienen el inconveniente de ser formatos propietarios, de forma que para recuperarlos se necesita el mismo programa (incluso la misma versión).

- Una solución genérica, disponible para cualquier plataforma hardware habitual. Consiste en la utilización de LiveCD

Congelación

- En algunos entornos interesa dar una configuración estable al ordenador y después impedir cualquier cambio, venga del usuario o de algún intruso (virus, troyano, etc). El ejemplo más típicos son las salas de cibercafé ; cuando se acaba el tiempo de alquiler del puesto, hay que borrar cualquier rastro para que el siguiente cliente encuentre el ordenador limpio.
- Esta es la misión del software de congelación; una vez instalado toma nota de cómo está el sistema (snapshot) y, desde ese instante, cualquier cambio que ocurra en el sistema podrá ser anulado cuando el administrador la solicite.
- Los sistemas Windows incluyen la funcionalidad de crear puntos de restauración, pero la funcionalidad es limitada, porque solo preocupan los programas no los datos.
- Las herramientas de congelación suelen mantener varios snapshot, para facilitar volver a otras situaciones pasadas, aunque el espacio ocupado en el disco puede llegar a ser un problema..
- En algunos programas hay que descongelar, instalar y volver a congelar. La solución de congelación tiene una aplicabilidad bastante limitada porque es difícil administrar los diferentes snapshot.