Seguridad Informática - 2º SMR
Tema 3: Seguridad pasiva. Copias de seguridad

3.1. Introducción

Hoy en día guardamos gran cantidad de información en nuestros equipos informáticos.

Por acción de virus, de usuarios malintencionados, por fallos del hardware, o simplemente por accidente la información almacenada en nuestro equipo puede resultar dañada o desaparecer. Las copias de seguridad son réplicas de datos que nos permiten recuperar la información original en caso de ser necesaria.

La copia de seguridad es útil por varias razones:

- Para restaurar un ordenador a un estado operacional después de un desastre (copias de seguridad del sistema)
- Para restaurar un pequeño número de ficheros después de que hayan sido borrados o dañados (copias de seguridad de datos).

Las copias de seguridad garantizan dos de los objetivos de la seguridad informática: la integridad y la disponibilidad de la información.

Estas copias de seguridad se podrán hacer en multitud de soportes de almacenamiento como cintas, CD, DVD, discos duros externos o en dispositivos de almacenamiento remoto (NAS, SAN).

3.2 Tipos de copias de seguridad

Dependiendo de la cantidad de ficheros que se almacenen en la copia podemos distinguir tres clases de copias de seguridad:

- **Completa, total o íntegra**: como su nombre indica, realiza una copia de todos los ficheros y directorios seleccionados.
- **Incremental**: Copia solo los archivos que se hayan modificado desde la última copia de seguridad, ya sea incremental, diferencial o completa. Por ejemplo si hacemos una copia de seguridad completa todos los viernes a las 12 de la noche y copias incrementales todos los días a la misma hora, cada copia incremental sólo guardará los datos creados o modificados durante ese día. Para restaurar el sistema de ficheros tendríamos que recurrir a la última copia completa + todas las incrementales realizadas hasta la fecha del fallo.
- **Diferencial**: copia solo los ficheros que se hayan creado o modificado desde la última copia de seguridad completa. Copia más ficheros que la incremental, por lo tanto, tarda más tiempo en realizarse y ocupa más espacio, pero a la hora de recuperar sólo nos hará falta la última completa + la última diferencial, con lo que la restauración será más rápida.

3.2.1 Recomendación sobre el tipo de copia a efectuar

- Si el volumen de datos de nuestra copia de seguridad no es muy elevado (unos 10 GB), lo más práctico es realizar **siempre copias totales** ya que en caso de desastre, tan solo debemos recuperar la última copia.
- Si el volumen de datos de nuestra copia de seguridad es mayor (unos 100 GB) pero el volumen de datos que se modifican no es elevado (sobre 10 GB), lo más práctico es realizar una primera copia total y posteriormente realizar **siempre copias diferenciales**. Así, en caso de desastre, tan solo debemos recuperar la copia total y la última diferencial. Periódicamente debemos realizar una copia total y así empezar de nuevo.
- Si el volumen de datos de nuestra copia de seguridad es muy elevado (mayor de 100 GB) y el volumen de datos que se modifican también lo es, las copias diferenciales ocuparán mucho espacio, por lo tanto en este caso lo más práctico será realizar una primera copia total y posteriormente realizar **siempre copias incrementales** ya que son las que menos espacio ocupan. El problema es que en caso de desastre debemos recuperar la última copia total y todas las incrementales realizadas desde que se hizo la última copia total. En estos casos, conviene hacer copias totales más a menudo para no tener que mantener un número muy elevado de copias incrementales.

En grandes compañías donde la realización de copias de seguridad está perfectamente planificada, se suelen utilizar sistemas mixtos. Por ejemplo en un caso típico se realizarían las siguientes tareas:

- Todos los días 1 de cada mes, a las 23:00 horas: copia de seguridad total
- Todos los viernes a las 23:00 horas: copia de seguridad diferencial desde la copia de día 1
- Todos los días (excepto los viernes y el día 1) a las 23:00 horas: copia de seguridad incremental desde la copia del día anterior

Con esta planificación nos aseguramos disponer de copia de seguridad diaria. En caso de desastre deberíamos recuperar la copia total, la última diferencial y todas las incrementales desde la última diferencial.

3.3 Copias de seguridad de los datos

Estas copias de seguridad como su nombre indican son copias de la información, y se almacenan en un lugar diferente al original. Debemos recordar que las copias de datos no se deben guardar en la misma ubicación que el original o muy cerca, para evitar perder todos los datos de forma definitiva en caso de incendio o inundación.

Otro de los problemas clásicos de las copias de datos es la mala etiquetación de las copias. Debemos ser exhaustivos cuando etiquetamos copias de respaldo. Se recomienda etiquetarlas mediante códigos impresos, códigos cuyo significado sea conocido sólo por los técnicos encargados de las copias.

Debemos hacer copia de aquellos datos que sean difíciles o imposibles de reemplazar.

3.3.1 Soportes para las copias de seguridad

- **Discos**: CD o DVD regrabables. Son baratos pero ofrecen un número muy limitado de escrituras.

- **Cinta**: Es uno de los soportes más antiguos pero se siguen utilizando hoy en día. Ofrecen un gran volumen de almacenamiento y una alta fiabilidad. El inconveniente es que es más lenta que cualquier otro dispositivo de acceso aleatorio ya que las cintas sólo tienen acceso secuencial.
- **Memorias de tipo flash** (pendrive, microSD, compactFlash y similares) no son muy recomendables ya que se suelen estropear con facilidad y tienen una capacidad bastante escasa.
- **Discos duros** basados en la grabación de datos por la imantación del soporte. Han evolucionado rápidamente proporcionando actualmente una gran capacidad, rapidez de acceso y fiabilidad.
- **Soportes SSD**. Empiezan a hacerse copias en estos soportes aunque el precio es bastante alto y su capacidad limitada, pero tiene grandes ventajas frente a los discos convencionales porque no tienen elementos mecánicos lo que los hace mucho más fiables. El rendimiento es mayor y el tiempo de acceso es bastante inferior al de los discos duros tradicionales.

> **Ejercicios propuestos**
>
> **3.3.1.** Realizar una tabla comparativa de los distintos soportes con su capacidad máxima actual y su precio medio por GB.
>
> **3.3.2.** Elege la política de copias (frecuencia con la que se realizará, tipo de copia y soporte usado) más adecuada para los siguientes casos:
>
> - Casa particular con 3 ordenadores
> - Empresa pequeña con un servidor con pocos datos y pocos cambios diarios.
> - Empresa mediana con un servidor con pocos datos y muchos cambios diarios.
> - Empresa grande con varios servidores con muchos datos y muchos cambios diarios.

3.4 Copias de seguridad del S.O.

Como los datos, el sistema operativo puede fallar o funcionar de forma no correcta. Igual que hacemos copias de seguridad de los datos, podemos hacer copias del sistema operativo para restablecer su funcionamiento correcto lo más rápidamente posible.

3.4.1 Puntos de restauración del sistema

En el caso de los sistemas operativos de la familia Microsoft podemos usar puntos de restauración para intentar devolver al estado al que se encontraba el sistema antes de realizar la acción que produjo el fallo. La restauración permite devolver los archivos del sistema a un momento anterior.

En caso de tener activada la protección automática del sistema, este creará los puntos de restauración todos los días y justo antes de detectar el comienzo de la realización de cambios en el equipo.

En caso de no tener activada la protección automática debemos crear los puntos de restauración manualmente.

Cuando creamos puntos de restauración, se guarda una “instantánea” del estado del sistema.

La restauración a un punto anterior solo afecta a la configuración de los ficheros del sistema, programas, ficheros ejecutables y el registro, y no afecta a los documentos personales.

3.4.2 Inicio en la última configuración válida conocida

Hay ocasiones en las que la restauración del sistema no puede hacerse, bien porque no se han creado puntos de restauración o bien porque el sistema se encuentra demasiado degradado. En este caso existe otra posibilidad que es: si la última vez que se inició el sistema se inicio de forma correcta podemos utilizar la opción de inicio en la última configuración válida conocida.

Cada vez que apagamos el ordenador y el sistema operativo Windows se cierra correctamente, la configuración del sistema se guarda en el registro.

3.4.3 Restaurar el sistema desde el símbolo del sistema

En el caso de que la última configuración válida no hubiese solucionado el problema, podemos intentar restaurar el sistema desde el símbolo del sistema. Escribiremos rstrui.exe una vez hayamos arrancado en modo seguro.

3.4.4 Reparación de inicio

La reparación de inicio es una herramienta de recuperación de Windows que permite solucionar algunos problemas como la falta de archivos del sistema o bien archivos corruptos del mismo.

> **Ejercicios propuestos**
>
> **3.4.1.** Restaura un “punto de restauración” creado en un Windows VM. Toma capturas de pantalla de cómo lo has hecho. Una vez restaurado, expica si tienes los mismos documentos y los mismos programas que antes de la restauración. ¿Qué ha cambiado?

3.5 Creación de imágenes del sistema

Hacer copias de seguridad de los datos ya hemos visto que es muy importante. Hacer copias del sistema aunque no tan importante, sí que puede ahorrar bastante tiempo en caso de tener que reinstalar.

Para hacer copias de seguridad del sistema existen aplicaciones que realizan las llamadas imágenes.

Realizan una copia completa del sistema tal como está de forma que en caso de fallo se puede restaurar el sistema en muy poco tiempo y seguir trabajando.

3.6 Políticas de copias de seguridad

Las políticas de copias de seguridad deben definir:

1. Determinar las personas responsables de las copias y restauraciones.
2. Los datos que se copiarán, analizando cuales son los más importantes y difíciles de recuperar.
3. El tipo de copia, que dependerá del volumen de datos que se manejan.

4. Periodicidad de la misma, teniendo en cuenta cuanta información estamos dispuestos a perder.
5. Soporte para su realización.
6. Ubicación de los centros de respaldo.
7. La ventana de backup: franja horaria donde se realizarán las copias.

3.6.1 Centros de respaldo

Los centros de respaldo son las ubicaciones donde se guardan las copias de seguridad.

En empresas pequeñas suelen encontrarse muy cerca de la ubicación original de los datos, para comodidad de los técnicos y por cuestiones de espacio.

Pero en grandes empresas, las copias se guardan en estancias los suficientemente alejadas como para que no se vean afectadas por el mismo percance que los datos originales.

Estas ubicaciones deben estar protegidas con las mismas medidas que el CPD.

3.6.2 Etiquetado de las copias.

Como ya hemos visto, las copias deben estar bien etiquetadas para poder ser localizadas de forma rápida a la hora de realizar una posible recuperación.

Una etiqueta correcta debe incluir:

1. Identificador de la copia: Cadena alfanumérica que identifique de forma unívoca la copia.
2. Tipo de copia: Completa, diferencial o incremental.
3. Fecha de realización de la copia
4. Contenido: Siempre en clave tanto en la etiqueta como dentro de la copia.
5. Responsable: Técnico que realizó la copia, para posibles consultas posteriores.

3.6.3 Registro de las copias y restauraciones

Igualmente se debe llevar un registro exhaustivo de las copias de seguridad y restauraciones realizadas. Este registro debe incluir al menos:

1. Identificador de la etiqueta de la copia.
2. Soporte donde se ha realizado la copia.
3. Ubicación de la copia. Y por otro lado se debe llevar un registro de las restauraciones realizadas:
4. Fecha de restauración.
5. Incidencia que motivó la restauración.
6. Ubicación del equipo donde se restaura la copia.
7. Técnico que realiza la restauración

3.7 Bibliografía:

- Costas Santos, Jesús Seguridad informática Editorial RA-MA
- Seoane Ruano, César et al. Seguridad informática Editorial McGraw- Hill

- http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m5/copias_de_seguridad.html