Unidad 3:

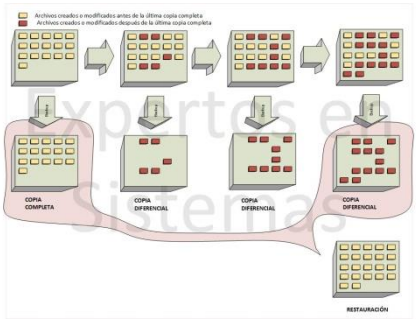
Seguridad pasiva. Recuperación de datos

Índice

1. Tipos de copias de seguridad

En los ordenadores, ya sean particulares o de empresas, se guarda gran cantidad de información, cuya pérdida podría ser un desastre. Es por eso, que tanto unos como otros deben realizar copias de seguridad de la información guardada en los ordenadores. Las copias de seguridad garantizan la integridad y disponibilidad de la información. Estas copias de seguridad se podrán hacer en soportes de almacenamiento como cintas, CD, DVD, en discos duros externos o en dispositivos de almacenamiento remotos.

Hay tres clases de copias de seguridad:



- **Completa**: realiza una copia de todos los archivos y directorios seleccionados. Es la copia que debemos hacer cuando creamos la primera copia de seguridad.
- **Diferencial**: se copian todos los archivos que se han creado o actualizado desde la última copia completa que se ha hecho.
- **Incremental**: se copian los archivos que se han modificado desde la última copia de seguridad completa o diferencial realizada.

2. Regla de copias de seguridad 3, 2, 1

Las copias de seguridad de datos se deben de guardar en un sitio diferente al original y deben de estar perfectamente etiquetadas con códigos que sólo deben de conocer aquellas personas que los manejan. Las copias se deben de guardar una en el mismo centro de trabajo o edificio y otra en un lugar diferente. De esa manera se dificulta el acceso a esta información de los intrusos. Las copias se harán de todos los archivos, ya que la finalidad de la copia de seguridad es poder recuperar los datos en caso de desastre, y en distintos soportesLas cintas se caracterizan por el gran volumen de almacenamiento, pero son más lentas que los discos duros convencionales y el acceso a los datos es secuencial.

Una copia de seguridad 3, 2, 1 es básicamente una estrategia para asegurar la replicación de tus datos de forma eficiente frente a desastres. Básicamente se trata de lo siguiente:

- realizar **3** copias de tus datos,

- almacenar en al menos **2** soportes diferentes
- enviar una de estas copias a **1** lugar físico diferente.

Lo ideal en esta regla es tener como mínimo **3 copias de seguridad** de tus datos. Y si además trabajas con contenido sensible y cuya perdida sería desastrosa, sería recomendable que estas tres copias se hicieran de forma manual o automática cada día o cada semana.

Por probabilidad, tarde o temprano un disco duro que hayamos comprado morirá, bien por viejo, bien por un problema con la corriente o porque nosotros mismos hayamos borrado sin querer los datos. Mientras más copias de archivos tengamos, más difícil, será perderlos, es obvio, claro que lo mejor es que estén en soportes diferentes. Es improbable que nuestro "Mayus Supr" coja las tres copias realizadas de una vez, o que dos o tres discos duros fallen al mismo tiempo.

Pero claro, esto es bastante molesto si lo tenemos que hacer de forma manual, así que hay **programas** como Acronis True Image, EaseUS, iDrive o Paragon que harán estas copias de forma automatizada si así los configuramos.

Una vez que tenemos la forma de hacer las tres copias de seguridad, ahora es turno de **almacenarlas** en dispositivos diferentes, podemos utilizar dos discos duros o dos unidades físicamente distintas en donde almacenar cada copia. Hay que tener cuidado, ya que tener dos particiones no os protege de un fallo en la unidad, o incluso de un formateo para los más despistados.

Y un disco duro tiene un tiempo medio entre fallos (MTTF) de 1 millón de horas, almacenar copias en dos unidades duplica la integridad a 2 millones de horas y así sucesivamente. Pero claro, lo ideal en este caso es evitar tener estas dos o tres unidades conectadas a la misma alimentación o al mismo sistema, ya que podría producirse un fallo en cascada, por ejemplo por una subida de tensión.

En este punto podemos utilizar bastante cantidad de soportes de almacenamiento, como un segundo disco si andamos mal de presupuesto, una unidad flash USB, CD-ROM, o mucho mejor, un NAS o unidades de red, o almacenamiento en la nube.

Dicen que un rayo no cae dos veces en el mismo lugar, aunque siempre hay personas más propensas a la mala suerte. Por ello, lo ideal será que al menos una de las copias de seguridad que hagamos esté ubicada en **un lugar físico diferente**.

No sirve que cojas tu unidad flash y la metas en un cajón de la mesa, ya que posiblemente el rayo que le caiga a tu PC podría afectar también al USB o CD-ROM. Así que lo mejor sería enviar esta tercera copia lejos de nosotros, tan lejos como si estuviese en la nube.

El **almacenamiento en la nube** consiste en servidores de almacenamiento conectados a Internet en los que cada usuario puede acceder desde cualquier lugar con un usuario y contraseña. Esos sistemas tienen detrás un soporte técnico y matrices de discos en RAID que ofrecen las máximas garantías de integridad de datos al usuario.

3. Modos de recuperación frente a pérdidas en el sistema operativo

Al igual que se crean copias de seguridad de los datos, debemos realizar otras copias del sistema operativo. Entre los métodos de recuperación más comunes se hallan:

a) **Restauración**. Podremos intentar restaurar el sistema al estado en el que se encontraba antes de realizar la acción que produjo la avería.

b) **Arranque con la última configuración válida conocida**. Hay veces en la que la restauración del sistema no puede realizarse, bien porque no se hayan creado puntos de restauración o bien porque el sistema se encuentre demasiado degradado. En el caso de que no podamos iniciar Windows, pero sí se haya iniciado correctamente la última vez que se encendió el equipo, podremos utilizar este método.

c) **Restaurar en modo seguro con sólo símbolo del sistema**. Se usa en el caso en el que la última configuración válida no hubiese corregido el mal funcionamiento del sistema operativo.

d) **Reparación de inicio de Windows o recuperación automática del sistema**. Si falla todo lo anterior se usa este otro método. Cuando ejecutamos dicha opción el sistema examina el equipo en busca del problema e intenta corregirlo.

e) **Creación y restauración de imágenes del sistema**. Una imagen del sistema es una copia exacta de una unidad, incluyendo Windows y la configuración del sistema, así como sus programas y archivos. Existen aplicaciones como **Norton Ghost o Acronis True Image,** que hacen esto. Cuando creamos una copia de seguridad o imagen, podemos guardarla en una partición oculta del mismo disco donde tengamos instalado el sistema, de modo que si más tarde necesitamos su restauración, la haremos utilizando una utilidad que **Acronis True Image** instalará en nuestro disco.

4. Copia de seguridad del registro

El Registro de Windows es una base de datos que contiene información del hardware, de las aplicaciones que tenemos instaladas e información de las cuentas.
Habitualmente no es necesario que toquemos el Registro, ya que son las aplicaciones las que suelen introducir los cambios directamente en él. Se aconseja que siempre que se vaya a tocar el Registro se realice antes una copia de seguridad. La palabra clave que hay que escribir en el editor del Registro es **regedit**.

5. Políticas de copias de seguridad

Las políticas de copias de seguridad deben definir el **tipo de copias** y la **periodicidad** de las mismas, así como los **soportes** en las que se deben realizar y las **ubicaciones** de

los centros de respaldo. Los centros de respaldo son las ubicaciones donde se guardan las copias de seguridad. Al realizar copias de seguridad y proceder a su **etiquetado**, una etiqueta correcta debería incluir la siguiente información:

- **Identificador de copia**. Mediante esta cadena alfanumérica identificamos de manera unívoca cada una de las copias de seguridad realizadas.
- **Tipo de copia**. Se debe de decir si la copia es incremental, diferencial o completa.
- **Fecha** en la que se realizó la copia.
- **Contenido**. Siempre se incluirá el contenido en clave que almacena la copia de seguridad. En caso de querer recuperar un determinado archivo lo buscaremos sin necesidad de estar cargando cada una de las copias en el equipo.
- **Responsable**. Debe figurar el técnico que realizó la copia de seguridad para poder pedirle que facilite las consultas o las peticiones de actualización y restauración de la misma.

Al igual que debemos etiquetar correctamente las copias de seguridad, se debe llevar un **registro** exhaustivo de las mismas y de las restauraciones realizadas.

Un **posible diseño** de una hoja de registro es el siguiente, que, además de la información que se almacenaba en la etiqueta que adjuntamos al soporte, deberá incluir los siguientes campos:

- **Identificador de la etiqueta**. Es un código que se incluye en la etiqueta para poder localizar de manera rápida la copia de seguridad.
- **Tipo de soporte**. Especificar si la copia se ha realizado en una cinta, disco duro, unidad USB, la nube…
- **Ubicación**. Dependiendo del número de copias de seguridad y de la importancia de las mismas estarán ubicadas en unos u otros lugares.

Se deberán registrar las restauraciones realizadas y los motivos que han ocasionado dicha recuperación. En las hojas de **registro de las restauraciones** se deben incluir los siguientes campos:

- **Fecha de restauración** en la que se realizó la recuperación de la copia.
- **Incidencia** que ha motivado la restauración. Decir la causa que ocasiona la pérdida de información.
- **Ubicación**. Decir el equipo en el que se realiza la restauración de la información perdida.
- **Técnico**. Saber quién es el **responsable** que lleva a cabo la actuación.

Toda política de copias de seguridad debe contemplar los siguientes puntos:

- Determinar la **persona o personas responsables** encargadas de realizar y mantener las copias de seguridad.

- Debemos analizar los **datos** susceptibles de ser salvaguardados en copias de seguridad.

- Debemos determinar el **tipo de copia** a realizar en función de los datos a salvaguardar y de la periodicidad con la que se modifican.

- Debemos determinar la **frecuencia** con la que se realizarán las copias de seguridad.

- Debemos determinar la **ventana de backup** teniendo en cuenta la duración que cada tipo de copia consumirá.

- Debemos determinar el tipo de **soporte** en el que se realizarán las copias de seguridad.

- Debemos determinar la **ubicación** de las copias de seguridad.

Tareas

En todas las tareas se tendrá que justificar la realización de las mismas, realizando capturas de pantalla y explicando los pasos desarrollados siempre que sea necesario.

1º Busca un programa gratuito para realizar copias de seguridad. Debes de justificar tu elección. Lo más normal es que elijas el que consideras mejor, así que tendrás que estar seguro de tu elección.

2º Realiza un estudio de la forma en la que se puede realizar una copia del registro de Windows y realiza una copia del registro.

3º Estudia cómo realizar una copia de seguridad en Linux y realízala.

4º Otra posibilidad en cuanto a la realización de copias de seguridad es la realización de un clonado del sistema con Clonezilla busca información de este programa y sus características.

5º Otra opción cuando instalamos un equipo en Windows es tener la posibilidad de "congelarlo". Estudia en qué consiste y realiza el "congelado" de tu equipo.

6º Busca información de lo que es la "ventana de backup". Explica en qué consiste.

7º Vamos a realizar una copia de seguridad de la siguiente forma:

a. Tenemos 50 archivos llamados a1, a2, …, a50
b. El día 1 se realiza una copia de seguridad completa
c. El día 2 se realizan cambios en los ficheros desde el a1 hasta el a20 y se crean los ficheros a51 y a52
d. El día 3 se realizan cambios a los ficheros desde el a1 hasta el a22 y se crea el fichero a53
e. El día 4 se realiza una copia de seguridad completa en un disco llamado EXTERNO1

f. El día 5 se realiza una modificación en los ficheros a51 y a52 y se crea el fichero a54
g. El día 6 se realiza una copia de seguridad diferencial en EXTERNO2
h. El día 7 se realizan cambios en los ficheros desde a1 hasta a10 y se crea el fichero a54
i. El día 8 se crea una copia de seguridad incremental en EXTERNO3
j. El día 9 se crea una copia diferencial en EXTERNO4
k. El día 10 se realizan cambios en el fichero a50 y se crea el fichero a55
l. El día 11 se realiza una copia de seguridad incremental en EXTERNO5 y una diferencial en EXTERNO6

Completa el contenido de estos discos duros externos y al día en el que corresponde la copia, como en el ejemplo:

EXTERNO1	EXTERNO2	EXTERNO3	EXTERNO4	EXTERNO5	EXTERNO6
A1…a50 (día 1)					