

Guía de Backups

O

Copias de Seguridad

1. Introducción

Esta guía pretende explicar por qué la realización de un backup es una operación necesaria y muy útil que todos debemos acostumbrarnos a realizar cada cierto periodo. Con esta guía pretendemos mostrar cómo realizar una copia de seguridad de la información en el sistema operativo Windows, y algunos consejos a fin de poder realizar su copia de manera correcta y sin inconvenientes.

2. Backups

2.1. Definición: En informática, realizar una copia de seguridad o Backup (en inglés) es la operación que consiste en duplicar y asegurar datos e información contenida en un sistema informático.

2.2. Objetivos Las copias de seguridad son útiles principalmente para dos cosas: La primera y más evidente es que permite restaurar un sistema informático y retornarlo a un estado anterior funcional (un disco duro, una memoria USB, etc.). Al restaurar sistemas informáticos completos, se involucra el sistema operativo, ya que este se realiza a través de programas de restauración del sistema; en algunas ocasiones esto es bastante complejo, por lo cual no vamos a entrar en detalles sobre este procedimiento. La segunda, la cual también se puede incluir en la primera, es facilitar la restauración de una parte del sistema informático (una carpeta, un archivo, una base de datos, etc.). Este procedimiento es mucho más sencillo, y vamos a detallarlo a continuación

3. Como Realizar un Backup o Copia de Seguridad

La técnica más usada para realizar backups es copiar simplemente los archivos que queremos guardar a otro dispositivo de almacenamiento ya sea una memoria, CD-ROM, DVD, etc. Cuando uno realiza esta copia, lo importante es que los archivos que vaya a copiar, no se estén usando a fin que no genere errores al realizar la copia.

El procedimiento no tiene ninguna dificultad simplemente seleccionamos los archivos que queremos copiar y los pasamos al dispositivo que tengamos; al copiar información a un CD o DVD utilizamos como tal el sistema operativo o también programas que nos ayudan a realizarlo como Nero, Roxio, etc. (el funcionamiento de estos programas no es objetivo de esta guía).

Es muy importante tener en cuenta la periodicidad con que se realiza la copia de seguridad, esto depende mucho del manejo de la información en cada dependencia, ya que hay información que se actualiza o se agrega o elimina, muy seguido o también su actualización se realiza esporádicamente. Hay que tener en cuenta esto ya que la copia debe estar lo más actualizada posible, si por ejemplo la información se actualiza diariamente, es bueno tener el hábito de hacer la copia a diario o dependiendo de la actualización sea semanal, quincenal, mensual, etc. Otra cosa importante es clasificar la información, esto se hace para que realizar la copia de seguridad no sea un proceso largo y tedioso por la cantidad de información que se está

copiando; es necesario hacer una clasificación de la información en donde por un lado tenemos la información que manejamos seguido, esta información debe ser liviana a fin de poder realizar copia de manera rápida; y por otro lado tenemos la información histórica en donde es mucho más robusta y pesada, pero esta información no se modifica periódicamente sino de manera esporádica; de esta manera podemos hacer un backup diario o semanal de la información liviana o la que trabajamos a diario y podemos estipular de manera semestral o anual un backup de toda la información histórica junto con la actual y así tener un repositorio de información organizado y efectivo. También es importante en la clasificación tener los archivos y documentos que son de la dependencia, y son de importancia para la Facultad; la información personal como son los archivos personales, música y demás, deben estar aparte y cada persona tiene su responsabilidad por dicha información, pero es bueno tener claro la diferencia entre la información laboral y la información personal, porque al realizar una copia al tener esta información mezclada también ocasiona congestión y demoras si se quiere hacer una copia.

4. Consejos

4.1. Sobre la organización de la información en un sistema operativo Es aconsejable que en los computadores se puedan crear dos particiones. La primera corresponderá al lugar en el cual se instalará el Sistema Operativo, la segunda corresponderá al lugar en el cual se guardarán los demás datos, aunque esto no garantiza la permanencia de la información ni tampoco sea una regla que se deba tener en los computadores, si se facilitan las cosas a la hora de hacer una restauración del computador por daño en el Sistema Operativo, porque simplemente los datos los estamos guardando en una partición y los archivos de programas y demás en donde se encuentra el Sistema Operativo. Si quieren contar con esto es bueno comunicarse con nosotros en el área de Soporte Técnico para que a la hora de instalar el equipo puedan optar por esta opción.

4.2. Sobre el nombre de los archivos Es muy recomendable que no se guarden archivos con nombres muy largos. Aunque suena extraño esto es vital a la hora de realizar un Backup pues en ocasiones, los archivos que tienen nombres muy largos ocasionan problemas. Otro punto vital es nombrar los archivos con nombres que nos permitan reconocer que contenido tiene un archivo dado. Esto se hace para no tener que revisar todos los archivos que tenemos en el computador abriéndolos, sino que simplemente nos podremos limitar a leer el nombre del archivo, y con esto debería ser suficiente para decidir si se guarda o se elimina. Algunos Sistemas Operativos no permiten ingresar unos caracteres especiales al nombre del archivo, pero no está de más sugerirles que no nombren archivos o carpetas utilizando caracteres especiales como (#\$%&?'i'¿). En ocasiones, queremos guardar páginas de Internet, guardándolas en formato html. Por lo general estos archivos html que guardamos de Internet, vienen con nombres extremadamente largos y extraños. Así que si queremos guardar información de una página de Internet recomendamos copiar y pegar la información en algún otro archivo. Si lo que queremos guardar no es la información contenida en la página sino el código html de esta, pues guarden la página con un nombre con el cual se identifique la página. Pero renombrarla puede llevar problemas a la hora de bajar un conjunto de páginas de Internet que tienen vínculos entre sí.

El Backup de archivos permite tener disponible e íntegra la información para cuando sucedan los accidentes. Sin un backup, simplemente, es imposible volver la información al estado anterior al desastre.

Como siempre, será necesario realizar un análisis Costo/Beneficio para determinar qué información será almacenada, los espacios de almacenamiento destinados a tal fin, la forma de realización, las estaciones de trabajo que cubrirá el backup, etc.

Para una correcta realización y seguridad de backups se deberán tener en cuenta estos puntos:

1. Se debe de contar con un procedimiento de respaldo de los sistemas operativos y de la información de los usuarios, para poder reinstalar fácilmente en caso de sufrir un accidente.
2. Se debe determinar el medio y las herramientas correctas para realizar las copias, basándose en análisis de espacios, tiempos de lectura/escritura, tipo de backup a realizar, etc.
3. El almacenamiento de los Backups debe realizarse en locales diferentes de donde reside la información primaria. De este modo se evita la pérdida si el desastre alcanza todo el edificio o local.
4. Se debe verificar, periódicamente, la integridad de los respaldos que se están almacenando. No hay que esperar hasta el momento en que se necesitan para darse cuenta de que están incompletos, dañados, mal almacenados, etc.
5. Se debe de contar con un procedimiento para garantizar la integridad física de los respaldos, en previsión de robo o destrucción.
6. Se debe contar con una política para garantizar la privacidad de la información que se respalda en medios de almacenamiento secundarios. Por ejemplo, la información se debe encriptar antes de respaldarse.
7. Se debe de contar con un procedimiento para borrar físicamente la información de los medios de almacenamiento, antes de desecharlos.
8. Mantener equipos de hardware, de características similares a los utilizados para el proceso normal, en condiciones para comenzar a procesar en caso de desastres físicos. Puede optarse por:
 - Modalidad Externa: otra organización tiene los equipos similares que brindan la seguridad de poder procesar la información, al ocurrir una contingencia, mientras se busca una solución definitiva al siniestro producido.
 - Modalidad Interna: se tiene más de un local, en donde uno es espejo del otro en cuanto a equipamiento, características técnicas y capacidades físicas. Ambos son susceptibles de ser usados como equipos de emergencia.

Se debe asegurar reproducir toda la información necesaria para la posterior recuperación sin pasos secundarios. Por ejemplo, existe información que es función de otra (checksums). Si sólo se almacenara la información principal, sin sus checksums, esto puede derivar en la inutilización de la misma cuando se recupere el backup.