

Copia de seguridad y recuperación de sistemas.

Por qué hacer un backup

Actualmente, todo el mundo experimenta el continuo incremento de la cantidad de datos que necesita archivar, consultar y transmitir. Los datos de computación son el motor que hace avanzar a las empresas y nadie debería poner en riesgo sus negocios por no haberse preocupado de resguardar sus datos. Una estrategia de back-up adecuada es el seguro más efectivo contra incendios, inundaciones, crash de discos, errores humanos, robos, boicots o virus. Todas esas cosas pueden provocar la pérdida de sus datos y con ellos los datos de sus clientes, sus proyectos, y negocios; o -en el mejor de los casos- horas y horas de operaciones para recuperar los datos.

La creación e implementación de un plan de copia de seguridad y recuperación es una de sus tareas más importantes como **administrador de sistemas**. Piense en las copias de seguridad del sistema como una especie de póliza de seguros para el futuro... y para su propio trabajo.

¡ Recuerde !

**Sólo hay dos tipos de datos...
Los datos que han sido "salvaguardados"
y los datos que no perdió... TODAVÍA.**

Planificación inicial de las copias de seguridad y la recuperación

La creación e implementación de un plan de copia de seguridad y recuperación requiere su tiempo. Será necesario determinar de qué tipo de datos es necesario hacer copias de seguridad, con qué frecuencia hay que hacer dichas copias, y otros aspectos. Para ayudarlo a crear el plan, considere los siguientes puntos:

- **¿Qué importancia tienen los datos que queremos salvaguardar?** La importancia de los datos puede ayudar bastante a determinar cuándo y cómo es necesario hacer copias de seguridad de los mismos. Mientras que es posible que realicemos una copia de seguridad de una base de datos de desarrollo semanalmente, probablemente convenga realizar una copia de seguridad de una base de datos de producción al menos de manera diaria, e incluso copias de seguridad cada hora para los registros de transacciones.
- **¿Con qué frecuencia se hacen cambios en los datos?** La frecuencia de actualización nos puede dar una idea de la necesidad de realizar una copia de seguridad. Por ejemplo: Una base de datos de sólo lectura no cambia normalmente, por lo que no sería necesario hacer copias de seguridad con regularidad. Por otro lado, una base de datos que se actualiza cada noche debería disponer de un mecanismo que realizara copias de seguridad una vez insertados los cambios nocturnos. Por su parte, una base de datos que sea actualizada de manera continua, a cualquier hora del día, requerirá que se realicen copias de seguridad también de manera continua.

- **¿Con qué rapidez es necesario poder recuperar los datos?** Se trata de un aspecto importante a la hora de crear un plan de copia de seguridad. Para las bases de datos críticas, puede ser necesario ponerlas en línea con gran rapidez; para hacer esto, quizá sea preciso modificar el plan de copia de seguridad. En lugar de realizar las copias de seguridad en cinta, puede que se necesite realizarlas en unidades de disco, o usar múltiples dispositivos de copia de seguridad.
- **¿Dispone del equipo necesario para realizar copias de seguridad?** Para realizar copias de seguridad, hace falta disponer del hardware apropiado. Las copias de seguridad con requisitos temporales estrictos, puede ser necesario disponer de varios dispositivos de copia de seguridad. El hardware de copia de seguridad puede incluir unidades de cinta, unidades ópticas, unidades de disco extraíble y unidades de disco tradicionales. Generalmente, las unidades de cinta son menos caras, pero más lentas, que los otros tipos de unidades.
- **¿Cuál es el mejor momento para programar las copias de seguridad?** Conviene programar la realización de copias de seguridad para que tenga lugar cuando el uso de los datos sea lo más bajo posible. Esto hará que se acelere el proceso de copia de seguridad. Sin embargo, en el mundo real no siempre es posible programar las copias de seguridad para que tengan lugar en la horas de menor congestión.
- **¿Es necesario almacenar las copias de seguridad fuera de las oficinas?** El almacenamiento de duplicados de las cintas de copia de seguridad fuera de las oficinas es fundamental para la recuperación de los sistemas en caso de un desastre total (incendio, inundación, etc.). Fuera de las oficinas deberían guardarse también copias del software necesario para poder restaurar un nuevo sistema.

Selección de medios y dispositivos de copia de seguridad

Hay disponibles muchas soluciones diferentes para la copia de seguridad de los datos. Algunas de ellas son rápidas y caras; otras son lentas pero muy fiables. La solución de copia de seguridad apropiada para su organización, dependerá de muchos factores, incluyendo:

- **Capacidad:** ¿Puede admitir el hardware de copia de seguridad el nivel de carga requerido, dadas las restricciones existentes de tiempo y de recursos?
- **Fiabilidad:** ¿Puede permitirse sacrificar algo de fiabilidad para cumplir con las necesidades presupuestarias o de tiempo?
- **Ampliabilidad:** ¿Satisfará esta solución sus necesidades a medida que su organización crezca?
- **Velocidad:** ¿Puede permitirse sacrificar algo de velocidad para reducir los costes?
- **Coste:** ¿Encaja dicha solución dentro de su presupuesto'?

Algunas de las soluciones de copia de seguridad más comúnmente utilizadas son:

- **Unidades de cinta:** Estas unidades son los dispositivos de copia de seguridad más comunes. Utilizan cartuchos de cinta magnética para almacenar los datos. Las cintas magnéticas son relativamente baratas, pero no son extremadamente fiables; las cintas se pueden romper o arrugar, y también pueden perder información con el paso del tiempo. La capacidad media de los cartuchos de cinta va desde 100 MB hasta 2 GB. Comparadas con otras soluciones de copia de seguridad, las unidades de cinta son bastante lentas. A pesar de esta desventaja, el factor principal que juega en su favor es el bajo coste de las unidades de cinta y de las cintas magnéticas.
- **Unidades DAT:** Las unidades DAT (digital audio tape, cinta de audio digital) están reemplazando rápidamente a las unidades de cinta normales como dispositivo preferido de copia de seguridad. Las unidades DAT utilizan cintas de 4 y 8 mm para almacenar los datos. Las cintas y unidades DAT son más caras que las cintas y unidades de cinta estándar, pero ofrecen una mayor velocidad y una mayor capacidad. Las unidades DAT con cintas de 4 mm pueden almacenar normalmente más de 30 MB por minuto, y tienen capacidades de hasta 16 GB. Las unidades DAT con cintas de 8 mm pueden almacenar normalmente más de 10 MB por minuto y tienen capacidades de hasta 10 GB (con compresión).
- **Sistemas de cinta con cargador automático:** Estos sistemas utilizan un conjunto de cintas para crear volúmenes ampliados de copia de seguridad, capaces de satisfacer las demandas de alta capacidad de las empresas. Gracias a un sistema de carga automática, las cintas del conjunto se cambian automáticamente según sea necesario durante el proceso de copia de seguridad o recuperación. La mayoría de los sistemas de cinta con cargador automático utilizan cintas DAT. El sistema típico utiliza conjuntos formados por entre 4 y 12 cintas. La desventaja principal de estos sistemas es su alto coste.
- **Unidades magneto-ópticas:** Estas unidades combinan la tecnología de cintas magnéticas con láser ópticos, para crear una solución de copia de seguridad más fiable que la ofrecida por las cintas DAT. Las unidades magneto-ópticas utilizan discos de 3,5" y 5,25" que tienen un aspecto similar al de los disquetes, pero que son mucho más gruesos. Normalmente, los discos magneto-ópticos tienen capacidades comprendidas entre 1 y 4 GB.
- **Jukebox:** Estas unidades son similares a los sistemas de cinta con cargador automático, pero emplean discos magneto-ópticos en lugar de cintas DAT para ofrecer soluciones de alta capacidad a la empresa. Estos sistemas cargan y descargan una serie de discos almacenados internamente para las operaciones de copia de seguridad y recuperación. Su desventaja principal es, de nuevo, el alto coste.
- **Discos extraíbles:** Los discos extraíbles, como Iomega Jaz. Estos discos ofrecen una buena velocidad y facilidad de uso para la copia de seguridad de una única unidad o de un único sistema. Sin embargo, las unidades de disco utilizadas y los propios discos extraíbles tienden a ser más caros que las soluciones basadas en unidades DAT o de cinta estándar.
- **Unidades de disco:** Las unidades de disco proporcionan la forma más rápida de copia y restauración de datos. Con las unidades de disco, a menudo puede llevarse a cabo en sólo unos pocos minutos lo que con una unidad de cinta tardaría horas. Cuando sus necesidades exijan una recuperación muy rápida, no hay ninguna solución que supere a las unidades de disco. Sin embargo, las unidades de disco presentan como desventajas su alto coste y su poca ampliabilidad.

Aunque la selección del dispositivo de copia de seguridad es un paso importante a la hora de implementar un plan de copia de seguridad y recuperación, no es el único paso. También es necesario comprar las cintas o los discos (o ambos) que permitan implementar el plan de copia de seguridad y recuperación. El número de cintas, discos o unidades que necesite dependerá de:

- El volumen de los datos que vaya a copiar.
- La frecuencia con la que vaya a realizar copias de seguridad de los datos.
- El tiempo durante el que necesite conservar conjuntos de datos adicionales.

Qué elementos debemos tener en cuenta para calcular el costo del backup?

Cuando calculamos el costo de un sistema de back-up, se deben tener en cuenta muchos elementos. Algunos son fáciles de identificar y su costo es claro. Otros son menos obvios y variarán entre una y otra instalación.

- **El dispositivo:** Habrá que seleccionar el dispositivo más adecuado a las necesidades de back-up presentes y futuras: capacidad, velocidad de transferencia, tiempo que tarda en cargar el soporte, velocidad de acceso a los archivos, costo, confiabilidad (MTBF) y posibilidad de escalabilidad futura.
- **Número de medios o soportes** necesarios, que dependerán de la estrategia de back-up utilizada.
- **El software:** Un sistema de Back-up requiere un software. Este puede estar embebido en el Sistema Operativo o se adquiere como un software externo (permiten realizar operaciones de back-up más versátiles y automatizadas). El mercado ofrece una rica variedad de software de back-up. Sin embargo debe observarse la compatibilidad del software con el dispositivo, para que la instalación no se convierta en una verdadera complicación. Una buena alternativa para estos casos, es la adquisición de *Soluciones integrales de Software y Dispositivo*.
- **La operativa:** La operación y mantenimiento deben ser muy sencillos una vez realizada la instalación. Para ello, es necesario definir un esquema de back-up, regulando las operaciones de back-up que se necesitan realizar diariamente y la limpieza de cabezales del dispositivo.
- **Reemplazo de medios:** Es necesario reemplazar las cintas en uso. Las diferentes tecnologías de cintas tienen distintos tiempos de vida útil y costo. Por ejemplo: un cartridge utilizado diariamente debería reemplazarse una vez al año.
- **La limpieza de los dispositivos** es absolutamente necesaria. Por lo que debe definirse un esquema de limpieza.

El costo de no hacer back-up

Siempre existe la posibilidad de que ocurra un desastre. Sin llegar a este extremo, es muy frecuente la pérdida de archivos aislados. El costo de recuperar esos datos puede ser muy significativo. La pérdida de datos, implica una gran pérdida de tiempo e incluso la pérdida de negocios o clientes.

Anualmente, en USA se gastan diez millones de dólares en rehacer la información perdida. Incluso, hay empresas especializadas en regenerar archivos y datos dañados (por ejemplo [CompExcell](#)). Todo esto sería evitable si las empresas dispusieran de un buen plan de back-up.

Los sistemas RAID (Redundant Array of Inexpensive Disks)?

Se trata de un sistema redundante de almacenamiento para proteger los datos, pero bajo ningún concepto debe suplir a un sistema de back-up. Además, una estrategia de back-up correcta requiere guardar las cintas de back-up fuera del lugar del Sistema o Server. Por ejemplo, después del ataque al *World Trade Center en New York*, más del 50% de las oficinas no tenían resguardadas sus cintas de back-up fuera del edificio.

Principios básicos del back-up

- **Back-up** significa hacer copias de archivos almacenados originalmente en discos rígidos. El back-up es necesario para recuperar archivos perdidos o dañados o para recuperar un sistema que ha caído.
- **Archiving** significa copiar uno o más archivos sobre la cinta, para almacenar por un largo período de tiempo (históricos), ya sea por cuestiones legales o para hacer espacio en el disco.
- **Disaster recovery** significa recuperar desde una situación de desastre. Se requiere entonces el back-up guardado off-site a partir del cual puede recuperarse gran parte -y hasta todo- el sistema. Por ejemplo, todos los Bancos españoles están obligados a restaurar sus servicios en pocas horas, aún habiéndose producido un desastre total, por lo que cuentan con copias off-site y CPDs duplicados en otros edificios.

Tres Reglas de oro

- **Rotación de la cinta** - No use la misma cinta dos días seguidos. Si su sistema falla durante el proceso de back-up usted perderá los datos del disco y de la cinta
- **Copias off-site** - Un back-up completo se realiza guardando las copias fuera de la oficina. Siempre asegúrese de guardar una cinta de back-up, de no más de una semana de antigüedad, fuera del sitio donde está su Sistema.
- **Back-up diario** - Realizar un back-up cada día toma poco tiempo. La mayoría de los datos se vuelven obsoletos rápidamente.

Esquemas de Back-up

Los back-ups pueden ser: **completos, diferenciales o incrementales**, y pueden ser combinados de varias formas. Para conocer qué archivos han sido modificados o creados desde el último backup, los sistemas de backup se apoyan en la fecha de última modificación del archivo y, en algunos sistemas, en un atributo, que se activa cada vez que se modifica el archivo y se desactiva después de ser salvaguardado (por ejemplo: el atributo de archivo en W98, que en XP aparece en *propiedades del archivo-atributos-opciones avanzadas-Archivo listo para archivar históricamente*).

- Un **backup total** debería siempre guardarse en un lugar seguro (off-site). En un back-up total, se salvaguardan todos los datos y los archivos son marcados como salvaguardados.
- Con el **back-up incremental**, se almacenan todos los datos modificados desde el último back-up total o incremental (se almacenan sólo los datos modificados desde el último back-up y se marcan los ficheros como salvaguardados). El back-up incremental es más veloz pero la recuperación de datos desde una serie de back-ups incrementales será más lenta.
- Con un **back-up diferencial**, se almacenan los datos modificados o creados después del último back-up total o incremental, y **no** se marcan los archivos como salvaguardados, por tanto, si posteriormente realizamos otro back-up diferencial, se volverán a copiar todos los datos que hayan cambiado desde la última copia de seguridad total o incremental (aunque estén incluidos en el back-up diferencial anterior). Puesto que sólo se almacenan los cambios, la operación de copia de seguridad es más rápida que un backup total y puede ser realizada más a menudo.

NOTA: A la hora de restaurar no hay que confundir las copias de seguridad **diferenciales** con las **incrementales**. Las copias de seguridad **diferenciales** almacenan todos los cambios producidos desde la última copia de seguridad completa o incremental (lo que implica que el tamaño de la copia de seguridad diferencial crece con el tiempo, y a la hora de restaurar sólo se utilizará la última copia diferencial). Las copias de seguridad **incrementales** almacenan los cambios producidos desde la copia de seguridad completa o incremental más reciente (lo que significa que el tamaño de la copia de seguridad incremental es normalmente mucho menor que el de una copia de seguridad diferencial, pero a la hora de restaurar tendremos que utilizar todas la copias incrementales, restaurándolas en orden cronológico de realización).

Back-up diario y semanal

No es cuestión de hacer uno u otro, sino que deben hacerse ambos. Hacer un back-up total todos los días puede resultar muy lento. Pero tampoco es necesario. Si todos los días se almacenan en un back-up incremental o diferencial de los datos modificados, haciendo sólo un back-up total una vez a la semana tendrá la seguridad necesaria en los sistemas pequeños.

Estrategias de Backup

A continuación sugerimos algunos **esquemas de rotación** de cintas para pequeñas y medianas empresas. Estos esquemas se muestran como estrategias de **back-up básicas**. Además, deberían incluirse los requerimientos de **archiving** y dependiendo de las condiciones del entorno, deberían analizarse las precauciones de **disaster recovery**.

La forma normal de implementar las copias de seguridad consiste en utilizar una programación cíclica, en la que se va rotando entre 2 o más conjuntos de cintas, discos o archivos. La idea es que se pueda incrementar la longevidad de los medios reduciendo el uso de los mismos, y al mismo tiempo reducir el número de cintas, discos o archivos necesarios para garantizar que los datos estén disponibles cuando se requiera.

Para las bases de datos de gran importancia, nuestra recomendación sería utilizar 4 conjuntos de medios. Utilice 2 conjuntos para las rotaciones normales, el tercer conjunto para el primer ciclo de rotación al principio de cada mes y el cuarto conjunto para el primer ciclo de rotación al principio de cada trimestre. Esta técnica le permitirá recuperar la base de datos en una amplia variedad de situaciones.

Por qué no usar 2 o 3 cartridges?

Seguir un **esquema simple** para hacer las copias, puede resultar **muy peligroso**. Por ejemplo, hacer una copia de seguridad periódica sobre el mismo soporte puede provocar que perdamos información. Ya que, si surge un virus que machaca los datos o un fichero se corrompe, los **datos en buen estado podrían ser sobrescritos con datos dañados antes de haberse manifestado el problema**. Es decir, **tanto los datos originales como los de la copia de seguridad pueden estar mal**.

Rotación de 5 cartridges en 5 días

Se asignan 5 cartridges, cada uno para uno de los días hábiles de la semana. Un back-up total por noche. Por la noche, siempre se lleva fuera de la oficina la última copia completa.

	Lu.	Mar.	Mié.	Jue.	Vie.	Sáb.	Dom.
Cartridge:	1	2	3	4	5	-	-

*** Los pro:** es muy simple

*** Los contra:** el backup histórico que guarda es muy corto (1 semana). Debe contar con una versión de archivos de semanas anteriores. Con este esquema de rotación, no está disponible.

Rotación de 5 cartridges en 7 (ó 5) días, 2 semanas, con una copia off-site

- Se asignan 2 cartridges para el back-up diferencial diario [1-2]
- Se asignan 2 cartridges para el backup total semanal. Cada cartridge se rota cada 15 días [3-4]
- Un cartridge se usa para un backup total mensual, que se guarda fuera de la oficina. [5]

	Lu.	Mar.	Mié.	Jue.	Vie.	Sáb.	Dom
Semana 1 -Cartridge:	1 - 5	2	1	2	3	1	2
Semana 2 -Cartridge:	1	2	1	2	4	1	2

*** Los Pro:** Su simplicidad. Contar con cierta redundancia reduce el peligro de no poder recuperar la historia. Se resguarda una copia off-site.

*** Los Contra:** Los cartridges usados para alternar el back-up diariamente brindan muy poca redundancia. Aún, el back-up de dos semanas atrás puede perderse.

Rotación de 11 cartridges en 5 días /4 semanas/3 meses

- Se asignan 4 cartridges para backup diferencial diario [1-4]
- Se asignan 3 cartridges para backup incremental semanal [5-7]
- Se asignan 3 cartridges para back-up total mensual, el 4to. viernes de cada mes [8-10]
- Se usa 1 tape más para backup incremental si hubiera un 5to. viernes en el mes [11]

	Lu.	Mar.	Mié.	Jue.	Vie.	Sáb.	Dom
Cartridge:	1	2	3	4	5	-	-
Cartridge:	1	2	3	4	6	-	-
Cartridge:	1	2	3	4	7	-	-
Cartridge:	1	2	3	4	8-10	-	-
Cartridge:	1	2	3	4	11	-	-

*** Los Pro:** La redundancia reduce el riesgo de no poder reconstruir la historia. En el peor de los casos se podrá reconstruir la información de hasta por lo menos 4 semanas atrás.

*** Los Contra:** Dado que hay involucradas mayor número de cintas, se complica un poco el esquema, por lo que requiere mayor precisión para la operación.

Rotación de 12 cartridges 5 días / 4 semanas / 3 meses

- Hijo: se asignan 4 cartridges para back-up incremental diario [1-4]
- Padre: se asignan 5 cartridges para back-up total semanal [5-9]
- Abuelo: se asignan 3 cartridges para backup total mensual [10-12]

	Lu.	Mar.	Mié.	Jue.	Vie.	Sáb.	Dom
Cartridge:	1	2	3	4	5	-	-
Cartridge:	1	2	3	4	6	-	-
Cartridge:	1	2	3	4	7	-	-
Cartridge:	1	2	3	4	8	-	-
Cartridge:	1	10-12 ¹	-	-	9 ²	-	-

1- Sobre el último días hábil del mes 2- Cuando hay un 5to. viernes en el mes

*** Los Pro:** La redundancia reduce el riesgo de no poder recuperar la historia. En el peor de los casos se podrá reconstruir la información de hasta por lo menos 4 semanas atrás. Las copias mensuales deben guardarse fuera de las oficinas.

*** Los Contra:** Ya que hay involucradas mayor cantidad de cintas, se complica un poco el esquema, por lo que requiere mayor precisión para la operación.

Este esquema de backup (**abuelo-padre-hijo**) es muy utilizado ya que cubre la mayoría de las necesidades de *backup*, *disaster recovery* y *archiving*. Para archivo por largos períodos de tiempo, las cintas pueden ser sacadas del esquema de rotación y reemplazadas.

Software de Back-Up

El programa para copias de seguridad (Copia de Seguridad de Microsoft) que se incluye con Windows por medio de un asistente en el que se detalla perfectamente cada paso cómo hacer la copia. Lo tenemos en **Inicio-Programas-Accesorios-Herramientas del sistema-Copia de Seguridad**.

También podemos utilizar muchos programas, incluso gratuitos, para hacer nuestras copias de seguridad. Estos programas permiten seleccionar archivos desde cualquier unidad, ya sea disco duro, unidad de red, vías FTP, grabadora, unidad ZIP, JAZ o disquetes. Permiten hacer copias normales o comprimirlas en formato ZIP y encriptarlas con un password.

Es interesante que tengan posibilidad de hacer copias de seguridad de los ficheros de sistema, así como programar las copias en fechas y horas determinadas. Y que quede un registro de las operaciones realizadas.

Bushido Backup (<http://www.users.yourvillage.com/bricker3>) **gratis**.

Brirespa (<http://www.brindys.com/brirespa/cas.html>) **gratis**

Polder Backup (<http://www.xs4all.nl/~philippo/PolderBackup.htm>) **gratis**.

Backup Latest (<http://www.geocities.com/SiliconValley/Bay/2965/backuplatest.html>) **gratis**.