

A1. Copias de seguridad.

Índice.

1.	¿Qué es una copia de seguridad?.....	2
2.	¿Cuántas copias y con qué frecuencia?.....	5
3.	Consejos para hacer copias de seguridad.....	6
4.	Tipos de copias de seguridad.....	7
5.	Política de copias de seguridad.....	10
6.	Planificación de copias de seguridad.....	12
7.	Herramientas útiles.....	13

A1. Copias de seguridad.

1. ¿Qué es una copia de seguridad?



A1. Copias de seguridad.

1. ¿Qué es una copia de seguridad?

Una **copia de seguridad** (respaldo o de reserva) es una copia de los datos originales realizada para disponer de alguna forma de recuperación de los mismos ante una pérdida debido a:

- Una causa accidental (corrompido).
- Una causa debida a un virus informático (u otras causas)
- Otras causas (guardar información histórica, traslado a otras ubicaciones, etc.).



A1. Copias de seguridad.

1. ¿Qué es una copia de seguridad?

Una **copia de seguridad** de todos los documentos no sólo sirve para que sea utilizada para recuperar un archivo dañado o inaccesible, sino también para ser consultada por alguna información que, por un motivo u otro, ya no existe en la versión actual del Proyecto (o trabajo) en que estemos trabajando.

Resulta importante definir claramente:

- Finalidad del archivo backup.
- Frecuencia en que será actualizado.

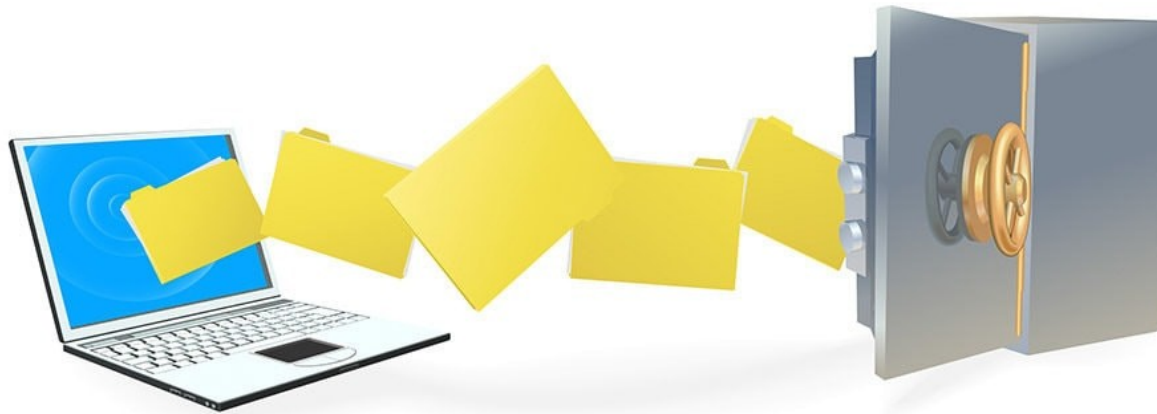


A1. Copias de seguridad.

2. ¿Cuántas copias y con qué frecuencia?

El número de copias depende de:

- Importancia de los archivos → en función de lo importante que sean los datos contenidos.
- Dispositivos de almacenamiento disponibles → en función de si vale la pena adquirir un equipamiento propio para dichas copias de seguridad o de si puedo usar lo que tengo a mano.



Gran inconveniente → manejo de la gran cantidad de copias de seguridad, es decir, el control de cambios entre las versiones de los archivos, con el fin de asegurar que los datos estén actualizados junto con las versiones anteriores.

A1. Copias de seguridad.

3. Consejos para hacer copias de seguridad.

Algunos consejos para realizar backups de una forma sencilla y eficiente son los siguientes:

- Ante trabajos académicos → enviar copias a los compañeros de grupo por si ocurriese cualquier cosa.
- Ante colecciones de música, vídeo, fotos o libros → enviar copias a compañeros con gustos similares.
- Ante colecciones de fotos de los móviles → subirlas a algún servicio de almacenamiento en la nube, procurando su almacenamiento en carpetas compartidas con familiares o amigos.
- Ante copias de seguridad de diferentes versiones → guardar cada cambio significativo en un archivos con otro nombre o en otro directorio.
- Ante copias de seguridad de archivos importantes → guardarlas con contraseñas o con herramientas de criptografía, protegiéndolas ante el robo, pérdida o cualquier ojo curioso.
- Ante servicios de empresas especializadas en copias de seguridad → referencias en la calidad de los servicios, confidencialidad, disponibilidad, privacidad, disponibilidad y seguridad del servicio web.
- Ante adquisición de herramientas para realizar copias de seguridad → si poseen alguna forma de poder validar las copias para evitar copias alteradas, dañadas o generadas de forma incorrecta.
- Ante la innumerable cantidad de copias de seguridad → se deben organizar por fecha o categoría.
- Ante el mantenimiento de una página web (o blog) → siempre hay que tener, al menos, una copia de seguridad del sitio en el ordenador, en la nube, en una unidad de almacenamiento externo o en otro dispositivo por cuestiones de rapidez en la restauración.

A1. Copias de seguridad.

4. Tipos de copias de seguridad.

Una primera clasificación de las copias de seguridad es:

- **Copia en frío vs caliente** → en función de si se detiene o no el servicio de la base de datos.
- **Copia física (o binaria) vs lógica (o textual)** → en función de si se copia los archivos binarios referentes al almacenamiento de las bases de datos o si se copia los datos y los diferentes objetos a archivos de texto.
- **Copia completa vs incremental** → en función de si se copia todos los datos o sólo aquéllos que se han modificado desde la última copia.
- **Copia manual vs automática** → en función de si se realiza a través de comandos escritos por el Administrador o en función de una fecha y hora programada.

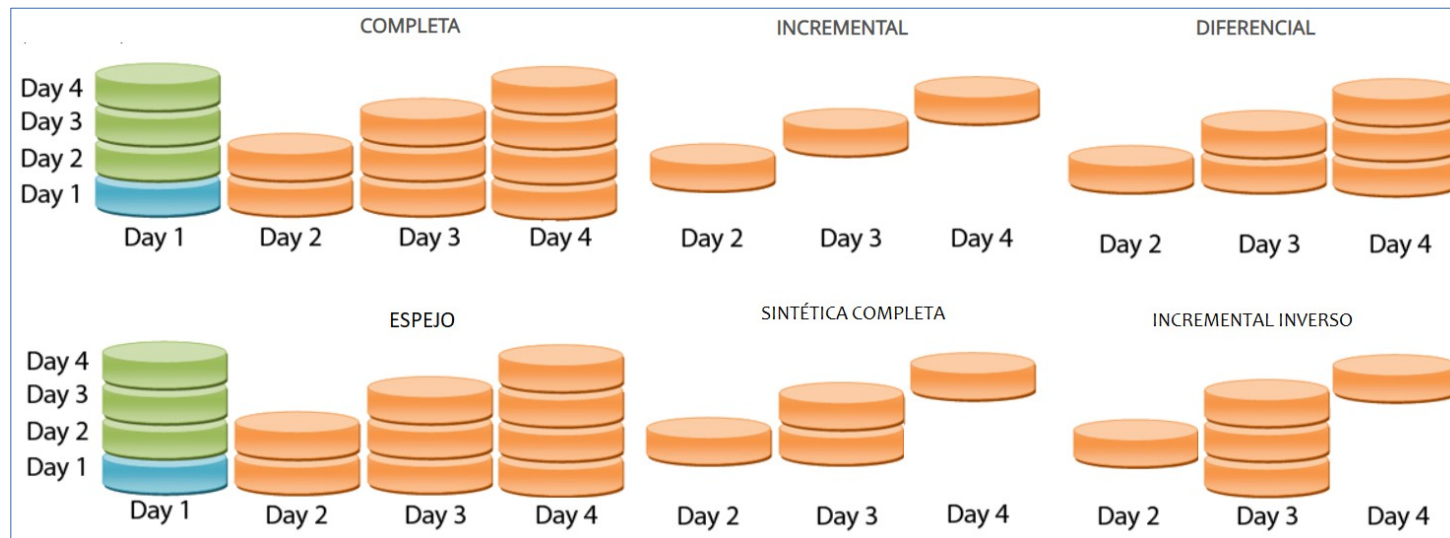


A1. Copias de seguridad.

4. Tipos de copias de seguridad.

Otra clasificación de las copias de seguridad es:

- **Completa** → copia de seguridad de todos los archivos y carpetas seleccionados.
- **Incremental** → copia de seguridad de todos los cambios realizados desde la última copia de seguridad (completa o incremental).
- **Diferencial** → copia de seguridad de todos los cambios realizados desde la última copia de seguridad completa.
- **Espejo** → reflejo fiel de la fuente que se está respaldando, lo que implica que un archivo eliminado en origen, también se borrará en la copia de seguridad.
- **Sintética completa** → reconstruye la imagen de la copia de seguridad completa en función de todas las copias incrementales o diferenciales.
- **Backup incremental inverso** → copia de seguridad incremental de los cambios realizados entre dos instancias de una copia espejo.
- **Protección de datos continua (CDP)** → permite una mayor cantidad de puntos de restauración con respecto a los demás tipos de copias de seguridad.

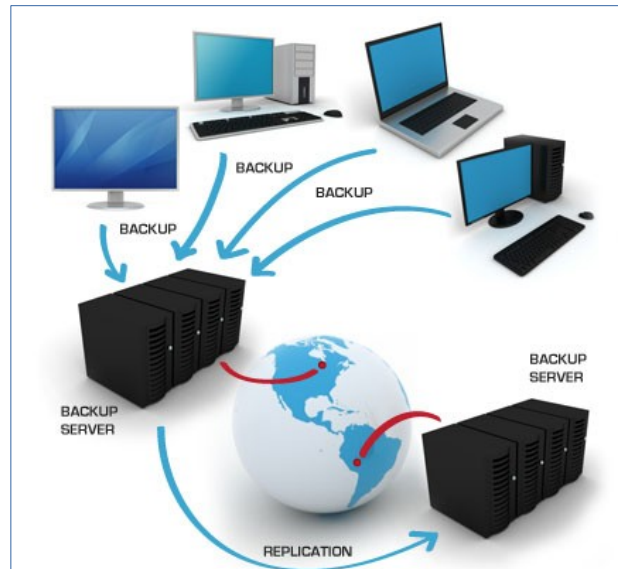


A1. Copias de seguridad.

4. Tipos de copias de seguridad.

Otra clasificación de las copias de seguridad es:

- **Física vs Lógica** → en función de si se copia los archivos binarios referentes al almacenamiento de las bases de datos o si se copia los datos y los diferentes objetos a archivos de texto.
- **Online vs Offline** → en función de si la copia se hace con la base de datos apagada o en funcionamiento.
- **Local vs Remoto** → en función de si la copia se realiza en el mismo equipo donde está la base de datos o en otro equipo distinto.
- **Snapshots** → copias lógicas de la base de datos en un momento determinado.
- **Completa vs Incremental** → en función de si se copia todos los datos o sólo aquéllos que se han modificado desde la última copia.
- **Mantenimiento de las tablas** → la integridad de las tablas puede verse comprometida si se hallan corruptas.
- **Backup Scheduling, Compression y Encriptación** → Backup scheduling se valora para la automatización de procedimientos de backup. La compresión de backup ayuda a reducir los requerimientos de tamaño. La encriptación proporciona mayor seguridad ante accesos indeseados.



A1. Copias de seguridad.

5. Política de copias de seguridad.

Las políticas de copias de seguridad definen:

- Tipo de copias.
- Periodicidad de las copias.
- Soportes en los que se deben realizar las copias.
- Ubicaciones de los centros de respaldo, en donde se guardan las copias de seguridad.
- Etiquetado correcto → identificación, tipo, fecha, contenido, responsable de la copia.
- Registro exhaustivo de las copias y de las restauraciones realizadas → identificación de la etiqueta, soporte, ubicación.
- Datos de cada restauración → fecha, incidencia que la motivó, ubicación, técnico responsable.



A1. Copias de seguridad.

5. Política de copia de seguridad.

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

- Persona o personas responsables encargadas de realizar y mantener las copias de seguridad.
- Análisis de los datos susceptibles de ser salvaguardados en las copias de seguridad.
- Determinar el tipo de copia a realizar en función de los datos a salvaguardar y de la periodicidad en que se modifican.
- Determinar la frecuencia de realización de las copias de seguridad.
- Determinar la ventana de backup en función de la duración que llevará la realización de cada copia.
- Determinar el tipo de soporte en el que se realizará cada copia de seguridad.
- Determinar la ubicación de las copias de seguridad.



A1. Copias de seguridad.

6. Planificación de copias de seguridad.

La planificación de las copias de seguridad requiere tener en consideración los siguientes elementos:

- Guardar la copia de seguridad en un disco o en un dispositivo externo a la unidad de origen.
- Realizar copias de seguridad regularmente (recomendable programar la copia para que se realice automáticamente de forma eventual).
- Comprobar con frecuencia la integridad de los archivos y la lectura de las unidades externas de las copias de seguridad realizadas.
- Evitar guardar la copia en el mismo lugar que los archivos originales, es decir, en el mismo disco duro.



A1. Copias de seguridad.

7. Herramientas útiles.

Algunas herramientas útiles para la realización de copias de seguridad son las siguientes:

- Utilidades gratuitas → CobianBackup, Genie TimeLine.
- Utilidades de pago → Genie TimeLine Professional, Acronis.
- En la nube → Drive de Google, Dropbox, OneDrive, Box, Mega.

