LA INFORMACIÓN

Copias de seguridad, borrado seguro y tipos de almacenamiento

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

UNIVERSIDAD DE GRANADA

crue Universidades Españolas

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_
www.incibe.es

ÍNDICE

1. Copias de seguridad pág. 03

1.1. Qué información copiar pág. 03

1.2. ¿Cada cuánto tiempo se debe realizar la copia de seguridad? pág. 03

1.3. ¿Dónde almacenar la copia de seguridad? pág. 04

1.4. ¿Qué tipo de copia elegir? pág. 05

1.5. La estrategia 3-2-1 pág. 07

2. Borrado seguro de la información pág. 08

3. Almacenamiento en local, en red o en la nube pág. 10

4. Referencias pág. 11

1. COPIAS DE SEGURIDAD

Una copia de seguridad es un proceso mediante el cual se duplica la información existente de un soporte a otro, con el fin de poder recuperarla **[Ref. - 1].** Desde el punto de vista institucional, ante un incidente grave o un desastre, una copia de seguridad puede marcar la diferencia entre recuperarse o sufrir las consecuencias, en ocasiones tan severas que pondrán en riesgo su continuidad.

Cualquier universidad debe contar con un sistema de copias de seguridad que proteja su información ya que en muchos casos esta es la única garantía de poder continuar con la actividad institucional.

1.1. ¿Qué información copiar?

El primer paso, será **determinar la información que se debe copiar**. Para ello, como ya explicamos en el apartado primero del tema anterior, **se tiene que clasificar.** En función de esa clasificación se identificarán aquellos activos de información sin los cuales la empresa no podría seguir con su actividad diaria.

1.2. ¿Cada cuánto tiempo se debe realizar la copia de seguridad?

Determinar la periodicidad con la que se harán las copias de seguridad dependerá de cada empresa en particular. Se ha de definir **una frecuencia adecuada para que ante un problema con cualquier activo de información, no suponga una gran pérdida y no afecte negativamente a la actividad laboral.**

1.3. ¿Dónde almacenar la copia de seguridad?

El tipo de soporte a elegir para almacenar las copias de seguridad dependerá de varios factores como la cantidad de información a copiar, del sistema seleccionado y la inversión a realizar. Las ventajas e inconvenientes de los tipos de almacenamiento más comunes son:

- **Cintas magnéticas:** la principal ventaja de este medio de almacenamiento es su reducido coste para almacenar grandes cantidades de datos. Diferentes estudios demuestran que el auge de esta tecnología como medio de almacenamiento para las copias de seguridad se debe a que se considera más fiable que los discos duros, además de poseer una vida útil superior a 30 años y un menor coste por terabyte.

- **Discos duros externos:** este tipo de soportes presentan varias ventajas como la facilidad de configuración o mejores tasas de rendimiento respecto a las cintas magnéticas. Por el contrario, presentan una vida útil inferior y un mayor coste por terabyte que las cintas. En empresas cuyo volumen de datos es reducido puede ser la opción más conveniente.

- **Dispositivos NAS o Network Attached Storage:** este tipo de dispositivos de almacenamiento se han diseñado, específicamente, para almacenar información. Su coste varía en función del número y tipo de discos empleados, además la gestión de las copias se simplifica al utilizar, únicamente, un dispositivo central. La mayoría de los fabricantes de estos dispositivos disponen de aplicaciones de copia de seguridad.

- **Servicios de almacenamiento en la nube:** este tipo de almacenamiento consiste en salvaguardar las copias de seguridad en servidores de terceros. La única preocupación será exigir las garantías de seguridad pertinentes a la empresa que se encargue de facilitar dicho servicio. Las ventajas de utilizar la nube como sistema de copias de seguridad son varias.

  » copia de seguridad fuera de la empresa;

  » disponibilidad de los datos en cualquier momento;

  » opia protegida ante incidentes dentro de la empresa.

  Pero también presenta desventajas, siendo las dos principales la **pérdida de confidencialidad y la dependencia de la conexión a Internet.** Como en cualquier copia de seguridad que se aloja fuera de la oficina, es recomendable cifrarla antes de subirla a la nube.

- **Discos ópticos:** la utilización de blu-rays como dispositivos de almacenamiento está ganando popularidad en empresas que no necesitan una gran capacidad de almacenamiento, ni hacer copias de seguridad muy frecuentemente. Uno de sus mayores atractivos es la protección que ofrece ante posibles ataques de tipo ransomware dirigidos a las copias de seguridad, ya que permanece en un soporte generalmente no conectado y además suelen ser de una sola escritura. Por otra parte, su coste es muy ajustado.

1.4. ¿Qué tipo de copia elegir?

El siguiente paso será establecer la estrategia a seguir en cuanto a cómo realizar la copia de seguridad. Existen, principalmente, cuatro formas de realizar las copias de seguridad:

- **En espejo o RAID 1:** mediante este método se crea una copiaexacta de los datos en tiempo real, mientras se trabaja, se crea una copia espejo de la información en otra ubicación. Sus ventajas son:
  - copia realizada en tiempo real;
  - la recuperación es un proceso muy ágil;
  - se optimiza el espacio de almacenamiento, ya que no se guarda información antigua o en desuso.

Su principal desventaja es que ante borrados, modificaciones o infecciones por malware ambos discos se verían afectados.

- **Completa:** consiste en hacer una copia de todos los datos de nuestro sistema en otro soporte haciendo que la recuperación, en caso de incidente, sea mucho más rápida. Pero este método también presenta desventajas:
  - requiere una mayor capacidad de espacio;
  - mayor tiempo en realizar la copia;
  - mayor coste debido a la necesidad de más espacio de almacenamiento..

1. COPIAS DE SEGURIDAD

- **Diferencial:** cúnicamente se copian los archivos y directorios que han sido creados o modificados desde la última copia completa. Sus principales ventajas son:
  - » no requiere tanto espacio como la completa;
  - » la restauración de la copia es un proceso bastante simple;

  Aunque también presenta desventajas:
  - » no es la solución más optimizada en cuanto a tiempo y espacio utilizado.

- **Incremental:** solo se copiarán los datos que hayan variado desde la última copia de respaldo realizada, ya fuera incremental, diferencial o completa. Sus principales ventajas son:
  - » Su principal ventaja es que se necesita un espacio y tiempo menores que en las otras opciones. La restauración de la copia es un proceso bastante simple.
  - » Por el contrario, su principal desventaja es la restauración, ya que esta puede resultar mucho más compleja.

1.5. La estrategia 3-2-1

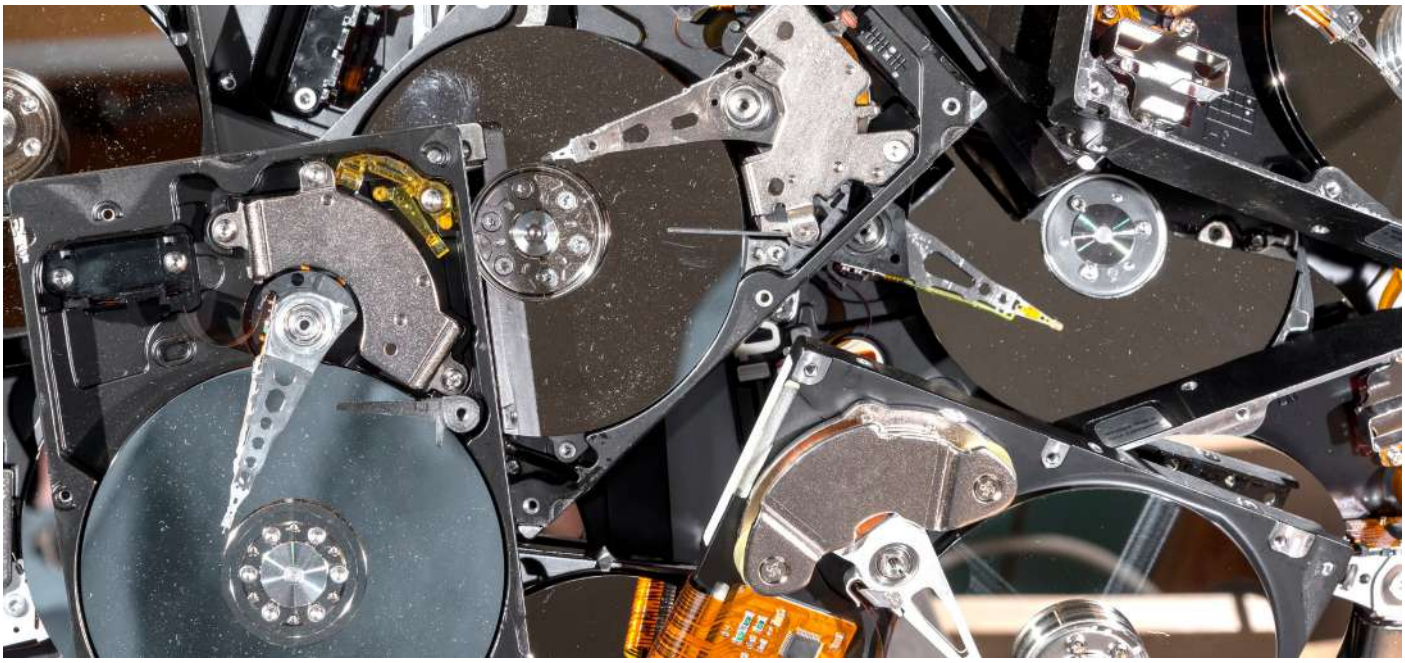
Una buena práctica a la hora de realizar copias de seguridad es adoptar **la estrategia 3-2-1 que se basa en diversificar las copias de seguridad.** Sus claves de actuación son:

- 3: mantener 3 copias de cualquier fichero importante: el archivo original y 2 backups;
- 2: almacenar las copias en 2 soportes distintos de almacenamiento para protegerlas ante distintos riesgos.
- 1: almacenar 1 copia de seguridad fuera de nuestra empresa, lo que también se conoce como backup offsite. La copia de seguridad en la nube es un claro ejemplo de este tipo de copia.

2. BORRADO SEGURO DE LA INFORMACIÓN

¿Qué ocurre cuando la información deja de ser necesaria o útil para la empresa? **Una vez llega a la última fase de su ciclo de vida, será necesario destruirla, de forma segura, de tal manera que no vuelva a ser accesible [Ref. - 2].**

Existen muchos tipos de datos, contables, fiscales, de videovigilancia, etc., y todos ellos presentan una vida útil distinta. Cuando estos datos dejen de ser necesarios para la organización deben eliminarse y se debe garantizar que la información no vuelva a ser accesible para nadie. Cuando la destrucción de la información no se realiza correctamente se expone a la empresa a sanciones legales y a posibles daños de imagen, además de aumentar el riesgo a que se produzca una fuga de información.



En los casos en que el dispositivo de almacenamiento, ya sea un ordenador, un smartphone o cualquier otro, sea retirado de los activos empresariales por el motivo que sea, también debe de pasar por el proceso de eliminación, de forma segura, de toda la información que contenga.

El primer paso será realizar un inventariado de activos para que ninguno sea extraviado. Se deben inventariar **todos los dispositivos y soportes que permitan el almacenamiento** como DVD, memorias USB, discos duros, ordenadores o smartphones. También se debe tener bajo control la información en formato físico.

2. BORRADO SEGURO DE LA INFORMACIÓN

El siguiente paso será eliminar la información:

- para la información **en soportes no electrónicos como papel y soportes magnéticos** como los DVD o cintas magnéticas, se deberá utilizar el triturado como modo seguro de eliminación;
- **los dispositivos de almacenamiento que permitan su reutilización deben ser sobrescritos múltiples veces** para evitar que la información vuelva a ser accesible;
- los **teléfonos móviles** que se vayan a reutilizar, se cifrarán antes de borrarlos y se restaurarán a sus valores de fábrica;
- **los soportes de almacenamiento electrónico que no funcionen** o se hayan quedado obsoletos, se deberán borrar por medio de **desmagnetización o destrucción física;**
- habrá que prestar **especial atención a los dispositivos móviles, así como a la memoria SD** que tienen algunos modelos en el momento de deshacernos de los mismos, ya que podrían contener información importante o confidencial.

Será importante hacer uso de herramientas que permitan documentar todas las operaciones de borrado.

También existe la posibilidad de hacer uso de la **destrucción certificada.** Este tipo de borrado se realiza a través de una empresa que llevará a cabo los procesos de eliminación de la información, garantizando tanto la gestión, como el control de recogida, transporte y destrucción del material. Posteriormente, estas empresas emitirán un certificado que garantizará y legitimará la validez del proceso.

3. ALMACENAMIENTO EN LOCAL, EN RED O EN LA NUBE

Almacenar la información usada en el día a día de la empresa, en el lugar adecuado, [Ref.–3] es importante, ya que de esta manera todos los activos estarán protegidos.

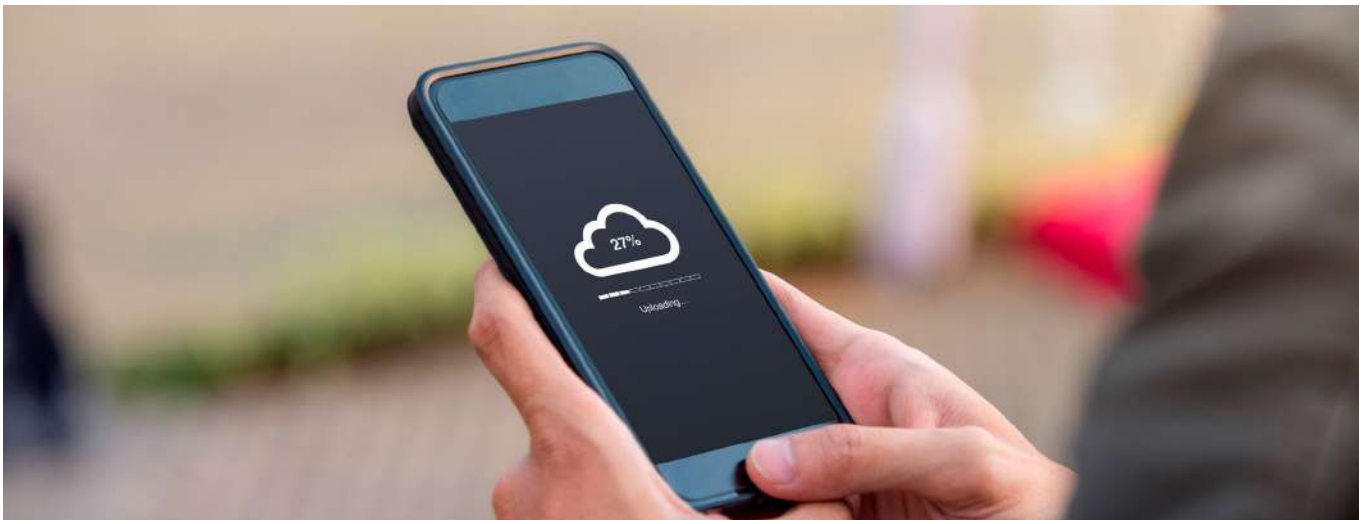
Supongamos que se guardan ciertos documentos importantes en el almacenamiento local de tu equipo por comodidad cuando se supone que deberían estar en un servidor interno. Si el ordenador, por el motivo que fuera, se averiara, todo el trabajo hecho no valdría de nada. De igual forma, sucede si se sube a la nube información confidencial sin consentimiento y sin las medidas de seguridad adecuadas, ya que se estaría poniendo en riesgo la información y a la propia empresa.

Cada tipo de almacenamiento tiene sus pros y contras, pero se ha de seguir el criterio establecido por la organización para que ningún archivo pueda quedar sin protección:

- **Local [Ref. - 5]:** almacenamiento en los propios dispositivos que es de rápido acceso y que siempre estará accesible a no ser que se produzca un fallo en el equipo. Al ser solo accesible por los usuarios de cada equipo, se producen silos no compartidos de información y de fallar el equipo, podría perderse definitivamente.

- **Red:** almacenamiento en un equipo de la red interna de la empresa que requiere de acceso a la red y permisos para poder gestionar la información. En caso de que exista esta opción en la empresa, será la que debamos utilizar, ya que así toda la información estará centralizada y se podrán aplicar las medidas de seguridad de forma máseficiente.

- **Nube [Ref. - 6]:** almacenamiento que siempre estará accesible si se cuenta con Internet y los permisos adecuados. Por el contrario, existe la problemática de almacenar información confidencial fuera de la mpresa, por lo que habrá que utilizar herramientas de cifrado para protegerla.i



4. REFERENCIAS

1. INCIBE – Protege tu Empresa - Guías - Copias de seguridad: una guía de aproximación para el empresario - https://www.incibe.es/protege-tu-empresa/blog/copias-seguridad-guiaaproximacion-el-empresario

2. INCIBE – Protege tu Empresa - Guías – Borrado seguro de la información: una guía de aproximación para el empresario - https://www.incibe.es/protege-tu-empresa/guias borradoseguro-informacion-aproximacion-el-empresario

3. INCIBE – Protege tu Empresa - Guías – Almacenamiento seguro de la información: una guía de aproximación para el empresario - https://www.incibe.es/protege-tuempresa/guias/almacenamiento-seguro-informacion-guiaaproximacion-el-empresario

4. INCIBE – Protege tu Empresa – Blog - Si la información ya no es necesaria, bórrala de forma segura - https://www.incibe.es/protege-tu-empresa/blog/si-informacion-no-necesariaborrala-forma-segura

5. INCIBE – Protege tu Empresa – Herramientas – Políticas - Almacenamiento en los equipos de trabajo. Políticas de seguridad para la pyme - https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/almacenamiento-enlos-equipos-trabajo.pdf

6. INCIBE – Protege tu Empresa – Blog - Recomendaciones para hacer copias de seguridad en la nube - https://www.incibe.es/rotege-tu-empresa/blog/recomendaciones-hacercopias-seguridad-nube

7. INCIBE – Protege tu Empresa – Herramientas – Políticas - Almacenamiento en la nube. Políticas de seguridad para la pyme - https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/almacenamiento-nube.pdf