2 POLÍTICAS DE ALMACENAMIENTO

Actualmente, todo el mundo (particulares y empresas) conserva mucha información en los **soportes de almacenamiento** de los equipos informáticos.

La protección de esta información pasa por instalar programas específicos para ello (como los antivirus o los *firewalls*) y por realizar copias de seguridad para poder restaurar la información si hubiera pérdidas debido a desastres de diversa índole (como incendios, apagones, inundaciones, etcétera). De otro modo, la información se perdería, con todas las consecuencias que eso supone.

Es fundamental tener el control de la información para afianzar la seguridad del almacenamiento de datos. A nivel europeo existe un reglamento de protección de la información de las personas físicas en relación con sus datos personales y la circulación de dichos datos. Este reglamento es el **Reglamento General de Protección de Datos** (**RGPD**), que entró en vigor el 25 de mayo de 2016, pero fue de aplicación obligatoria a partir del 25 de mayo de 2018.

La regulación será aplicada a toda organización que recopile datos de residentes de la Unión Europea. Por lo tanto, la regulación también se aplica a las organizaciones con sede fuera de la Unión Europea.

Este reglamento considera que la protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental. Además, la Carta de los Derechos Fundamentales de la Unión Europea establece que toda persona tiene derecho a la protección de sus datos de carácter personal que le conciernen.

PARA + INFO

Según la Comisión Europea, se entiende por datos personales de una persona física toda información sobre el individuo que refiera a su vida personal, profesional o pública. Por ejemplo, una fotografía, una dirección, un correo electrónico, información bancaria, nombres, información sobre redes sociales, direcciones IP, etcétera.

En caso de no cumplimiento de la ley, una organización podría llegar a pagar multas de hasta 20 millones de euros. El reglamento podría no aplicarse en actividades de seguridad nacional o aplicaciones de ciertas leyes en la Unión Europea.

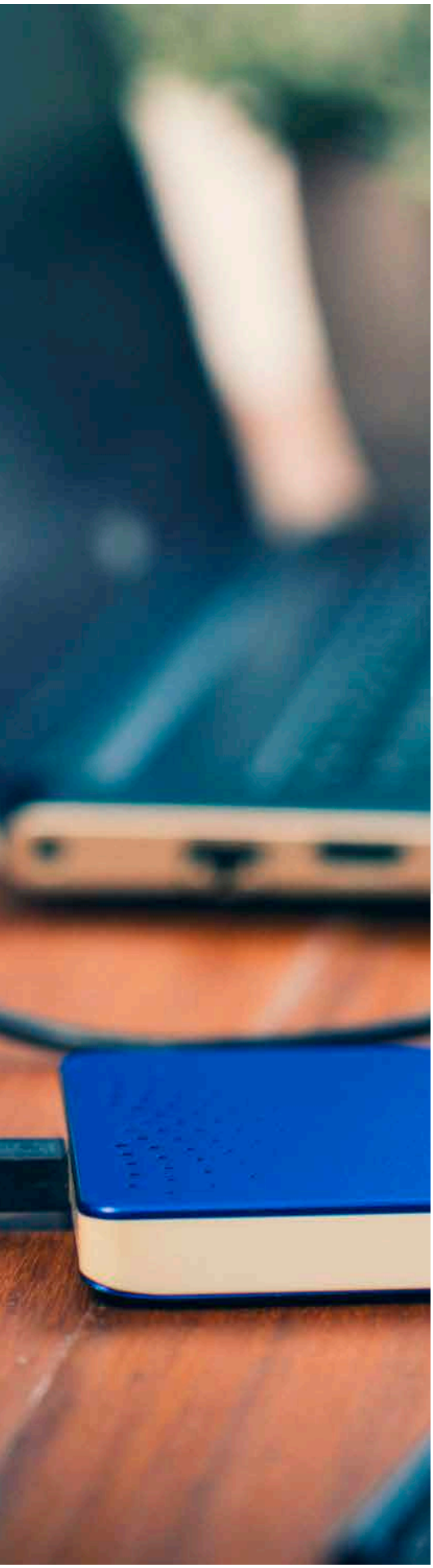
Este reglamento ofrece una serie de derechos digitales para los ciudadanos de la Unión Europea, de tal manera que las organizaciones deben garantizar una serie de principios:

- **Principio de responsabilidad**: las organizaciones deben ser capaces de demostrar que cumplen las exigencias de la ley.
- **Principio de transparencia**: las organizaciones deberán explicar los avisos legales y las políticas de privacidad de manera más simple, inteligible, comprensible y completa a las personas físicas afectadas.
- **Principio de protección de datos por defecto**: las organizaciones deberán adoptar medidas que garanticen el cumplimento de la norma desde el momento que se diseñe un producto, servicio o actividad que vaya a tratar datos personales de personas físicas.

BUSCA EN LA WEB

La **Agencia Española de Protección de Datos** es el organismo público que se encarga de asegurar el cumplimiento de la Ley Orgánica de Protección de Datos de Carácter Personal en España. Para más información:

https://www.agpd.es



Uno de los mecanismos para salvaguardar los datos es realizar copias de seguridad continuamente, ya que nuestros equipos siempre están expuestos a un ataque o pérdida de una información bastante sensible.

Las **copias de seguridad** garantizan la integridad y disponibilidad de la información; son útiles para restaurar el sistema operativo, las aplicaciones y los datos, en caso de ocurrir algún desastre. Seguro que conocemos a alguien (o nos ha pasado a nosotros mismos) que, en alguna ocasión, después de haber dedicado mucho tiempo a una tarea o trabajo, ha perdido todo lo hecho hasta el momento ante un corte de luz o un fallo del equipo. Es entonces cuando llegan las lamentaciones por no haber ido haciendo copias de seguridad de vez en cuando.

Otro de los métodos que podemos utilizar a la hora de salvaguardar los datos comprende la destrucción de algún dispositivo, soporte o equipo informático, la cual debe ser total para que ya no se pueda acceder a los datos que contienen. No obstante, claro está que previamente habremos realizado una copia de seguridad, si deseamos su conservación. En el mercado hay diferentes métodos que aseguran la destrucción de los datos.

2.1. Almacenamiento de la información: parámetros de configuración, rendimiento, disponibilidad y accesibilidad

Para llevar un proceso adecuado en las empresas a la hora de realizar una gestión sobre el **almacenamiento de la información**, debemos tener predefinidas unas **políticas de almacenamiento**. Estas deben recoger unas normas sobre la conservación de la información, el uso de los dispositivos externos y las copias de seguridad. También deben reflejar cuáles serán las pautas de seguridad de los datos en la red.

En todos los equipos disponemos de dispositivos para el almacenamiento de la información (de una forma no caduca). Dependiendo de la envergadura del sistema, necesitamos uno o varios discos duros dedicados al almacenamiento de la información.

Se puede producir una avería debido a un golpe o caída que afecte a las partes que componen un **disco duro** (brazo mecánico y discos magnéticos). Si esto ocurriese, el acceso a la información sería imposible. Por lo tanto, hay tres elementos que debemos asegurar: el hardware, el software y los datos. Estos últimos son los más importantes, pues

son los más difíciles de recuperar. Podemos sufrir ataques en contra de cualquiera de los elementos anteriores, ya que están expuestos a diferentes amenazas. Generalmente, la taxonomía más elemental de estas amenazas se puede dividir en los siguientes grupos:

- **Interrupción**: un recurso del sistema es destruido, deshabilitado o deja de estar disponible.
- **Interceptación**: un elemento no autorizado consigue un acceso a un determinado objeto del sistema.
- **Modificación**: es un caso de interceptación donde el intruso logra modificar el objeto. Algunos autores consideran la destrucción un caso especial de modificación, entendiéndola como una modificación que hace inutilizable el objeto.
- **Fabricación**: cuando el ataque está destinado a realizar una modificación a través de la suplantación del original. Actúa realizando una copia exacta para que sea difícil distinguir entre los dos.

2.1.1. Características de un dispositivo de almacenamiento

Los dispositivos de almacenamiento tienen distintas características, las cuales influirán a la hora de decidirnos por uno u otro:

Rendimiento

Es la capacidad de disponer de un determinado **volumen de datos** en un tiempo concreto, lo que se mide en tasas de transferencia (MBits/s). Las tecnologías para fabricar dispositivos de almacenamiento son variadas. Se diferencian en función del coste por bit, el tiempo de acceso y la capacidad de almacenamiento. A la hora de observar el rendimiento de un dispositivo hay que centrarse en el procesador, que es el elemento principal del ordenador, porque nos interesa que los datos con los que se va a trabajar se almacenen lo más rápido posible con el objetivo de tardar el menor tiempo posible.

La memoria más cercana y rápida en acceso es la **caché**, después está la memoria **RAM** y, finalmente, el **disco duro**, los discos ópticos, etcétera. Los datos a los que se accede de forma reciente se guardan en las memorias localizadas más próximas al procesador, aunque, a pesar de que son las más rápidas, tienen un escaso espacio de almacenamiento y son volátiles, es decir, que cuando se les deja de suministrar energía pierden toda su información.

Los dispositivos no volátiles, de gran capacidad, pero alejados del procesador, son los elementos que contendrán los datos que procesará en un futuro y por tanto no los necesita aún. Estas memorias tienen la característica de ser lentas en el acceso a la información.

Disponibilidad

La **capacidad** y **seguridad** de que la información puede ser recuperada en el momento en que se necesite. Ante un ataque o intento de bloqueo, ejecutaremos las medidas preventivas para salvaguardar la información y así evitar la pérdida total o parcial de nuestra información.

Actualmente, disponemos de métodos para favorecer la disponibilidad de los datos:

- **Redundancia de la información con los sistemas RAID de almacenamiento**: para llevar a cabo esta técnica debemos disponer de varios dispositivos de almacenamiento.
- **Centros de respaldo de la información**: podemos realizar copias de seguridad en la nube o contratar un servidor para alojar allí nuestras copias de respaldo.
- **Información distribuida**: aconsejada por la Agencia de Protección de Datos, para que toda la información no se concentre en un único lugar, debido a los ataques o incendios de la ubicación. Consiste en tener distintas memorias externas para realizar el trasvase y en mantener un control para conocer en todo momento qué información se encuentra en cada lugar.

Accesibilidad

Consiste en tener **disponible la información** por parte de los usuarios autorizados. Normalmente, se controla mediante técnicas de control de acceso (este concepto lo hemos tratado en el apartado anterior, lo que demuestra su importancia en el sistema de seguridad del equipo).

2.2. Métodos de almacenamiento locales y en red

Hemos comprobado la importancia de los dispositivos de almacenamiento a la hora de salvaguardar la información de un sistema informático. Un fallo, una avería o una sustracción en uno de estos elementos puede ocasionar un incidente bastante complejo y costoso si no se ha llevado a cabo una buena política de seguridad.

En este apartado, veremos la clasificación de estos dispositivos en función de varias características.

2.2.1. Naturaleza del soporte

El soporte del dispositivo es el **material** en el que se **fabrica**. En él queda registrada la información. Dependiendo de los materiales usados, tendrá mayor o menor velocidad de transferencia, coste o capacidad de almacenamiento.

En función del medio que se utilice:

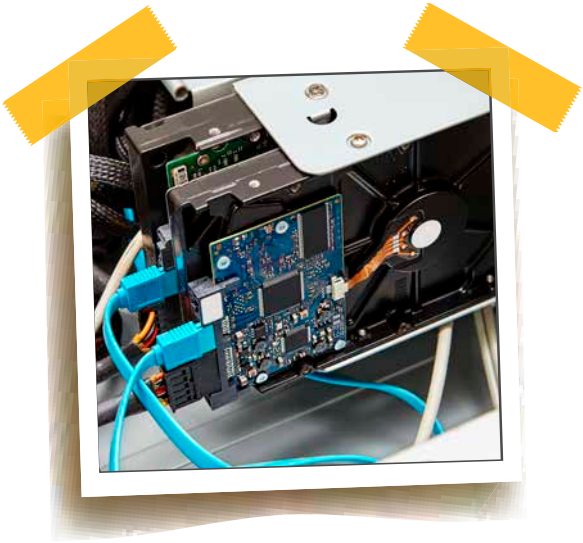
- **Medios magnéticos**: los dispositivos de almacenamiento por medio magnético son los más antiguos. Utilizan las características magnéticas de los materiales para almacenar datos digitales en forma de unos y ceros. Se usan a gran escala y la principal ventaja que tienen es que permiten almacenar mucha información. Entre ellos están los antiguos disquetes, los discos duros y las cintas magnéticas.
- **Medios ópticos**: en estos dispositivos, tanto el almacenamiento como la lectura de la información se lleva a cabo con un rayo láser de alta precisión. En el almacenamiento de los datos se necesita de un material específico cuya superficie permite que se marquen surcos que representan los unos y ceros del código binario. Este tipo de dispositivo es el más utilizado para el almacenamiento de datos multimedia. Algunos ejemplos son el CD, el DVD o el Blu-ray.
- **Medios electrónicos o memorias de estado sólido**: estos dispositivos son los más novedosos y muy comunes en la actualidad. Se emplean circuitos electrónicos para el almacenamiento de los datos, por lo que no necesitan movimiento para realizar su cometido. El almacenamiento se realiza a través de los chips que lo componen, en los cuales existe una diminuta capa de óxido que va representando 1 cuando está cargada y 0 cuando no. Entre estos dispositivos está la memoria *flash USB*, la tarjeta de memoria o el disco duro SSD.
- **Otros**: entre el resto de los dispositivos podemos destacar las memorias híbridas (que combinan unidades magnéticas con memorias *flash*) o los discos magneto-ópticos (que combinan la forma magnética con el rayo láser).

2.2.2. Operaciones que se pueden realizar

Dependiendo de la operación que podamos realizar, los dispositivos se diferencian entre *solo lectura* o *lectura/escritura*:

- **Reutilizables o regrabables**: pueden usarse más de una vez, ya que es posible tanto almacenar la información como leerla. Actualmente, en el mercado existen memorias *flash USB*, CD-RW y discos duros tanto magnéticos como con tecnologías *flash*.

- **No reutilizable o de solo lectura**: una vez grabada la información no es posible modificarla, únicamente leerla. Es el caso de los CD y los DVD. Toda memoria que sea de tecnología ROM será de solo lectura, ya que viene escrita de fábrica.



2.2.3. Acceso a la información

- **Secuencial**: no es posible acceder a un dato sin leer o escribir los anteriores. Es lo que sucede, por ejemplo, en una cinta magnética la lectura y escritura y al grabar un CD.
- **Directo**: el acceso a cualquier dato es prácticamente inmediato y no es necesario acceder a todos los archivos para leer uno. Es lo que sucede, por ejemplo, con la lectura de un CD, un disco duro o una memoria USB.

2.2.4. Ubicación de la unidad

La localización del dispositivo también determina su clasificación:

- **Interna**: se encuentra en el interior de la carcasa del equipo, está conectado directamente a la placa y se gestiona por el propio ordenador. Son, por ejemplo, los discos duros y las unidades de CD.
- **Externa**: se ubica fuera de la carcasa y, por lo tanto, la información sale del sistema. Actualmente, hay dos tipos de dispositivos externos:
  - Los elementos que realmente están **fuera de la carcasa**, pero que el usuario puede gestionar físicamente porque los controla él mismo. Es el caso de las memorias USB, los discos duros externos y las unidades lectoras de DVD y CD externas.
  - Los dispositivos de almacenamiento que se ubican en **otro lugar del mundo** y que, por tanto, no podemos controlar. Estos son los llamados **dispositivos en la nube**, en los cuales se guarda información sensible en servidores de almacenamiento localizados a kilómetros de nosotros.

    Estos servidores remotos los gestionan empresas externas que ofrecen hueco en sus instalaciones para que nuestros datos no nos ocupen espacio. Su servicio puede ser de pago o gratuito, de lo cual depende tener más o menos facilidades como espacio, velocidad de transmisión o límite diario de carga.

    No obstante, el inconveniente de estos servicios es que la ubicación de nuestros datos es totalmente desconocida, por lo que hay que depositar nuestra confianza

en estas empresas. Además, las compañías de *cloud* pública disponen de internet para su acceso y gestión, mientras que el *cloud* privado suministra acceso a una red privada (VPN) con una mayor seguridad y restricción en el acceso. Algunas de estas empresas son Google, SkyDrive, Dropbox y Windows OneDrive.

Cuando el volumen de almacenamiento de los datos va al alza, necesitamos tener dispositivos de **almacenamiento masivo**. Para solucionar esta necesidad hay distintas opciones:

- Podemos adquirir más **almacenamiento interno** (discos duros internos), pero para ello tendremos que realizar tareas de gestión y necesitaremos espacio en la carcasa.
- Otra opción es adquirir **dispositivos de almacenamiento masivo externo** como, por ejemplo, discos duros externos. También es posible comprar de servidores nuevos. A un conjunto de servidores que trabajan de forma conjunta se le denomina **granja de servidores**. Sin embargo, si no se realiza con una buena gestión del almacenamiento, esta solución puede llegar a empeorar el problema.
- Los **servicios de almacenamiento remotos** también son otra opción. En este caso, son empresas externas las que proporcionan el espacio necesario. Esta opción la hemos nombrado anteriormente y es la que se denomina **almacenamiento en la nube**. Normalmente, se puede elegir entre una versión gratuita (con menos espacio de almacenamiento) y una versión de pago (con la que puedes elegir el espacio según tu demanda). En ocasiones, este almacenamiento en la nube se suele utilizar para respaldar los datos de un equipo físico.

Una buena solución para no empeorar el problema del almacenamiento cuando no se lleva una buena gestión es usar las tecnologías NAS y SAN, que explicamos a continuación:

- ***Network attached storage*** (**NAS**): permite su acceso desde la red y amplia la capacidad del sistema sin necesidad de cambiar alguna configuración en el sistema. Estos dispositivos se acceden a través de los protocolos TCP/IP, por lo que están diseñados para que todos los clientes de la red puedan entrar al dispositivo de almacenamiento auxiliar. No obstante, además del dispositivo físico necesitamos también el software necesario para crear sistemas NAS, como puede ser el FreeNAS, que transforma cualquier equipo en un servidor de almacenamientos NAS.
- ***Storage area network*** (**SAN**): proporciona el acceso de varios servidores a diversos dispositivos de almacenamiento en una red compartida. Esta tecnología de almacenamiento crea una red específica para almacenar los datos, y es complementaria. De manera remota, las aplicaciones solicitan datos directamente al sistema de ficheros. Se emplean diferentes protocolos de acceso como el *fibre channel* y el *gigabit ethernet*. Es lo contrario a la tecnología NAS. Al ser una red de ordenadores complementaria, el rendimiento de esta tecnología está directamente relacionado con el tipo de red, lo que permite disponer de miles de TB si la red lo permite.

Una SAN posibilita que se compartan datos entre varios equipos de la red sin perjudicar al rendimiento debido a que el tráfico SAN se encuentra completamente separado del tráfico de usuarios (son servidores de aplicaciones). Al ser una red complementaria a la que los usuarios utilizan, mantener una red SAN es mucho más costoso que una NAS.

Almacenamiento SAN.

Conexión entre soporte y unidad

Es posible agrupar los dispositivos en tres grupos dependiendo de la **conexión** que se efectúa entre el soporte y la unidad:

- **Removibles**: el soporte que almacena la información se puede cambiar, de forma que la unidad lectora-grabadora permanece. Como ejemplos de dispositivos removibles tenemos los CD y DVD.
- **No removibles**: aquellos en los que el soporte (donde está almacenada la información) y la unidad lectora-grabadora están juntos. Son, por ejemplo, los discos duros y las memorias USB.
- **Otros**: hay otro tipo de dispositivos que no se pueden definir como removibles o no removibles. Entre ellos está el almacenamiento en la nube. Aunque la información de la nube se almacena en servidores, para nosotros el proceso es invisible y nos desvinculamos de ellos confiando en la empresa externa.

2.3. Tecnologías de almacenamiento redundante y distribuido

Uno de los factores que hay que tener presente para un almacenamiento seguro es la **disponibilidad** de la información. Al crear duplicados exactos es posible recuperar los datos en el caso de pérdidas.

Existen dos tipos de sistemas destacables en este apartado: los **sistemas RAID** de almacenamiento redundante y los **sistemas distribuidos** o centros de respaldo con sincronización de datos.

RAID

Las siglas **RAID** (*Redundant arrays of independent disks*) refieren la utilización de varios discos de almacenamiento en los cuales se distribuyen los datos y las copias de seguridad de una forma específica. De esta forma, se mejora el rendimiento de los datos y la seguridad ante cualquier incidente.

Los RAID ofrecen una **mayor integridad**, **tolerancia a fallos**, **rendimiento y capacidad**. Este sistema de almacenamiento es la combinación de varios discos duros en una sola unidad lógica. De este modo, no se dificulta el proceso porque el sistema no detecta que hay varios. Normalmente, los RAID se instalan en el servidor, ya que es donde se almacenan los datos de la red y se centralizan todas las operaciones de la red. Debido al coste de los dispositivos de los discos duros y a la disponibilidad de los datos, es muy frecuente su utilización en empresas, si las características de la placa base lo permiten.

Además, los RAID son una opción que presentan también los ordenadores personales más avanzados, habitualmente en los equipos que se dedican a tareas intensivas de almacenamiento como la edición de audio y vídeo.

La gestión de los datos en los discos duros se puede llevar a cabo mediante software o hardware o ambos, llamados híbridos:

- Cuando la **implementación** se realiza con **software**, el sistema operativo gestiona los discos mediante una controladora de disco normal. Esta forma es más lenta, pero ofrece un rendimiento mayor en los procesadores porque deja más tiempo de proceso a las demás tareas del sistema.
- La implementación de RAID **basada en hardware** necesita como mínimo una controladora RAID (ya sea dedicada o integrada en la placa base). La controladora que se instala como una tarjeta de expansión será la encargada de gestionar las operaciones de los discos y efectuar los cálculos de paridad. Las ventajas de este tipo de implementación es que su rendimiento normalmente es mayor y que el soporte del sistema operativo resulta más sencillo. Además, por lo general soportan una **sustitución en caliente**, posibilitando que los discos que fallen puedan ser sustituidos sin que haya que detener el sistema. Asimismo, si la caja no entra en el equipo debido a su tamaño, es posible instalar la controladora en cajas externas. En ocasiones, el sistema RAID es completamente autónomo y se conecta al sistema como NAS.
- Los **RAID híbridos** se han vuelto muy populares al emplear la controladora de un disco duro normal de un equipo con una aplicación de bajo nivel, que posibilita que los usuarios construyan RAID controlados por la BIOS. La desventaja de los RAID por software es que necesitan reconstruir el conjunto de discos RAID todas las veces que el sistema se reinicia después de un fallo, con el fin de garantizar la integridad de los datos. Por el contrario, los sistemas gestionados por software son mucho más flexibles, por lo que permiten construir RAID a partir de participaciones o incluso agrupar en un mismo RAID discos que están conectados en varias computadoras.

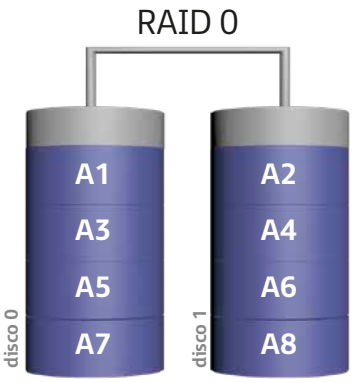
Cabe mencionar que todas las implementaciones son capaces de soportar el uso de uno o más discos de reserva (unidades instaladas que pueden desmontarse inmediatamente tras el fallo de un disco RAID), reduciendo el tiempo de reparación al acortar el tiempo de reconstrucción del RAID.

Las **configuraciones RAID** más usados son:

- **RAID 0**: para su implementación se precisan, como mínimo, dos discos. La información se distribuye en bandas o stripes. De esta forma, se puede acceder a los datos de una forma más rápida. Este tipo de RAID no almacena información redundante.

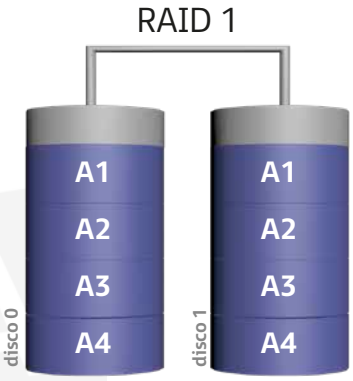
  Se utiliza habitualmente para **aumentar el rendimiento**. Igualmente, es posible usarla para crear un pequeño número de grandes discos virtuales a partir de un gran

número de pequeños discos físicos. La ventaja de esta estructura es que aporta un mejor rendimiento, pero, al no contener información redundante, no suministra ningún tipo de técnicas para asegurar la conservación de los datos en caso de incidente ni presenta tolerancia a fallos.



- **RAID 1** (***disk mirroring***): un RAID 1 también necesita dos discos, pero, a diferencia del RAID anterior, no distribuye la información, sino que elabora una copia o espejo de un conjunto de datos en, al menos, dos discos. Esto es de utilidad cuando el rendimiento en lectura es más importante que la capacidad, pues se incrementa el almacenamiento. La capacidad de un RAID 1 tiene como máximo la capacidad máxima del disco más pequeño. Tiene la ventaja de que la seguridad de los datos se incrementa porque dispone de una copia íntegra en otro disco.

Debido a la doble escritura en ambos discos, esta operación se hace de forma lenta, pero, a su vez, podemos aprovechar la doble situación de la información en varios discos para realizar una operación de lectura en paralelo y simultánea.

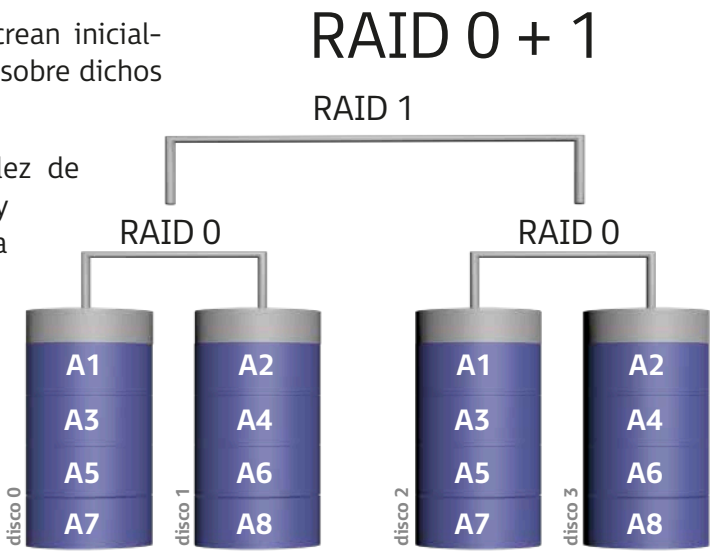


Para aprovechar al máximo los beneficios sobre el rendimiento del RAID 1 es recomendable emplear controladores de disco independientes (una para cada disco). Esta práctica es conocida como *splitting* o *duplexing*.

- **RAID ANIDADOS**: son los sistemas RAID donde se combinan al menos dos niveles diferentes de RAID. El objetivo es obtener un RAID que cuente con las distintas características de diferentes niveles RAID. Los RAID anidados también se llaman RAID híbridos.

Algunos ejemplos de RAID anidados son el RAID 0+1 y el RAID 1+0.

RAID 0+1: en este tipo de RAID se crean inicialmente conjuntos de RAID 0. Después, sobre dichos conjuntos se crea un RAID 1.



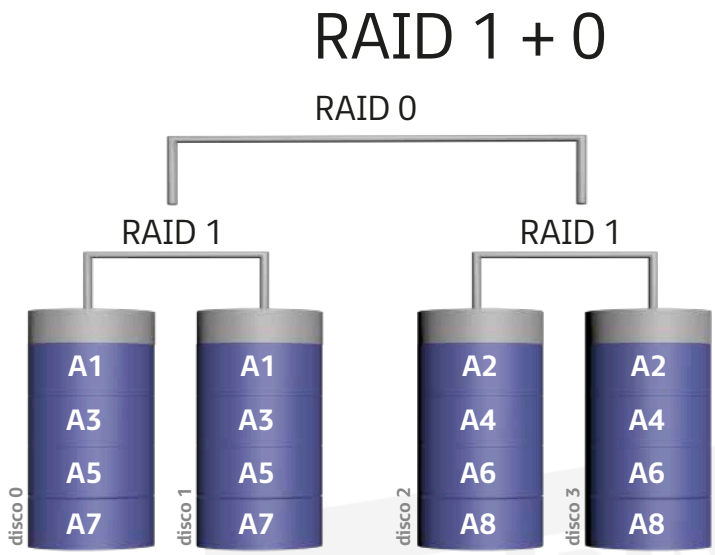
De este modo, conseguimos la rapidez de acceso a datos que nos da el RAID 0 y conseguimos también la redundancia que nos aporta RAID 1.

Si un disco duro falla, los datos perdidos pueden ser copiados del otro conjunto de discos.

Este sistema es poco escalable, dado que si aumentamos un disco en un conjunto, también tendremos que aumentarlo en el resto de conjuntos.

RAID 1+0: también llamado RAID 10, en este tipo de RAID se crean inicialmente conjuntos de discos que funcionan en modo espejo (RAID 1). Y después en un nivel superior se realiza un RAID 0 y por tanto se distribuyen los datos entre los distintos conjuntos de discos

Este sistema RAID 1+0 ofrece mejor tolerancia a fallos y mejor rendimiento que el RAID 0+1. Requiere un mínimo de cuatro discos.



- **RAID 5**: un RAID 5 ofrece un rendimiento similar al RAID 0, pero de forma más económica. Esta opción es, quizás, la más elegida por las empresas. Su funcionamiento se basa en distribuir bloques de información en distintas unidades (repartiendo la información de paridad entre todos los discos miembros del conjunto).

  El RAID 5 permite realizar tanto la lectura como la escritura de forma simultánea. En este caso, se aceleran los pequeños procesos de escritura y, además, la no redundancia de datos de este tipo proporciona una capacidad de almacenaje más elevada que la que ofrecen los RAID 1 y 10. La seguridad de los datos está en la paridad que se usa al reconstruir los datos en caso de avería. Por tanto, esta opción es recomendables para las copias de seguridad. Como desventaja, cabe destacar que se necesita un mínimo de tres discos, aunque lo normal es que sean cinco.

- **RAID 6**: esta opción es similar al RAID 5, pero incluye un sistema adicional de paridad. La ventaja es que este puede utilizarse en caso de que se pierdan los datos, mientras que el inconveniente es que se obtiene un menor almacenamiento al reconstruirse las unidades de forma simultánea.

  Una buena opción para este tipo sería el caso de las unidades SATA de gran capacidad, las cuales pueden permitirse un nivel de rendimiento menor en ciertas ocasiones.

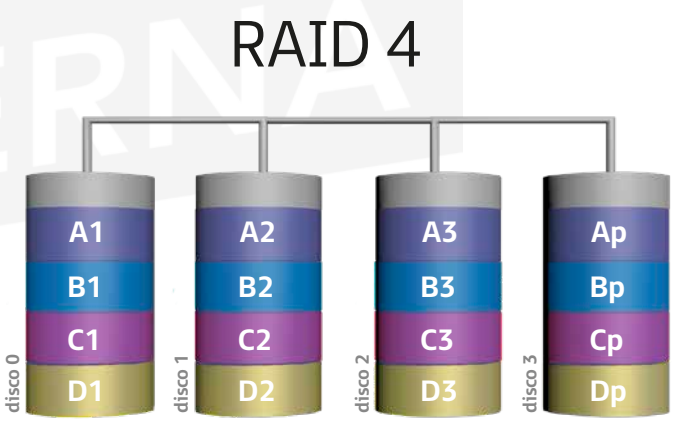
- **RAID 50** (**RAID 5+0** y **RAID 0+5**): es una combinación del RAID 0 y el RAID 5. En este caso, se realiza una distribución idéntica a la del RAID 0, pero en grupos de RAID 5 (disfrutando de la paridad distribuida). Esto mejora el rendimiento respecto al RAID 5, aunque tienen un mayor coste y menos capacidad usable.

  El RAID 50 es una buena opción para las aplicaciones que necesitan un mejor rendimiento (especialmente en la escritura) y tolerancia a fallos.

Otros tipos de RAID, aunque menos relevantes, son los siguientes:

- **RAID 2** separa los datos a nivel de bits en vez de a nivel de bloques y emplea un código de *Hammig* para corregir errores. La controladora sincroniza los discos para funcionar a la par. Este es el único nivel RAID original que no se utiliza en la actualidad. Además, permite tasas de transferencias sumamente altas.
- **RAID 3** utiliza la división a **nivel de bytes** con un disco de paridad dedicado. En realidad, no suele usarse, pues uno de los efectos secundarios es que habitualmente no puede atender varias peticiones simultáneas. Esto es porque, por definición, cualquier bloque simple de datos se dividirá entre todos los miembros del conjunto y dentro de cada uno residirá la misma dirección. De este modo, toda operación de lectura o escritura requiere que se activen todos los discos del conjunto.
- **RAID 4**: esta distribución se utilizó como antesala al RAID 5. Organiza la información a **nivel de bloques** (con un disco de paridad dedicado) y necesita un mínimo de tres discos físicos.

  Su inconveniente es que, en caso de que le ocurra algo al disco de información redundante, el sistema deja de ser seguro porque pierde toda la copia de seguridad que se había realizado. Por esta razón, el RAID 5 aparece después para organizar la información. Aunque también tiene una ventaja, y es que esta estructura permite las peticiones de lectura simultánea porque concentra toda la información redundante en el disco y, al escribir esta información repetida, el proceso se convierte en un cuello de botella del conjunto.



- **Niveles RAID anidados**

Como un avance de las estructuras RAID vistas anteriormente, para seleccionar las ventajas de las estructuras y poder solventar sus inconvenientes, existen muchas controladoras que permiten anidar niveles RAID. De esta forma, se combina la organización de la información conforme a los distintos niveles a los que hace referencia. Por ejemplo, existe el RAID 1+0, que consiste en organizar distintos conjuntos mediante su almacenamiento en un solo disco físico.

- **Centros de respaldo**

También podemos organizar nuestros datos junto con los datos redundantes mediante los denominados **centros de respaldo**, los cuales posibilitan la redundancia y distribución de la información de un CPD (centro de procesamiento de datos) principal en el supuesto de que ocurriera alguna contingencia o fallo.

Este centro de respaldo se ubica a una distancia de unos veinte o cuarenta kilómetros del principal, ya que, ante cualquier incidencia (robo o incendio de la instalación), su proximidad no se ve afectada.

Seguidamente, expondremos el equipamiento electrónico e informático a implantar en este centro, ya que debe ser compatible con el principal para que tengamos una buena comunicación. Esto no implica que tenga que ser exactamente igual. Dependiendo de su equipamiento, hay dos tipos diferentes:

- **Sala blanca**: cuando el centro de respaldo tiene el mismo equipamiento que el principal y, por tanto, se considera equipamiento redundante.
- **Sala *backups***: cuando el equipamiento no es igual pero el funcionamiento es idéntico, ya que solo tiene la función de centro de respaldo.

- **Almacenamiento remoto**

Últimamente ha habido un crecimiento de las posibilidades de almacenamiento, puesto que manejamos mucha información y que la comunicación las redes de computadoras es buena. Hoy en día, existe la posibilidad de acumular esta información en equipos que se encuentran en ubicaciones desconocidas a las que hay que conectarse de forma remota.

2.4. Creación y restauración de copias de seguridad

Para muchas empresas, es de vital importancia la seguridad de los datos que manejan, así que, como medida preventiva, se recomienda realizar una copia de la información almacenada en los discos duros. Gracias a ella, podremos recuperar los datos sin ningún problema ante cualquier futura incidencia.

Según su contenido, podemos diferenciar entre algunas copias de seguridad:

- Un ***backup* completo** elabora una copia de todas las unidades, carpetas y archivos seleccionados, sin tener en cuenta el estado anterior de las copias de seguridad o si ha habido alguna modificación desde la última que se realizó.

  Este es el tipo de copia de seguridad más recomendable para guardar un sistema completo, al menos, una vez por semana. Además, las copias incrementales guardan solo los ficheros modificados o creados desde la última copia incremental efectuada. En este tipo, la primera copia será idéntica a una copia total.

Para reconocer los archivos creados o con cambios se utiliza el *atributo modificado* que poseen los archivos. Este tipo de copia es el que se recomienda para los *backups* más frecuentes (diarios).

- Un ***backup* diferencial** también copia los ficheros que han sido modificados o creados últimamente, pero, en vez de usar como referencia la última copia incremental, utiliza la última copia completa. En este sentido, igual que la primera copia incremental se corresponde con una copia total, la segunda es diferencial. Hay que destacar la rapidez con la que se restaura esta última.

Una vez hemos detallado los tipos de *backups*, el siguiente paso es el **establecimiento de una estrategia** para realizar las copias de seguridad según las necesidades del sistema. Por eso, es importante decidir qué tipos de *backups* y temporalidad se usarán.

Basándonos en esto, debemos razonar las ventajas que aporta en cuanto a la velocidad en la recuperación, la eficiciencia en el proceso y la seguridad en sus datos.

2.5. Programación temporal de copias de seguridad siguiendo esquemas de rotación

Hemos podido comprobar, en apartados anteriores, la importancia de las copias de seguridad. Para adaptar el sistema de copias de seguridad al equipo desde el que lo vamos a realizar, es necesario evaluar las necesidades concretas de seguridad sobre la información que se encuentra almacenada en el ordenador o en la red local, así como establecer la estrategia de copias de seguridad más adecuada en cada caso. De esta forma, es posible plantear una estrategia que tenga en cuenta factores como la importancia de los datos que serán guardados, la periodicidad de la creación de copias o la cantidad de medios (soportes) que se utilizarán y cuándo.

De forma general, si varias veces al día modificamos los documentos con los que trabajamos, se aconseja hacer, por lo menos, una copia al día. Además, en ciertos casos será necesario crear copias de respaldo provisionales en otras unidades de almacenamiento tras unas horas de trabajo.

El tiempo que permanezcan los datos guardados en un soporte determinado (**periodo de retención**) debe estar relacionado con la **importancia de los datos**. Como probablemente el coste de los soportes para copias de seguridad será menor al valor de los datos que contienen, lo aconsejable es emplear varias cintas, que se irán alternando a lo largo de copias sucesivas.

Por otro lado, el **ataque de un virus** en el software puede **influir** en la copia de seguridad. Un virus no tiene por qué manifestarse de manera inmediata, sino que es posible que lo haga después de unos días o semanas. Si se produce esto, la manera más eficaz de solucionarlo es restaurar el sistema y sus datos a un estado anterior más seguro. No obstante, lo más eficaz es tener disponibles, en todo momento, las copias anteriores denominadas de **almacenamiento alternativo**.

También existen otros métodos para hacer copias de seguridad, como el del **esquema de rotación**, que se trata de emplear diferentes soportes para guardar las copias de seguridad. La gestión de la información en cada soporte se hace como nos convenga, ya que el número de dispositivos, la información contenida y la temporalidad dependen del responsable de la seguridad en el sistema.

El máximo nivel de seguridad y de rendimiento de este método puede obtenerse si llevamos un estricto **plan de rotación** entre los distintos dispositivos, tanto en la temporalización como en la información y en los tipos de copias de seguridad. Además, su principal ventaja es que, ante cualquier avería o incidencia en los datos originales y en los dispositivos, tenemos otros para solventar lo más rápido posible el error.

Debemos gestionar el esquema de rotación de tal forma que en todos los dispositivos tengamos una copia de seguridad completa y otras incrementales. También es posible utilizar cada dispositivo para un día de la semana, semanas del mes o meses del año, para que sepamos identificar en cada momento qué datos existen en cada uno y conseguir un moderado ahorro de tiempo.

Una variación del modelo anterior consiste en usar la misma cinta para llevar a cabo las copias incrementales y dejar para las copias completas otro dispositivo. Gracias a ello, se alcanza un nivel de seguridad similar, pues se consigue también un periodo de retención máximo mayor que supone una protección adicional frente a pérdidas masivas de información.

Antes de elegir la técnica que se llevará a cabo para gestionar las copias de seguridad, debemos **decidir de qué manera estará más segura** la información. Dependiendo de las necesidades, evaluamos la ubicación de la información en el sistema, el tipo de sistema, la importancia de los datos, la dificultad de recuperar algún documento concreto, el coste de los medios utilizados o el tiempo necesario para llevarlas a cabo, entre otros aspectos. Además, hay que tener en cuenta que no todos los sistemas informáticos son iguales y, por tanto, no todas las estrategias son adecuadas.

Las **propiedades** para tener en cuenta de una **estrategia de *backups*** son:

- **Periodo de retención**: tiempo que permanece una copia de seguridad en un soporte, sin utilizarse.
- **Protección contra fallos en el soporte**: número de medios usados para llevar a cabo la técnica. A mayor número de dispositivos, menor el riesgo ante una incidencia.
- **Coste**: la partida presupuestaria disponible para llevar a cabo la técnica puede ser un rasgo decisivo.
- **Almacenamiento alternativo**: la posibilidad de guardar en otra ubicación diferente al lugar de trabajo una de las copias durante un tiempo elevado. Es un rasgo que aumenta el nivel de seguridad en el sistema.

En los grandes sistemas informáticos, la seguridad de la información es un aspecto crítico, por lo que el coste asociado al empleo de un gran número de medios de almacenamiento es secundario.

¿SABÍAS QUE...?

Uno de los **esquemas más empleados**, que alcanza un periodo de retención máximo de casi un año, es el que está basado en 19 cintas que se utilizan con una periodicidad semanal (para las copias incrementales) y mensual (en el caso de las totales). También cuenta con cintas guardadas como copias alternativas de respaldo, que se usan aproximadamente una vez al año.

2.6. Realización de copias de seguridad siguiendo diversas estrategias

En el apartado anterior hemos podido conocer una técnica llamada rotatoria, aunque existen otras en el mercado que a continuación detallaremos. Es preciso conocer a fondo las técnicas existentes para poder decidir cuál es la que mejor se ajusta a nuestras necesidades.

Copia de seguridad incremental progresiva

La copia incremental solo realiza la **copia de aquellos datos que se han modificado desde la última copia incremental o completa**. Este proceso es el predeterminado y presenta la ventaja de no realizar copias de seguridad redundante, ya que solo lo hace de los archivos modificados. Como consecuencia, no tiene un gran flujo de utilización de la red porque se transmite solo la información que modifica.

La **eficiencia** y el **ahorro** del espacio son los rasgos más destacados de este tipo de técnica. Además, la recuperación de los archivos no requiere mucho tiempo ni resulta difícil, pues la versión guardada es incremental. Como desventaja, debemos mencionar que, alguna vez en un periodo de tiempo razonable, hay que crear una copia de seguridad completa, algo que no se tiene en cuenta en esta técnica.

Copia de seguridad con registro por diario

También es posible hacer una **copia de seguridad incremental, pero utilizando un diario de cambios**. De esta forma, es posible conocer en un breve periodo de tiempo cuál es el fichero que ha cambiado en el último día, aunque no resuelve la problemática que teníamos en el apartado anterior. Por eso, es recomendable que cada cierto tiempo hagamos una copia de seguridad completa.

Copia de seguridad con eficiencia de memoria

Una de las problemáticas que presentan las técnicas descritas anteriormente es que tienen limitaciones de memoria. Ejecutar un archivo por parte del cliente **permite conocer en todo momento y antes de que empiece la copia si tiene espacio suficiente**, lo que asegura que no habrá ningún tipo de problema. De esta forma, realizar la copia de seguridad es más eficiente.

Copia de seguridad de puntos de montaje virtuales

Los discos virtuales existentes en la red son el destino de almacenamiento de las copias de seguridad. Esto **proporciona una ruta directa a los archivos**, lo que se traduce en un ahorro en el tiempo de procesamiento y en la búsqueda de información.

Los puntos de montaje virtuales están orientados a llevarlo a cabo en grandes empresas, donde se busca un equilibrio entre la división lógica de las particiones.

Copia de seguridad de la lista de archivos

Podemos llevar el control de los datos de los que se hace la copia de seguridad realizando una lista de archivos que hemos modificado. La seguridad selectiva **permite encontrar un archivo determinado en menos tiempo que las anteriores**.

Copia de seguridad de sesión múltiple

Es posible hacer copias de seguridad en diferentes sesiones de forma simultánea, algo para lo que el servidor debe estar preparado. Con esta técnica **aumentamos la eficiencia**, y podemos aplicarla con distintas herramientas que nos facilitarán el proceso. No obstante, cabe destacar que requiere de una persona especializada en la importancia que presenta esta distribución, las versiones de las distintas sesiones, si disponemos de un buen gestor.

2.7. Utilización de soportes de almacenamiento remotos y extraíbles

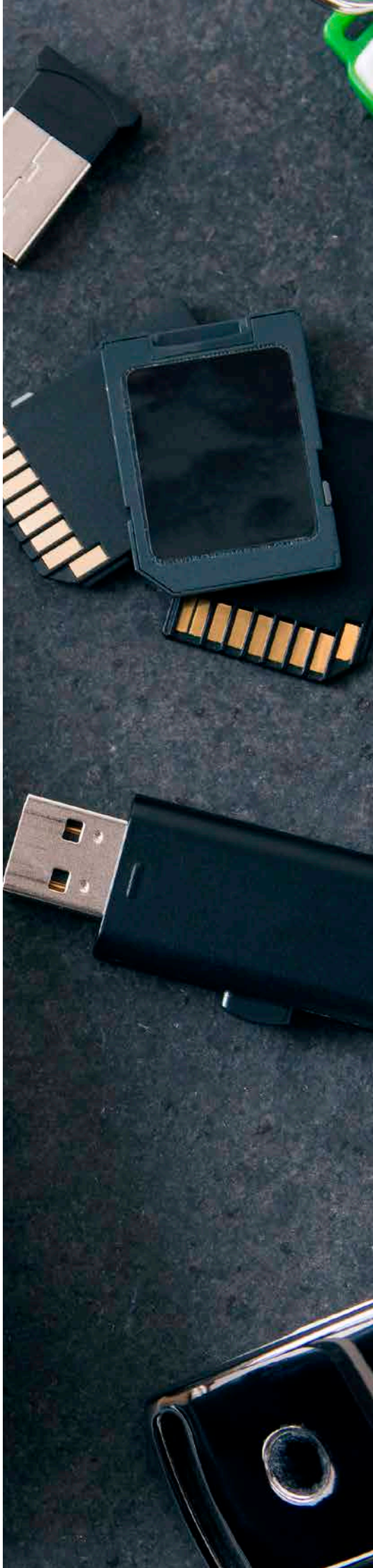
El **soporte** del almacenamiento de datos es el **material físico** donde se almacenan los datos que pueden ser procesados por una computadora. Puede ser un dispositivo electrónico o un sistema informático, aunque este término también abarca el concepto de documento no necesariamente informatizable (papel, cartulina o similar). Algunos de los soportes manejados por ordenadores o similares son los discos magnéticos (disquetes, discos duros), los discos ópticos (CD, DVD, Blu-ray), las cintas magnéticas, los discos magneto-ópticos (discos Zip, Jaz, SuperDisk) y las tarjetas de memoria, entre otros.

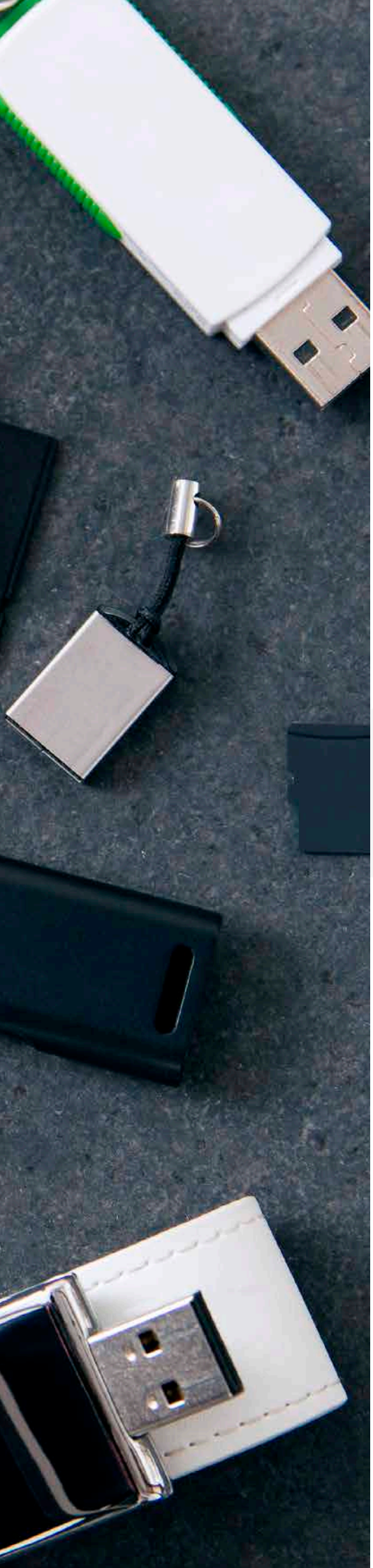
El **objetivo** de los dispositivos de almacenamiento es guardar y recuperar la información de forma automática y eficiente. Realizan tanto la lectura de datos (para su consulta) como su escritura (para almacenar la información deseada).

Los dispositivos mencionados anteriormente pueden considerarse dispositivos de almacenamiento extraíble, pues después de realizar la operación pertinente es posible quitarlos del equipo para guardarlos en un lugar seguro. De esta forma, los podemos asegurar en ubicaciones diferentes, lo que se considera otra medida preventiva más que aplicamos a la seguridad del sistema.

Además, a causa de la evolución tecnológica sufrida en esta época, han surgido otros medios con un concepto novedoso: los **dispositivos remotos**. Están encargados de guardar información, pero su ubicación es desconocida o está fuera de nuestro alcance porque solo podemos acceder a ellos mediante conexión a Internet. Algunos ejemplos de este tipo de almacenamiento en la nube son Dropbox, OneDrive o Google Drive.

Su principal **ventaja** es que, además de guardarse en servidores ubicados fuera de nuestras instalaciones, podemos acceder a ellos desde cualquier equipo que tenga una conexión a internet. No obstante, al estar fuera de nuestro alcance (físicamente hablando), no llevaremos el control de estos servidores, lo que se plantea como una desventaja que hay que tener en cuenta a la hora de decidirnos por este tipo de almacenamiento.





2.8. Aplicación de procedimientos de medida de rendimiento, de verificación y de detección de anomalías

Una vez realizados los distintos tipos de copias de seguridad, aplicaremos el procedimiento para tener en cuenta los **indicadores de rendimiento**, **verificación** y **detección** de anomalías.

En este caso, veremos los pasos a seguir para realizar un proceso óptimo de copias de seguridad. Ya que hemos visto los distintos tipos que existen de estas, los combinaremos para mejorar el rendimiento. Haremos copias de seguridad completas cada cierto tiempo y, entre cada una de ellas, realizaremos incrementales. Este es un proceso muy eficiente y con un rendimiento muy alto.

- Como medida preventiva, haremos un *planning* para gestionar el control de las copias de seguridad.
- Verificaremos los datos contenidos en las copias y nos aseguraremos de que aquellos que se encuentran tanto en las copias completas como en las incrementales son los necesarios para asegurar nuestro sistema.
- Podemos detectar las pertinentes anomalías en este proceso de verificación. Así, buscaremos solución antes de que ocurra un altercado y podremos prevenir las incidencias, por lo que nuestro sistema será mucho más seguro.

2.9. Custodia de los soportes de almacenamiento

Debido a la gran cantidad de información que maneja la empresa, no deja de aumentar la importancia de la gestión de esos datos en un entorno cada vez más exigente.

Actualmente, existen herramientas y compañías dedicadas a la custodia y al almacenamiento de datos de forma segura. Cuando se externaliza este servicio es posible ahorrar determinados costes pues, según las necesidades, pueden ser bastante elevados. De esta forma, se libera a la empresa o individuo del mantenimiento de su documentación.

Al contratar este servicio, lo primero que se realiza es un inventario de toda la documentación que se va a almacenar, la cual será transportada en vehículos hasta los **centros de custodia** y se guardará según el protocolo interno de la empresa pertinente.