Seguridad Pasiva: Almacenamiento

Tema 4

Álvaro Rodríguez - IES Alonso de Madrigal (Ávila)
2° SMR

Seguridad Pasiva: Almacenamiento

INTRODUCCIÓN

Algunos contenidos que veremos en este tema serán:

- Estrategias de almacenamiento: Sistemas de almacenamiento y su seguridad
  - Dispositivos de almacenamiento
  - Sistemas de almacenamiento lógico
    - *Ficheros y sus metadatos*
    - *Sistemas de Ficheros*
  - Recuperación de datos borrados
- Integridad y Disponibilidad de los datos:
  - Copias de Seguridad
    - *Almacenamiento en red: NAS y SAN.*
  - Imágenes del sistema.
  - Sistemas RAID
- Registro de Windows y puntos de recuperación.
- Herramientas de chequeo de discos.

Seguridad Pasiva: Almacenamiento

EL ALMACENAMIENTO DE DATOS

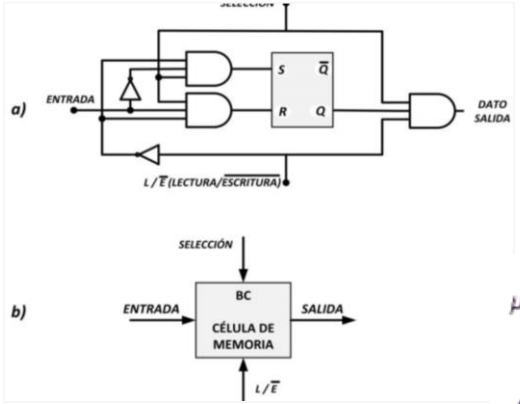
Los datos son un elemento crucial con respecto a la seguridad informática. Los datos que almacenamos requieren de:

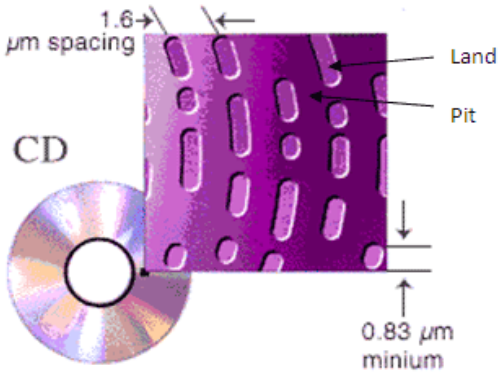
- Confidencialidad: que sean accedidos sólo por las entidades permitidas
- Integridad: que no se modifiquen ni eliminen sin que lo queramos
- Disponibilidad: que no se borren o que tengamos acceso ellos incluso ante fallos del propio dispositivo de almacenamiento

Para entender todos estos ámbitos de la seguridad con respecto al almacenamiento de datos debemos estudiar bien cómo son los datos digitalmente a todos los niveles: desde el nivel más bajo, donde se almacenan físicamente en un dispositivo, hasta el nivel más alto de abstracción, donde un usuario los utiliza a través de una aplicación

Seguridad Pasiva: Almacenamiento

EL ALMACENAMIENTO DE DATOS

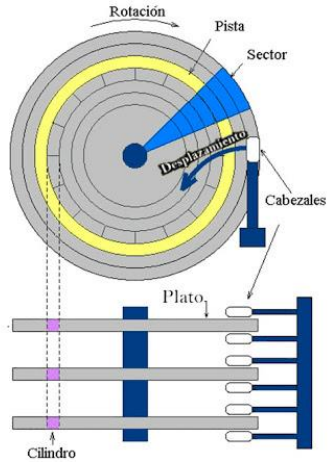




Los datos digitales son bits. Valores 0 o 1 que se almacenan en un dispositivo de almacenamiento concreto.

Por ejemplo:

- En un pendrive: cada bit será un valor de voltaje almacenado en celdas electrónicas
- En un CD o DVD: cada bit se representa en función de las muescas que reflejan o no la luz de un láser
- En un disco magnético: cada bit se representa por un valor de voltaje almacenado en una porción minúscula del disco magnético



Seguridad Pasiva: Equipos

ACTIVIDAD

- Instala en linux un visor hexadecimal de ficheros:

```
sudo apt-get update
sudo apt-get install ghex
```

- Crea un fichero de texto con nano y léelo con ghex
  - ¿Por qué aparecen esos valores hexadecimales ?
  - ¿Qué pasa si cambias un bit?
- Bájate una imagen de internet y lee el archivo con ghex
  - ¿Aparece algo legible?

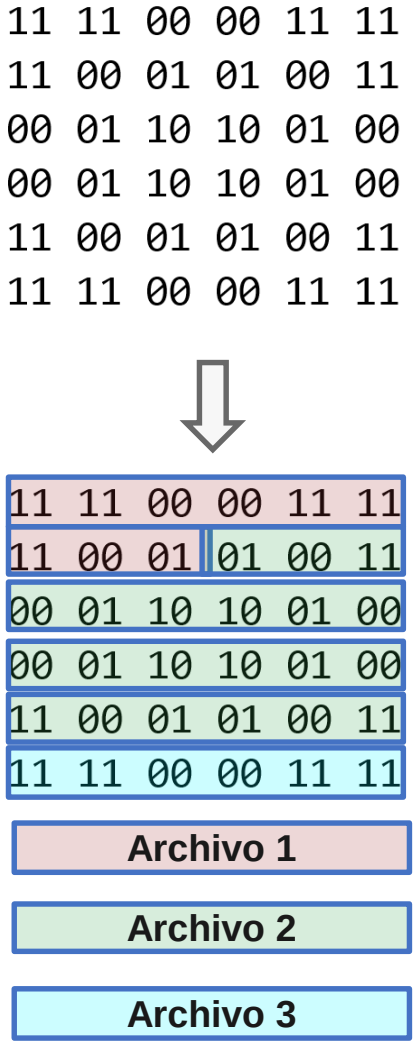
Seguridad Pasiva: Almacenamiento

EL ALMACENAMIENTO DE DATOS

Para que un ordenador pueda acceder fácilmente a los datos se utilizan estructuras, creadas para tal fin. Si no, sería muy difícil saber dónde empieza un dato y acaba otro dentro del disco.

Esas estructuras son:

- Ficheros: encapsulan la información en función del tipo de datos, de aplicación que los va a usar, etc. Permiten tratar varios datos como una sola unidad de información.
- Sistemas de Ficheros: El sistema operativo necesita un sistema mediante el cual ubicar los ficheros, que optimice el espacio del dispositivo al mismo tiempo que permite un acceso a los datos rápido, eficaz y confiable.
- Directorios: A nivel de usuario, el sistema operativo lo que pone a su disposición no es el sistema de ficheros en sí, sino que crea una estructura de directorios para facilitar el acceso.
- Bases de Datos: son estructuras más complejas que permite organizar, dar acceso y controlar mucho mejor los datos que almacenamos



Seguridad Pasiva: Almacenamiento

FICHEROS

Son estructuras que permiten almacenar datos de manera persistente. Suelen estar asociados a un tipo de aplicación, lo cual se indica con la extensión del archivo (usado en Windows) o con sus primeros valores (magic numbers, usado en Linux).

Por ejemplo, un archivo con extensión .jpg Windows lo asocia a que puede abrirlo un intérprete de imágenes digitales.

En Linux para saber el tipo de fichero que es se utilizan los magic numbers. Por ejemplo, para JPEG "FFD8"

Sin embargo, la extensión es fácilmente modificable. La mejor manera que tienen los ficheros de indicar qué datos contiene son los metadatos.

Los metadatos (datos sobre sí mismo) guardan mucha información sobre el propio fichero

Seguridad Pasiva: Equipos

ACTIVIDAD

Busca un fichero con extensión .doc en un buscador (utiliza Google Dorks)

- Analiza qué metadatos se han almacenado sobre el archivo
- ¿Qué problemas crees que pueden derivar del almacenamiento de metadatos?
- ¿Crees que es buena idea tener este tipo de archivos, conteniendo metadatos, disponibles en internet?
- Busca la manera de borrar los metadatos con exiftool

Comprueba que metadatos se guardan en las imágenes de servicios web (apps) de fotografía:

Flickr
VSCO
Picsart

- Intenta bajarte algunas imágenes **en tamaño original**
- Utiliza el programa exiftool para descubrir sus metadatos.
- ¿Qué metadatos has encontrado?
- ¿Crees que los usuarios de esta aplicación son conscientes de que con su foto suben también estos datos?

Seguridad Pasiva: Almacenamiento

SISTEMAS DE FICHEROS

Son el mecanismo que tienen los SO para gestionar los ficheros en un dispositivo de almacenamiento.
Oculta al usuario y a las aplicaciones detalles sobre el almacenamiento físico de los datos, dando la impresión de trabajar con ficheros distribuidos en un árbol de directorios.

Cada dispositivo de almacenamiento ➡ Formateado según un sistema de ficheros
Define la estructura del dispositivo, los sistemas de localización de archivos, etc.

- NTFS y FAT : Microsoft Windows
- HFS+ y Apple File System (APFS) en Apple
- Ext2, Ext3 y Ext4 en Linux

Seguridad Pasiva: Almacenamiento

SISTEMAS DE FICHEROS

La seguridad informática debe tener en cuenta los sistemas de ficheros. Esto le va a permitir atender a:

- Disponibilidad de los datos en función de compatibilidades SO-Sistema de Archivos
- Control de acceso a ficheros: Nombres de usuario, grupos, permisos, etc.
- Sistemas de cifrado propios de los sistemas de archivos
- Sistemas de borrado de archivos

Seguridad Pasiva: Almacenamiento

ACTIVIDAD

No todos los sistemas de ficheros son legibles en según qué sistemas operativos. Rellena la siguiente tabla:

Sistema de ficheros	Creador	En Windows	En Mac	En Linux	Otros compatibles	Otros no compatibles
FAT32						
NTFS						
ExFAT						
HFS+						
APFS						
EXT4						

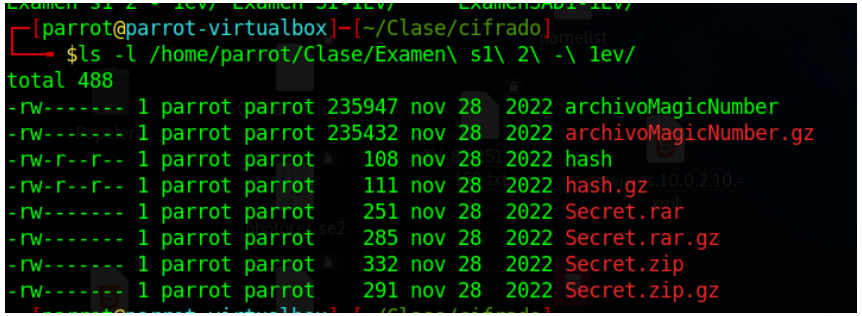
Seguridad Pasiva: Almacenamiento

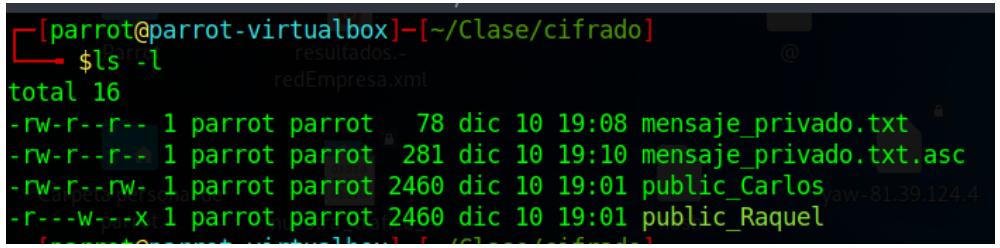
SISTEMAS DE FICHEROS: CONTROL DE ACCESO

Podemos comprobar el **propietario** y los **permisos** de un archivo o de un directorio lanzando ls –l sobre la ruta elegida.

***ls** –l ruta_a_directorio_o_archivo*

Si no le indicamos una ruta mostrará los archivos y directorios del directorio actual



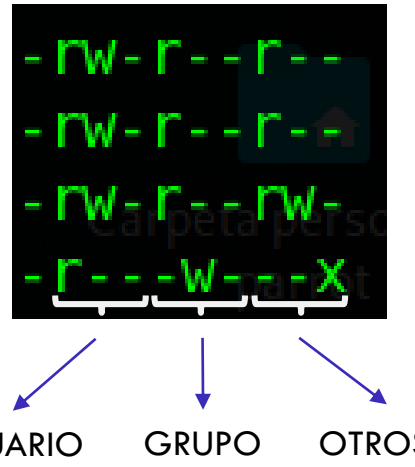


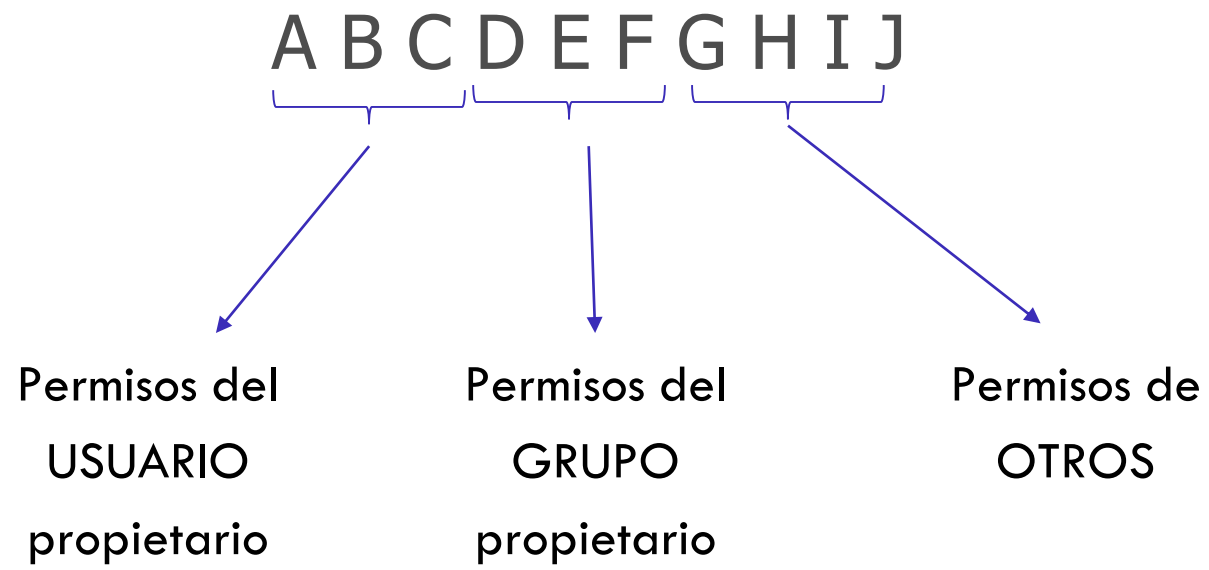
Seguridad Pasiva: Almacenamiento

PERMISOS DE FICHEROS Y DIRECTORIOS

Los accesos a los ficheros vienen descritos por en bloque de símbolos

Los permisos solo los pueden cambiar: **el usuario propietario del fichero** y **root**





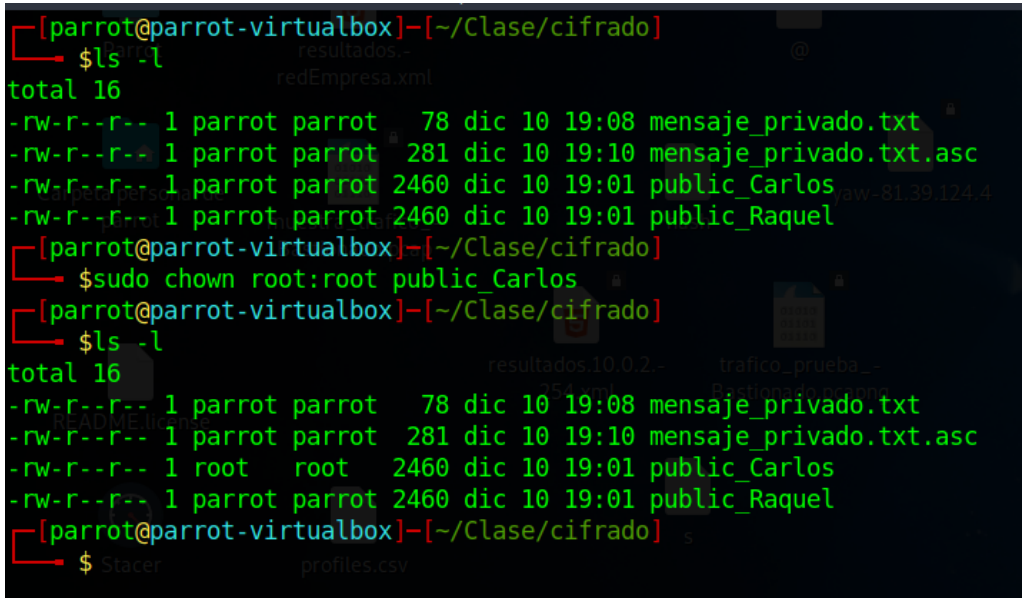
Seguridad Pasiva: Almacenamiento

PERMISOS DE FICHEROS Y DIRECTORIOS

Herramienta **chown:**

Con este comando podrás modificar el propietario y grupo propietario de un archivo.

chown *nuevo-propietario:nuevo-grupo ruta_al_fichero*



Seguridad Pasiva: Almacenamiento

PERMISOS DE FICHEROS Y DIRECTORIOS

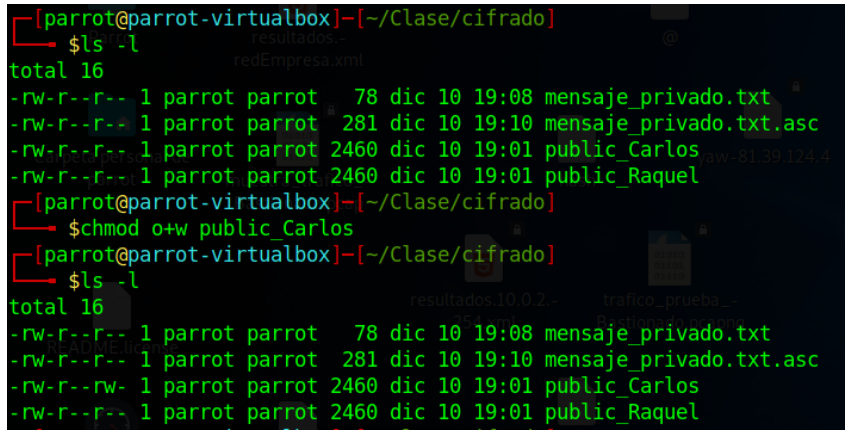
Herramienta **chmod**

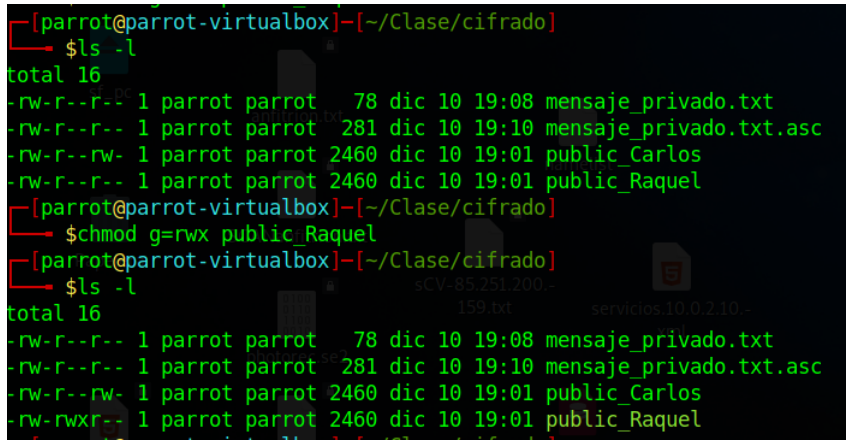
Se utiliza para cambiar cualquier permiso de los ficheros a cualquier usuario del mismo. Se puede utilizar de varias formas:

Opción 1:

chmod [-R] [ugoa]{+|-|=}[rwx] archivo

-R: Recursivo (para directorios)
-u : usuario propietario
-g : grupo propietario
-o : otros
-a : todos
+ - = →Dar, quitar o asignar permisos





Seguridad Pasiva: Almacenamiento

PERMISOS DE FICHEROS Y DIRECTORIOS

Opción 2:

Utilización “chmod” en modo numérico.

Chmod NNN

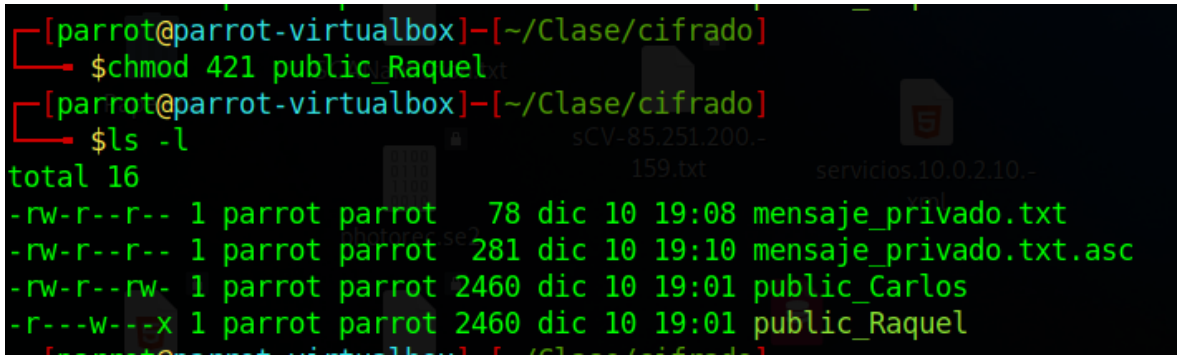
- Cada N se refiere a usuario, grupo y resto.
- Se usa nomenclatura octal (0-7)
- Cuando un permiso está activa se codifica con 1, en caso contrario con 0.

Ejemplo: Damos :

- Al usuario propietario sólo permiso de lectura
- Al grupo propietario sólo permiso de escritura
- A Otros sólo permiso de ejecución

d	r--	-w-	--x
	100	010	001

La orden sería → chmod 421

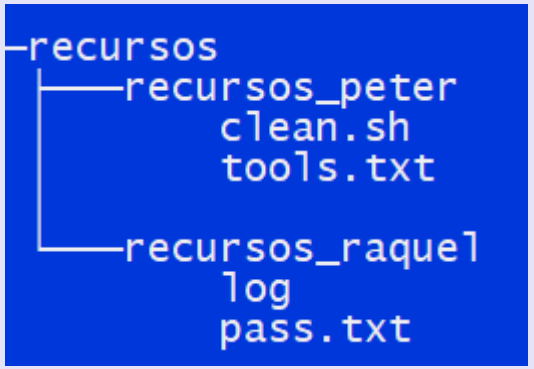


Seguridad Pasiva: Equipos

ACTIVIDAD

1. Cambio de permisos sobre directorios y archivos

- Crea los usuarios peter y raquel
- Crea con tu usuario habitual la siguiente estructura de directorios y archivos sobre el directorio /tmp
- Cambia los permisos y propietarios para que tengan las siguientes características
  - El propietario de la carpeta recursos_peter y los archivos en su interior debe ser peter
  - El propietario de la carpeta recursos_raquel y los archivos en su interior debe ser raquel
  - Peter debe poder escribir sobre “log”, pero no leerlo ni ejecutarlo
  - Peter no debe tener ningún permiso sobre pass.txt
  - Peter debe poder leer, escribir y ejecutar clean.sh
  - Raquel no debería modificar ni leer el contenido de clean.sh



2. Investigación
   - ¿Qué son los permisos SUID?
   - Encuentra un método para buscar en tu máquina archivo con el permiso SUID. ¿Qué archivos tienen ese permiso en ella?
   - ¿Por qué esos archivos tienen esa propiedad?
   - ¿Cómo se añade/quita el permiso SUID a un archivo?

Seguridad Pasiva: Almacenamiento

SISTEMAS DE FICHEROS: BORRADO DE ARCHIVOS

¿Cómo se borran los datos en un dispositivo de almacenamiento?

- Marcando el espacio que ocupa el archivo como bits libres: en los que se podrá escribir información nueva
- No "borra" literalmente el dato, ya que sigue estando escrito
- Para borrar un dato definitivamente es necesario sobrescribir cada byte de información que ocupaba

¿Y el formateo del dispositivo? ¿Borra los datos?

Seguridad Pasiva: Almacenamiento

ACTIVIDAD

1. Debes llevar a la práctica el borrado y recuperación de archivos en dos de tus máquinas virtuales:
   - LINUX: Utilizando testdisk (+ info aquí)
   - WINDOWS: Utilizando Recuva

Utiliza para ello cualquier archivo: un pdf, una imagen, un documento de texto...

2. Busca alguna aplicación con la que conseguir esto en tu teléfono móvil.

Seguridad Pasiva: Almacenamiento

COPIAS DE SEGURIDAD

Existen diferentes sistemas que van a permitir hacer copias de seguridad de los datos:

- Realizar copias manual o automáticamente
  - En dispositivos de almacenamiento diferente
  - En lugares dispares

Ventajas del almacenamiento en la nube

- Utilizar una aplicación que gestione las copias de seguridad

Se suele recomendar la estrategia 3-2-1: **3** copias diferentes, en **2** soportes de almacenamiento diferentes y al menos **1** de ellas fuera de la empresa (normalmente en la nube)

Seguridad Pasiva: Almacenamiento

COPIAS DE SEGURIDAD

Dispositivos usados para realizar las copias:

- Cintas magnéticas: a pesar de parecer un sistema obsoleto, se siguen usado debido a su gran durabilidad, muy superior a la del resto de sistemas. Además, son soportes baratos.
- Discos magnéticos o de estado sólido (HDD o SSD): grandes velocidades y tamaño de datos combinando varios discos.

Menos utilizados, los discos ópticos o las memorias flash, con poca capacidad y cada vez más en desuso.


MCPRO

NOTICIAS A FONDO ENTREVISTAS OPINIÓN EVENTOS RECURSOS TODOS LOS ARTÍCULOS | DESCARGA LA

OPINIÓN

Almacenamiento de datos: porqué la cinta es más necesaria que nunca

Publicado el 2 agosto, 2015 por RedaccionMCP

Ignacio Chico, director general de Iron Mountain.

La cinta magnética se usó por vez primera para almacenar datos informáticos en 1951. A mediados de los 70 casi todo el mundo confiaba en cartuchos y cassettes de cintas. Con la

https://www.muycomputerpro.com/2015/08/02/almacenamiento-datos-cinta

Seguridad Pasiva: Almacenamiento

COPIAS DE SEGURIDAD

Automatización de copias de seguridad:

- Con procedimientos del Sistema Operativo
  - Scripts de comandos
  - Servicios del propio sistema

- Con aplicaciones externas
  - Ejemplos: **Genie TimeLine,** EaseUS Todo Backup...
  - Ejemplos de backup en la nube: **OneDrive de Microsoft,** box... O a nivel empresarial Azure Backup, AWS Backup….

Seguridad Pasiva: Almacenamiento

COPIAS DE SEGURIDAD

Las copias de seguridad deben gestionarse de una manera formal, para asegurar que existe copia de los datos importantes y que están debidamente actualizados.

Para ello será esencial:

1. Planificar las copias de seguridad: indicando cada cuanto tiempo y dónde se harán las copias
2. Encontrar los métodos oportunos
   - Diferente granularidad
     - Copias completas
     - Copias diferenciales: se copian solo los datos modificados desde que se hizo la última completa
     - Copias incrementales: se hace copia de los datos modificados desde la última (ya sea completa, diferencial o incremental)
   - Por operatividad del sistema
     - En frio: los datos a copiar no se usan durante la copia
     - En caliente : los datos a copiar siguen siendo usados durante la copia.
3. Determinar qué copiar

Seguridad Pasiva: Equipos

ACTIVIDAD

Automatiza la copia de seguridad de una carpeta importante en tu propio disco duro, por ejemplo, tu carpeta de usuario. La copia debe realizarse a un dispositivo externo:

En Linux: con crontab y un script en bash. La copia debe hacerse cada día a las 14:40

En Windows: https://www.xataka.com/basics/copias-seguridad-windows-10-sirven-que-tipos-hay-como-se-hacen

> ¿Podría hacerse también con un script como has hecho para Linux? Explica teóricamente como lo harías.

Recursos:

https://geekflare.com/es/crontab-linux-with-real-time-examples-and-tools/
https://blog.desdelinux.net/cron-crontab-explicados/

Seguridad Pasiva: Almacenamiento

IMÁGENES DE SISTEMA

Las imágenes del sistema nos permiten recuperar todo el sistema a un punto anterior en el que el comportamiento era estable.

Aunque en la práctica se utiliza en muchas ocasiones para hacer una reinstalación del sistema operativo:

- **Completa**: ya que permite copiar una imagen con aplicaciones ya instaladas y con configuraciones para las aplicaciones y el sistema ya optimizados
- **Rápida**: por medio de un proceso automático y más fácil.

La copia de la imagen del sistema no es un método útil para la copia de datos de una empresa u organización:

- Copia tanto datos como programas, lo cual no es siempre interesante
- El proceso de copia es lento y detiene el comportamiento normal del sistema, por lo que no es recomendable hacerlo periódicamente.

Seguridad Pasiva: Almacenamiento

CONGELACIÓN DE SISTEMA

En algunas ocasiones conviene llevar a cabo la congelación del sistema.

Cuando los ordenadores suelen tener diversos usuarios y no se quiere guardar la información que éste genera para posteriores usos del ordenador, el sistema se congela antes de que el usuario comience a usarlo, de modo que al finalizar, el sistema vuelva por completo al punto anterior.

Esto permite que no se almacenen datos personales como el historial de Internet, las cookies, archivos temporales generados por las distintas, aplicaciones, cambios en el registro, etc.

El principal inconveniente de esta solución aparece cuando queremos instalar un programa nuevo y la dificultad para actualización de parches de aplicaciones y del propio sistema operativo.

Ejemplos de software: Reboot Resore RX, Deep Freeze...

Seguridad Pasiva: Almacenamiento

IMÁGENES DE SISTEMA

Habitualmente se utiliza software dedicado a la creación de imágenes de sistema: Norton Ghost, Acronis True Image...

Tienen el inconveniente de que para recuperar la copia necesitas ese mismo programa (a veces incluso la misma versión)

Soluciones recomendadas:

- Uso de LiveCd con Linux para la copia y recuperación de la imagen del sistema. Clonezilla, DRBL...
- Uso de herramientas de copia y recuperación en red. Ejemplo: FOG
- Uso de máquinas virtuales y la gestión de **instantáneas** del sistema virtualizado

Seguridad Pasiva: Almacenamiento

PUNTOS DE RESTAURACIÓN EN WINDOWS

Los sistemas Windows incluyen una funcionalidad similar al software de congelación del apartado anterior: se llaman puntos de restauración y recogen el **estado de los ejecutables** y la **configuración del sistema operativo** (no se incluyen los documentos de los usuarios).

Es importante crear un punto de restauración antes de efectuar cambios importantes en el sistema, como la instalación o sustitución de drivers o la aplicación de parches. De hecho, las actualizaciones automáticas de Windows siempre crean primero un punto de restauración

Si el cambio solo afecta a la configuración, entonces nos podemos limitar a proteger el registro. El registro es una base de datos interna donde el sistema operativo y las aplicaciones anotan información de configuración

Seguridad Pasiva: Equipos

ACTIVIDAD

Realiza en una de tus máquinas virtuales de Windows:

- La comprobación de puntos de restauración existentes en el sistema y la creación de uno para el momento actual.

Seguridad Pasiva: Almacenamiento

SISTEMAS RAID

El nombre son las siglas de *Redundant Array of Independent Disks* o *Matriz redundante de discos independientes*, y es un método para **combinar los discos duros como un matriz que se reconoce** como una sola unidad por el sistema operativo.

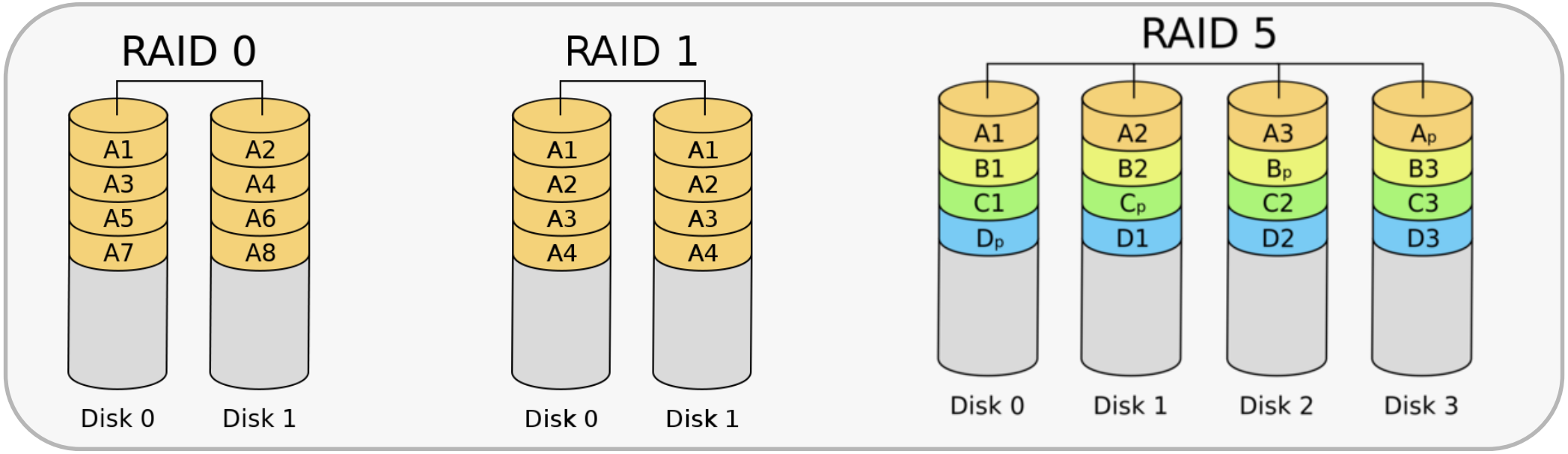
Dicho de forma sencilla, sería como configurar una unidad de almacenamiento formada por varios discos duros.

Es una forma de almacenar datos distribuida ya que utiliza varios discos duros, y también redundante porque habrá veces en la que estos datos se escriban en varios discos duros a la vez. **Esto dependerá del tipo de RAID que configures**

Seguridad Pasiva: Almacenamiento

SISTEMAS RAID

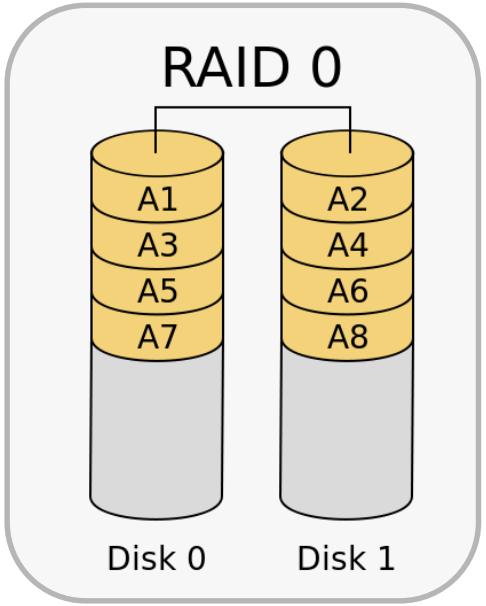
Existen diferentes tipos de configuraciones RAID a las que se puede optar dependiendo de los resultados que se quiera obtener en seguridad y rendimiento



Seguridad Pasiva: Almacenamiento

RAID 0

Agrupamos discos para tener un disco más grande, incluso más rápido.
Desde ese momento, los bloques que lleguen al disco RAID 0 se escribirán en alguno de los discos del grupo. Por supuesto, para el usuario este proceso es transparente: él solo ve un disco de 1 TB donde antes había dos discos de 500 GB.
En el RAID 0 podemos elegir entre spanning y striping (que es lo más común). En cualquier caso, si falla uno de los discos, lo perdemos todo.



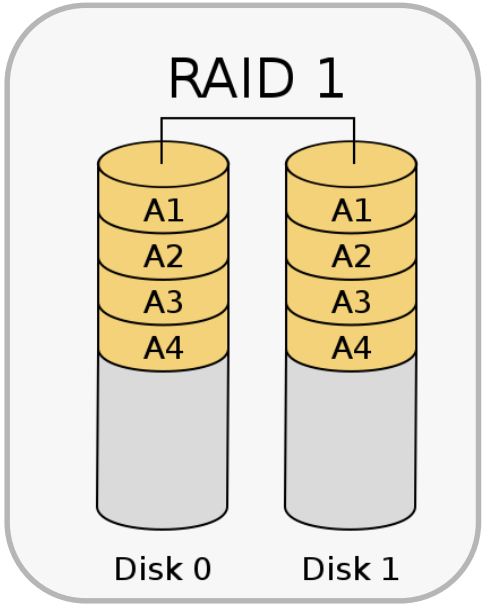
Spanning. Los bloques se escriben en el primer disco hasta que lo llenan; entonces pasan al siguiente, y así sucesivamente. Por tanto, la lectura o escritura de cada bloque tiene que esperar hasta que el disco haya terminado la anterior.

Striping. Los bloques se escriben cada vez en un disco distinto. Es más rápido que el spanning porque hace trabajar a todos los discos a la vez.

Seguridad Pasiva: Almacenamiento

RAID 1

Se le suele llamar mirror o espejo. Agrupamos discos por parejas, de manera que cada bloque que llegue al disco RAID 1 se escribirá en los dos discos a la vez.
Si falla uno de los discos, no perdemos la información, porque estará en el otro.
A cambio, sacrificamos la mitad de la capacidad (el usuario ha conectado dos discos de 500 GB y solo tiene disponibles 500 GB, en lugar de 1 TB) y no ganamos rendimiento.



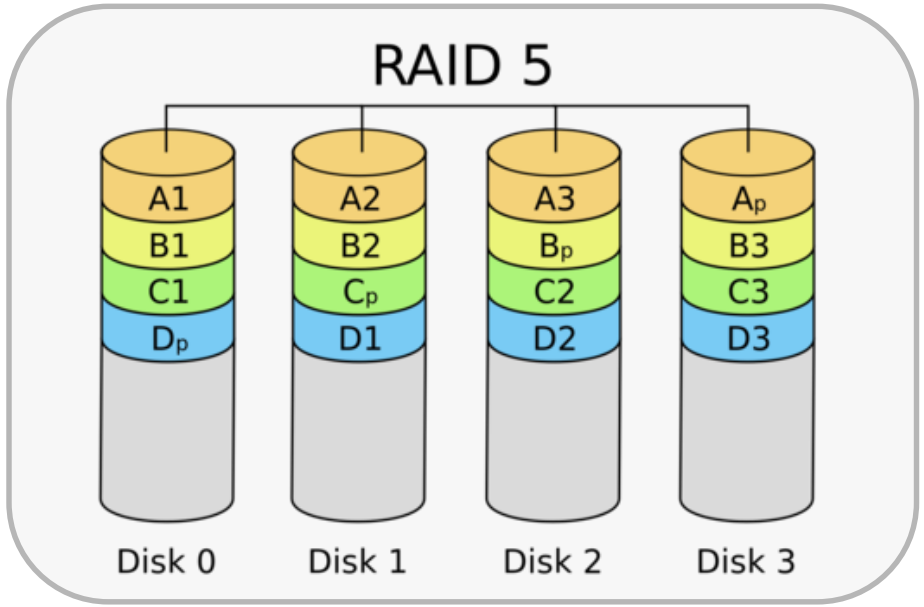
Seguridad Pasiva: Almacenamiento

RAID 5

Si el RAID 0 aporta rapidez y el RAID 1 seguridad, el RAID 5 consigue ambas cosas aplicando dos mecanismos:

- Para cada dato que el sistema quiere almacenar en el RAID, este aplica un procedimiento matemático (en general, la paridad) para obtener información complementaria a ese dato, de tal manera que se puede recuperar el dato en caso de perder cualquier disco (sea disco de datos o paridad).

- Una vez obtenida la paridad, se hace striping para repartir el dato y su paridad por los discos conectados al RAID

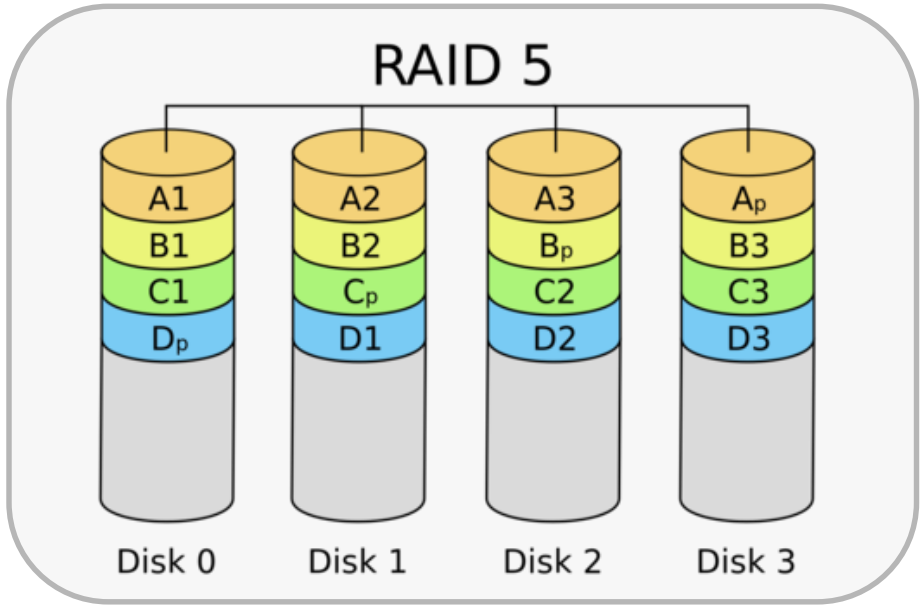


Seguridad Pasiva: Almacenamiento

RAID 5

Gracias al striping hemos conseguido mejor rendimiento que el disco individual, y gracias a la paridad estamos más seguros que en RAID 0. A cambio, sacrificamos la capacidad de un disco (aunque cuantos más discos, menos porcentaje de capacidad perdida).

Por ejemplo, si queremos una capacidad de 1 TB, necesitamos tres discos de 500 GB (o cinco discos de 250 GB).



Seguridad Pasiva: Almacenamiento

SISTEMAS RAID

Más allá de estos tres principales, también hay otros tipos de RAID que **suelen ser combinaciones de los anteriores**, pero que pueden ser útiles sobre todo cuando tienes cuatro o más discos duros disponibles para la configuración de la matriz. Estos son los otros tipos más comunes:

- **RAID 6**: Esta no es una combinación de las anteriores, sino una variante del RAID 5. La diferencia es que los datos no se duplican en un solo disco duro, mientras se reparten en el resto, sino que se duplican en dos.
- **RAID 0+1 o RAID 01**: Requiere por lo menos cuatro discos duros, con los que crear al menos dos matrices RAID 0 con cada uno de los pares de discos. Entonces, luego compones una matriz de RAID 1 utilizando las dos matrices de RAID 0, por lo que tienes la velocidad de las 0 pero con los datos duplicados.
- **RAID 1+0 o RAID 10**: Es la inversa a la anterior. Tienes que crear dos matrices RAID 1, y combinarlas para crear entre las dos una matriz RAID 0. También requiere de un mínimo de 4 discos duros.
- **RAID 5+0 o RAID 50**: Vas a necesitar al menos nueve discos duros, con los que crearás un mínimo de tres matrices RAID 5. Estas matrices, a su vez, se conectarán entre ellas formando una RAID 0.

Seguridad Pasiva: Almacenamiento

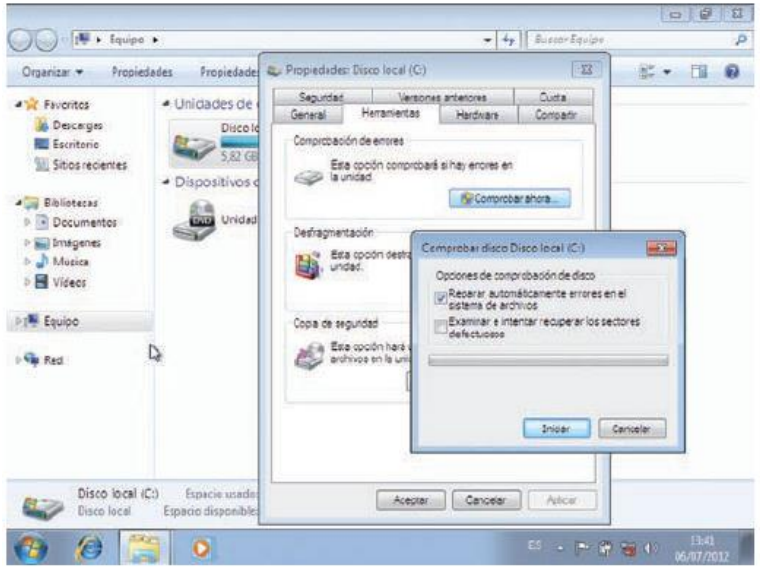
CHEQUEO DE DISCOS

Aunque existan medidas para que el fallo de un disco duro o cualquier otro sistema de almacenamiento no suponga la pérdida de los datos (Copias de seguridad, sistemas RAID, etc.) es importante prevenir esos fallos antes de que ocurran.

Existen herramientas de chequeo:

- Propias del Sistema Operativo
  - Chkdsk en Windows
  - Fsck en Linux

- Herramientas externas
  - CrystalDiskInfo
  - HDDScan



Seguridad Pasiva: Equipos

ACTIVIDAD

Realiza una comprobación de:

- El sistema de ficheros de una máquina virtual Windows con chkdsk
- El sistema de ficheros de una máquina Linux con fsck
- El disco duro con alguna de las herramientas externas vistas en la página anterior

Seguridad Pasiva: Almacenamiento

ALMACENAMIENTO EN RED: NAS Y SAN

Hemos visto que podemos mejorar el rendimiento y la fiabilidad del almacenamiento de un ordenador conectando varios discos y configurándolos en RAID. Pero en las empresas se suele trabajar en equipo, compartiendo ficheros entre varios ordenadores.

Tenemos que pensar cómo compartir ficheros y cómo hacerlo con seguridad (quién puede leer esos ficheros y quién puede modificarlos, borrarlos o incluir nuevos).

¿Qué máquinas y sistemas serán los más adecuados para almacenar los datos de una empresa u organización?

Seguridad Pasiva: Almacenamiento

ALMACENAMIENTO EN RED: NAS Y SAN

Podríamos pensar en incluir los datos en un ordenador de un puesto de trabajo, pero no es la solución más recomendable porque:

- Hacer de servidor de ficheros afectará al rendimiento de sus aplicaciones (Office, Chrome...), y viceversa.
- Estaríamos pendientes de si la otra persona lo ha apagado al salir de la oficina (y puede que estemos en edificios diferentes).
- Es un ordenador personal, luego es probable que no disponga de RAID ni copias de seguridad.
- Estamos más expuestos, ya que será un sistema más vulnerable: más aplicaciones, más necesidades de conexión, más usuarios...

Por tanto, lo mejor es ponerlo en un servidor dedicado y, a ser posible, especializado en almacenamiento. De esta manera:

- Podemos instalar el software estrictamente necesario y tenerlo actualizado (menor riesgo de infecciones).
- Estará bajo la supervisión del personal del CPD (centro de proceso de datos), lo que garantiza estar encendido todo el tiempo, formar parte de la política de copias de seguridad de la empresa, detectar cuando el disco está próximo a llenarse, facilita la monitorización del servicio de almacenamiento, etc.
- Si, además, es un servidor especializado en almacenamiento, dispondrá de hardware suficiente para desplegar configuraciones RAID, una memoria caché de alto rendimiento, etc.

Seguridad Pasiva: Almacenamiento

ALMACENAMIENTO EN RED: NAS Y SAN

Por tanto, lo mejor es ponerlo en un servidor dedicado y, a ser posible, especializado en almacenamiento. De esta manera:

- Podemos instalar el software estrictamente necesario y tenerlo actualizado (menor riesgo de infecciones).
- Estará bajo la supervisión del personal del CPD (centro de proceso de datos), lo que garantiza estar encendido todo el tiempo, formar parte de la política de copias de seguridad de la empresa, detectar cuando el disco está próximo a llenarse, facilita la monitorización del servicio de almacenamiento, etc.
- Si, además, es un servidor especializado en almacenamiento, dispondrá de hardware suficiente para desplegar configuraciones RAID, una memoria caché de alto rendimiento, etc.s

Seguridad Pasiva: Almacenamiento

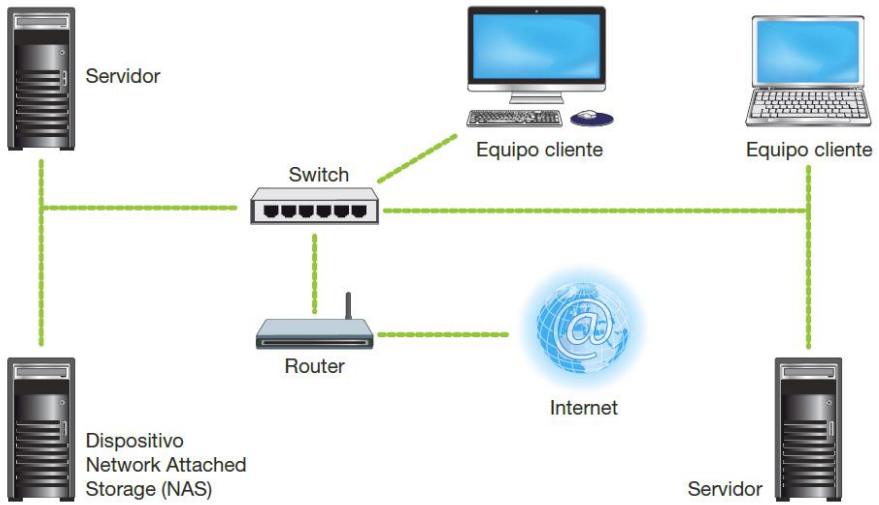
ALMACENAMIENTO EN RED: NAS Y SAN

Tener un equipo de la red ofreciendo su capacidad de almacenamiento se conoce como **NAS (Network Attached Storage, almacenamiento conectado a la red).**

En ese esquema tenemos un equipo con almacenamiento local que desea ofrecerlo a otros equipos de la red. Este equipo servidor ejecutará un determinado software servidor que responde a un determinado protocolo. Aquel equipo que necesite acceder a esa carpeta compartida, ejecutará un software cliente capaz de interactuar con el servidor de acuerdo con el protocolo del servidor.

Como la mayoría de los equipos de usuario son Windows, el protocolo más común es CIFS (Common Internet File System), que es una evolución de SMB (Server Message Block).

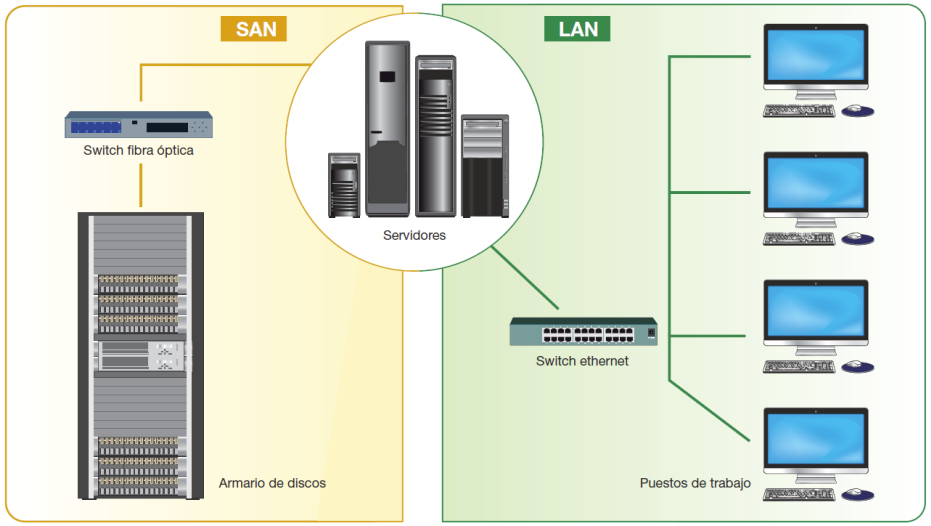
Existen soluciones como OpenMediaVault o TrueNAS que facilitan la gestión de este tipo de sistemas



Seguridad Pasiva: Almacenamiento

ALMACENAMIENTO EN RED: NAS Y SAN

En un entorno empresarial necesitamos mucho más rendimiento y seguridad, por lo que el equipo servidor necesitará potencia de procesamiento, amplia memoria caché, tarjetas de red de alta capacidad y configuraciones RAID. Si otros servidores también lo necesitan, seguramente optaremos por una solución **SAN (Storage Area Network).**



En un SAN los discos están en lo que se llama un «armario», donde se realiza la configuración RAID. El armario dispone de cachés de alto rendimiento para reducir los tiempos de operación. Su mayor ventaja es que es altamente escalable.

Los servidores se conectan al armario mediante conmutadores de fibra óptica (por eso hablamos de network), y normalmente mediante el protocolo SCSI.

Referencias

Seguridad informática. **José Fabián Roa Buendía**. **McGraw-Hill** España, 2013.

Seguridad informática (Edición 2020) **POSTIGO PALACIOS**, **ANTONIO**. Ediciones Paraninfo, S.A., May 19, 2020