Practica 2 Fonaments de maquinaria:

Part2

Denis Pérez

Index:

Antivirus:

Que es:

Es un programa que detecta la presencia de virus informáticos, el malware que altera el funcionamiento normal del ordenador sin que el usuario lo sepa o consienta, para posteriormente eliminarlos o repararlos.

Cómo funciona:

- **Escaneo**: El antivirus analiza los archivos y programas en el dispositivo para detectar comportamientos sospechosos o patrones conocidos de malware. Esto se hace mediante dos métodos principales:

  - Firmas: Compara los archivos con una base de datos de firmas de malware conocidas.
  - Heurística: Evalúa el comportamiento de los archivos para identificar posibles amenazas nuevas o desconocidas.

- **Prevención**: Muchos antivirus incluyen características de prevención en tiempo real, que monitorean las actividades del sistema y bloquean amenazas antes de que puedan causar daño.

- **Actualizaciones**: Los antivirus se actualizan regularmente para añadir nuevas definiciones de virus y mejorar su capacidad para detectar y eliminar amenazas.

- **Cuarentena**: Si se detecta malware, el antivirus puede poner en cuarentena esos archivos para evitar que se ejecuten y causen daños, permitiendo al usuario decidir qué hacer con ellos.

- **Eliminación**: Una vez que se ha identificado una amenaza, el antivirus ofrece opciones para eliminarla de manera segura.

Sirve para:

- **Protección de datos**: Prevenir la pérdida o el robo de información personal y sensible.
- **Seguridad del sistema**: Mantener el rendimiento y la estabilidad del dispositivo.
- **Navegación segura**: Proteger al usuario mientras navega por internet, evitando sitios web maliciosos.
- **Tranquilidad**: Ofrecer a los usuarios la confianza de que sus dispositivos están protegidos contra amenazas cibernéticas.

Firewall:

También conocido como “cortafuegos”, es un filtro de la red o el sistema que se realiza para bloquear accesos no autorizados y permitir los que sí lo están.

Pueden implementarse por medio de software o hardware para brindar una mayor protección a las redes. Son especialmente importantes en empresas que operan con datos confidenciales que deben ser protegidos.

Qué funciones tiene el firewall:

-Filtrado de tráfico: Evalúa los paquetes de datos que intentan entrar o salir de la red y decide si deben ser permitidos o bloqueados basándose en reglas predefinidas.

-Protección contra intrusiones: Detecta y bloquea intentos no autorizados de acceder a la red, protegiéndo así contra ataques cibernéticos.

-Registro y monitoreo: Puede registrar el tráfico de red y alertar a los administradores sobre actividades sospechosas o inusuales.

-Control de acceso: Permite establecer políticas que controlen qué usuarios o dispositivos pueden acceder a recursos específicos dentro de la red.

-VPN (Red Privada Virtual): Algunos firewalls ofrecen la posibilidad de crear conexiones seguras y cifradas a través de redes no confiables.

Que te aporta este sistema:

- Seguridad de la red: Proteger la red de amenazas externas e intrusiones no autorizadas.
- Integridad de los datos: Ayudar a mantener la integridad y confidencialidad de la información transmitida.
- Control de acceso: Asegurar que solo usuarios y dispositivos autorizados puedan acceder a recursos críticos.
- Prevención de malware: Bloquear el tráfico malicioso que pueda contener virus, troyanos u otro tipo de malware.

Spyware:

El spyware es un tipo de software malicioso diseñado para recopilar información sobre un usuario o una organización sin su conocimiento. Su principal propósito es espiar, recopilar datos sensibles, y, en algunos casos, realizar actividades fraudulentas.

Funciones del spyware:

-Recopilación de información: Captura datos personales como contraseñas, información de tarjetas de crédito, historial de navegación y correos electrónicos.

-Monitoreo de actividad: Registra las pulsaciones de teclas (keylogging) y puede tomar capturas de pantalla para observar lo que el usuario está haciendo.

-Acceso remoto: Permite a los atacantes acceder y controlar el dispositivo de manera remota, lo que puede incluir la activación de la cámara o el micrófono.

-Publicidad no deseada: Algunos tipos de spyware se utilizan para mostrar anuncios dirigidos y generar ingresos para sus creadores.

-Robo de identidad: Recopila información personal para suplantar la identidad del usuario y cometer fraudes.

Como prevenirlo:

Para protegerse contra el spyware, se recomienda utilizar software antivirus actualizado, evitar descargar aplicaciones de fuentes no confiables, y mantener el sistema operativo y el software actualizado.

Para qué sirve una copia de seguridad:

Las copias de seguridad son fundamentales para proteger la información y garantizar la recuperación de datos en caso de pérdida, daño o corrupción. Su importancia radica en varios aspectos:

Importancia de las copias de seguridad:

-Protección contra la pérdida de datos: Ayudan a recuperar información importante en caso de fallos de hardware, errores humanos, ataques de malware o desastres naturales.

-Continuidad del negocio: En entornos empresariales, las copias de seguridad son esenciales para garantizar que las operaciones puedan continuar sin interrupciones significativas.

-Recuperación ante desastres: Permiten restaurar datos críticos rápidamente, minimizando el tiempo de inactividad y la pérdida de productividad.

-Cumplimiento normativo: Muchas regulaciones requieren que las empresas mantengan copias de seguridad de ciertos datos, por lo que es una práctica necesaria para cumplir con la ley.

-Tranquilidad: Saber que los datos están respaldados proporciona tranquilidad y confianza en la seguridad de la información.

Tipos principales de copias de seguridad:

-Copia de seguridad completa: Se realiza una copia de todos los datos seleccionados en un momento dado. Es la más segura, pero también la que más tiempo y espacio requiere.

-Copia de seguridad incremental: Solo se respaldan los datos que han cambiado desde la última copia de seguridad (completa o incremental). Esto ahorra tiempo y espacio, pero la recuperación puede ser más lenta.

-Copia de seguridad diferencial: Se copian todos los datos que han cambiado desde la última copia de seguridad completa. Es más rápida que la completa y más fácil de restaurar que la incremental.

-Copia de seguridad en la nube: Los datos se almacenan en servidores remotos a través de Internet. Ofrece accesibilidad y seguridad, además de proteger contra desastres locales.

-Copia de seguridad local: Se guardan en dispositivos físicos como discos duros externos, USB o cintas. Es rápida y no depende de Internet, pero es vulnerable a robos o daños físicos.

-Copia de seguridad automática: Configuradas para realizarse de forma programada sin intervención manual, lo que garantiza que siempre haya una copia reciente.

Gestión de Discos:

Que es?

Es una utilidad de sistemas de windows que permite ver y gestionar las unidades de almacenamiento instaladas y crear.
Aquí dejo algunas tareas que puede realizar :

-Configurar una nueva unidad.

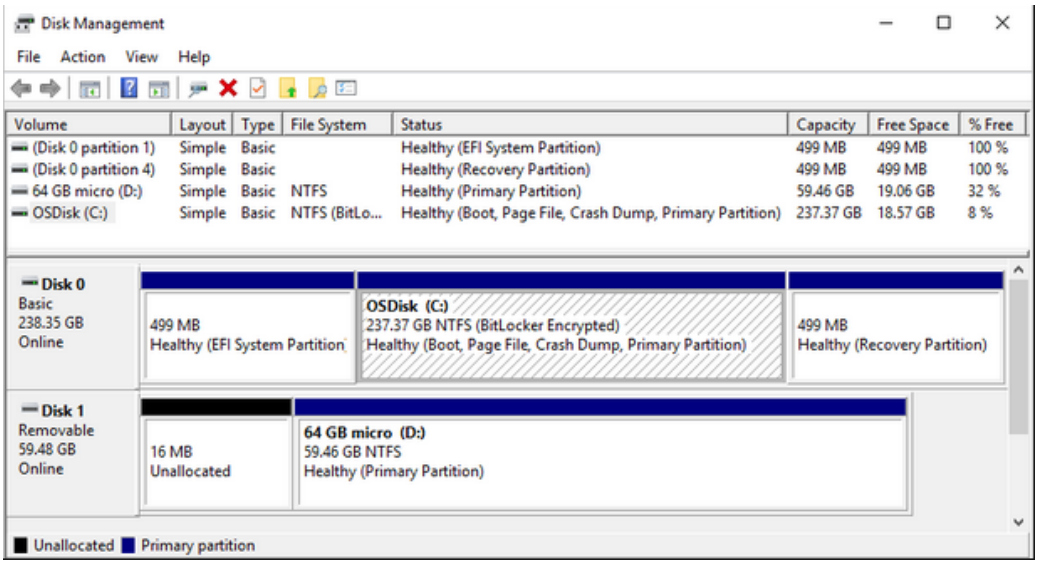
-Extender en volumen en el espacio que aún no forma parte de un volumen en la misma unidad.

-Reducir una partición para habilitar la extensión en una partición vecina.

-Cambiar una letra de unidad o asignar una letra de unidad nueva.

Revisión de las unidades y sus particiones:

La administración muestra los detalles de cada unidad del equipo y todas las particiones de cada unidad.
En la siguiente imagen se especifica mejor la información general de administración de discos de varias unidades:



Windows suele tener tres particiones en la unidad principal, estas incluyen sistema EFI, una partición del disco local (C:) y una de recuperación.

-En el apartado de Disco Local tenemos instalado el sistema operativo Windows, está se encarga del almacenamiento de las siguientes aplicaciones y archivos.

-El sistema EFI estan los mas modernos para iniciar el equipo y el sistema operativo.

-La recuperación almacena herramientas especiales para ayudar a recuperar Windows, en caso de que haya algún problema en el arranque u otros.

Solución de problemas:

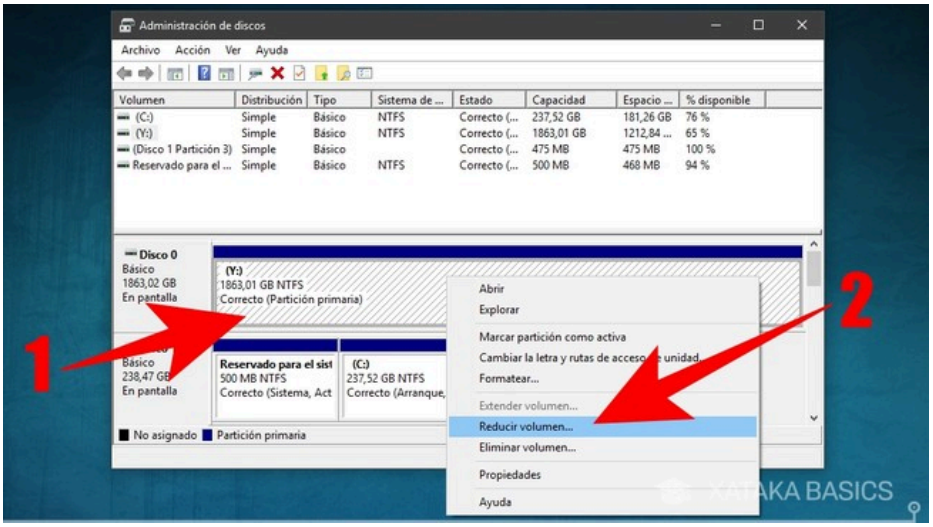
En ocasiones el disco notifica algún procedimiento que no funciona como debería, para esto existen varias soluciones para resolver el problema:

Definir que es una partición y para que sirve las primarias y las lógicas:

Una partición es una división lógica de un disco duro que permite organizar y gestionar el espacio de almacenamiento de manera más eficiente. Cada partición actúa como una unidad independiente, lo que facilita la instalación de diferentes sistemas operativos, la organización de datos y la mejora del rendimiento.

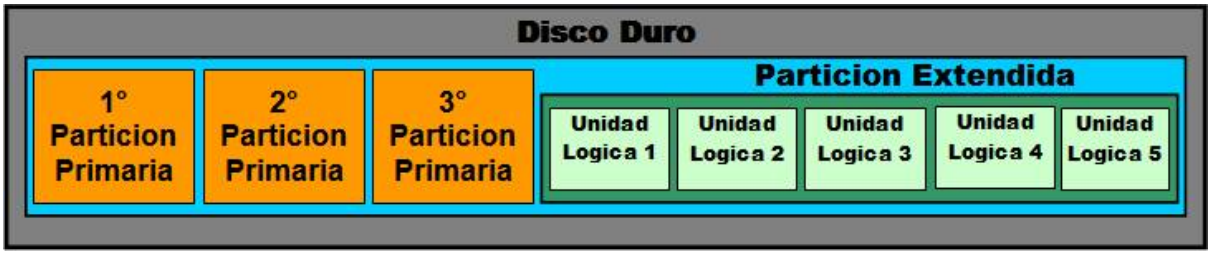
Particiones primarias

Las particiones primarias son aquellas que se pueden utilizar para arrancar un sistema operativo. Un disco duro puede tener hasta cuatro particiones primarias. Estas particiones se gestionan directamente por el sistema BIOS o UEFI y son necesarias para el funcionamiento del sistema.



Particiones lógicas

Las particiones lógicas, en cambio, se crean dentro de una partición primaria (generalmente dentro de una partición extendida) y permiten superar la limitación de cuatro particiones. Son útiles para organizar datos adicionales, instalar sistemas operativos alternativos o gestionar archivos de manera más flexible.

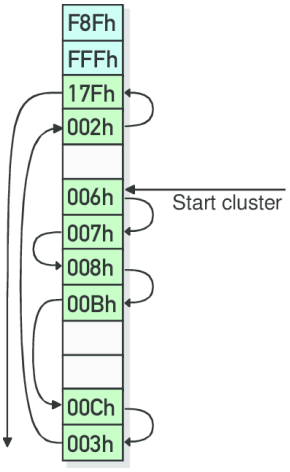


Explicació dels principals sistemes d'arxius

1. FAT (File Allocation Table)

Su versión puede ser FAT12, FAT16, FAT32. y tiene un uso común en unidades flash y tarjetas sd. Sus caracteristicas principales son:

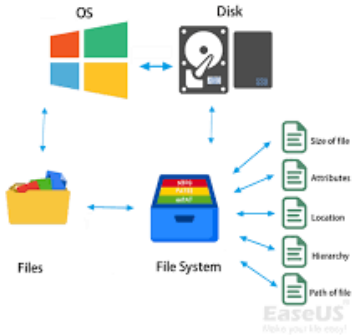
-Simple y fácil de implementar
-Soporta archivos de hasta 4 GB en fat32.
-No incluye características avanzadas como permisos de archivos.



2. NTFS (New Technology File System)

Se usa principalmente en windows y sus características son:

-Soporta archivos de tamaño muy grande.
-Implementa características de seguridad como permisos de archivos y cifrados.
-Registros de cambios para recuperación de datos.
-Soportar enlaces simbólicos y compresión.



3. ext (Extended File System)

Versiones: ext2, ext3, ext4.

Uso: Principalmente en sistemas Linux.

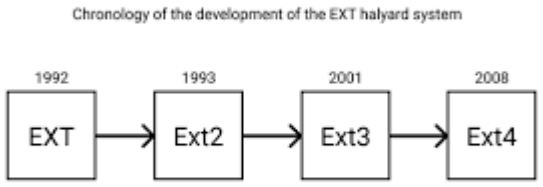
Características:

-ext2: Sin journaling (registro de cambios).

-ext3: Añade journaling para mejor recuperación.

-ext4: Mejoras en el rendimiento y soporte para archivos grandes.

-Soporta características como cuotas de usuario y recuperación de errores.



4. HFS+ (Hierarchical File System Plus)

Uso: Principalmente en macOS.

Características:

-Soporta archivos grandes y tiene journaling.

-Permite etiquetas y versiones de archivos.

-Optimizado para la gestión de archivos en entornos Mac.

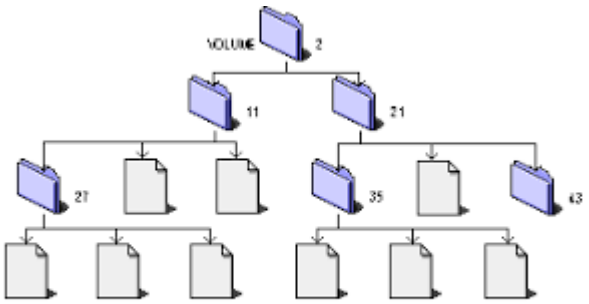


FIG 3 - MACINTOSH HIERARCHICAL FILE SYSTEM

5. APFS (Apple File System)

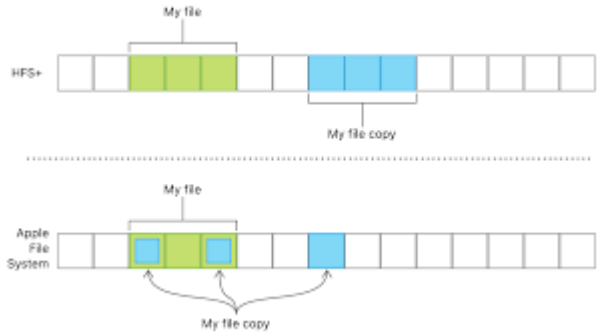
Uso: Sustituto de HFS+ en macOS y iOS.

Características:

-Mejor rendimiento y cifrado por defecto.

-Soporta instantáneas y copias de seguridad rápidas.

-Optimizado para almacenamiento SSD.



6. XFS

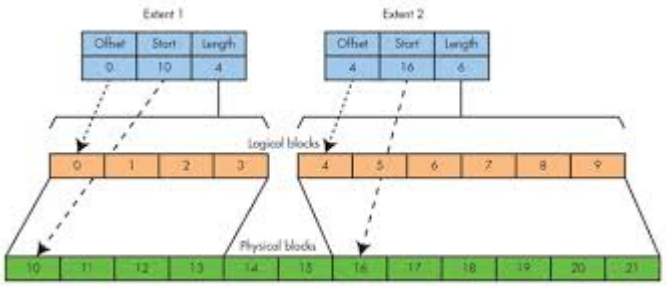
Uso: Principalmente en sistemas Linux, especialmente en servidores.

Características:

-Soporta archivos muy grandes y volúmenes de almacenamiento.

-Gran rendimiento en sistemas con alta carga de trabajo.

-Incluye capacidades de journaling.



7. Btrfs (B-tree File System)

Uso: En Linux, como un sistema de archivos moderno.

Características:

-Soporta instantáneas, compresión y RAID integrado.

-Diseñado para ser escalable y flexible.

-Capacidad de administración avanzada.

Eines de gestió de discs durs que permetin formatar i gestionar particions:

Para Windows:

1. Gestor de discos de Windows:
   Integrado en el sistema operativo, permite crear, eliminar, redimensionar y formatear particiones.
2. EaseUS Partition Master:
   Herramienta gráfica que facilita la gestión de particiones, incluyendo la recuperación de datos.
3. MiniTool Partition Wizard:
   Ofrece una interfaz amigable y varias opciones para gestionar particiones y sistemas de archivos.
4. AOMEI Partition Assistant:
   Permite gestionar particiones de manera sencilla, con opciones avanzadas para usuarios.

Para Linux:

1. GParted:
   Herramienta gráfica muy popular que permite crear, eliminar, redimensionar y formatear particiones.
2. Parted:
   Herramienta de línea de comandos que ofrece funcionalidades avanzadas para gestionar particiones.
3. fdisk:
   Herramienta de línea de comandos para gestionar particiones, adecuada para usuarios experimentados.
4. KDE Partition Manager:
   Herramienta gráfica para entornos de trabajo KDE, útil para gestionar discos y particiones.

Herramientas Multiplataforma:

1. Rufus:
   Principalmente para crear USB de instalación, también permite gestionar particiones en dispositivos USB.
2. Clonezilla:
   Herramienta de copia de seguridad y clonación que permite gestionar discos y particiones en varios sistemas operativos.
3. GParted Live:
   Versión en vivo de GParted que se puede ejecutar desde un USB o CD, compatible con diversos sistemas operativos.

Webgrafia:

https://www.docusign.com/es-mx/blog/desarrolladores/antivirus

https://www.deltaprotect.com/blog/que-es-un-firewall

https://latam.kaspersky.com/resource-center/threats/spyware?srsltid=AfmBOop4uCLc722y5aEz-ipRytGD9B345F01k6Lof0uZ6W6C_IGCg8C3

https://www.risoul.com.es/blog/diferencia-entre-antivirus-anti-spyware-y-firewall