TÉCNICO SUPERIOR EN DESARROLLO DE APLICACIONES MULTIPLATAFORMA

MÓDULO:
Sistemas informáticos

UNIDAD:
Explotación de sistemas microinformáticos

CEAC
FP Oficial

UNIDAD:

Explotación de sistemas microinformáticos

CEAC FP Oficial

Madrid (España), 2025

ÍNDICE

5.

NORMAS DE SEGURIDAD Y PREVENCIÓN DE RIESGOS LABORALES 25

6.

CARACTERÍSTICAS DE LAS REDES. VENTAJAS E INCONVENIENTES 30

7.

TIPOS DE REDES 33

8.

COMPONENTES DE UNA RED INFORMÁTICA 38

1. Objetivos

Identificar los componentes clave de los sistemas informáticos y sus respectivas funciones.

Analizar y describir las características y especificaciones técnicas de diferentes sistemas informáticos.

Evaluar el rendimiento y la eficiencia de los sistemas informáticos mediante pruebas y comparaciones.

2. Introducción

Este tema se centra en ofrecer una comprensión detallada de los diferentes **componentes de hardware** y su correcta gestión. El estudio comienza con la identificación, instalación y mantenimiento de dispositivos clave como **procesadores**, **memorias RAM** y **discos duros**, asegurando un conocimiento profundo de su funcionamiento y características.

A continuación, se exploran las **funciones del sistema operativo**, evaluando cómo sistemas como Windows, Linux y macOS actúan como intermediarios entre el hardware y el usuario, y gestionan recursos a través de tareas esenciales como la administración de usuarios y permisos. La creación, configuración y manejo de **máquinas virtuales** es otro punto fundamental, permitiendo la emulación de múltiples entornos operativos en un solo equipo para fines de prueba y desarrollo.

En paralelo, se estudian las **redes informáticas**, desde la configuración de redes locales (LAN) hasta la gestión de protocolos de comunicación, y se subraya la importancia de las **medidas de seguridad informática** para proteger datos y sistemas frente a amenazas cibernéticas. Esta integración de conocimientos proporciona una base sólida para la resolución eficiente de problemas técnicos y la optimización de los entornos informáticos, facilitando el desarrollo y mantenimiento de aplicaciones.

Desde 2024, el uso de tecnologías emergentes como la **inteligencia artificial generativa y la computación en la nube híbrid**a ha redefinido el enfoque hacia la optimización de entornos informáticos. Estas tecnologías permiten gestionar y automatizar la configuración de hardware y software mediante plataformas como Terraform y Ansible, proporcionando escalabilidad y flexibilidad en entornos de desarrollo web y multiplataforma.

3. Placas base. Formatos

En las placas base, los factores de forma determinan su tamaño y compatibilidad con el chasis. Los conectores, como los de la CPU, RAM y almacenamiento, son esenciales para la comunicación entre componentes. Además, conocer elementos clave como el chip BIOS y los slots de expansión es vital para el ensamblaje y actualización del equipo. Un adecuado mantenimiento e instalación de la placa base asegura un rendimiento óptimo y reduce fallos técnicos, prolongando la vida útil del ordenador.

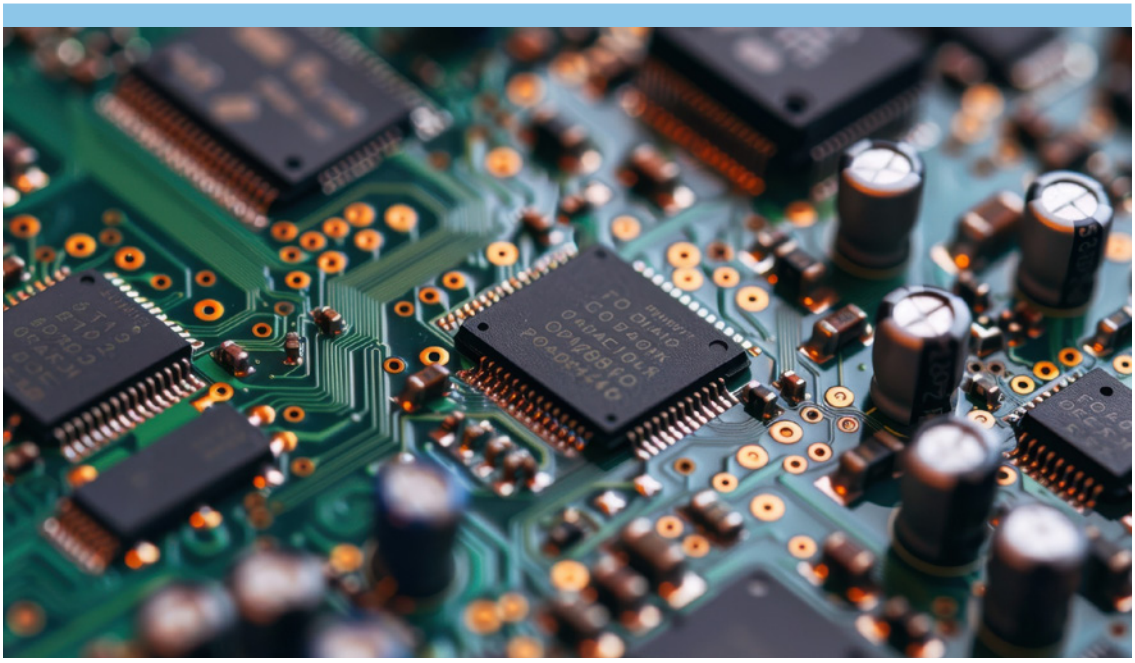


Figura 1. Arquitectura de una placa base

3.1. Factores de forma de las placas base.

En el mundo de las **placas base**, los factores de forma juegan un papel clave al definir las dimensiones físicas, las especificaciones de montaje y la compatibilidad con otros componentes del sistema. Existen diversos formatos, cada uno diseñado para satisfacer necesidades específicas de rendimiento y espacio.

ATX

- El **ATX (Advanced Technology eXtended)** es el formato estándar actual que resolvió muchas deficiencias del antiguo formato AT. Una de sus mejoras clave fue la incorporación de puertos externos en el propio estándar y la ubicación estratégica de la **RAM** cerca del procesador, lo cual mejoró significativamente el rendimiento general del sistema. La **microATX**, una variante reducida del ATX, y la **FlexATX**, creada por Intel en 1999, son pruebas de que la reducción de tamaño no necesariamente compromete las prestaciones; de hecho, FlexATX es la versión más pequeña del mercado ATX, con dimensiones de 23 x 19 cm.

- En la mayoría de las placas base ATX se han estandarizado la inclusión de puertos de teclado, ratón, puerto paralelo, puerto serie y **USB**, lo que facilita la conectividad de múltiples dispositivos. Muchos modelos actuales incluso integran puertos de red, sonido e incluso video, lo que reduce la necesidad de tarjetas adicionales y aumenta la fiabilidad del conjunto debido a la disminución de conexiones mecánicas.

Mini ITX

- Por otro lado, el **Mini ITX** es un formato mucho más pequeño, con un tamaño de 6.7 x 6.7 pulgadas, ideal para sistemas compactos como Mini PCs o Barebones, donde el espacio es un lujo. Este formato es estándar en aplicaciones industriales donde la eficiencia y el tamaño reducido son esenciales. El **NLX** y el **LPX** también son formatos orientados a PCs que requieren eficiencia en el consumo y, como el LPX, estructuras ajustadas como las slim.

La elección del formato adecuado es una tarea que depende de varios factores como el **tipo de PC** (viejo, reciente, para consumo), la **caja** donde se alojará la placa base, y la **fuente de alimentación** necesaria.

Para aquellos que deben tomar la decisión de qué placa base elegir, es esencial evaluar la idoneidad en términos de **tipo, prestaciones, precio y posibilidades de ampliación**. Las placas base **OEM**, utilizadas mayoritariamente en PCs y pequeños servidores, siguen formatos estándar de tamaño (form factors). Estos tamaños no necesariamente dictaminan características técnicas específicas, pero sí influyen en el **rendimiento y la adecuación** del sistema al uso previsto.

Por ejemplo, una placa Mini ITX es ideal para un sistema de entretenimiento en casa, mientras que una placa ATX sería más adecuada para una estación de trabajo o un servidor pequeño.

3.2. Conectores de las placas base.

Las placas base, como matriz central de cualquier sistema informático, son esenciales para la **conexión y comunicación de todos los componentes, internos y periféricos**. Estas conexiones, que se han estandarizado para garantizar la compatibilidad universal, establecen el puente entre el núcleo del sistema y sus diversos elementos.

Conexiones internas	Conexiones externas
Las conexiones internas incluyen las de **alimentación**, vitales para proporcionar energía a todos los componentes. Los **puertos EIDE y FDD**, aunque en desuso en sistemas modernos, históricamente han permitido la conexión de discos duros y unidades de disquete, respectivamente. Hoy en día, los dispositivos de almacenamiento utilizan **puertos SATA**, que ofrecen mayores velocidades de transferencia y una mejora significativa en la gestión de cables. Además, existen las **salidas a ventiladores**, necesarias para la refrigeración de componentes críticos, y conexiones específicas para el frontal del equipo, como el P**ower On, Power LED, HD LED, Reset y altavoz**. También se incluyen los **puentes / switches**, esenciales para diversas configuraciones de hardware.	En cuanto a conexiones externas, estas permiten la interacción del usuario con el sistema y la conexión de periféricos adicionales. Los más comunes incluyen los conectores **PS/2 para ratón y teclado**, las interfaces **USB y Firewire**, cruciales para un sinfín de dispositivos modernos. La conexión a redes es posible mediante el puerto de **Red Ethernet**, mientras que los puertos **serie y paralelo**, aunque obsoletos, coexistieron con las tarjetas madre más antiguas para conectar impresoras y otros dispositivos. Las placas modernas también incluyen puertos específicos para **sonido y gamepad**, y cada vez más, soluciones integradas para **video / TV**.

Los **conectores EIDE**, aunque en retirada frente a las soluciones SATA, fueron pioneros en estandarizar la conexión de discos duros y unidades ópticas. Estos puertos, con sus característicos **40 pines**, permitieron la conexión de dos dispositivos por conector mediante cables adecuados. Este diseño contemplaba la separación entre señales para evitar errores y mejorar la velocidad.

Las **conexiones frontales**, muy prácticas para el usuario, permiten una interacción directa y cómoda. El conector **Power On** activa o detiene el sistema, mientras que el **Power LED** indica el estado operativo del equipo. El **HD LED** muestra la actividad del disco duro, y el **Reset** permite reiniciar el sistema fácilmente. Aunque ya en desuso, el **KeyLock** se utilizaba para bloquear el uso del teclado, una medida de seguridad en sistemas anteriores.

La integración de controladoras en la placa madre moderna ha **eliminado la necesidad de tarjetas controladoras externas**, simplificando el diseño de sistemas y mejorando la fiabilidad y la velocidad de las conexiones. Esta evolución ha sido esencial para soportar el incremento en la multiplicidad de conexiones y las velocidades asociadas a los dispositivos actuales.

En placas base actuales, las **conexiones Thunderbolt 4** han ganado protagonismo, ofreciendo tasas de transferencia de hasta 40 Gbps y soporte para múltiples dispositivos en cadena (**daisy chain**). Además, los conectores **USB-C Power Delivery** integrados permiten alimentar dispositivos de mayor consumo, facilitando la compatibilidad con periféricos avanzados.

3.3. Componentes de las placas base

Los componentes de las placas base son variados y tienen distintas funciones especializadas para mantener el rendimiento y la compatibilidad del sistema.

Chipset

- Uno de los elementos centrales es el chipset, que se compone de dos partes principales: el Northbridge y el Southbridge. El Northbridge es responsable de mediar entre la CPU y la RAM, y debido a que trabaja a alta velocidad, disipa calor considerablemente, lo que requiere un radiador. Este componente se sitúa físicamente entre la CPU y la RAM. Por su parte, el Southbridge se encarga de gestionar las entradas y salidas del sistema, además de los buses y dispositivos de almacenamiento, ubicándose entre la CPU y las ranuras de expansión.

- La tecnología de los chipsets se actualiza continuamente para alinearse con los avances en las tecnologías de los procesadores y las mejoras en prestaciones generales. En algunos casos, como en los miniportátiles, los chipsets están integrados en los micros, lo cual representa una evolución en la fabricación de placas base.

La **placa base** es la infraestructura esencial para la conexión de todos los componentes de un PC. Estas conexiones están **estandarizadas** para permitir a diferentes fabricantes diseñar componentes compatibles. Todos los componentes de un sistema informático, ya sea de forma directa o indirecta, se conectan a la placa base. Dado que el núcleo del ordenador necesita ser **compacto**, la creciente cantidad de conexiones y el aumento en las velocidades hacen que la integración sea imprescindible. Los distintos **subsistemas** de la placa base influyen significativamente en las prestaciones globales del sistema.

Entre los componentes y zócalos más destacados de una placa base, encontramos el **zócalo del procesador**, las **ranuras de memoria** y el propio chipset con sus dos variantes, el Northbridge y el Southbridge. Además, existen otros chips especializados para funciones de **red Ethernet, sonido, video y SCSI** para sistemas de gama alta. Estos chips permiten incorporar puertos y controladoras adicionales dentro de la placa base, mejorando la funcionalidad del sistema.

Las **conexiones y buses de la placa base** también son fundamentales.

Internamente, se encuentran las conexiones de alimentación, salidas a ventiladores, puertos EIDE y FDD, puertos SATA, conexiones frontales y puentes o switches.	Externamente, destacan las conexiones para ratón y teclado PS/2, buses USB y Firewire, red Ethernet, puertos serie y paralelo, sonido y gamepad, video/TV, SCSI de gama alta y docking/backplane.

Las placas base modernas integran una serie de chips especializados para optimizar funciones específicas. Por ejemplo, **chips de Ethernet** permiten añadir puertos Ethernet de par trenzado, como los de la casa Realtek. Los **chips de sonido**, que deben ser compatibles con el estándar AC'97, proporcionan soporte de audio al sistema. En algunos casos, las **placas de video** pueden estar separadas o integradas en el chipset, aunque también pueden incluir circuitería independiente para esta función. En sistemas más avanzados, como servidores, se pueden incorporar controladoras SCSI con circuitería especializada.

3.4. Instalación, mantenimiento y cuidado de la placa base

La **placa base** actúa como el cimiento de cualquier ordenador, proporcionando soporte y conectividad para todos los componentes del sistema. El proceso de **instalación** de una placa base comienza con la elección del modelo adecuado, según las necesidades específicas del sistema y las compatibilidades con otros componentes, como la **CPU, la RAM y las tarjetas de expansión**. Es fundamental fijar la placa de manera segura en el chasis, utilizando los tornillos adecuados y asegurándose de que está bien alineada con los postes distanciadores para evitar cortocircuitos.

Mantenimiento

- El **mantenimiento** de la placa base implica diversas tareas. Una de las más esenciales es la limpieza periódica del polvo y otros residuos que pueden acumularse en su superficie y en sus componentes. El uso de **aire comprimido** es recomendado para esta tarea, prestando especial atención a las conexiones y ranuras. Además, es fundamental **revisar las conexiones** y verificar que todos los cables y conectores estén correctamente asentados. Los **cambios en el hardware**, como la actualización de la RAM o la instalación de tarjetas de expansión, deben realizarse con cuidado, asegurando que el dispositivo esté apagado y desconectado de la alimentación.

Cuidado

- El **cuidado** de la placa base también incluye la monitorización de la temperatura. Las **placas base modernas** suelen incorporar sensores de temperatura que pueden ser monitoreados a través del software del sistema. Es importante garantizar que los **ventiladores**, tanto el de la CPU como los adicionales (CPU_FAN, SYS_FAN), funcionen adecuadamente para evitar el sobrecalentamiento. El fallo de estos ventiladores puede desencadenar alarmas o incluso la **desactivación automática** del sistema, protegiendo así el hardware de posibles daños.

Dentro de los **componentes críticos** de una placa base, el **chipset** juega un clave en el rendimiento del sistema. Mantener estos componentes a temperaturas adecuadas, a menudo mediante **disipadores de calor**, es vital para su correcto funcionamiento. La **actualización de la BIOS** de la placa base es otra tarea importante en el mantenimiento, ya que puede proporcionar mejoras en la estabilidad y compatibilidad del sistema.

Para el **mantenimiento preventivo** y el cuidado de la placa base, es recomendable contar con herramientas adecuadas como un juego de **destornilladores, pulseras antiestáticas, y aerosol de aire comprimido**. Adicionalmente, se deben seguir prácticas de instalación seguras, como evitar la electricidad estática, que puede dañar los circuitos sensibles de la placa base.

Con el auge de la personalización en PC, las prácticas de mantenimiento incluyen la **integración de sistemas de refrigeración líquida** todo en uno (AIO) para optimizar la gestión térmica en placas base de alto rendimiento. Asimismo, los **diagnósticos automatizados** mediante software como HWMonitor o ASUS AI Suite permiten monitorear continuamente las condiciones de la placa, minimizando riesgos de fallos.

4. Estructura y componentes: procesador (conjunto de instrucciones, registros, contador, unidad aritmeticológica, interrupciones); memoria interna, tipos y características (RAM, xPROM y otros); interfaces de entrada-salida; discos periféricos. Adaptadores para la conexión de dispositivos

La CPU, como núcleo del sistema, ejecuta instrucciones mediante ciclos de búsqueda, decodificación y ejecución, apoyada por registros como el contador de programa y la unidad aritméticológica. La RAM, memoria volátil, almacena datos y programas en uso, mientras que la memoria secundaria, como discos duros y SSDs, asegura almacenamiento persistente con diferencias en velocidad y capacidad. Los interfaces I/O, mediante interrupciones o DMA, gestionan la interacción con dispositivos periféricos. Además, los adaptadores de periféricos integran componentes de hardware, garantizando una comunicación eficiente y la funcionalidad del sistema.

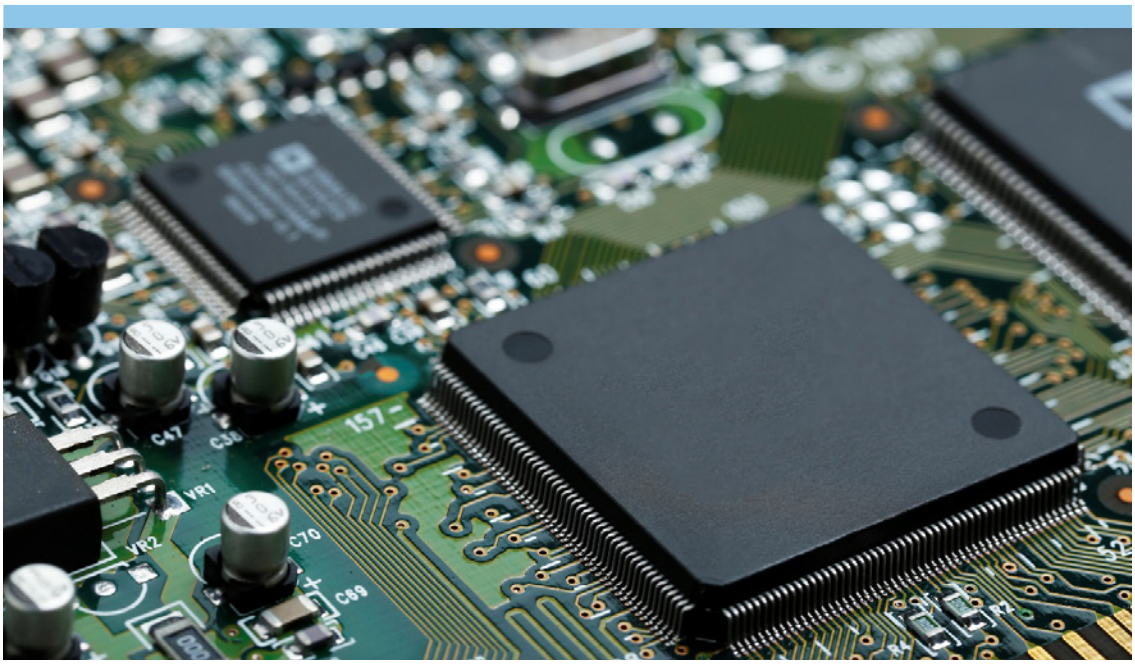


Figura 2. Chips integrados en una placa base

4.1. Unidad Central de Proceso. Funcionamiento

La **CPU** es el núcleo de un sistema informático, encargado de ejecutar instrucciones y procesar datos. Está compuesta por la **ALU**, que realiza operaciones matemáticas y lógicas, y la **Unidad de Control**, que coordina el flujo de datos entre la memoria, la ALU y los periféricos. Como veremos, su funcionamiento conjunto asegura la ejecución eficiente de las instrucciones y el correcto desarrollo de software multiplataforma y web.

4.1.1. Unidad Aritmético-Lógica

La **Unidad Aritmético-Lógica (ALU)** es uno de los componentes centrales de la Unidad Central de Proceso (CPU) o procesador en los ordenadores. Su misión es fundamental porque realiza todas las operaciones aritméticas y lógicas que permiten que los datos se procesen adecuadamente. La ALU está diseñada para **ejecutar tareas matemáticas** como sumas, restas, multiplicaciones y divisiones, así como comparaciones y **operaciones bit a bit** como AND, OR, XOR y NOT, que son esenciales en la toma de decisiones y la ejecución de programas.

Combinación de la ALU con la Unidad de Control (UC)

La combinación de la ALU con la Unidad de Control (UC) da lugar al corazón del sistema de cómputo, conocido como CPU. Mientras que la UC dirige y controla la operación de los demás componentes del sistema según las instrucciones de control proporcionadas por el programador, la ALU se centra en la ejecución de dichas instrucciones a través de cálculos específicos. La UC también contiene un reloj o generador de pulsos que controla la velocidad a la que se llevan a cabo estas operaciones elementales, medida en MegaHercios (MHz).

La capacidad de la ALU para procesar **valores binarios (0 y 1)** es fundamental, ya que todos los datos en el sistema se representan de esta manera. Un bit es la unidad mínima de información que puede almacenar el sistema, siendo un 0 o un 1. Ocho bits conforman un byte, suficiente para almacenar un carácter. La **capacidad de almacenamiento** se mide habitualmente en bytes, reflejando la cantidad de información que el sistema puede manejar.

El rendimiento del sistema depende en gran medida de la ALU y su capacidad para manejar **operaciones aritméticas complejas y lógicas** con rapidez y precisión. Las instrucciones residuales en la memoria principal son ejecutadas por la ALU bajo la supervisión de la UC, lo que garantiza que los datos sean **procesados correctamente** y los resultados se transmitan a otros componentes del sistema, como las unidades de almacenamiento y los dispositivos de entrada/salida (E/S).

Es importante destacar la importancia del rendimiento de la ALU en aplicaciones complejas como el **desarrollo de juegos, simulaciones científicas y procesamiento de gráficos**, donde las operaciones precisas y rápidas son esenciales para un funcionamiento eficaz del software. Asimismo, su papel es relevante en otras áreas tecnológicas innovadoras, tales como **inteligencia artificial y aprendizaje automático**, donde el procesamiento en tiempo real de grandes volúmenes de datos es esencial para entrenar y ejecutar modelos predictivos.

4.1.2. Unidad de Control

La **Unidad de Control (UC)** es uno de los componentes más importantes de un sistema de cómputo. Su función principal es dirigir y coordinar las operaciones de otros componentes del ordenador. Este se asegura de que las instrucciones del programa que residen en la memoria principal se **ejecuten correctamente**, y de que los datos se procesen de forma ade-

cuada. La UC trabaja en estrecha colaboración con la **Unidad Aritmético-Lógica (ALU)** para formar la **Unidad Central de Proceso (CPU)**, también conocida como microprocesador.

El corazón de la UC es un **reloj o generador de pulsos**, que determina la velocidad a la que se realizan las operaciones elementales del ordenador. La velocidad del reloj se mide en **MegaHercios (MHz)** o **GigaHercios (GHz)**, y esta frecuencia determina cuántas operaciones puede realizar la CPU por segundo. Un reloj con una frecuencia más alta implica que el ordenador puede realizar más operaciones por segundo, mejorando así el rendimiento general del sistema.

Dentro de la estructura de la UC, se encuentran varios componentes clave, tales como los **registros**, que son pequeñas unidades de almacenamiento utilizadas para guardar temporalmente datos e instrucciones. La UC también contiene **decodificadores y circuitos de control** que interpretan las instrucciones provenientes de la memoria y generan señales de control para ejecutar dichas instrucciones.

Unidades de almacenamiento

Las **unidades de almacenamiento** juegan un papel crítico en el funcionamiento de la UC. La memoria principal, que incluye la **ROM (Memoria de Solo Lectura) y la RAM (Memoria de Acceso Aleatorio)**, es donde residen los programas en ejecución y los datos asociados. La UC accede a la RAM para obtener las instrucciones y datos necesarios, y utiliza estas informaciones para dirigir las operaciones del sistema. Por otro lado, el almacenamiento externo, como discos duros, cintas, CDs y DVDs, se utiliza para guardar grandes cantidades de datos de manera persistente.

Unidad de Entrada/Salida (E/S)

La UC coordina también las operaciones con la **Unidad de Entrada/Salida (E/S)**. Los dispositivos de E/S, como el teclado, ratón, monitor e impresora, permiten la interacción entre el usuario y el ordenador. La UC garantiza que los datos ingresados a través de estos dispositivos se transmitan correctamente a la memoria y que los resultados procesados se muestren de manera adecuada en los dispositivos de salida.

Para ilustrar su funcionamiento, imagine un escenario en el que se desea realizar una **operación aritmética básica**, como la suma de dos números. La UC recupera las instrucciones de la memoria principal que indican cómo realizar la suma. Luego, estas instrucciones se decodifican para generar las señales de control apropiadas, que permiten que la ALU realice la operación de suma. Finalmente, los resultados se almacenan en un registro o se envían a un dispositivo de salida bajo la supervisión de la UC.

4.2. Memoria principal y memoria secundaria. Diferencias. Conexión

La **memoria principal**, también conocida como memoria central o interna, incluye los tipos **ROM** (Read-Only Memory) y **RAM** (Random Access Memory).

ROM y RAM

- La **ROM** es permanente y no volátil, lo que significa que mantiene su contenido incluso cuando el equipo se apaga. Por otro lado, la **RAM** es volátil y pierde su contenido al apagar el ordenador. La RAM es donde residen los programas que están en ejecución y sus datos asociados, proporcionando un acceso casi inmediato debido a su alta velocidad. Sin embargo, esta memoria es costosa y suele tener una capacidad limitada, lo cual restringe la cantidad de datos y programas que se pueden gestionar simultáneamente.

Almacenamiento externo

- En contraste, el **almacenamiento externo** o **memoria secundaria** incluye dispositivos como discos duros, cintas, CDs y DVDs. Esta memoria está diseñada para almacenar grandes cantidades de información de manera no volátil, lo que implica que los datos se conservan incluso cuando el equipo se apaga. Aunque ofrece una mayor capacidad y es menos costosa, su tiempo de recuperación es considerablemente más lento en comparación con la memoria principal. La información en esta memoria se organiza en archivos o ficheros independientes, permitiendo una estructura más flexible para el almacenamiento a largo plazo.

Figura 3. Plato magnético de disco duro y brazo lector/escritor

La **conexión** entre estos tipos de memoria es fundamental para la operatividad del ordenador. Cuando un programa o dato se requiere para su uso inmediato, se transfiere desde la memoria secundaria a la memoria principal.

- Esta transferencia se gestiona a través del **bus del sistema**, que facilita la comunicación eficiente entre ambos tipos de memoria y con el procesador.

- Además, existen jerarquías de buses que mejoran el rendimiento del sistema, como el **bus local** que conecta el procesador con la memoria caché.

- Este bus local permite aislar el tráfico de entrada/salida (E/S) del procesador, posibilitando transferencias de información entre la memoria y los dispositivos de E/S sin interrumpir la actividad del procesador.

- Otra característica clave es el **bus de expansión**, que reduce el tráfico en el bus del sistema y permite transferencias más eficientes entre la memoria caché y la memoria principal.

Estos buses de expansión son **estándar y accesibles** por el usuario, proporcionando una interfaz para conectar dispositivos adicionales como tarjetas de video, adaptadores de red y otros periféricos. Esta arquitectura modular permite que los dispositivos de distintas velocidades se conecten al sistema **sin degradar el rendimiento global**.

Esta organización y diferencia en la funcionalidad entre la memoria principal y la memoria secundaria no solo optimiza el rendimiento del sistema, sino que también asegura una **gestión eficaz de los recursos**, permitiendo al usuario ejecutar múltiples aplicaciones de manera eficiente.

Las **memorias DDR5**, introducidas en 2023, han duplicado el ancho de banda respecto a DDR4, alcanzando velocidades de hasta 6.4 Gbps. Esto, combinado con **discos NVMe Gen4**, ha reducido considerablemente los tiempos de carga en aplicaciones de alto consumo de recursos, como análisis de datos y renderización gráfica.

4.3. Unidad de entrada-salida. Tipos de entrada-salida

En el ámbito del desarrollo de aplicaciones, la **unidad de entrada-salida (E/S)** desempeña un papel clave al facilitar la comunicación entre el usuario y el ordenador, en la que los dispositivos de E/S actúan como **intermediarios** que permiten la transmisión de datos e instrucciones. Los dispositivos de entrada posibilitan al usuario introducir datos y comandos en el sistema, mientras que los dispositivos de salida muestran los resultados y el estado del sistema.

Entre los dispositivos de entrada más comunes se encuentran el **teclado**, el **ratón**, y el **micrófono**.

El teclado se conecta al sistema a través de un conector especial y es esencial para la introducción de texto y otros comandos escritos.

El ratón, que se conecta mediante puertos serie o PS/2, permite la navegación gráfica y es vital en entornos de interfaz gráfica de usuario (GUI).

Por otro lado, el micrófono se utiliza para la captura de sonido, fundamental en aplicaciones multimedia y de reconocimiento de voz.

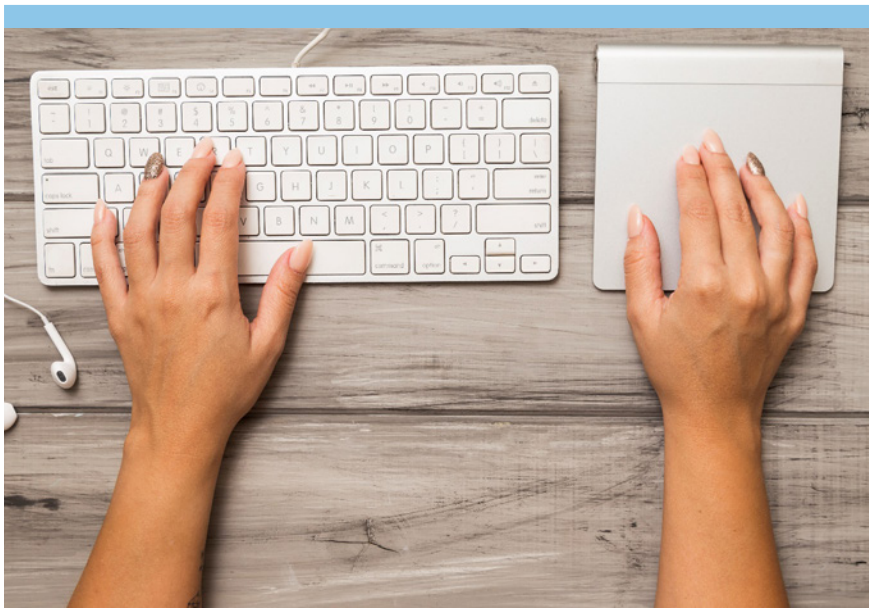


Figura 4. Persona usando teclado y ratón

Del lado de los dispositivos de salida, el **monitor** y la **impresora** son los más comunes. El monitor, conectado a través de un conector específico en la tarjeta de video, muestra **información visual** y es esencial en cualquier sistema informático para la visualización de datos e interacción con el software. La impresora, generalmente conectada por puerto USB en equipos actuales, permite la producción física de documentos y gráficos.

Figura 5. Impresora en funcionamiento

Existen diferentes tipos de entrada-salida que varían según su función y la forma en que interfieren con el sistema.

Un primer tipo es la entrada-salida por programa

- Donde el procesador o CPU gestiona directamente la comunicación con los dispositivos de E/S, lo que puede llegar a ser ineficiente debido al alto consumo de tiempo de procesamiento.

Otro tipo es la entrada-salida por interrupciones

- Dnde el dispositivo de E/S señala a la CPU que necesita atención, permitiendo que el procesador realice otras tareas mientras espera la señal. Esto aumenta la eficiencia del sistema al reducir el tiempo que la CPU debe dedicar a la gestión de E/S.

Finalmente, está la entrada-salida directa (DMA)

- En la que un controlador de DMA maneja la transferencia de datos entre la memoria y los dispositivos de E/S sin intervención constante de la CPU. Esto optimiza aún más el rendimiento, especialmente en sistemas que requieren transferencias de grandes volúmenes de datos.

El avance en las tecnologías de conexión, como el **Puerto USB**, ha revolucionado la interacción con dispositivos de E/S al proporcionar una alta velocidad de transferencia y la posibilidad de conectar una **amplia gama de periféricos**, incluyendo impresoras y escáneres, de manera más eficiente que con los antiguos puertos serie y paralelo.

La adopción de **USB4** o USB-C ha optimizado el rendimiento en la comunicación de dispositivos E/S, permitiendo transferencias de hasta 40 Gbps y soporte para **pantallas 4K simultáneas**. Además, los controladores de E/S basados en inteligencia artificial han comenzado a priorizar tareas de alta demanda, asegurando una distribución eficiente de los recursos.

4.4. Conexión con periféricos

La conexión con periféricos en el desarrollo de aplicaciones es un aspecto esencial que garantiza la comunicación efectiva entre el sistema y los dispositivos externos. Los periféricos, que abarcan desde dispositivos de almacenamiento masivo hasta equipos de entrada-salida y puertos de comunicación, son fundamentales para la funcionalidad de cualquier entorno informático.

Dispositivos de almacenamiento masivo

Los dispositivos de almacenamiento masivo como disqueteras, discos duros, y unidades de CD-ROM o DVD, se conectan a la placa madre a través de controladores de discos. Tradicionalmente, estos dispositivos eran de tipo IDE, aunque los dispositivos SCSI también son comunes debido a su mayor velocidad, aunque a un costo superior. Además, ciertos dispositivos, como las unidades ZIP o grabadoras de CD-ROM, pueden conectarse mediante puertos paralelos. Esto proporciona una ventaja en términos de portabilidad, ya que permite trasladar la unidad fácilmente de un lugar a otro, aunque con un impacto en la velocidad de transferencia de datos.

Puertos de comunicación

Puertos de comunicación juegan un papel vital en la conexión de periféricos. La evolución tecnológica ha visto una transición desde los puertos serie y paralelo hacia el uso cada vez más común del puerto USB. El puerto serie transmite información bit a bit, lo que limita su velocidad en comparación con el puerto paralelo, que transmite byte a byte, aumentando la velocidad de transferencia ocho veces. Sin embargo, ambos tipos de puertos están siendo reemplazados progresivamente por el puerto USB debido a su mayor velocidad y versatilidad para conectar una amplia gama de dispositivos como impresoras, escáneres y más.

5. Normas de seguridad y prevención de riesgos laborales

Las normas de seguridad en el desarrollo de aplicaciones, tanto multiplataforma como web, buscan garantizar un entorno seguro mediante el cumplimiento de leyes de protección de datos, la adopción de estándares como la ISO/IEC 27001 y la mitigación de riesgos como el phishing o el malware. Esto incluye políticas de ciberseguridad, capacitación continua y medidas preventivas, promoviendo así seguridad y eficiencia operativa en el ámbito laboral.

5.1. Entorno legislativo

Las normativas vigentes en el ámbito de desarrollo de aplicaciones multiplataforma y desarrollo de aplicaciones web requieren un conocimiento detallado del **entorno legislativo**. Esta área abarca diversas regulaciones que afectan tanto a las condiciones de trabajo como a la seguridad y salud de los profesionales involucrados en este sector.

Condiciones de seguridad

- En primer lugar, es esencial comprender las **condiciones de seguridad** relativas a la **selección, adquisición, instalación, uso y mantenimiento de los equipos e instalaciones** utilizados en el desarrollo de aplicaciones. Normativas como la Ley 31/1995 de Prevención de Riesgos Laborales y el **Real Decreto 486/1997** establecen las disposiciones mínimas de seguridad y salud en los lugares de trabajo, asegurando la estabilidad, el espacio y los servicios auxiliares necesarios. Estos reglamentos proporcionan un marco para garantizar que las instalaciones, como las eléctricas y de climatización, cumplan con los estándares de seguridad.

Operaciones potencialmente peligrosas

- Los **procedimientos para la realización de operaciones potencialmente peligrosas** son asimismo regulados. Realizar tareas en entornos con riesgos específicos, como la manipulación de cargas pesadas o trabajos en atmósferas explosivas, exige seguir protocolos estrictos. Por ejemplo, el Real Decreto 487/1997 sobre la manipulación manual de cargas establece normativas claras para la prevención de riesgos dorsolumbares.

Ambiente de trabajo

- La legislación también aborda las **condiciones aplicables al ambiente de trabajo físico, químico y biológico**. Factores como el ruido, las vibraciones y las radiaciones deben ser controlados para minimizar el estrés térmico y otros riesgos. La implementación de reglamentos que regulan los niveles permitidos de estos factores es esencial para mantener un ambiente de trabajo seguro y saludable.

Colectivos específicos

- Además, es vital considerar las normativas sobre s**eguridad y salud en el trabajo para colectivos específicos**, como embarazadas, menores o trabajadores con condiciones de hipersensibilidad. La adecuación de las jornadas laborales y la contratación temporal también están reguladas para proteger a estos grupos vulnerables, asegurando que tengan condiciones de trabajo seguras y justas.

Un aspecto no menos importante es la **formación e información de los trabajadores**. Las normativas exigen que los empleados estén adecuadamente informados sobre los riesgos asociados a su trabajo y las medidas de prevención necesarias. De acuerdo con el **Real Decreto 39/1997**, los servicios de prevención deben proporcionar formación continua y detallada, basada en la información proporcionada por fabricantes y expertos en seguridad.

La normativa de ciberseguridad ha incorporado directrices específicas como el **Reglamento Europeo de Ciberresiliencia** (Cyber Resilience Act), que obliga a los desarrolladores de software y hardware a garantizar que sus productos cumplan con estándares de seguridad durante todo el ciclo de vida del producto. Esto es especialmente relevante en entornos multiplataforma donde la interoperabilidad aumenta los riesgos de vulnerabilidades.

5.2. Normas ISO sobre gestión de seguridad de la información

La norma **UNE-ISO/IEC 27002** reemplaza a la antigua **UNE-ISO/IEC 17799:2002** y establece un conjunto actualizado de **buenas prácticas para la gestión de la seguridad de la información**. Esta normativa proporciona directrices para desarrollar, implementar, mantener y mejorar los sistemas de gestión de seguridad en cualquier organización, cubriendo áreas clave como la política de seguridad, la organización de la seguridad, la gestión de activos, la protección de recursos humanos, la seguridad física y del entorno.

- La **política de seguridad** sigue siendo el núcleo de estas buenas prácticas, definiendo cómo gestionar y proteger la información. Es esencial que se asignen responsabilidades específicas, distinguiendo entre los encargados de la información, los servicios, la seguridad y los sistemas, para evitar confusiones y asegurar un control adecuado. Además, esta política debe incluir mecanismos para coordinar y resolver conflictos de forma efectiva.

- En el ámbito de la **seguridad física y del entorno**, se deben implementar controles que protejan instalaciones, equipos y personal frente a amenazas. Esto incluye el uso de medidas preventivas para mitigar riesgos como robos, desastres naturales o accesos no autorizados. Por otro lado, la **gestión de activos** exige asegurar la protección de todos los recursos críticos, como datos, hardware y software, durante todo su ciclo de vida.

- La norma también pone énfasis en la gestión de recursos humanos, abarcando desde la selección hasta la desvinculación del personal. Es imprescindible garantizar que los empleados comprendan sus responsabilidades de seguridad, mediante programas de formación y concienciación continuos.

Entre los aspectos destacados de la norma están la **gestión de la continuidad del negocio** y la **respuesta a incidentes de seguridad**, que aseguran que las operaciones puedan continuar ante interrupciones y que los incidentes se gestionen de manera efectiva. Estas medidas deben ser revisadas y actualizadas periódicamente para mantenerse vigentes frente a nuevas amenazas.

Por su parte, la norma **ISO/TR 21965:2019** y la **ISO 15489** actualizan las directrices sobre preservación y gestión documental. Estas normas garantizan la conservación segura de los documentos electrónicos a largo plazo y la creación de políticas de gestión de documentos que respalden las actividades de la organización. Estas prácticas son esenciales para asegurar la **evidencia, trazabilidad y rendición de cuentas** en las transacciones y operaciones de las empresas.

5.3. Riesgos más frecuentes del trabajo informático

En el ámbito del desarrollo de aplicaciones , los **riesgos más frecuentes del trabajo informático** son diversos y abarcan desde problemas de seguridad hasta trastornos relacionados con la ergonomía y el estrés psicosocial.

Caídas	Riesgo eléctrico	Riesgo de incendio
Uno de los riesgos más recurrentes son las **caídas**, que pueden ocurrir tanto al mismo nivel como a distinto nivel. Estos accidentes frecuentemente tienen lugar debido a la presencia de cables mal gestionados en el suelo o al uso incorrecto de escaleras de mano. Para mitigar estas situaciones, es esencial mantener las áreas de trabajo ordenadas, asegurarse de que los cables estén organizados y utilizar correctamente las escaleras.	Otro aspecto relevante es el **riesgo eléctrico**. La manipulación de dispositivos eléctricos y electrónicos conlleva la posibilidad de cortocircuitos y descargas eléctricas. Es crucial asegurarse de que todo el equipo esté correctamente aislado y ubicado lejos de fuentes de agua para evitar accidentes.	El **riesgo de incendio** también está presente dado el uso continuo de equipos eléctricos. Implementar medidas preventivas, como tener extintores disponibles y evitar la sobrecarga de enchufes, es fundamental para minimizar este riesgo.

La **exposición a factores ambientales** como el disconfort térmico y acústico puede ser perjudicial para los desarrolladores. Trabajar en un ambiente con temperatura y ruido inadecuados puede afectar la **concentración y productividad**, además de generar malestar físico. Adecuar el entorno laboral, proporcionando una temperatura confortable y reduciendo el ruido, es esencial.

El uso continuado de **pantallas de visualización de datos** sin seguir prácticas ergonómicas adecuadas puede llevar a trastornos musculoesqueléticos y fatiga visual. Para evitar estos problemas, es recomendable colocar la pantalla a unos 40 cm de distancia, con la parte superior a la altura de los ojos. Además, es conveniente utilizar reposamuñecas, mantener el codo apoyado en la mesa formando un ángulo de 90° y graduar el brillo y contraste de la pantalla.

En lo que respecta a los riesgos psicosociales, la **elevada carga de trabajo** y las **altas demandas cognitivas** pueden ocasionar estrés y agotamiento mental en los desarrolladores. Una estrategia para mitigar estos riesgos incluye la implementación de pausas regulares, la rotación de tareas y la promoción de un equilibrio entre la vida laboral y personal.

Aunque no es común en el trabajo informático, la **manipulación ocasional de cargas** pesadas puede presentar un riesgo. Es esencial evitar levantar más de 25 kg en el caso de los hombres y más de 15 kg en el de las mujeres, utilizar medios auxiliares como carretillas siempre que sea posible y situar los objetos a una altura adecuada para no forzar la postura.

Desde 2023, se ha promovido el uso de **herramientas basadas en realidad aumentada** para la formación en prevención de riesgos. Estas tecnologías permiten simular entornos laborales peligrosos y capacitar a los empleados sin exponerlos a situaciones reales de riesgo, mejorando significativamente la conciencia y las prácticas preventivas.

6. Características de las redes. Ventajas e inconvenientes

Las redes de ordenadores facilitan la interconexión de dispositivos y recursos, permitiendo compartir información y aplicaciones de forma eficiente y segura, lo que optimiza costos y aumenta la productividad empresarial. Aunque son clave en la comunicación rápida y precisa en un mundo globalizado, también conllevan desafíos como riesgos de seguridad y complejidad en su gestión. Un adecuado diseño y mantenimiento, apoyado en conocimientos especializados, es crucial para garantizar su eficiencia y protección ante amenazas.

6.1. Motivación e importancia de las redes de ordenadores

Las redes de ordenadores han evolucionado desde la transmisión de voz en el siglo XIX hasta convertirse en una estructura compleja que conecta dispositivos a nivel global, utilizando conexiones físicas e inalámbricas. Inicialmente, los ordenadores funcionaban de forma centralizada, pero este modelo dio paso a sistemas interconectados que distribuyen recursos de manera más eficiente.

Actualmente, estas redes facilitan la comunicación y el intercambio de información de forma rápida y eficaz. Tecnologías como las redes locales (LAN) y de área amplia (WAN) han transformado el acceso, almacenamiento y distribución de datos, aportando flexibilidad y escalabilidad tanto a organizaciones como a individuos.

6.1.1. Topologías y tecnologías de red

Las topologías de red más comunes, como la **estrella**, **anillo**, **malla** y **bus**, presentan diferentes ventajas y particularidades dependiendo del escenario de aplicación. Por ejemplo, las redes en estrella facilitan la detección de **fallos** y el mantenimiento, mientras que las redes en malla ofrecen una mayor **redundancia** y resiliencia, esenciales para aplicaciones críticas.

Ethernet y tecnologías como **Wi-Fi** son ejemplos de avances contemporáneos que han permitido la conexión de dispositivos tanto mediante cables como de manera inalámbrica.

Ethernet, conocida por su **estándar 802.3**, es predominante en redes de área local debido a su robustez y velocidad, mientras que Wi-Fi, bajo el estándar 802.11, ha permitido la conectividad móvil y la flexibilidad de ubicación de dispositivos.

6.1.2. Componentes y protocolo

El diseño y la arquitectura de las redes de ordenadores no serían posibles sin los componentes de hardware y software que los conforman. **Routers**, **switches**, **servidores** y **puntos de acceso** inalámbrico son algunos de los elementos esenciales que constituyen la infraestructura física de estas redes. Por otro lado, el software de red y los **protocolos** de comunicación, como TCP/IP, permiten la organización y gestión de la transmisión de datos.

Es importante mencionar que la **arquitectura de red** está estructurada en diferentes niveles según el modelo de referencia OSI (Interconexión de Sistemas Abiertos). Este modelo está dividido en siete capas: **física, enlace de datos, red, transporte, sesión, presentación y aplicación**. Cada capa tiene una función específica, desde la caracterización del medio físico hasta la codificación y abstracción de la información transmitida.

6.1.3. Beneficios de una red bien estructurada

Una red bien planificada y ejecutada no solo mejora la comunicación, sino que también **incrementa la productividad**, mejora la **seguridad** de los datos y facilita la **colaboración** entre los usuarios. Un ejemplo práctico de los beneficios de una red descentralizada se observa en un entorno corporativo donde múltiples departamentos pueden acceder a recursos compartidos, como bases de datos y aplicaciones, sin los cuellos de botella típicos de un sistema centralizado.

Tecnologías como **Zero Trust Network Access (ZTNA)** han ganado popularidad en la seguridad de redes locales y sistemas distribuidos. Este enfoque niega por defecto todo acceso a la red, otorgando permisos únicamente a dispositivos y usuarios autenticados, lo que minimiza los riesgos de acceso no autorizado. Además, la integración de herramientas como **Cisco Secure Network Analytics** permite supervisar el tráfico interno para detectar y responder proactivamente a amenazas.

6.1.4. Inconvenientes de las redes de ordenadores

Aunque las redes de ordenadores aportan numerosos beneficios, también presentan una serie de inconvenientes que deben ser considerados para su correcta implementación y gestión. Algunos de los principales son:

Riesgos de seguridad

- La interconexión global expone los sistemas a diversas amenazas, como ataques cibernéticos, malware y accesos no autorizados. A pesar de los avances en herramientas de protección como ZTNA y análisis de tráfico, mantener la seguridad sigue siendo un desafío constante.

Complejidad en la gestión

- Diseñar, implementar y mantener una red, especialmente aquellas con topologías y tecnologías avanzadas, requiere conocimientos técnicos especializados. Esto incluye garantizar la compatibilidad entre dispositivos, gestionar configuraciones y actualizar componentes regularmente.

Altos costos iniciales

- La inversión en infraestructura, como routers, switches y puntos de acceso, puede ser significativa, especialmente en redes complejas y robustas. Además, los costos de mantenimiento y actualización pueden incrementarse con el tiempo.

Dependencia de la red

- En entornos corporativos, una caída de la red puede generar interrupciones significativas en las operaciones, afectando la productividad y la capacidad de respuesta.

Obsolescencia tecnológica

- La rápida evolución de las tecnologías de red obliga a las organizaciones a actualizarse constantemente para mantenerse competitivas, lo que implica gastos adicionales y una curva de aprendizaje para el personal técnico.

7. Tipos de redes

Las redes se clasifican según su alcance y funcionalidad. Las PAN (Personal Area Networks) son redes de área personal, limitadas a un individuo y su entorno cercano, permitiendo la conexión de dispositivos como teléfonos y wearables. Las LAN (Local Area Networks) abarcan áreas más grandes, como edificios o pequeños campus, y se utilizan en entornos corporativos para conectar computadoras y recursos. Las WLAN (Wireless Local Area Networks) extienden las LAN al ámbito inalámbrico, permitiendo la conexión de dispositivos a través de Wi-Fi, lo que aumenta la flexibilidad y accesibilidad en diversos entornos.

7.1. PAN

Las **redes personales** o **PAN** (Personal Area Networks) son aquellas destinadas a la interconexión de dispositivos y servicios a través de una misma persona, generalmente en un espacio reducido como un cuarto, oficina o entorno doméstico. La característica primordial de una PAN es la **limitación de su alcance**, que generalmente no supera los diez metros. Esta limitación permite que los dispositivos personales —como teléfonos móviles, tabletas, ordenadores portátiles, auriculares, impresoras y otros periféricos— se conecten de manera eficiente y sin necesidad de infraestructura compleja.

A diferencia de las LAN (Local Area Networks) y WAN (Wide Area Networks), las PAN están diseñadas principalmente para **facilitar la vida diaria de los usuarios en un entorno inmediato**. Por lo tanto, utilizan tecnologías de conexión, como Bluetooth, ZigBee o incluso infrarrojos, que son adecuadas para cortas distancias. Estas tecnologías tienen la ventaja de ser económicas y de bajo consumo energético, lo que las hace ideales para dispositivos móviles y wearables.

Figura 5. Interconexión de dispositivos en redes LAN

Un aspecto clave en el diseño y utilización de las PAN es la **privacidad y seguridad de los datos**. Dada la proximidad física de los dispositivos conectados, es fundamental implementar mecanismos de cifrado robustos para asegurar que las comunicaciones entre dispositivos sean seguras y no puedan ser interceptadas por intrusos. Esto es especialmente relevante en redes inalámbricas, donde el medio de transmisión es compartido y más susceptible a ataques.

Internet de las Cosas

El uso de PAN se ha extendido con el auge del **Internet de las Cosas (IoT)**, donde múltiples dispositivos inteligentes interactúan entre sí para proporcionar servicios automatizados y personalizados. Por ejemplo, una PAN podría conectar un smartwatch a un smartphone, a una bicicleta eléctrica y a un sistema de alarma doméstico, permitiendo una integración fluida y control centralizado desde el teléfono móvil del usuario.

Con el crecimiento del **Internet de las Cosas (IoT)** y los dispositivos interconectados, las PAN han incorporado tecnologías como **Bluetooth 5.2**, que ofrece mayor velocidad, menor latencia y un alcance extendido, superando los límites tradicionales. Además, el desarrollo de **UWB (Ultra-Wideband)** ha permitido una precisión superior para dispositivos de geolocalización y control gestual, ampliando las aplicaciones de estas redes en hogares inteligentes y dispositivos médicos.

7.2. LAN

En el ámbito del diseño y desarrollo de aplicaciones, la comprensión y administración de **redes de área local (LAN)** es esencial. Estas redes están diseñadas para cubrir distancias limitadas, abarcando desde unos pocos metros hasta varios kilómetros, adaptándose perfectamente para conectar dispositivos en hogares, oficinas o campus universitarios. La estructura de una LAN permite a los usuarios compartir recursos y datos de manera eficiente y rápida, gracias a la proximidad física y la utilización de tecnologías avanzadas.

- Inicialmente, las LAN se caracterizaban por emplear un medio de difusión para enviar información, lo que implicaba un único canal de comunicación compartido por todos los dispositivos de la red.

- Sin embargo, con la evolución tecnológica, el uso de conmutadores y la adopción de topologías de estrella y árbol han transformado las LAN en redes de conexiones punto-a-punto.

- Esta evolución ha permitido un incremento considerable en la velocidad y confiabilidad de la red, facilitando una mejor gestión del tráfico de datos y reduciendo las colisiones de información.

Un aspecto destacado de las LAN es la forma en que conectan diferentes dispositivos a través de **nodos intermedios**, como routers y switches, que optimizan la ruta de los datos. A pesar de los avances, algunas LAN aún utilizan medios de difusión como las **redes inalámbricas (WiFi)**. Estas redes inalámbricas, aunque comparten ciertos principios de las LAN alámbricas, tienen características únicas debido a su utilización del aire como medio de transmisión, lo que las hace susceptibles a interferencias y variaciones en la calidad de la conexión.

Los **objetivos del diseño de una LAN** incluyen varios factores clave que deben considerarse para asegurar su funcionalidad y eficiencia. En primer lugar, la **funcionalidad** de la red debe estar alineada con los requisitos laborales de los usuarios, garantizando la conectividad necesaria entre usuarios y aplicaciones con una velocidad y confiabilidad adecuadas. La **escalabilidad** es otra consideración crucial; una LAN debe ser capaz de crecer y adaptarse sin necesidad de cambios significativos en su diseño original, permitiendo la inclusión de nuevos dispositivos y tecnologías.

Asimismo, la **adaptabilidad** de la red es vital para asegurar que futuras tecnologías puedan ser integradas sin obstáculos. Las organizaciones deben evitar la implementación de componentes que puedan limitar la evolución tecnológica. La **facilidad de administración** es otro objetivo esencial. Una red bien diseñada debe ser fácil de supervisar y administrar, asegurando una operación continua y estable.

Ethernet de par trenzado	Tarjeta de red
Una de las tecnologías más comunes en las LAN es el **Ethernet de par trenzado** con conector RJ-45, soportando conexiones de 100 Mbps o 1 Gbps. Este tipo de conexión es estándar en la mayoría de los dispositivos modernos, incluyendo placas base que incorporan estas interfaces de red. Esta tecnología es vital no solo en entornos empresariales, sino también en hogares, donde los routers ADSL con conexión Ethernet son comunes.	La **tarjeta de red** es uno de los componentes más importantes en una LAN, permitiendo la conexión física del dispositivo a la red. Algunas tarjetas de red ofrecen funciones adicionales como **Wake On LAN (WOL)**, que permite encender remotamente un equipo a través de la red, y **PXE (Pre-Boot Execution Environment)**, que facilita la inicialización de un equipo desde la red, lo cual es útil en entornos corporativos para tareas de mantenimiento y despliegue de sistemas.

7.3. WLAN

Una **WLAN (Wireless Local Area Network)**, también conocida como red WiFi, es un tipo de red informática que utiliza ondas de radio para transmitir información sin necesidad de cables físicos. Estas redes permiten interconectar dispositivos como ordenadores, smartphones, tablets y otros equipos habilitados para WiFi, cubriendo distancias que pueden variar desde unos pocos metros hasta aproximadamente 100 metros, dependiendo de los obstáculos y del entorno.

IEEE 802.11

La tecnología WLAN se basa en el estándar **IEEE 802.11**, que ha evolucionado significativamente desde su creación. Inicialmente, este estándar permitía velocidades de transmisión de hasta 11 Mbps, pero versiones posteriores, como **802.11n, 802.11ac**, y la más reciente **802.11ax** (WiFi 6), han incrementado las velocidades y capacidades de la red. Por ejemplo, **WiFi 6** ofrece una velocidad teórica de hasta 9.6 Gbps y mejoras en la eficiencia y capacidad de la red, haciéndola ideal para entornos con alta densidad de dispositivos.

Las WLAN emplean generalmente una arquitectura basada en **topologías de estrella**, donde un punto de acceso (AP) actúa como centro de la red y coordina la comunicación entre los distintos dispositivos conectados. Además, los puntos de acceso pueden estar conectados entre sí a través de una red cableada o inalámbrica, formando lo que se conoce como una **red de malla**. Esta configuración permite extender el alcance de la WLAN y mejorar su cobertura.

Dado que las WLAN utilizan el espectro de radio frecuencias, pueden enfrentar problemas de **interferencias** y **seguridad**. Las interferencias pueden provenir de otros dispositivos que utilizan la misma banda de frecuencia, como microondas o teléfonos inalámbricos. Para mitigar esto, se pueden utilizar canales no solapados y tecnologías de mitigación de interferencias. En cuanto a la seguridad, es crucial implementar medidas como **WPA3 (Wi-Fi Protected Access 3)**, que ofrece un cifrado más robusto y protección contra ataques de fuerza bruta.

Respecto a las aplicaciones prácticas en el ámbito del desarrollo de aplicaciones, es esencial comprender cómo estas redes afectan la **latencia**, el **ancho de banda** y la **disponibilidad** de los servicios. Por ejemplo, una aplicación web que requiere transmisión de video en alta definición necesitará una WLAN con buena capacidad y baja latencia para asegurar una experiencia de usuario fluida.

Con la adopción de **WiFi 6E** y la llegada de **WiFi 7** en 2024, las WLAN han experimentado una mejora sustancial en velocidad, capacidad y reducción de latencia. Estas tecnologías utilizan bandas adicionales, como la de 6 GHz, para minimizar la congestión y mejorar el rendimiento en entornos densos. Esto es particularmente beneficioso en **oficinas modernas y espacios públicos**, donde múltiples dispositivos compiten por el ancho de banda. También destacan las aplicaciones en entornos industriales, donde las WLAN soportan redes privadas para IoT.

8. Componentes de una red informática

Los nodos son dispositivos conectados a una red, como ordenadores y servidores, mientras que los medios de transmisión, como fibra óptica, cableado de cobre o tecnologías inalámbricas, facilitan el flujo de datos. Protocolos como TCP/IP aseguran una comunicación eficiente y segura entre nodos, siguiendo reglas estándar. El modelo OSI divide esta interacción en siete capas, simplificando el diseño y solución de problemas. El Protocolo IP gestiona la asignación de direcciones únicas y el enrutamiento de paquetes, apoyándose en técnicas como subnetting y supernetting para optimizar el uso de direcciones y mejorar la eficiencia de las redes.

8.1. Nodos y medios de transmisión

En una red de ordenadores, la comunicación entre distintos dispositivos se realiza a través de **nodos y medios de transmisión**.

Nodos	Medios de transmisión
Entendemos por nodos tanto a los dispositivos finales, como ordenadores o servidores, como a aquellos que facilitan y gestionan el tráfico de información, tales como routers y switches. Cada nodo en una red debe identificarse de forma única para asegurar una comunicación efectiva y evitar confusiones. Este proceso de identificación se logra comúnmente mediante direcciones IP y direcciones MAC.	Los **medios de transmisión** son los canales físicos a través de los cuales se envía la información entre los nodos. Estos pueden ser alámbricos, como cables de cobre y fibra óptica, o inalámbricos, como ondas de radio y tecnologías de infrarrojos. La elección del medio de transmisión depende de varios factores, como el alcance requerido, la velocidad de transmisión y el costo. Por ejemplo, las redes basadas en fibra óptica pueden proporcionar velocidades superiores y menor latencia en comparación con los cables de cobre, aunque a un costo mayor.

Es importante tener en cuenta los problemas que pueden surgir al transmitir información a alta velocidad entre nodos. Un emisor puede **enviar datos demasiado rápido para que el receptor los procese adecuadament**e, lo que podría llevar a la pérdida de información. Para mitigar esto, se emplean técnicas de **control de flujo** como la retroalimentación, donde el receptor envía señales al emisor para indicar si puede manejar la velocidad de transmisión. Además, se pueden implementar **mecanismos para limitar la velocidad** del emisor cuando sobrepasa ciertos umbrales.

Otro desafío es la **longitud de los mensajes**. Algunos niveles del sistema de red no pueden manejar mensajes largos y requieren que estos se dividan en unidades más pequeñas. Los mecanismos de **fragmentación y reensamblaje** permiten desglosar la información para su transmisión y posteriormente reconstruir los mensajes completos en el destino final.

Multiplexación y desmultiplexación	Gestión del enlace
La **multiplexación y desmultiplexación** son técnicas utilizadas para optimizar la transmisión cuando varias conexiones deben compartir un número limitado de circuitos físicos. La multiplexación combina múltiples señales en un solo canal, mientras que la desmultiplexación separa estas señales en el destino apropiado.	La eficiencia de una red también depende de la **gestión del enlace**, que incluye el inicio, mantenimiento y finalización de las conexiones entre nodos. Una correcta gestión asegura que la comunicación se realice eficientemente y sin interrupciones.

En las redes de difusión, donde múltiples dispositivos comparten un medio único, es esencial controlar el acceso al medio para evitar colisiones. Este control, denominado **MAC (Medium Access Control)**, garantiza que cada nodo tenga la oportunidad de transmitir datos sin interferencias de otros nodos. Las redes de difusión permiten que los mensajes se propaguen a todos los nodos. Sin embargo, solo el nodo destinatario acepta el mensaje, mientras que los demás lo ignoran.

La **capa de transporte** tiene un rol vital en garantizar que los datos lleguen desde el emisor hasta el receptor de manera segura y eficiente. Esta capa es responsable de **establecer, mantener y finalizar las conexiones**, además de gestionar el flujo de datos y corregir errores

de transmisión. A diferencia de las capas inferiores que manejan la comunicación por saltos, la capa de transporte facilita un diálogo de extremo a extremo entre los dispositivos finales.

La implementación de redes de fibra óptica pasiva (PON) ha permitido alcanzar **velocidades ultrarrápidas en conexiones punto-a-multipunto**, eliminando la necesidad de equipos activos intermedios. Estas redes optimizan el consumo energético y la escalabilidad, resultando ideales para aplicaciones empresariales e infraestructuras urbanas.

8.2. Protocolos de red

Los **protocolos de red** son un conjunto de normas y reglas que permiten la comunicación entre dispositivos en una red informática. Estas normas dictan cómo se **envían, reciben y gestionan los datos en una red**, garantizando que la información llegue a su destino de manera eficiente y segura. Los protocolos de red se dividen en diferentes capas según el modelo OSI y el modelo TCP/IP, que son las arquitecturas de red más ampliamente utilizadas.

Capa física

- En la capa física, los protocolos especifican el medio de transmisión y las señales eléctricas, ópticas o inalámbricas que se utilizan para enviar datos. Ejemplos de estos protocolos incluyen las normas EIA RS-232-C, usadas en los puertos serie de los ordenadores personales, y las especificaciones IEEE 802.3, 802.4 y 802.5 para redes LAN de difusión. Los dispositivos que operan en este nivel incluyen hubs Ethernet, multiplexores y módems.

Capa de enlace

- La capa de enlace se encarga de proporcionar una comunicación fiable de bits a través de un medio físico. Sus principales funciones son la sincronización a nivel de trama, el control de acceso al medio y la corrección de errores. Este nivel agrupa los bits en tramas y establece delimitadores de origen y destino para asegurar la correcta recepción de los datos. Los conmutadores de circuitos y los Hubs Token Ring son equipos típicos en esta capa.

Capa de red

- En la capa de red, se destaca la gestión del encaminamiento y el control de la congestión. Esta capa es central en la arquitectura de la red, ya que permite la interconexión de múltiples redes. El protocolo IP es el más importante en este nivel y se encarga de la fragmentación y reensamblaje de paquetes, la gestión de direcciones IP y el reenvío de paquetes entre redes. Otros ejemplos de protocolos en esta capa incluyen ITU-T X.25, IPv6 y OSPF.

Capa de transporte

- La capa de transporte proporciona una transferencia fiable de datos entre aplicaciones que corren en hosts diferentes. En esta capa se encuentran los protocolos TCP y UDP. TCP es un protocolo orientado a conexión que garantiza la entrega de los datos en el orden correcto y sin pérdidas, mientras que UDP es un protocolo no orientado a conexión que permite el envío de datagramas sin garantizar su entrega.

Capa de aplicación

- En la capa de aplicación, se gestionan las interacciones entre aplicaciones y el intercambio de datos. Algunos ejemplos de protocolos en este nivel son HTTP para la transferencia de páginas web, FTP para la transferencia de archivos y SMTP para el envío de correos electrónicos.

8.3. Modelo OSI

El modelo OSI, **Open Systems Interconnection**, fue desarrollado por la Organización Internacional de Estándares (ISO) con el propósito de establecer normas y estándares que permitieran la **interoperabilidad** entre software y dispositivos de diferentes fabricantes. Esta iniciativa busca facilitar las comunicaciones entre sistemas variopintos y evitar la hegemonía de arquitecturas de un solo fabricante, como la SNA de IBM, que imperaban en la época.

El modelo OSI se compone de siete niveles o capas, donde cada capa agrupa funciones o **protocolos específicos** necesarios para la comunicación entre sistemas. Estos niveles son: físico, de enlace de datos, de red, de transporte, de sesión, de presentación y de aplicación. Los principios que guiaron la definición de estas capas incluyen la creación de **una capa para cada nivel de abstracción requerido**, la realización de una función bien definida por cada capa y la resolución de problemas dentro de una capa sin afectar a las demás.

Cada capa del modelo OSI desempeña un papel clave en el proceso de comunicación:

1. **Capa Física**: Se encarga de la transmisión de bits a través de un medio físico. Define las características eléctricas y físicas del hardware.

2. **Capa de Enlace de Datos**: Proporciona la transferencia de datos entre dos nodos conectados directamente y corrige errores de transmisión.

3. **Capa de Red**: Se ocupa del direccionamiento y el envío de paquetes entre dos sistemas que no están conectados directamente.

4. **Capa de Transporte**: Asegura la transferencia confiable de datos entre sistemas, incluyendo la segmentación y reensamblaje de los datos.

5. **Capa de Sesión**: Maneja y controla las conexiones entre sistemas, estableciendo, gestionando y terminando sesiones entre aplicaciones.

6. **Capa de Presentación**: Traduce entre la forma de datos utilizada por la red y la forma utilizada por la aplicación, incluyendo la encriptación y la compresión de los datos.

7. **Capa de Aplicación**: Proporciona servicios de red a las aplicaciones del usuario final, como correo electrónico, transferencia de archivos y terminal remoto.

El modelo OSI no solo sirve como guía teórica para entender y diseñar redes, sino que también ofrece un marco de referencia para comparar y contrastar otras arquitecturas de red, como el **modelo TCP/IP**. Aunque el OSI es más teórico y modular, diferenciando claramente entre servicios, interfaces y protocolos, el TCP/IP ha sido más implementado en la práctica. Ambos modelos tienen sus particularidades y aplicaciones, con el TCP/IP siendo más orientado a la implementación práctica y OSI proporcionando un mayor grado de estructura teórica.

> Para visualizar cómo funciona la comunicación en el modelo OSI, se puede imaginar un escenario donde un correo electrónico (que opera en la capa de aplicación) es enviado a través de distintas capas, **encapsulándose y desencapsulándose** los datos en cada capa hasta llegar a su destino.

Así, el modelo OSI sigue siendo una referencia esencial en el estudio y comprensión de redes, a pesar de que nunca se implementó de manera tan extensiva como TCP/IP.

8.4. Protocolo IP

El Protocolo de Internet (**IP** por sus siglas en inglés, Internet Protocol) es una pieza fundamental en la arquitectura de la red y se encuentra en la **capa de red** del modelo TCP/IP. Su principal función es el **encaminamiento** de paquetes desde un origen hasta un destino a través de **direcciones IP jerárquicas**. Este método de direccionamiento permite identificar redes y subredes de manera eficiente, facilitando la transmisión de información a través de diversos nodos.

Capa de red

La capa de red es crucial para mantener la comunicación y estabilidad del sistema, ya que esta se encarga de gestionar la congestión en la red y de determinar las mejores rutas para los datos. En el contexto de Internet, la capa de red proporciona un servicio de conmutación de paquetes no orientado a conexión, lo que significa que cada paquete puede tomar distintos caminos para llegar a su destino. Esta flexibilidad asegura la resistencia a interrupciones, característica vital en el diseño inicial de Internet promovido por el Departamento de Defensa de los Estados Unidos.

Los primeros protocolos orientados a implementar la transmisión de paquetes IP fueron **SLIP** y **PPP**, ambos utilizados principalmente en conexiones entre nodos a través de líneas dedicadas. Estos protocolos permiten encapsular los paquetes IP para su **transmisión por diversos medios físicos**, desde cables de cobre hasta enlaces inalámbricos.

En IP, existen dos tipos fundamentales de protocolos de nivel 3: **protocolos encaminados** y **protocolos de encaminamiento**. Los primeros son responsables de llevar la información de usuario desde una fuente hasta un destino, mientras que los segundos son utilizados por los nodos de la red para descubrir y seleccionar las mejores rutas para la transmisión de datos. Esta doble funcionalidad permite a IP no solo transferir información eficientemente, sino también mantener un **conocimiento actualizado de la topología de la red.**

La evolución de IP ha llevado al desarrollo de **IPv6**, que está siendo implantado gradualmente para solucionar limitaciones de su predecesor, **IPv4**, principalmente la escasez de direcciones disponibles. Además, el protocolo IP se complementa con dos protocolos auxiliares clave: **ARP** (Address Resolution Protocol), que traduce direcciones lógicas a direcciones físicas, e **ICMP** (Internet Control Message Protocol), que maneja mensajes de control y errores en la red.

8.5. Subnetting y supernetting. Supuestos prácticos

La segmentación de redes es fundamental para mejorar la eficiencia y la seguridad de los sistemas informáticos. **Subnetting** y **supernetting** son técnicas esenciales para gestionar y optimizar el uso de las direcciones IP disponibles.

El subnetting permite dividir una red grande en subredes más pequeñas, lo que facilita la gestión y el control del tráfico de red.

Por otro lado, el supernetting combina varias redes más pequeñas en una sola red más grande, lo que puede ser útil para reducir la carga en las tablas de enrutamiento.

Uno de los requisitos clave para la segmentación de red es que el tráfico debe segregarse de manera que cada dispositivo solo tenga acceso a la información que necesita. Esto se puede lograr mediante el uso de **Redes de Área Local Virtuales (VLAN)**, que permiten la creación de múltiples dominios de difusión dentro de la misma infraestructura física. Cada VLAN puede configurarse para servir a **diferentes grupos de usuarios**, por ejemplo, separando a los usuarios, servicios y administración en distintas subredes.

Además, las comunicaciones inalámbricas deben implementarse en **segmentos separados** para minimizar las interferencias y mejorar la seguridad. Las VLAN pueden ser útiles en este contexto, ya que permiten separar el tráfico inalámbrico del tráfico por cable. A nivel avanzado, se podría emplear **Redes Privadas Virtuales (VPN)** para extender la segmentación a través de diferentes ubicaciones geográficas, mejorando así la seguridad y el control del tráfico de red.

8.5.1. Supuestos prácticos

SUBNETTING

Supongamos que se tiene una red con la dirección IP 192.168.1.0/24 y se necesita dividirla en cuatro subredes. El primer paso es calcular el nuevo prefijo de subred. Al dividir en cuatro subredes, se necesitan dos bits adicionales (2^2 = 4), pasando así de /24 a /26. Las subredes resultantes serían 192.168.1.0/26, 192.168.1.64/26, 192.168.1.128/26 y 192.168.1.192/26. Cada subred albergará 62 hosts útiles, mejorando la eficiencia y facilitando el control del tráfico, proporcionando acceso exclusivo según los diferentes requisitos de información y servicios.

SUPERNETTING

Ahora imagine que se gestionan múltiples subredes pequeñas, todas con direcciones IP en el rango de 172.16.0.0/24. Para simplificar la administración y reducir la carga en las tablas de enrutamiento, se puede utilizar supernetting. Si combinamos ocho de estas subredes, el nuevo prefijo será /21 (8 subredes —> 3 bits de subred original: 172.16.0.0/21). Esto permite que los routers gestionen una sola entrada en lugar de ocho, reduciendo significativamente la complejidad.

Ejemplo ilustrativo de VLAN y VPN

Para escenarios empresariales, se podría utilizar VLANs para separar el tráfico entre diferentes departamentos, como Usuarios (VLAN 10), Servicios (VLAN 20), y Administración (VLAN 30). Por ejemplo, los empleados que acceden a servicios internos estarían en VLAN 20 y tendrían acceso limitado a información administrativa. Además, al utilizar VPNs, los trabajadores remotos podrían acceder a estas VLANs de manera segura, como se muestra en un campus universitario donde los profesores y el personal administrativo acceden a sus respectivas VLANs desde ubicaciones remotas.

9. Topologías de red

Las topologías de red más comunes en el desarrollo de aplicaciones incluyen estrella, anillo, bus y árbol, cada una con características que las hacen idóneas según el contexto. La topología en estrella destaca por su facilidad de gestión y aislamiento de fallos individuales, aunque depende críticamente del nodo central. La configuración en anillo asegura una transmisión eficiente y ordenada, pero puede ser compleja y vulnerable a fallos en cualquier nodo. La topología en bus es económica en recursos, pero limitada en escalabilidad y susceptible a interrupciones. Elegir la topología adecuada según las necesidades del proyecto es clave para garantizar eficiencia y fiabilidad en la red.

9.1. Topologías de red más usadas

Todos los equipos en una red de topología **bus** están conectados a un único medio de transmisión que es compartido entre todas las estaciones de la red. La estructura lineal de esta topología requiere **establecer un sistema de acceso al medio** para evitar que más de una estación transmita al mismo tiempo, lo que produciría colisiones. Este método de acceso es importante para garantizar un **flujo de datos ordenado y eficiente**. En escenarios prácticos, la red Ethernet es una aplicación clásica de esta topología, a menudo configurada en entornos con una carga de datos relativamente baja y una configuración sencilla.

En una topología **anillo**, los nodos están conectados en serie formando un bucle. Cada estación se conecta al anillo mediante dos enlaces: uno de entrada y otro de salida. Cuando una estación emisora recibe su propio paquete lo elimina de la red, **evitando redundancias**. Sin embargo, esta estructura conlleva un mayor costo y una eficiencia inferior comparada con alternativas como Ethernet. Antes común en tecnologías como Token Ring y FDDI, la topología anillo sigue siendo relevante en aplicaciones específicas como la **Resilient Packet Ring (IEEE 802.17)**, utilizada en anillos de fibra óptica para transportar tráfico Ethernet y servicios IP.

Una topología **estrella** se organiza alrededor de un nodo central que actúa como nodo intermedio de la red, gestionando el envío y recepción de datos. Este nodo puede ser un **conmutador o un encaminador** y su función principal es centralizar la gestión del tráfico de la red. Los equipos finales están conectados directamente a este nodo central, facilitando el aislamiento y solución de problemas. Esta estructura es típica en entornos **LAN** (Red

de Área Local) y ha demostrado ser muy eficiente en términos de rendimiento y escalabilidad, permitiendo upgrades simples y expansiones mediante la adición de nuevos nodos sin afectar la operativa global de la red.

La **topología en árbol** combina características de las topologías en bus y estrella, creando una estructura jerárquica. Varios nodos intermedios se conectan entre sí y a su vez tienen conectados equipos finales. Esta configuración es la más utilizada en la actualidad dada su **flexibilidad y capacidad para gestionar grandes redes** de forma eficiente. Se puede encontrar frecuentemente en redes corporativas y sistemas complejos donde es necesario tener diferentes niveles de acceso y control sobre las distintas partes de la red. La **jerarquía** facilita la organización y segmentación del tráfico, mejorando la seguridad y gestión de recursos.

En una topología **mallada**, todos los equipos están conectados entre sí, formando una red de alta redundancia. Existen variantes parciales donde las estaciones no forman una malla completa, pero aún mantienen un **nivel significativo de conectividad redundante**. Esta topología es ideal para aplicaciones críticas que no pueden permitirse fallos en la red, como en sistemas militares o de control industrial, donde la fiabilidad y resistencia a fallos son esenciales. La topología mallada ofrece múltiples caminos entre nodos, lo que **minimiza la probabilidad de interrupciones** en el servicio debido a fallos en uno o varios enlaces.

Desde 2024, las **topologías híbridas** han ganado protagonismo al combinar características de diferentes modelos, como estrella y malla, para adaptarse a las **necesidades de redes modernas**. Estas configuraciones son comunes en grandes centros de datos y redes empresariales, donde la redundancia y escalabilidad son esenciales para soportar servicios en la nube y aplicaciones IoT.

9.2. Ventajas y desventajas de cada topología

Como hemos visto, las topologías de red presentan características distintas que se adaptan a necesidades específicas. La **topología en bus** destaca por su simplicidad y bajo costo, siendo ideal para redes pequeñas, aunque sufre de vulnerabilidad ante fallos en el cable principal y limitaciones en su capacidad de expansión. En contraste, la **topología en anillo** minimiza colisiones y mantiene la calidad de transmisión mediante nodos repetidores, pero su complejidad y costos elevados la han relegado en favor de alternativas más modernas.

La **topología en estrella**, una de las más utilizadas actualmente, centraliza el control de la red, lo que facilita la gestión y mejora la eficiencia. Sin embargo, el nodo central representa un punto único de fallo crítico. Por otro lado, la **topología en árbol** combina las ventajas del bus y la estrella, ofreciendo una estructura jerárquica adecuada para redes grandes, aunque su complejidad puede ser un desafío en términos de mantenimiento.

Finalmente, la **topología mallada** proporciona máxima redundancia, siendo ideal para aplicaciones críticas, pero a un costo elevado debido a la gran cantidad de conexiones necesarias. Las redes híbridas y las tecnologías como las redes definidas por software (SDN) han permitido mitigar las desventajas de estas topologías al introducir mayor flexibilidad y control dinámico.

10. Tipo de cableado. Conectores

En el desarrollo de aplicaciones, la infraestructura de red utiliza diversos tipos de cableado según las necesidades. El par trenzado, común en redes LAN, emplea conectores RJ para conexiones rápidas y fiables. Para ambientes con alta interferencia electromagnética, el cable coaxial con conectores RG y BNC ofrece durabilidad y robustez. La fibra óptica es esencial en aplicaciones de alta velocidad y largas distancias, con conectores como MT-RJ, FC, ST, LC y SC, que minimizan pérdidas de señal y maximizan la transferencia de datos. La instalación adecuada de estos sistemas requiere herramientas especializadas para garantizar una red eficiente y confiable.

10.1. Cable de par trenzado. Conectores RJ

En el desarrollo de redes de telecomunicaciones para aplicaciones multiplataforma y aplicaciones web, el **cable de par trenzado** con **conectores RJ** es un componente esencial. La estructura básica del cable de par trenzado consiste en dos cables de cobre que se entrelazan en espiral para reducir la interferencia electromagnética, tanto externa como entre los mismos pares. Esta característica es vital para mantener la integridad de la señal en entornos con interferencias elevadas, como oficinas llenas de equipos electrónicos.

Existen varias **categorías de cables de par trenzado**, desde la categoría 3, que soporta velocidades de hasta 10 Mbps, hasta la categoría 7, que puede manejar hasta 10 Gbps. Las categorías superiores utilizan un blindaje adicional para cada par de cables, lo que proporciona mayor protección contra las interferencias electromagnéticas.

Conectores RJ

- Los cables de par trenzado se conectan mediante conectores RJ, comúnmente RJ-45 para las redes Ethernet. Estos conectores tienen ocho pines que se alinean con los cables del par trenzado, permitiendo la transmisión de datos. Para una correcta instalación, es esencial seguir los estándares de cableado T568A o T568B. Dichos estándares definen el orden de los cables dentro del conector para asegurar la compatibilidad y el rendimiento óptimo de la red.

- Un aspecto crucial de los conectores RJ-45 es su orientación y la importancia de una terminación adecuada. Utilizando herramientas como el crimpador, se asegura una conexión firme y estable entre el cable de par trenzado y el conector. Además, la consistencia en la ordenación de los cables es vital para evitar problemas de red, como la pérdida de paquetes o la reducción de la velocidad de transmisión.

Desde 2024, la **categoría 8 de cables de par trenzado** ha ganado popularidad en entornos de centros de datos y redes empresariales avanzadas. Este estándar permite alcanzar velocidades de hasta **40 Gbps** en distancias cortas, siendo ideal para infraestructuras de alta densidad y aplicaciones como la virtualización de servidores y el almacenamiento en red.

10.2. Cable coaxial. Conectores RG, BNC

Veamos ahora las características de los siguientes cables:

Cable coaxial

- El **cable coaxial** es un tipo de cable eléctrico que consta de un conductor central de cobre rodeado por una capa de aislamiento, un apantallado metálico que actúa como segundo conductor y una cubierta exterior protectora. Su diseño singular, en el cual los dos conductores están dispuestos de forma concéntrica, proporciona una transmisión eficiente de señales eléctricas a frecuencias de radio.

Conectores RG

- Los conectores RG (Radio Guide) son un estándar para diseños de cables coaxiales que se utilizan en una variedad de aplicaciones que van desde la transmisión de video y audio, hasta comunicaciones e instalaciones de redes de datos. Estos conectores se dividen en varios tipos, donde cada tipo se identifica por un número único como RG-6, RG-59, etc., cada uno con características específicas que los hacen idóneos para diferentes usos, como la transmisión de señales de televisión en el hogar o líneas de transmisión de datos en entornos industriales.

Conectores BNC

- Por otro lado, los conectores BNC (Bayonet Neill-Concelman) son comunes en conexiones de radiofrecuencia. Estos conectores cuentan con un mecanismo de bayoneta que proporciona una conexión estable y segura. Son ampliamente utilizados en dispositivos de video profesional, instrumentación y redes coaxiales. La facilidad con la que se pueden conectar y desconectar hace que los BNC sean una opción popular en entornos donde se necesita una instalación rápida y segura.

En términos de **componentes del cable coaxial**, el conductor central de cobre está rodeado por un aislamiento dieléctrico, usualmente de **PVC o un material plástico** similar, que separa el conductor del apantallado externo. Este apantallado puede ser una malla de cobre o una lámina metálica que actúa como una **barrera contra el ruido electromagnético y evita la pérdida de señal**. La capa final es una cubierta externa que generalmente está hecha de material resistente a las condiciones ambientales y proporciona protección mecánica adicional.

Dentro de la seguridad y rendimiento, los **coaxiales** están clasificados en varias categorías de **niveles de tensión**, que varían desde muy baja tensión (hasta 50 V) hasta muy alta tensión (por encima de 770 kV). Los cables coaxiales utilizados en aplicaciones de baja y muy baja tensión generalmente son adecuados para transmisiones de datos y señales de video, mientras que los de alta tensión se utilizan en aplicaciones industriales y de telecomunicaciones que requieren una resistencia adicional.

En aplicaciones modernas, como las **redes 5G y las comunicaciones por satélite**, el cable coaxial sigue siendo relevante gracias a su capacidad para operar en frecuencias extremadamente altas. Los conectores BNC de nueva generación incluyen versiones con conectividad SDI (Serial Digital Interface), ampliamente utilizadas en la industria audiovisual para transmisión de **video en alta definición**.

10.3. Cable de fibra óptica. Conectores MT-RJ, FC, ST, LC y SC.

El cable de fibra óptica es un medio de transmisión hecho de plástico o vidrio, diseñado para transmitir señales en forma de luz. Esta tecnología permite la transmisión de datos a gran velocidad y con una alta resistencia a la corrosión e interferencias, lo cual lo hace ideal para comunicaciones en las que se requiere gran eficiencia y fiabilidad. Uno de los aspectos clave del cable de fibra óptica es la **propagación unidireccional de la luz**; para lograr una comunicación bidireccional, es necesario emplear dos fibras ópticas.

En el contexto de la fibra óptica, los **conectores de fibra óptica** son componentes indispensables que permiten establecer las conexiones mecánicas y ópticas entre el cable de fibra y otros dispositivos o cables. Entre los tipos más utilizados se encuentran:

- **Conector MT-RJ:** Este conector se destaca por su diseño compacto que integra dos fibras en una única unidad. Esta característica facilita la instalación y economiza espacio, siendo una opción popular en aplicaciones de alta densidad, como centros de datos y redes locales.

- **Conector SC (Subscriber Channel):** Utilizado comúnmente en aplicaciones de televisión por cable y dispositivos de red, el conector SC se caracteriza por su mecanismo de conexión y desconexión mediante un sistema de empuje y tirón, lo cual simplifica el proceso de instalación y mantenimiento.

- **Conector FC (Fixed Connection):** Conocido por su uso en aplicaciones de alta precisión como telecomunicaciones y mediciones científicas, el conector FC ofrece una conexión estable y segura mediante un sistema de rosca que asegura una conexión firme, minimizando la pérdida de señal.

- **Conector ST (Straight Tip):** Dotado de un diseño tipo bayoneta, el conector ST es ampliamente utilizado en redes de datos y entornos industriales. Su facilidad de conexión y desconexión lo hace ideal para instalaciones donde la modularidad y flexibilidad son necesarias.

- **Conector LC (Lucent Connector):** Este conector es similar al SC pero con un formato más reducido, lo que lo hace ideal para configuraciones de alta densidad. Es muy utilizado en redes de comunicación de alta capacidad, donde el espacio y el rendimiento son críticos.

El uso de la fibra óptica y sus conectores trae ventajas significativas, tales como una alta **resistencia a la corrosión y a las interferencias electromagnéticas**, y una mayor **inmunidad a la interceptación no autorizada**. A pesar de estos beneficios, uno de sus desafíos es la limitación a la propagación unidireccional de la luz, lo que implica la necesidad de usar dos fibras para comunicaciones bidireccionales.

10.4. Herramientas para el cableado de la red.

El diseño de la Capa 1 en una red, que abarca el tipo de cableado y la estructura general del mismo, es un componente primordial en la construcción de infraestructuras de red robustas y eficientes. Un diseño adecuado ayuda a mitigar problemas comunes de **conectividad y rendimiento**, siendo la auditoría de cableado una práctica esencial cuando se planean cambios significativos en la red. Esta auditoría identifica **áreas que necesitan actualizaciones y nuevo cableado**, asegurando que el sistema cumpla con los estándares y proporcione un rendimiento óptimo.

Para los conductos verticales y el backbone de la red, es recomendable utilizar **cable de fibra óptica**, dado su alto rendimiento y capacidad para manejar grandes cantidades de datos con mínima pérdida de señal. Por otro lado, para los tendidos horizontales, el **cable UTP Categoría 5e** es una opción sólida debido a su balance entre costo y rendimiento. Este tipo de cable asegura una transmisión efectiva dentro de un límite de 100 metros, lo que es adecuado para la mayoría de las aplicaciones en una red local Ethernet.

TIA/EIA-568-A

En relación con los estándares de cableado, el cumplimiento con la especificación **TIA/EIA-568-A** es esencial. Este estándar garantiza que cada dispositivo conectado a la red esté vinculado a una ubicación central a través de cableado horizontal, facilitando una estructura organizada y eficiente. Los tipos de medios utilizados en la Capa 1 incluyen el **par trenzado no blindado (UTP), el par trenzado blindado (STP) de Categoría 5, 5e o 6, y el cable de fibra óptica 100BaseFX**. Cada uno tiene características específicas que los hacen adecuados para distintos tipos de implementaciones y requerimientos de red.

La conexión local (LAN) del tipo **Ethernet de par trenzado** se ha estandarizado en los equipos actuales, lo cual permite una interconexión fácil y efectiva de dispositivos. Estas conexiones, que utilizan conector **RJ-45**, soportan velocidades de 100 Mbps y 1 Gbps, y son comunes en los hogares y oficinas gracias a su integración con routers ADSL. Las tarjetas de red también ofrecen funciones adicionales como **Wake On LAN (WOL)**, que permite el encendido remoto del equipo, y **PXE (Pre-Boot Execution Environment)**, que facilita la inicialización del sistema desde la red.

Herramientas como los **certificadores avanzados de cableado**, incluyendo el Fluke Networks DSX-8000, permiten no solo verificar la continuidad y el correcto crimpado, sino también certificar el **rendimiento del cableado** según los estándares más recientes. Esto resulta indispensable en entornos donde se instalan infraestructuras de alta velocidad como 10GBASE-T o enlaces de fibra óptica.

11. Mapa físico y lógico de una red local

En una red local, el mapa físico describe la disposición tangible de dispositivos, cables y conexiones, mientras que el mapa lógico detalla cómo se organizan y gestionan los flujos de datos entre los equipos, independientemente de su disposición física. Herramientas especializadas permiten visualizar y gestionar estos mapas, optimizando el rendimiento y la seguridad de la red en entornos de desarrollo de aplicaciones multiplataforma o web. Diferenciar ambos enfoques es clave para una infraestructura eficiente y segura.

11.1. Mapa físico

El **mapa físico** (Capa 1) es una representación visual detallada del diseño de la red a nivel de hardware. Este tipo de mapas incluye todos los elementos físicos y su interconexión dentro de una red de área local (LAN). La función principal de un mapa físico es proporcionar una guía clara y precisa para la **implementación** y el **mantenimiento** de la infraestructura de la red. Estos mapas son vitales para el diagnóstico de fallas, ya que permiten identificar y localizar rápidamente cualquier componente que esté causando problemas.

Elementos

- Entre los elementos que se suelen representar en un mapa físico se encuentran los **conectores, cables, puntos de acceso, routers, switches, servidores y estaciones de trabajo.** Estos componentes se muestran con sus especificaciones técnicas, como el tipo y grosor del cable, el número de pines de los conectores y las características del medio de transmisión. Por ejemplo, los cables de red pueden ser representados especificando si son de tipo **Cat5e, Cat6 o fibra óptica**. Además, se detalla la longitud del cableado y su disposición física dentro del espacio de la red.

Documentación

- La documentación de la implementación física y lógica de la red es un aspecto crucial para la **gestión eficiente** y la **escalabilidad** del sistema. En este sentido, los dibujos esquemáticos que forman parte del mapa físico deben actualizarse regularmente para reflejar cualquier cambio en la infraestructura. Un ejemplo de esto podría ser la reubicación de un servidor o la adición de un nuevo punto de acceso inalámbrico.

- La documentación de la capa física también considera **aspectos eléctricos**, **ópticos y electromagnéticos** que afectan la calidad de la transmisión de datos. Por ejemplo, la velocidad de transmisión y la impedancia del cable son factores que deben ser cuidadosamente ajustados y monitorizados para garantizar una comunicación eficiente. En algunos casos, se puede incluir información sobre el **voltaje y el tipo de señal de salida**, aspectos que son críticos para el correcto funcionamiento de la red.

En el diseño de red, la **diferencia entre el mapa físico y el lógico** debe ser bien entendida por los técnicos. Mientras que el primero se enfoca en los aspectos tangibles y las conexiones reales del hardware, el mapa lógico presenta una visión más abstracta de cómo los datos fluyen a través de la red. Esta documentación dual es esencial para abordar diferentes tipos de problemas y asegurar un mantenimiento riguroso y preciso de la infraestructura de red.

Herramientas como **NetBox** han ganado popularidad para documentar y gestionar redes físicas. NetBox permite registrar la ubicación y características de cada componente, desde racks de servidores hasta conexiones individuales, proporcionando una visión global y centralizada de la infraestructura física de una red.

11.2. Mapa lógico

El **mapa lógico** es una representación abstracta de la topología de red que se centra en la disposición y la interconexión de los dispositivos y la estructura de la red sin entrar en los detalles específicos de la instalación del cableado físico. Este tipo de mapa es esencial para la planificación, el diseño y la gestión de redes tanto en contextos de desarrollo de aplicaciones.

Mapa lógico de capa 3

En un **mapa lógico de Capa 3**, se describe cómo los dispositivos dentro de la red están conectados a nivel de red, incluyendo la dirección IP y la lógica de enrutamiento. Este tipo de mapa no solo ayuda a identificar el flujo de datos entre dispositivos, sino también a planificar la gestión y la resolución de problemas de la red. Por ejemplo, en una implementación donde se despliega una aplicación web de gran escala, tener un mapa lógico de Capa 3 permite a los adminis8tradores de red visualizar cómo el tráfico de datos fluye desde servidores de la aplicación hacia los routers y luego hacia los clientes.

Mapa lógico de LAN

- Por otro lado, el **mapa lógico de LAN** se centra en la topología interna de la red local (Local Area Network). Aquí se incluyen elementos clave como switches, puntos de acceso, routers y dispositivos finales, destacando las conexiones lógicas entre ellos. Este mapa es crucial durante la fase de diseño inicial para asegurar que todos los dispositivos puedan comunicarse de manera eficiente y efectiva. Por ejemplo, en el desarrollo de aplicaciones multiplataforma, este mapa facilita a los desarrolladores entender cómo diferentes dispositivos (como dispositivos móviles, computadoras del escritorio y servidores) están relacionados dentro de la misma red.

Para documentar la implementación física y lógica de la red, es necesario complementarlo con **mapas de dirección** que ilustran la asignación de direcciones IP y subredes dentro del sistema. Proporcionan una visión ordenada y clara de cómo se distribuyen las direcciones y permite a los administradores planificar la expansión futura de la red sin conflictos de dirección.

Con el auge de la virtualización y las redes definidas por software (SDN), los mapas lógicos han evolucionado para incluir elementos como **switches virtuales y flujos de datos entre entornos físicos y virtuales**. Herramientas como Cisco DNA Center y VMware NSX son utilizadas para mapear estas arquitecturas híbridas, asegurando una visión integral de la red, tanto física como lógica.

11.3. Herramientas para elaborar el mapa de red

Con el fin de diagnosticar fallos y optimizar el rendimiento, se utilizan diversas herramientas que facilitan la creación precisa y detallada de estos mapas. A continuación, se describen algunas de las herramientas más destacadas para esta tarea.

Microsoft Visio

- Una de las herramientas más populares y robustas es **Microsoft Visio**, que permite a los diseñadores de red crear diagramas detallados utilizando una amplia variedad de plantillas y símbolos específicos para los componentes de la red. Visio ofrece una interfaz intuitiva y funcionalidades como la vinculación de datos en tiempo real, lo cual facilita el seguimiento y la gestión de los dispositivos de la red. Además, Visio puede integrarse con otras herramientas de Microsoft Office, como Excel y SharePoint, permitiendo una actualización y colaboración más eficiente entre equipos.

SolarWinds Network Topology Mapper

- Otra herramienta destacada es **SolarWinds Network Topology Mapper**, que es especialmente útil para redes complejas. SolarWinds ofrece capacidades avanzadas como el mapeo automático de la red, la detección de nuevos dispositivos y la generación de informes detallados. Esta herramienta es capaz de descubrir todos los componentes de la red y generar un mapa interactivo que puede ser usado para análisis más profundos. SolarWinds también incluye funciones de monitoreo y alerta, permitiendo a los administradores identificar y resolver problemas antes de que afecten a los usuarios.

Lucidchart

- **Lucidchart** es otra solución basada en la nube que facilita la creación de diagramas de red. Ofrece una amplia gama de plantillas y símbolos de red y permite la colaboración en tiempo real, lo que es ideal para equipos distribuidos. Lucidchart se integra con múltiples plataformas como Google Drive, Atlassian, y otros servicios en la nube, permitiendo una administración centralizada y acceso fácil a los diagramas desde cualquier ubicación.

Nmap

- El uso de **Nmap** (Network Mapper) es una opción más técnica pero sumamente poderosa para la elaboración de mapas de red. Nmap es una herramienta de código abierto que se utiliza principalmente para la auditoría de seguridad y la exploración de redes. Permite a los usuarios descubrir hosts y servicios en la red, realizar escaneos de puertos y determinar la información del sistema operativo de los dispositivos, entre otras funcionalidades. Debido a su naturaleza extremadamente detallada y su capacidad de interpretación de datos complejos, Nmap es ideal para profesionales con un conocimiento avanzado en el manejo de redes.

12. Resumen

Tras la exposición del tema, queda claro que el estudio de los **sistemas microinformáticos** y las redes en el desarrollo de aplicaciones multiplataforma y web ofrece una base sólida para optimizar el diseño y la gestión de entornos informáticos. Se ha abordado desde la identificación y cuidado de componentes clave del hardware, como procesadores y placas base, hasta el **mantenimiento preventivo** que asegura un rendimiento prolongado. Estas acciones son esenciales para evitar fallos técnicos y mejorar la experiencia de los usuarios finales.

También se ha explicado la importancia de los **sistemas operativos**, que actúan como un puente entre el hardware y las aplicaciones. Destaca su capacidad para gestionar recursos, usuarios y permisos, lo que permite un control más eficiente del entorno de trabajo. Además, las **máquinas virtuales** han sido presentadas como herramientas fundamentales para simular múltiples sistemas operativos en un solo equipo, una solución práctica para pruebas y desarrollo seguro de aplicaciones.

En el ámbito de las redes, se ha subrayado el papel de las topologías, protocolos y medios de transmisión como la fibra óptica y el cableado de par trenzado, que garantizan la **conectividad eficiente** y segura de los dispositivos. Estas redes son vitales para soportar la comunicación y el intercambio de datos entre sistemas, especialmente en aplicaciones web que requieren alta disponibilidad y velocidad.

Finalmente, se han abordado las medidas de **seguridad informática**, abarcando tanto los riesgos físicos como las amenazas cibernéticas. Las normativas legales, las normas **ISO** y las políticas de ciberseguridad se presentan como herramientas indispensables para mitigar ataques y proteger los datos. Esto, combinado con una formación continua, asegura que los sistemas estén preparados para enfrentar desafíos tecnológicos en constante evolución.

13. Bibliografía

- Instituto Nacional de Seguridad y Salud en el Trabajo. (s.f.). *Manual básico de prevención de riesgos laborales*. Ticarte.com. https://www.ticarte.com/sites/su/users/7/arch/prevencion-riegos-laborales-informatica-comunicaciones.pdf

- Fernández, J. (s.f.). *Tema 1: Concepto de ordenador*. Uhu.es. https://www.uhu.es/javier.fernandez/tema1.pdf

- López, Q. (s.f.). *Placa base*. Dis.um.es. https://dis.um.es/~lopezquesada/documentos/IES_1415/LMSGI/curso/xhtml/html17/doc/placabase.pdf

- Molero, L.G. (s.f.). *Diseño de redes de área local*. Wordpress.com. https://anaylenlopez.wordpress.com/wp-content/uploads/2011/03/4-disec3b1o-de-redes-de-area-local.pdf

- Vilajosana Guillén, X., Font Rosselló, M., Lara Ochoa, E., & Serral i Gracià, R. (s.f.). *Redes de ordenadores*. Universitat Oberta de Catalunya. https://openaccess.uoc.edu/bitstream/10609/142846/11/PLA2_Redes%20de%20ordenadores.pdf

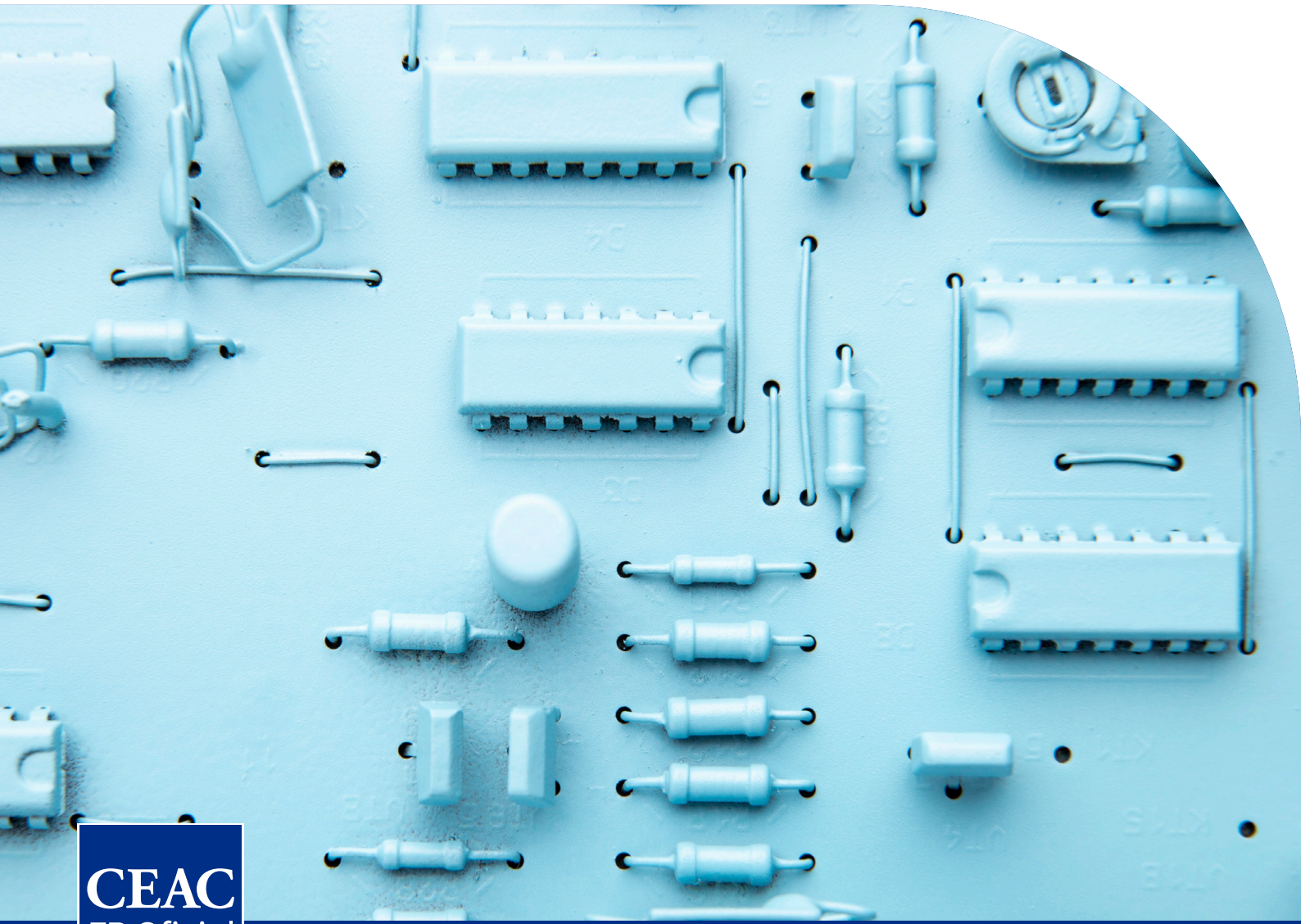
Desarrollo de aplicaciones multiplataforma

MÓDULO:

Sistemas informáticos

UNIDAD:

Instalación de sistemas operativos



CEAC
FP Oficial

MÓDULO:

Sistemas informáticos

UNIDAD:

Instalación de sistemas operativos

CEAC FP Oficial

ÍNDICE

1. Introducción

La mejor explotación de un ordenador pasa necesariamente por la correcta elección, instalación, configuración y mantenimiento de su sistema operativo, ya que es este conjunto de programas el responsable de la gestión de los recursos que proporciona el hardware. El desarrollo de aplicaciones web, el despliegue de dichas aplicaciones e incluso su explotación, son problemas cuyas respectivas soluciones requieren de sistemas informáticos adecuados; en estos casos, los sistemas operativos marcan la diferencia en cuanto a viabilidad y coste.

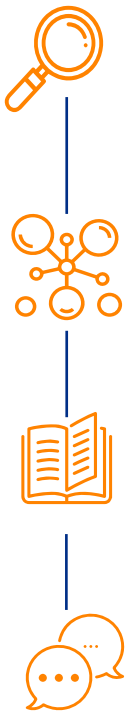
En esta unidad aprenderás a distinguir los diferentes tipos de programas que componen la inteligencia de un ordenador; también conocerás la funcionalidad de un sistema operativo, cuáles son los programas que la llevan a cabo y cómo se relacionan entre ellos. Verás, además, las principales características de un sistema operativo o aplicación y la importancia de las licencias.

También aprenderás a diferenciar los distintos sistemas operativos que existen en el mercado, tanto comerciales como de código libre, y verás las características que hay que tener en cuenta a la hora de implantarlos en un entorno profesional. Haremos un repaso a las razones por las que hay que mantener nuestro sistema actualizado y la manera de hacer dichas actualizaciones sin que produzcan conflictos con nuestro software ya instalado o sin que afecte a los trabajadores de una empresa.

En un último bloque seguiremos el proceso de arranque de un ordenador, viendo paso a paso el proceso que siguen hasta llegar a estar arrancados por completo. Veremos el concepto driver (controlador en inglés), muy extendido en la informática, y definiremos su importancia en todo sistema informático. Analizaremos los casos de aplicación de las máquinas virtuales, unos sistemas cada día más extendidos, que permiten aprovechar los recursos de una máquina compartiendo el hardware entre varios sistemas.

2. Objetivos pedagógicos

Los objetivos de aprendizaje que se pretenden alcanzar con esta unidad son:

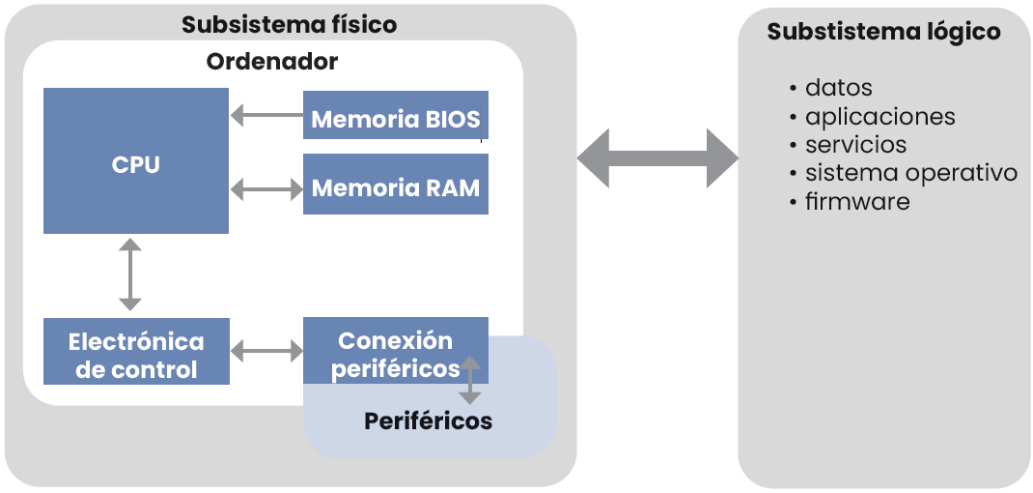


- **Comprender la importancia del sistema operativo en la explotación eficiente de un ordenador, identificando su función esencial en la gestión de recursos hardware y su impacto en la viabilidad y costos de aplicaciones web y su despliegue.**
- **Reconocer y diferenciar los componentes clave de la inteligencia de un ordenador, incluyendo los tipos de programas que lo componen y su relación con la funcionalidad del sistema operativo.**
- **Analizar y comparar diferentes tipos de sistemas operativos, tanto comerciales como de código libre, para evaluar sus características y determinar su idoneidad en entornos profesionales.**
- **Investigar y describir el proceso de arranque de un ordenador, detallando cada etapa del proceso hasta el arranque completo.**

3. Instalación de sistemas operativos

3.1. Estructura de un sistema informático

Recordemos que, como hemos visto en el módulo anterior, un sistema informático (un ordenador) está formado por dos subsistemas: el **subsistema físico**, que vimos con detalle en la unidad anterior, y el **subsistema lógico** o software.



Un sistema informático está formado por los subsistemas físico y lógico.

La siguiente clasificación muestra los diferentes tipos de software según su función en un sistema informático:

- **Software de base**: El software de base es esencial para la comunicación directa con el hardware y constituye los fundamentos sobre los cuales se apoyan otras categorías de software. Incluye dos aspectos principales:
- **Sistemas operativos**: Estos sistemas gestionan el hardware de un sistema informático y brindan una interfaz amigable para facilitar su uso por parte del usuario. Algunos ejemplos de sistemas operativos son Microsoft Windows (tanto la versión de escritorio como la de servidor), MacOS de Apple y varias distribuciones de GNU/Linux, como Debian, Fedora, Ubuntu, entre otras. También se incluyen los sistemas operativos de dispositivos móviles, como Android de Google y iOS de Apple.
- **Software incluido en el hardware**: Además de los sistemas operativos, el software de base también abarca el software que viene preinstalado en el hardware. Un ejemplo de esto es la BIOS (o su versión más moderna, UEFI), que es un tipo especial de firmware. Estos programas están integrados en los componentes del hardware y desempeñan funciones clave en la comunicación con el sistema operativo y la configuración inicial del dispositivo.

La BIOS, o Sistema Básico de Entrada y Salida, es un software incorporado en un chip de memoria no volátil en un sistema informático. Su función principal es realizar el arranque y la verificación inicial del sistema antes de ceder el control al sistema operativo.

El UEFI, o Interfaz Unificada de Firmware Extensible, es una especificación que establece una interfaz entre el sistema operativo y el firmware. Fue desarrollado por Intel en 2002 como una mejora y reemplazo de la interfaz BIOS.

El firmware se refiere al software que determina el funcionamiento en el nivel más bajo y controla los circuitos electrónicos de cualquier dispositivo. Es un tipo de software integrado en los componentes del dispositivo y proporciona instrucciones para su correcto funcionamiento.

- **Software de programación:** El software de programación ha evolucionado considerablemente en comparación con la época en la que los informáticos programaban en ensamblador o código máquina. En la actualidad, se utilizan herramientas avanzadas tanto para el desarrollo de la lógica de los programas como para ayudar a diseñar interfaces gráficas de usuario.

  Dentro de esta categoría de software se incluyen todas las herramientas diseñadas para asistir a los programadores de aplicaciones, permitiéndoles trabajar de manera eficiente e incluso detectar errores o deficiencias en sus programas.

  Algunos ejemplos de este tipo de software son NetBeans, Eclipse, Visual Studio Code, IntelliJ y PhpStorm. Estas herramientas ofrecen una amplia gama de funcionalidades y características que facilitan el proceso de desarrollo de software.

- **Software de aplicación:** Los software de aplicación son programas informáticos diseñados para realizar tareas específicas y satisfacer las necesidades de los usuarios en diferentes ámbitos. Estos programas están destinados a ser utilizados por personas o empresas para llevar a cabo diversas actividades, como gestionar información, realizar cálculos, crear documentos, editar imágenes, reproducir multimedia, comunicarse, entre otros.

  Los software de aplicación abarcan una amplia variedad de categorías y se pueden encontrar en diferentes áreas, como la productividad (procesadores de texto, hojas de cálculo, herramientas de presentación), la creatividad (editores de imágenes, software de diseño gráfico, programas de música), la comunicación (navegadores web, clientes de correo electrónico, aplicaciones de mensajería), la gestión (software contable, sistemas de gestión de proyectos) y muchas otras áreas.

  Estos programas están diseñados para facilitar y mejorar la realización de tareas específicas, ofreciendo una interfaz intuitiva y funcionalidades adaptadas a las necesidades de los usuarios. Algunos ejemplos comunes de software de aplicación incluyen Microsoft Office, Adobe Photoshop, Google Chrome, WhatsApp y Spotify, entre muchos otros.

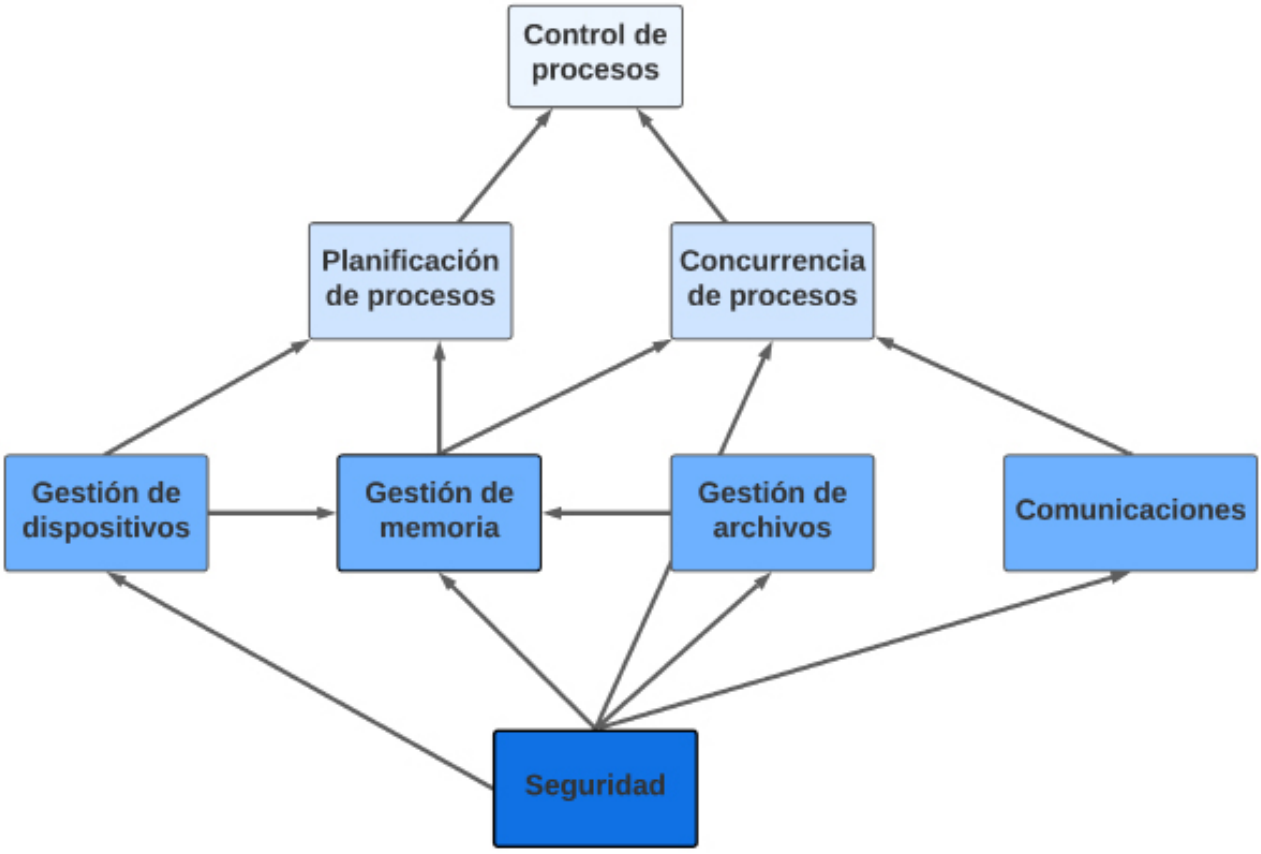
- **Datos**. Los datos son informaciones manejadas o procesadas por el ordenador, pero que en ningún caso le dicen a este lo que tiene que hacer para resolver un problema. Pueden ser números, textos, imágenes, vídeos, archivos, etc. Los datos se almacenan en diferentes formatos y se utilizan para realizar operaciones y generar resultados.

- **Redes**: Las redes permiten la comunicación y el intercambio de datos entre diferentes sistemas informáticos. Pueden ser redes locales (LAN) que conectan dispositivos dentro de un área limitada, como una oficina, o redes de área extensa (WAN) que conectan sistemas en diferentes ubicaciones geográficas. Las redes utilizan protocolos de comunicación y dispositivos de red como routers, switches y cables para transmitir datos de manera eficiente y segura.

2.2 Funciones de un sistema operativo

La misión de un sistema operativo es gestionar y facilitar el acceso del resto de programas a los recursos físicos de un ordenador. Realiza las siguientes funciones:

- **Gestión de tareas.** Los sistemas operativos actuales son multitarea, lo cual significa que la CPU debe repartir su tiempo de trabajo entre varios programas activos procesándolos en pequeños fragmentos en lugar de esperar a acabar uno para poder comenzar otro. Esto da la sensación al usuario de que los programas trabajan de manera simultánea. El sistema operativo se encarga de realizar todo este proceso, permitiendo que múltiples programas funciones de manera aparentemente simultánea para el usuario.
- **Gestión de dispositivos.** Un sistema operativo conoce cuáles son las operaciones que debe realizar sobre un dispositivo físico para que este cumpla su propósito, proporciona al resto de programas herramientas de comunicación para que estos puedan usar los recursos de manera simplificada y protege a los dispositivos de las consecuencias de un acceso desordenado.
- **Control de entrada y salida.** El sistema operativo gestiona y ordena la entrada de datos procedente del exterior, así como la salida de datos al exterior. Esto asegura una interacción uniforme entre el usuario y los dispositivos, adaptando las solicitudes y datos a cada dispositivo particular, y utilizando técnicas como el spooling para evitar bloqueos y optimizar el rendimiento del sistema.
- **Administración de la RAM.** El sistema operativo controla el acceso de programas y datos a la memoria RAM, así como el uso auxiliar de dispositivos externos para superar las limitaciones de capacidad física de esta y la reserva de una parte de la RAM para mejorar la velocidad efectiva al utilizar dispositivos externos.
- **Recuperación de errores.** Un sistema operativo debe contribuir a mantener funcionando las tareas que operan correctamente aun cuando se hayan producido sucesos inesperados debidos a un fallo de programación de una tarea o al mal funcionamiento de un dispositivo.



El sistema operativo gestiona los recursos mediante tareas interdependientes.

3.3. Arquitectura de un sistema operativo

Un sistema operativo se caracteriza por los siguientes elementos:

- **Núcleo o Kernel.** El núcleo es el corazón del sistema operativo y se encarga de administrar y coordinar todas las funciones del sistema. Controla el acceso al hardware y proporciona servicios básicos, como la gestión de memoria, la planificación de procesos, la administración de archivos y la comunicación entre los componentes del sistema.

  - ***Monolíticos.*** Es una arquitectura de sistema operativo donde este, en su totalidad, trabaja en el espacio del núcleo. Difiere de otras arquitecturas en que solo define una interfaz virtual de alto nivel sobre el hardware del ordenador. Este núcleo está programado de forma no modular y puede tener un tamaño considerable.

    A su vez, cada vez que se añada una nueva funcionalidad, el núcleo deberá ser recompilado en su totalidad y luego reiniciado. Un problema que presentan estas arquitecturas es que todos los componentes funcionales del núcleo tienen acceso a todas sus estructuras de datos internas y a sus rutinas, lo que implica que un error en una rutina podría propagarse a todo el sistema.

  - ***Micronúcleos.*** En este modelo, el núcleo se mantiene mínimo y solo proporciona servicios esenciales, como la gestión de memoria y la comunicación entre procesos. Otras funcionalidades, como la gestión de archivos y dispositivos, se implementan como servicios externos que se ejecutan fuera del núcleo. Este enfoque se basa en el principio de modularidad y separación de responsabilidades.

    Los micronúcleos son más robustos, ya que el mal funcionamiento de un proceso no tiene por qué bloquear el funcionamiento del resto del sistema-, son de pequeño tamaño y más flexibles que los núcleos monolíticos, pero son bastante más lentos y hacen el código más complejo.

  - ***Híbridos.*** Funcionan fundamentalmente como micronúcleos, pero el núcleo principal es bastante más grande y con funcionalidades propias de los núcleos monolíticos. Intentan guardar el mejor equilibrio entre eficiencia y flexibilidad, sin comprometer el rendimiento.

  - ***Exonúcleo***. Este diminuto núcleo solamente ofrece protección de procesos y manejo de recursos. Se denomina así debido a que toda la funcionalidad deja de estar presente en la memoria y pasa a estar en el exterior, en librerías activas.

- **Gestor de procesos:** Este elemento se encarga de administrar y controlar los procesos del sistema. Incluye funciones como la creación, ejecución, suspensión, reanudación y terminación de los procesos. También se encarga de la asignación de recursos y la planificación de la ejecución de los procesos en el procesador.

- **Gestor de memoria:** El gestor de memoria se encarga de administrar el espacio de memoria disponible en el sistema. Controla la asignación y liberación de memoria a los procesos, garantizando la eficiencia y evitando conflictos de acceso. También se encarga de la gestión de la memoria virtual, que permite utilizar más memoria de la disponible físicamente a través de técnicas como la paginación y la segmentación.

- **Sistema de archivos:** Este elemento se encarga de la gestión de los archivos y directorios en el sistema. Proporciona una estructura jerárquica para organizar y acceder a los datos almacenados en el sistema de almacenamiento. Permite la creación, lectura, escritura y eliminación de archivos, así como el control de los permisos y la seguridad de los mismos.

- **Gestor de dispositivos:** El gestor de dispositivos se encarga de administrar y controlar los dispositivos de hardware conectados al sistema. Proporciona una interfaz para la comunicación entre el sistema operativo y los dispositivos, permitiendo su detección, configuración, control y acceso por parte de los procesos.

- **Interfaz de usuario:** La interfaz de usuario es el medio a través del cual los usuarios interactúan con el sistema operativo. Puede ser una interfaz de línea de comandos (CLI) o una interfaz gráfica de usuario (GUI), que proporciona elementos visuales como ventanas, iconos y menús para facilitar la interacción con el sistema.

- **Llamadas al sistema.** Método por el cual los programas hacen peticiones al sistema operativo.

- **Bibliotecas**. Programas que no se incluyen en el núcleo porque resultaría ineficiente, pero que realizan parte de las funciones de este.

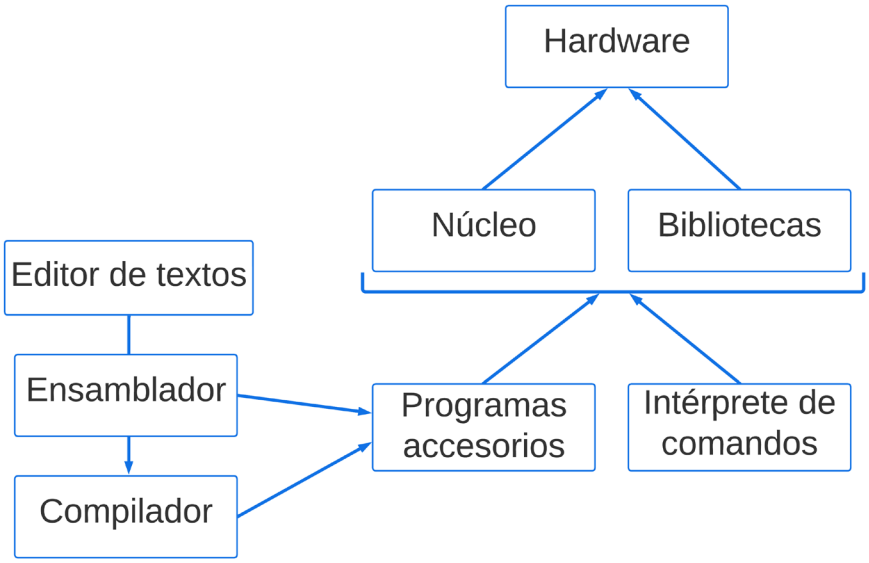
- **Programas del sistema base.** Son componentes esenciales de un sistema informático y desempeñan diversas funciones para su correcto funcionamiento. A continuación, se detallan algunos programas del sistema base:

  - ***Intérprete de comandos o Shell.*** Es una aplicación que permite al usuario pedir al sistema operativo prácticamente cualquier cosa que este pueda realizar mediante la escritura de órdenes en forma de texto llamadas comandos. El intérprete de comandos interpreta y ejecuta las órdenes ingresadas por el usuario, permitiéndole realizar diversas tareas y acceder a diferentes recursos del sistema.

  - ***Editor de textos.*** Es una aplicación para crear o modificar textos. No debe confundirse con un procesador de textos, ya que un editor no cambia la apariencia de un texto sino, solamente su contenido. Es necesario utilizar un editor de textos para la configuración y el mantenimiento de la mayoría de los sistemas operativos, ya que estas operaciones se realizan modificando textos legibles. También es necesario para escribir y modificar programas que pueden ser parte del sistema operativo.

- ***Ensamblador***. Un programa ensamblador traduce programas escritos en lenguaje ensamblador al lenguaje que entiende la CPU. Un lenguaje ensamblador permite programar un ordenador con instrucciones dirigidas directamente a la CPU, pero traduciendo uno por uno los símbolos binarios que entiende la máquina por símbolos de texto y números hexadecimales más manejables por una persona.

- ***Compiladores***. Los compiladores son programas que transforman programas escritos en lenguajes de alto nivel, similares al lenguaje humano, en programas ejecutables que entiende la CPU. Estos lenguajes de alto nivel, como C, C++, Java, entre otros, son más fáciles de entender y escribir para los programadores, y los compiladores se encargan de convertirlos en código de máquina que pueda ejecutarse en el sistema.



El sistema operativo está formado por el núcleo, las bibliotecas, el intérprete de comandos y programas

3.4. Tipos de sistemas operativos

Los sistemas operativos se clasifican según los siguientes criterios:

Según el número de usuarios simultáneos

- **Monousuario**. El sistema sólo admite un único terminal, es decir, un usuario con una pantalla, un teclado y un ratón. Ejemplos de sistemas operativos monousuarios son MS-DOS (Disk Operating System) y sistemas operativos embebidos utilizados en dispositivos específicos.
- **Multiusuario**. Admite la conexión de varios terminales al mismo tiempo, cada uno de los cuales puede tener conectado un usuario con diferente identidad y con diferentes derechos de acceso a los recursos del sistema. Ejemplos de sistemas operativos multiusuario son Linux, Unix y Windows Server.

Según los bits utilizados:

- **Sistemas operativos de 32 bits.** Diseñados para procesadores y hardware que admiten operaciones de 32 bits. Estos sistemas operativos pueden acceder y utilizar hasta 4 GB de memoria RAM. Ejemplos de sistemas operativos de 32 bits son Windows XP, Windows 7 (versiones de 32 bits) y Ubuntu 32 bits.
- **Sistemas operativos de 64 bits.** Diseñados para procesadores y hardware que admiten operaciones de 64 bits. Estos sistemas operativos pueden acceder y utilizar una cantidad mucho mayor de memoria RAM, lo que permite un mejor rendimiento en aplicaciones y tareas que requieren más recursos. Ejemplos de sistemas operativos de 64 bits son Windows 10 (versiones de 64 bits), macOS y distribuciones de Linux de 64 bits.

Según la capacidad de manejar tareas simultáneas:

- **Monotarea**. El sistema operativo no gestiona tareas, sino que responde a la solicitud de un usuario de ejecutar un programa cediendo totalmente el control de la CPU a dicho programa. El sistema operativo sólo recupera el control de la CPU si el programa así lo indica al finalizar. Ejemplos de sistemas operativos monotarea son los sistemas operativos más antiguos, como MS-DOS.
- **Multitarea**. Permiten la ejecución de múltiples tareas simultáneamente. Utilizan técnicas de planificación y administración de recursos para compartir eficientemente el tiempo de CPU y otros recursos entre las tareas. Ejemplos de sistemas operativos multitarea son Windows, Linux y macOS.

Arquitectura del núcleo:

- **Monolítico**. Un núcleo monolítico es un único programa que realiza todas las funciones del sistema operativo. Los monolíticos son núcleos rápidos, pero su tamaño es muy grande y no admiten cambios en la maquinaria que no hayan sido previstos inicialmente. Ejemplos de sistemas operativos con núcleo monolítico son Linux y Windows.
- **Microkernel**. El núcleo proporciona solo las funciones básicas, mientras que los servicios adicionales se ejecutan en espacios separados y se comunican con el núcleo a través de mecanismos de comunicación interprocesos. Ejemplos de sistemas operativos con núcleo microkernel son QNX y MINIX.
- **Otros tipos de núcleos.** También existen otros enfoques, como los núcleos híbridos que combinan características de los núcleos monolíticos y microkernel, y los núcleos exokernel que delegan gran parte de la administración de recursos a las aplicaciones.

Según la comunicación con el usuario:

- **Gráfico (GUI).** Sistema operativo tiene integrado un entorno gráfico para el usuario, que le permite interactuar con el sistema mediante ventanas, iconos y menús sino que se comunica con el usuario a través de comandos escritos en una línea de texto. Por ejemplo, el escritorio de Windows o el Mac OS de los ordenadores de Apple.
- **No gráfico (CLI).** El sistema operativo no integra un entorno gráfico. Es el caso de Linux o BSD, en los que los entornos gráficos son aplicaciones independientes que trabajan generalmente sobre el servicio XWindow System.

3.5. Tipos de aplicaciones

Las aplicaciones son los programas que el usuario pone en marcha para su propia utilidad. Se pueden clasificar en los siguientes grupos:

Aplicaciones ofimáticas y empresariales

Las aplicaciones ofimáticas son programas diseñados para facilitar tareas comunes de oficina, como procesamiento de texto, creación de hojas de cálculo, presentaciones, gestión de correo electrónico y agendas. Estas aplicaciones incluyen suites ofimáticas populares como Microsoft Office y Google Workspace. Por otro lado, las aplicaciones empresariales se centran en las necesidades específicas de una organización, como sistemas de gestión empresarial (ERP), sistemas de gestión de relaciones con clientes (CRM) y software de recursos humanos.

Bases de datos

Las aplicaciones de bases de datos permiten la gestión y organización de grandes volúmenes de datos de manera estructurada. Estas aplicaciones incluyen sistemas de gestión de bases de datos (SGBD) como MySQL, Oracle y Microsoft SQL Server, que ofrecen herramientas para almacenar, recuperar y manipular datos de manera eficiente.

Aplicaciones educativas

Las aplicaciones educativas son programas diseñados para facilitar el aprendizaje y la enseñanza en diferentes niveles educativos. Pueden incluir software de enseñanza en línea, tutoriales interactivos, plataformas de aprendizaje electrónico (e-learning) y aplicaciones específicas para el aprendizaje de idiomas, matemáticas, ciencias, entre otros.

Videojuegos

Las aplicaciones de videojuegos son programas interactivos de entretenimiento que permiten a los usuarios jugar y divertirse. Pueden variar desde videojuegos simples en dispositivos móviles hasta juegos de alta gama en consolas o computadoras. Los videojuegos pueden incluir diferentes géneros como acción, aventura, estrategia, deportes, entre otros.

Ingeniería de productos

Las aplicaciones de ingeniería de productos son programas especializados utilizados en el diseño, modelado y simulación de productos y sistemas. Estas aplicaciones se utilizan en campos como la arquitectura, la ingeniería civil, la ingeniería mecánica y la ingeniería eléctrica, y pueden incluir software CAD (diseño asistido por computadora), software de simulación y herramientas de análisis.

Aplicaciones de seguridad

Las aplicaciones de seguridad se utilizan para proteger los sistemas informáticos y los datos contra amenazas y ataques. Pueden incluir antivirus, firewalls, programas de detección de intrusiones, software de encriptación y herramientas de gestión de seguridad.

Navegadores

Los navegadores son aplicaciones diseñadas para acceder y visualizar contenido en la web. Permiten a los usuarios visitar sitios web, buscar información, ver multimedia y realizar transacciones en línea. Ejemplos populares de navegadores incluyen Google Chrome, Mozilla Firefox, Safari y Microsoft Edge.

Redes sociales y mensajería

Las aplicaciones de redes sociales y mensajería permiten a los usuarios comunicarse, interactuar y compartir contenido con otras personas a través de plataformas en línea. Estas aplicaciones incluyen redes sociales como Facebook, Twitter, Instagram, LinkedIn, así como aplicaciones de mensajería instantánea como WhatsApp, Telegram y Messenger.

3.6 Licencias y tipos de licencias

Según las leyes internacionales de propiedad intelectual, ninguna persona puede hacer uso de un programa de ordenador sin el permiso explícito de su autor.

Las licencias de software establecen los términos y condiciones bajo los cuales se puede utilizar, copiar, modificar y distribuir un programa de computadora. Aquí están los tipos de licencias más comunes:

	Tipos de licencias más comunes					
	Alquiler SaaS	**Uso Restringido**	**Prueba**	**Freeware**	**Libre Copyleft**	**Libre Permisiva**
Acceso a todas las características	Sí	Sí		Sí	Sí	Sí
Gratis			Sí	Sí	Opcional	Opcional
Uso sin restricciones					Sí	Sí
Estudio y modificación					Sí	Sí
Copia y redistribución					Sí	Sí
Redistribución del programa modifi cado					Sí	Sí
Cambio de licencia por otra más restrictiva						Sí

- **De uso restringido.** Conceden derecho a ejecutar el programa, generalmente a un único usuario y sobre un único ordenador. Permiten hacer una copia únicamente para ser utilizada en caso de que el programa original deje de funcionar.
- **Alquiler/SaaS.** Similar a la licencia de uso restringido, últimamente ha adquirido fuerza el concepto de alquiler de software, que limita el uso en el tiempo. De hecho, SaaS solo concede el uso del software remotamente, no su instalación. En lugar de adquirir una licencia de software y descargarlo en los dispositivos locales, los usuarios acceden a las aplicaciones a través de internet, generalmente mediante un navegador web.
- **De prueba**. Licencias promocionales que se conceden gratuitamente sobre programas de muestra para que sus usuarios puedan probar su funcionamiento antes de comprar una licencia de uso restringido sobre un programa completo.
- **Freeware**. Las licencias de freeware permiten a los usuarios utilizar y distribuir el software de forma gratuita. Sin embargo, el autor o titular de los derechos de autor retiene todos los derechos sobre el software, y puede imponer ciertas restricciones en su uso o distribución.

- **Libres.** De forma incondicional, ceden a los usuarios los derechos de ejecución, copia, estudio, modificación y redistribución de un programa original. También ceden el derecho a redistribuir un programa modificado, aunque en este caso se ponen condiciones relativas a los derechos morales del propietario y a las posibles modificaciones de la licencia.

  Según cual sea esta última condición, se dividen en los siguientes dos subtipos:

  - *Copyleft*. Este tipo de licencia se utiliza en el contexto del software de código abierto, y garantiza que el software y todas sus versiones derivadas también sean de código abierto. El software con licencia de Libre Copyleft permite a los usuarios modificar, distribuir y utilizar el software de forma gratuita, siempre y cuando las versiones modificadas también se distribuyan bajo la misma licencia de código abierto.

  - *Permisiva*. Las licencias de Libre Permisiva también se aplican al software de código abierto, pero son menos restrictivas que las licencias de Libre Copyleft. Estas licencias permiten a los usuarios modificar, distribuir y utilizar el software de forma gratuita, incluso en aplicaciones comerciales, sin requerir que las versiones modificadas sean distribuidas bajo la misma licencia de código abierto.

3.7 Gestores de arranque

Cuando un ordenador se pone en marcha, la CPU va a buscar su primera orden a la memoria Bios, o bien a la UEFI, que toma el control del ordenador, comprueba el buen estado del hardware, carga en memoria el gestor de arranque desde un dispositivo de arranque, generalmente un disco duro, y transfiere a este el control de la CPU.

Al ponerse en marcha el ordenador, se ejecuta la BIOS/UEFI y después el gestor de arranque, que cargará un sistema operativo.

Las principales funciones del gestor de arranque son:

- **Selección del sistema operativo:** Los gestores de arranque permiten al usuario seleccionar entre múltiples sistemas operativos instalados en el mismo equipo. Esto es útil en sistemas de arranque dual o múltiple, donde se puede tener instalados diferentes sistemas operativos, como Windows y Linux, y se desea elegir cuál iniciar.
- **Carga del sistema operativo:** El gestor de arranque carga el sistema operativo seleccionado desde el dispositivo de almacenamiento, como el disco duro o la unidad USB, y lo carga en la memoria del ordenador. Esto implica la transferencia del control al núcleo del sistema operativo para que pueda iniciar y ejecutarse.
- **Configuración del arranque**: Los gestores de arranque permiten configurar diferentes opciones de arranque, como la configuración de los parámetros de inicio del sistema operativo, la prioridad de arranque, la resolución de pantalla, la configuración de idioma, etc.
- **Gestión de errores y recuperación:** En caso de producirse un error durante el proceso de arranque, los gestores de arranque pueden mostrar mensajes de error o proporcionar opciones de recuperación, como la ejecución de herramientas de reparación del sistema o la restauración desde una copia de seguridad.

También existen varios gestores de arranque populares utilizados en diferentes sistemas operativos. Algunos ejemplos son:

- **GRUB (GRand Unified Bootloader)**: Es un gestor de arranque ampliamente utilizado en sistemas basados en Linux. Proporciona una interfaz gráfica o de línea de comandos para seleccionar el sistema operativo deseado y ofrece opciones de configuración avanzadas.
- **Windows Boot Manager (BOOTMGR)**: Es el gestor de arranque predeterminado en los sistemas operativos Windows modernos, como Windows 10. Permite seleccionar entre diferentes sistemas operativos y ofrece opciones de recuperación y reparación del sistema.
- **LILO (LInux LOader)**: Es un gestor de arranque utilizado en sistemas Linux más antiguos. Aunque menos común en la actualidad, todavía se utiliza en algunos sistemas y distribuciones Linux.
- **Clover Bootloader**: Es un gestor de arranque utilizado en sistemas macOS. Proporciona opciones de arranque dual entre macOS y otros sistemas operativos, como Windows o Linux.

3.8 Máquinas virtuales

Una máquina virtual (VM, por sus siglas en inglés) es un software o entorno que emula una computadora completa dentro de otra computadora física. En otras palabras, es una instancia virtual de un sistema operativo que se ejecuta dentro de un sistema operativo hospedador. La máquina virtual se comporta como una entidad independiente con su propio sistema operativo, recursos de hardware virtualizados y aplicaciones instaladas.

Las máquinas virtuales se crean mediante un software de virtualización que permite la creación y gestión de múltiples máquinas virtuales en un único equipo físico. Cada máquina virtual tiene su propio entorno aislado y se puede configurar con diferentes especificaciones de hardware, como memoria, espacio en disco y dispositivos virtuales.
Existen varios tipos de máquinas virtuales:

Nombre	Tipo	Descripción
Citrix Xen	Replicación de hardware.	Alto rendimiento en virtualización.
Microsoft Hyper-V	Replicación de hardware.	Migración "en vivo".
VWWare	Replicación de hardware.	Entorno muy utilizado en empresas.
VirtualBox	Replicación de hardware.	Con licencia libre.
Emu48	Emulación de hardware.	Emula una calculadora programable HP48.
Java Virtual Machine	De proceso.	Implementa el lenguaje Java.

- **De sistema.** Estas máquinas virtuales permiten la virtualización de sistemas operativos completos. Crean un entorno virtualizado en el que se puede instalar y ejecutar un sistema operativo completo, como Windows, Linux o macOS. Son utilizadas para la consolidación de servidores, pruebas de software y ejecución de aplicaciones en entornos controlados.
    - *De replicación*. Este tipo de máquina virtual es una réplica, normalmente simplificada, de la máquina real sobre la que funciona. Este tipo de máquinas virtuales tienen un buen rendimiento al no existir una conversión compleja de las instrucciones de los programas. Permiten instalar sistemas operativos diferentes y son muy utilizadas en entornos empresariales donde suele haber hardware infrautilizado.

Sus aplicaciones son numerosas: alojamiento de servicios que no pueden convivir con otros en una misma máquina, creación de entornos virtuales dedicados al desarrollo o la virtualización en hardware de servidores. Las máquinas virtuales pueden ser fácil y rápidamente copiadas y restablecidas, conservando íntegramente su estado, por lo que son ideales tanto para la experimentación como para entornos críticos. Pueden ser apagadas, con lo que dejan de consumir recursos de CPU, o destruirse, liberando completamente el disco duro.

- *De emulación.* Las máquinas virtuales de emulación recrean el funcionamiento de máquinas cuyo hardware es diferente de aquel que las soporta. Son muy interesantes para desarrollar software destinado a máquinas que serían incómodas de programar por sí mismas (como teléfonos móviles o sistemas informáticos industriales); también permiten realizar ensayos de nuevas tecnologías. Otra aplicación útil es recuperar programas de interés que funcionan sobre máquinas que ya no se encuentran disponibles en el mercado.

- **De proceso.** Estas máquinas virtuales no emulan un hardware real. En su lugar, crean un entorno completamente abstracto con el objetivo de ejecutar sobre él aplicaciones que no dependan de la máquina física sobre la que trabajan. De esta manera sólo hay que portar la máquina virtual de un ordenador a otro diferente y todas las aplicaciones desarrolladas para esta seguirán funcionando sin problemas.

En la actualidad, se ha generalizando la práctica de virtualizar los equipos de hardware por los beneficios que proporciona a las empresas. Existe una gran variedad de softwares que nos permiten realizar una virtualización de los equipos. Los softwares de virtualización más utilizados en la actualidad en entornos empresariales son la veterana VMWare, que se mantiene como líder del sector, seguida de cerca por Hyper-V y Citrix Hypervisor. Al decidir virtualizar nuestros equipos, deberemos conocer las ventajas e inconvenientes que esto implica.

Las principales ventajas y casos de uso de la virtualización son:

- **Consolidación de servidores:** Las máquinas virtuales permiten ejecutar múltiples servidores virtuales en un único servidor físico. Esto ayuda a aprovechar mejor los recursos de hardware y reducir los costos asociados con la adquisición y mantenimiento de varios servidores físicos.

- **Pruebas y desarrollo de software:** Las máquinas virtuales proporcionan un entorno aislado y reproducible para probar y desarrollar software. Los desarrolladores pueden crear diferentes configuraciones de máquinas virtuales para probar la compatibilidad de sus aplicaciones en diferentes sistemas operativos y configuraciones de hardware sin necesidad de tener múltiples equipos físicos.

- **Migración y recuperación de sistemas:** Las máquinas virtuales facilitan la migración de sistemas operativos y aplicaciones entre diferentes entornos físicos o en la nube. También permiten la realización de copias de seguridad y recuperación rápida en caso de fallos, ya que es posible crear instantáneas de una máquina virtual y restaurarlas en caso necesario.

- **Entornos de pruebas y formación**: Las máquinas virtuales son útiles para crear entornos de pruebas y formación, donde los usuarios pueden realizar experimentos y aprender sin afectar al entorno de producción.

  Esto es especialmente útil en entornos educativos, donde los estudiantes pueden practicar en máquinas virtuales sin riesgo de dañar sistemas reales.

- **Virtualización de aplicaciones:** Las máquinas virtuales también permiten la virtualización de aplicaciones, donde una aplicación específica se ejecuta en una máquina virtual independiente. Esto ayuda a aislar las aplicaciones y resolver posibles conflictos entre ellas, ofreciendo una mayor flexibilidad y seguridad en la gestión de aplicaciones.

Entre sus principales inconvenientes, se incluyen los siguientes:

- **Sobrecarga de recursos:** Las máquinas virtuales requieren recursos adicionales para ejecutar el hipervisor y mantener el entorno virtualizado. Esto puede generar una sobrecarga en el consumo de CPU, memoria y almacenamiento, lo que podría afectar el rendimiento general del sistema.
- **Complejidad de gestión:** La administración de un entorno de máquinas virtuales puede ser más compleja que la gestión de sistemas físicos. Requiere conocimientos técnicos específicos y un tiempo adicional para configurar, mantener y solucionar problemas en el entorno virtualizado.
- **Dependencia del hipervisor**: Las máquinas virtuales están estrechamente ligadas al hipervisor utilizado. Si el hipervisor experimenta fallas o vulnerabilidades de seguridad, todas las máquinas virtuales alojadas en él pueden estar en riesgo.
- **Rendimiento limitado de hardware**: Aunque las máquinas virtuales son capaces de ejecutar aplicaciones y sistemas operativos, pueden experimentar un rendimiento ligeramente inferior en comparación con una configuración física equivalente. Esto se debe a la necesidad de emular o compartir recursos físicos entre las máquinas virtuales.
- **Licenciamiento y costos adicionales:** Algunas aplicaciones y sistemas operativos pueden requerir licencias específicas para su ejecución en máquinas virtuales. Esto puede generar costos adicionales en términos de licenciamiento y mantenimiento.

Como acabamos de ver, uno de los principales inconvenientes de la virtualización es que un fallo en el hardware del equipo que aloja las máquinas virtualizadas provoca que todas las máquinas alojadas en él dejen de funcionar.

Para solucionar este problema, tanto VMWare como Hyper-V recomiendan montar los entornos de virtualización empresariales con dos nodos físicos que, como mínimo, alojen las máquinas virtuales y que estén conectados a un entorno de almacenamiento compartido; de tal forma que, si se produce un fallo de hardware en cualquiera de los dos hosts, el software de virtualización sea capaz de mover, en caliente y de forma automática, todas las máquinas virtuales que se están ejecutando en ese host físico al otro.

El servicio que se encarga de mover las máquinas virtuales en VMWare se llama Vmotion; mientras que, en Hyper-V, el servicio se llama Live Migration. Aunque el nombre del servicio es distinto, el propósito es el mismo: mantener una alta disponibilidad de las máquinas virtualizadas ante un fallo del hardware físico del host que las aloja.

¿Cómo funciona una virtualización?

La virtualización es un proceso mediante el cual se crea una versión virtual o simulada de un recurso de hardware o software, como un servidor, un sistema operativo o una aplicación. En el contexto de la virtualización de servidores, se crean múltiples máquinas virtuales que se ejecutan en un único servidor físico, lo que permite maximizar la utilización de los recursos y optimizar el rendimiento.

El funcionamiento de la virtualización se basa en el uso de un software especializado llamado hipervisor o monitor de máquina virtual. El hipervisor se instala en el servidor físico y actúa como una capa de abstracción que permite la creación y gestión de las máquinas virtuales. Hay dos tipos principales de hipervisores:

- **Hipervisor de tipo 1 (nativo o bare-metal)**: Se instala directamente en el hardware del servidor y proporciona una plataforma de virtualización independiente del sistema operativo host. Las máquinas virtuales se ejecutan directamente sobre el hipervisor, lo que ofrece un rendimiento óptimo y un mayor grado de aislamiento y seguridad.
- **Hipervisor de tipo 2 (alojado):** Se instala como una aplicación en un sistema operativo host. Las máquinas virtuales se ejecutan como procesos dentro del sistema operativo host. Aunque ofrece una mayor flexibilidad, puede tener un rendimiento ligeramente inferior en comparación con el hipervisor de tipo 1.
- **Una vez que se ha instalado el hipervisor,** se crean las máquinas virtuales, que son entornos virtuales completamente aislados que simulan el hardware de un servidor físico, incluyendo la CPU, la memoria, el almacenamiento y los dispositivos de red. Cada máquina virtual tiene su propio sistema operativo y aplicaciones instaladas, y se comporta como un servidor independiente.
- **El hipervisor asigna** y administra los recursos del servidor físico entre las máquinas virtuales de manera eficiente, asegurándose de que cada una reciba los recursos necesarios para su correcto funcionamiento. Esto permite que múltiples sistemas operativos y aplicaciones se ejecuten simultáneamente en un solo servidor físico, lo que maximiza la utilización de los recursos y reduce los costos de infraestructura.

El paso más importante al virtualizar un sistema operativo es definir los recursos del hardware que irán destinados a ejecutar el sistema. Deberán definirse parámetros como la cantidad de memoria o el tamaño de disco duro que se dedicarán exclusivamente a ese sistema.

Una vez definidos estos parámetros, que podrán ser modificados en cualquier momento, será necesario proceder a la instalación del sistema operativo de manera idéntica a como se realizaría en un equipo físico normal. Esto es gracias a que, como hemos comentado antes, los sistemas virtualizados disponen de los recursos hardware del equipo residente como el lector de CD desde donde se instalará el sistema operativo.

Existen complementos proporcionados por los programas de virtualización que pueden ser instalados en los sistemas operativos virtualizados para crear funcionalidades extendidas, como atajos de teclado para cambiar entre los sistemas o mejora de las conexiones de red. En VMWare, estas herramientas se llaman WMWare Tools y es recomendable instalarlas en todos los sistemas operativos virtuales.

El auge de la virtualización de los sistemas entra en conflicto con las compañías desarrolladoras de software, que ven que su sistema de licencias por usuario carece de sentido. Esto es debido a que los programas dejan de estar vinculados a un único equipo.

3.9 Consideraciones previas a la instalación de sistemas operativos libres y propietarios

Cada sistema operativo permite ejecutar unos programas concretos y controlar un hardware determinado. Dos sistemas operativos diferentes no tienen por qué ser compatibles. Los principales criterios para elegir un sistema operativo son los siguientes:

- **Requisitos de hardware y software:** Antes de instalar un sistema operativo, es importante verificar los requisitos de hardware y software necesarios para garantizar un funcionamiento adecuado. Esto incluye comprobar si el hardware del equipo cumple con los requerimientos mínimos de memoria, procesador, capacidad de almacenamiento y otros componentes necesarios. Además, se debe verificar si el software requerido, como controladores de dispositivos o aplicaciones específicas, es compatible con el sistema operativo que se va a instalar.

- **El uso al que van destinados:** personal, profesional o servidor:

  - *Uso personal:* Los sistemas operativos destinados al uso personal están diseñados para ser instalados en computadoras de uso doméstico. Proporcionan una interfaz amigable y fácil de usar, junto con una amplia gama de aplicaciones y herramientas orientadas a las necesidades del usuario común, como navegadores web, suites de oficina, reproductores multimedia y aplicaciones de entretenimiento.

  - *Windows*. Es el más común, ya que viene preinstalado en casi todos los ordenadores personales nuevos y tiene, con mucho, más aplicaciones compatibles que ningún otro sistema operativo.

  - *MacOS*. Es más estable y agradable de utilizar que Windows, aunque bastante más caro. Sólo está disponible para ordenadores de marca Apple.

- *Ubuntu, OpenSUSE, Debian.* Son tres ejemplos de distribuciones de programas libres y gratuitos. Basadas en el núcleo Linux, cubren las necesidades de un usuario personal. Son estables, eficientes y agradables de manejar, pero incompatibles con algunos dispositivos y con la mayoría de los programas comerciales.

- *Uso profesional.* Windows se utiliza en la mayoría de los casos por su alta disponibilidad de programas especializados; MacOS es muy apreciado en diseño gráfi co y producción musical por su fiabilidad; y, por último, Linux se valora principalmente en ambientes académicos y de investigación por su versatilidad.

- *Uso como servidor*. Los sistemas operativos utilizados como servidores están diseñados para administrar y controlar servidores de red. Proporcionan herramientas y funciones avanzadas para la gestión de recursos, el almacenamiento de datos, la administración de usuarios y la seguridad de la red. Estos sistemas operativos permiten que los servidores brinden servicios a otros dispositivos y usuarios en la red, como alojamiento de sitios web, almacenamiento en la nube, servicios de correo electrónico, bases de datos y más.

  La oferta del mercado se divide en sistemas operativos de tipo Unix, fundamentalmente Linux, Solaris y BSD, y sistemas del tipo Windows Server.

- **El soporte técnico que ofrecen.** En este caso, el software comercial tiene un soporte técnico profesional que no existe en el software libre, por lo que muchas empresas suelen decidir adquirir esos sistemas, sobre todo cuando no tienen personal cualificado propio. Si bien es cierto que a pesar de tener dicho soporte, generalmente es de pago y supone una cuota de mantenimiento o una inversión en las reparaciones.

  Por otro lado, los sistemas libres no tienen el respaldo de una empresa que proporcione un servicio técnico al usuario final. Sin embargo generalmente está constituida por una sólida comunidad de usuarios, desarrolladores y personal cualifi cado al que se le puede consultar en plataformas de soporte, como foros y páginas especializadas. Si bien este soporte es gratuito y suele contar con mucho apoyo, es necesario disponer de personal técnico dentro de la empresa para poder llevar a cabo las tareas requeridas.

- **Licencia libre o propietaria:**

  - *Sistemas operativos de licencia libre:*

    - ***Linux***: Es un sistema operativo de código abierto que se distribuye bajo diversas licencias de software libre, como la Licencia Pública General de GNU (GPL). Ejemplos de distribuciones de Linux incluyen Ubuntu, Fedora y Debian.

- *Sistemas operativos de licencia propietaria:*

  - ***Microsoft Windows:*** Es un sistema operativo desarrollado por Microsoft y se distribuye bajo una licencia propietaria. Ejemplos de versiones de Windows incluyen Windows 10, Windows 11, Windows Server, etc. macOS: Es el sistema operativo de Apple para sus computadoras Mac y también se distribuye bajo una licencia propietaria. Ejemplos de versiones de macOS incluyen macOS Monterey y macOS Ventura.

3.10 Instalación de sistemas operativos. Requisitos, versiones y licencias

La **elección de un sistema operativo** es una de las decisiones más críticas del grupo de IT de una empresa. Deben tenerse en cuenta multitud de factores, como los requisitos de hardware y software del sistema operativo, la versión a utilizar y la elección de una licencia adecuada.

Los requisitos técnicos son las especificaciones de un sistema operativo para poder funcionar de manera óptima. Normalmente, cuanto más moderna es una versión de un sistema operativo, más potencia necesitará en cuanto a procesamiento y cantidad de memoria del equipo, pero no siempre es así.

En ocasiones, un **cambio de versión** supone una optimización en la utilización de los recursos. Un ejemplo claro es el sistema operativo Microsoft Windows 8, que fue sustituido por una versión más reciente, Windows 11, mucho más eficiente, rápida y segura que la anterior. Al decidir sobre la versión de un sistema operativo, no solo debemos analizar la potencia del equipo, sino los programas que instalaremos en el sistema. Los programas desarrollados en una versión de un sistema operativo no siempre funcionan en el resto de versiones, por lo que deberemos comprobar que la versión del sistema operativo que vayamos a instalar es soportada por el software que utilizaremos.

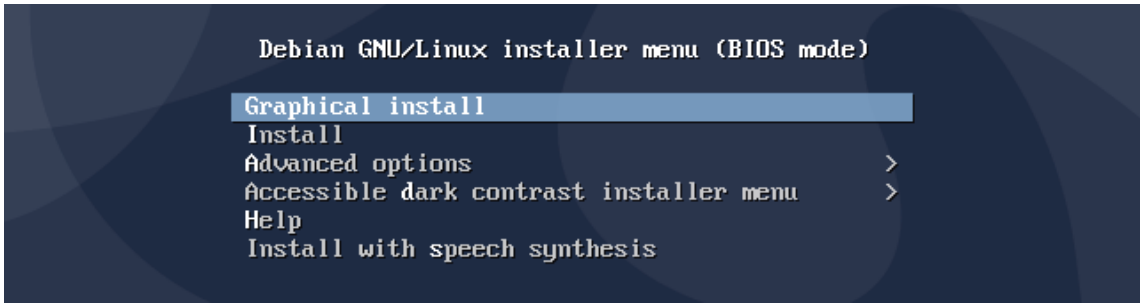
Las licencias definen el tipo de utilidad que podrá darse a un sistema operativo. Generalmente las licencias limitan el uso de un sistema operativo a una persona o un equipo únicamente. Esto sucede en los sistemas operativos Microsoft, en los que cada copia tiene asociado un número de identificación único. Esto no ocurre con sistemas operativos libres, en los que la licencia libre permite su instalación en tantos equipos como se desee y sin límite de usuarios.

Antes de **adquirir la licencia de un sistema operativo** deben realizarse los pasos que se detallan a continuación:

- Escoger la edición del software que mejor se adecúa a nuestros requisitos.
- Estudiar los planes de licencias que propone el proveedor.
- Asegurar que el hardware disponible cumple los requisitos del sistema operativo que instalar.

- Obtener la siguiente documentación: datasheets, guía de instalación y notas de la versión.
- Planificar el particionado de los discos duros de las máquinas.

Después, se podrá proceder a instalar el sistema operativo siguiendo paso a paso la guía de instalación.



Instalación del sistema operativo Debian. Hay distribuciones de Linux que apuestan por facilitar su acceso y utilización

3.11 Instalación y desinstalación de aplicaciones. Requisitos, versiones y licencias

3.11.1. Instalación de aplicaciones

Los pasos que se requieren para instalar requisitos, versiones y licencias son los mismos para instalar una aplicación que para un sistema operativo. Sin embargo, el proceso de instalación es diferente en cada sistema operativo:

- **Windows**. Para poder instalar software en Windows, es necesario que el proveedor del programa proporcione un archivo ejecutable (setup. exe, install.exe, etc.) que realice el proceso de copia de los archivos del programa al sistema, así como modificar el registro de Windows para incluir la información del programa en el sistema.
- **Linux**. Requiere de un programa nativo en el sistema operativo para instalar los paquetes del software. Generalmente, son necesarios conocimientos de administrador, puesto que se ha de escribir en la ventana de comandos una secuencia que ordene la instalación del programa con unos determinados parámetros, como la ubicación de los archivos o los permisos del programa.
- **Mac OS X.** En este sistema operativo, los programas están encapsulados en un mismo fichero que ha de ser arrastrado a una carpeta del sistema para proceder a su instalación. Es uno de los mecanismos de instalación más sencillos.

En cualquier caso, todos los sistemas operativos requieren que el usuario que realiza la instalación tenga los permisos de administrador o usuario avanzado para poder llevarla a cabo. Esto evita que usuarios inexpertos o no autorizados instalen software sin ningún tipo de restricción, lo que provocaría una reducción del rendimiento y un riesgo de se-

La instalación de las diferentes versiones de un programa no requiere de una reinstalación del software. Generalmente, basta con ejecutar un archivo de actualización para que los cambios se apliquen a los archivos ya instalados.

Es cada vez más común que los programas se conecten a Internet en segundo plano, es decir, sin conocimiento del usuario, para comprobar si existen actualizaciones y, de ser así, proceder a la descarga del archivo e incluso a su instalación de manera desatendida. Es una práctica muy habitual en programas como navegadores de Internet o plug-ins como Java, en los que un programa desactualizado pone en riesgo la seguridad del sistema.

3.11.2 Requisitos para la instalación de aplicaciones

Requisitos de hardware

Los requisitos de hardware son las especificaciones mínimas que debe cumplir el sistema para poder instalar y ejecutar una aplicación de manera adecuada. Estos requisitos varían según la aplicación y dependen de la complejidad y los recursos que requiere para funcionar correctamente. Algunos de los requisitos de hardware comunes incluyen:

- **Procesador**: Se especifica el tipo y velocidad mínima del procesador requerido para ejecutar la aplicación de manera óptima.
- **Memoria RAM**: Se indica la cantidad mínima de memoria RAM que debe tener el sistema para poder ejecutar la aplicación sin problemas. Esto es importante ya que las aplicaciones pueden requerir una cierta cantidad de memoria para funcionar adecuadamente.
- **Espacio de almacenamiento**: Se especifica la cantidad de espacio de almacenamiento necesario para la instalación de la aplicación. Esto incluye tanto el espacio requerido para la instalación inicial como el espacio necesario para los archivos de la aplicación y los datos generados durante su uso.
- **Tarjeta gráfica**: Algunas aplicaciones, especialmente los juegos y aplicaciones multimedia, pueden requerir una tarjeta gráfica específica para mostrar gráficos de alta calidad o ejecutar determinadas funciones. Los requisitos de la tarjeta gráfica pueden incluir el tipo, la capacidad y los controladores actualizados.
- **Otros dispositivos:** Dependiendo de la naturaleza de la aplicación, puede haber requisitos adicionales de hardware, como cámaras, micrófonos, escáneres o impresoras, si la aplicación necesita interactuar con estos dispositivos.

Es importante revisar cuidadosamente los requisitos de hardware de una aplicación antes de instalarla para asegurarse de que el sistema cumple con los mismos. Si el hardware no cumple con los requisitos mínimos, es posible que la aplicación no funcione correctamente o no se pueda instalar en absoluto.

Requisitos de software

Además de los requisitos de hardware, las aplicaciones también tienen requisitos de software, que son los componentes y configuraciones necesarios del sistema operativo y otros programas para que la aplicación se instale y ejecute correctamente. Algunos de los requisitos de software comunes incluyen:

- **Sistema operativo:** Se especifica la versión y el tipo de sistema operativo compatible con la aplicación. Puede ser Windows, macOS, Linux u otros sistemas operativos específicos.
- **Bibliotecas y frameworks:** Algunas aplicaciones pueden requerir bibliotecas o frameworks adicionales para funcionar correctamente. Estos componentes pueden ser proporcionados por el desarrollador de la aplicación o deben descargarse e instalarse por separado.
- **Versiones de software:** Algunas aplicaciones pueden requerir versiones específicas de software, como navegadores web, reproductores multimedia o controladores de dispositivos. Es importante asegurarse de que el sistema tenga las versiones adecuadas instaladas para evitar problemas de compatibilidad.
- **Configuraciones especiales:** Algunas aplicaciones pueden requerir configuraciones especiales del sistema operativo o de otros programas para funcionar correctamente. Esto puede incluir ajustes de seguridad, configuraciones de red o permisos de usuario.

3.11.3 Versiones de aplicaciones

En el ámbito de las aplicaciones, existen diferentes tipos de versiones que indican el estado de desarrollo y estabilidad del software. Algunos de los tipos de versiones más comunes son:

- **Versión estable:** Es la versión final y completa de la aplicación que se considera adecuada para su uso general. Esta versión ha pasado por rigurosas pruebas de calidad y se espera que funcione de manera confiable y sin errores importantes. Las versiones estables suelen ser recomendadas para la mayoría de los usuarios.
- **Versión beta:** Es una versión preliminar de la aplicación que se lanza para que los usuarios la prueben y brinden retroalimentación. Las versiones beta pueden contener errores conocidos y aún están en desarrollo. Los usuarios que optan por utilizar una versión beta deben estar dispuestos a encontrar posibles problemas y proporcionar comentarios para mejorar la aplicación.
- **Versión alfa:** Es una versión aún más temprana que la beta, y generalmente se utiliza internamente por los desarrolladores para probar y depurar la aplicación. Las versiones alfa pueden contener características incompletas y errores significativos, por lo que no se recomienda para uso general.

- **Versión de lanzamiento candidata:** Es una versión que se considera muy cercana a la versión final estable, pero aún está sujeta a pruebas adicionales y correcciones de errores. Las versiones de lanzamiento candidatas se lanzan para permitir a los usuarios finales probar la aplicación antes de su lanzamiento oficial y detectar problemas de último momento.

- **Otras versiones**: Además de los tipos mencionados, existen otros términos que se utilizan para describir el estado de una versión de software, como versiones de desarrollo, versiones experimentales, versiones nocturnas (nightly builds), entre otros. Estos términos pueden variar según la organización o comunidad de desarrollo y pueden tener significados específicos en su contexto.

Actualizaciones y parches

Las actualizaciones y parches son importantes para mantener las aplicaciones funcionando de manera óptima y segura. Estas actualizaciones pueden incluir mejoras de rendimiento, correcciones de errores, nuevas características y parches de seguridad. Algunos puntos clave sobre las actualizaciones y parches son:

- **Actualizaciones**: Las actualizaciones son versiones nuevas de la aplicación que se lanzan para proporcionar mejoras y correcciones. Estas actualizaciones pueden ser opcionales o recomendadas, y a menudo se ofrecen de forma gratuita a los usuarios que ya tienen la aplicación instalada. Las actualizaciones pueden ser periódicas y ofrecer nuevas funcionalidades, mejoras en la interfaz de usuario, optimización del rendimiento, etc.

- **Parches**: Los parches son actualizaciones más pequeñas que se lanzan para corregir problemas específicos en la aplicación. Estos problemas pueden incluir errores críticos, vulnerabilidades de seguridad u otros problemas identificados después del lanzamiento de la versión original. Los parches suelen ser lanzados de manera urgente y se recomienda su instalación para garantizar la estabilidad y seguridad del software.

- **Proceso de actualización:** El proceso de actualización puede variar según la aplicación, pero generalmente implica descargar e instalar la nueva versión o parche a través de un proceso guiado por el software o mediante la descarga manual desde el sitio web del desarrollador. Algunas aplicaciones también pueden ofrecer actualizaciones automáticas, donde el software se encarga de verificar y descargar las actualizaciones de forma transparente para el usuario.

3.11.4 Licencias de Software

Las licencias de software se dividen en dos categorías principales: licencias propietarias y licencias de código abierto. Las licencias propietarias otorgan al titular del software el control exclusivo sobre su uso, modificación y distribución.
Estas licencias suelen ser restrictivas y pueden implicar el pago de una tarifa para utilizar el software. Por otro lado, las licencias de código abierto promueven la distribución, acceso y modificación del software de forma libre y abierta. Estas licencias permiten a los usuarios acceder al código fuente, modificarlo y distribuirlo de acuerdo con los términos de la licencia.

Al utilizar software, ya sea bajo licencias propietarias o de código abierto, es importante tener consideraciones legales y éticas. Esto implica cumplir con los términos y condiciones establecidos en la licencia, respetar los derechos de autor y otros derechos de propiedad intelectual asociados al software, y utilizar el software de manera ética y legal. Además, al utilizar software de código abierto, se anima a los usuarios a contribuir a la comunidad proporcionando retroalimentación, mejoras o correcciones al software utilizado.

2.11.5 Desinstalación de aplicaciones

En cuanto a la desinstalación de aplicaciones, para que esta se realice de manera segura es importante seguir ciertos pasos y consideraciones:

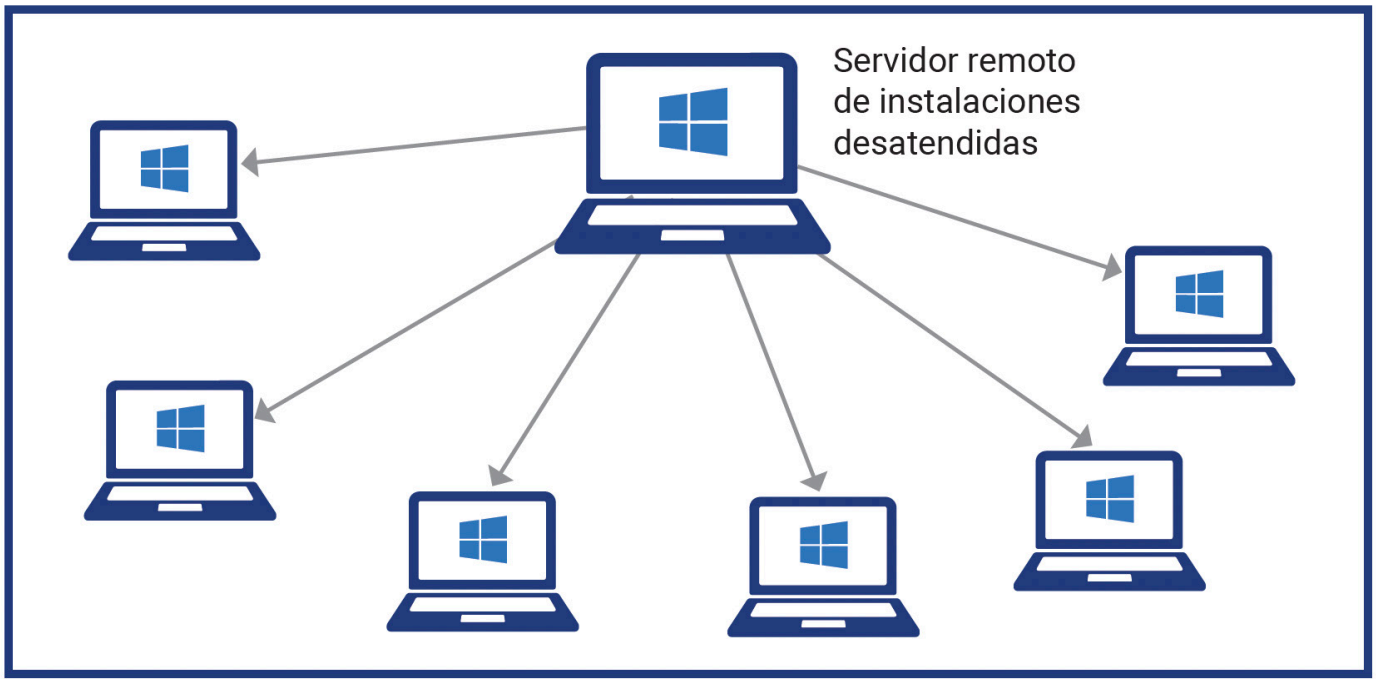
- **Desinstalación desde el sistema operativo:** La mayoría de los sistemas operativos ofrecen herramientas integradas para desinstalar aplicaciones. El usuario puede acceder a la lista de aplicaciones instaladas y seleccionar la que desea eliminar. Es recomendable utilizar esta función de desinstalación del sistema operativo, ya que se encarga de eliminar todos los archivos y entradas asociadas a la aplicación.
- **Utilización de herramientas de desinstalación proporcionadas por el desarrollador:** Algunas aplicaciones pueden proporcionar herramientas específicas de desinstalación. Estas herramientas pueden ser necesarias si la desinstalación regular a través del sistema operativo no es suficiente o si la aplicación dejó archivos o configuraciones residuales.
- **Eliminación de archivos y entradas adicionales:** En algunos casos, es posible que queden archivos o entradas de configuración residuales después de desinstalar una aplicación. El usuario puede realizar una limpieza adicional manualmente, eliminando los archivos y entradas relevantes. Sin embargo, es importante tener cuidado al eliminar archivos del sistema y asegurarse de no eliminar accidentalmente archivos necesarios para el funcionamiento del sistema operativo.

3.12 Uso de instalaciones desatendidas

Las **instalaciones desatendidas** son un método automatizado para instalar software en un sistema sin requerir la intervención del usuario durante el proceso de instalación. En lugar de que el usuario deba realizar manualmente cada paso de la instalación, las instalaciones desatendidas permiten configurar de antemano las opciones de instalación y ejecutar el proceso de manera automatizada.

Instalar sistemas operativos en un entorno empresarial puede suponer muchas horas de trabajo. Las siguientes técnicas pueden facilitarnos bastante la tarea:

- **Instalación desatendida.** Se graba en un fi chero todas las respuestas a las preguntas que el sistema operativo hace cuando se está instalando. El programa instalador utilizará ese fi chero para realizar la instalación sin hacer preguntas.
- **Instalación remota.** El sistema operativo se instala desde un servidor central a través de la red de ordenadores.



Instalación remota de un sistema operativo en varios ordenadores desde un servidor central.

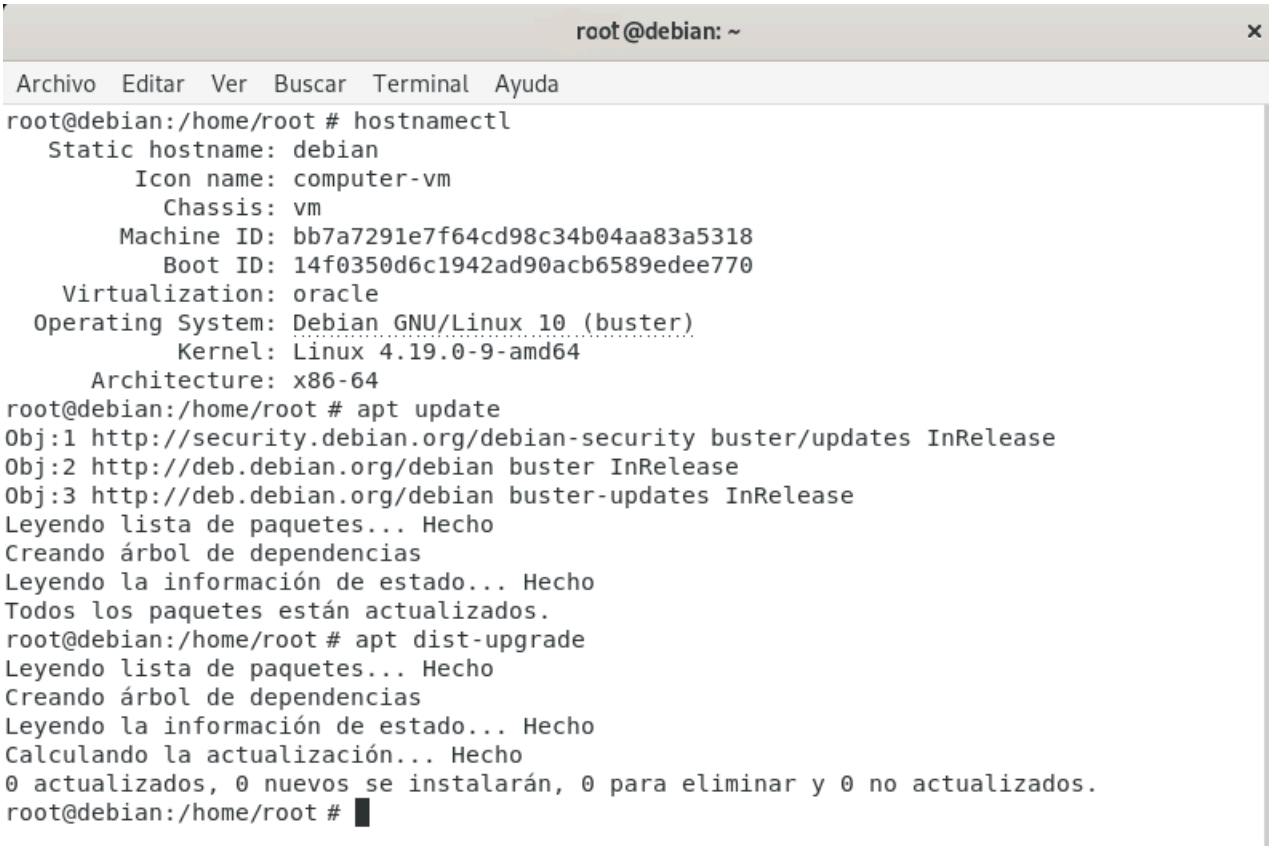
3.13 Actualización de sistemas operativos y aplicaciones

Las **actualizaciones de sistemas operativos y aplicaciones** son fundamentales para mantener la seguridad, estabilidad y funcionalidad de los sistemas informáticos. Las actualizaciones suelen incluir mejoras de seguridad, correcciones de errores, nuevas funciones y optimizaciones de rendimiento. Al aplicar regularmente las actualizaciones disponibles, se protege el sistema contra vulnerabilidades conocidas y se garantiza un funcionamiento eficiente y sin problemas.

Las actualizaciones de seguridad son especialmente cruciales, ya que ayudan a prevenir y mitigar las amenazas cibernéticas. Los desarrolladores de sistemas operativos y aplicaciones trabajan constantemente para identificar y corregir vulnerabilidades, y lanzan actualizaciones para solucionarlos. Al mantenerse al día con las actualizaciones, se asegura de contar con las últimas protecciones contra malware, ataques de hackers y otras amenazas en línea.

Pero, en ocasiones, sobre todo en **entornos profesionales,** es importante controlar las actualizaciones y testearlas previamente antes de implantarlas en el sistema; puesto que, a pesar de las mejoras de seguridad, podrían provocar incompatibilidades con el software utilizado por la empresa, que en muchas ocasiones ha sido desarrollado a medida para ella y no tiene un soporte adecuado en cuanto a actualizaciones.

Por otro lado, las actualizaciones requieren del reinicio de la máquina o de un servicio que puede estar siendo utilizado por el resto de los usuarios, por lo que existen herramientas tanto externas como nativas en los Sistemas Operativos Servidores que inician las actualizaciones en horas de baja producción, como por ejemplo horario nocturno o fines de semana



Debian (Linux) puede actualizar todos los programas del ordenador mediante la línea de comandos desde un terminal.

Algunos puntos claves en este aspecto son:

- **Identificar y etiquetar correctamente los dispositivos de red y las conexiones físicas.** Esto implica asignar nombres únicos a los dispositivos, como servidores, routers, switches, puntos de acceso, impresoras, etc. Además, se deben etiquetar los cables y conexiones para facilitar la identificación y el mantenimiento.
- **Documentar la configuración de los dispositivos de red, incluyendo la configuración de los routers, switches, servidores, puntos de acceso, etc.** Esto puede incluir información como la dirección IP asignada, la configuración de seguridad, las VLAN (Virtual LAN), las políticas de enrutamiento, entre otros. Además, se debe documentar la asignación de direcciones IP a los dispositivos en la red, asegurándose de tener un registro actualizado de las direcciones IP utilizadas.

PARA SABER MÁS: Los programas que mantienen el sistema actualizado en Linux se llaman Apt (Debian) y Yum (Red Hat).

A la hora de mantener actualizado el sistema operativo que tenemos instalado en nuestro ordenador, lo primero que debemos saber es que, en función de sistema operativo que tengamos instalado, la forma en que se realiza la actualización es diferente. Vemos a continuación cómo se hace la actualización en Windows y en Linux.

- **En entornos Windows.** El sistema operativo se actualiza de forma semiautomática mediante revisiones por iniciativa de Microsoft. Para actualizar a una versión superior, hay que comprar la licencia. Las aplicaciones dependen de su respectivo fabricante.
- **En entornos Linux.** El sistema operativo y todos los programas pueden actualizarse a la última revisión o a una nueva versión con una sola orden del administrador y sin coste.

Cuando se actualizan sistemas operativos servidores es vital que el administrador pueda gestionar las actualizaciones e impedir que se apliquen de manera automática. Los servidores son sistemas críticos de los que dependen muchos servicios: una actualización lanzada por la empresa del sistema operativo para corregir un error de seguridad puede fácilmente entrar en conflicto con algún programa instalado, haciendo que deje de funcionar.

Por ello, el equipo de IT de una empresa ha de testear cada una de las actualizaciones antes de aplicarlas al sistema operativo. Además, debe realizar un punto de restauración para que, en caso de fallo en algún servicio, se pueda volver a un estado anterior del sistema operativo. Además, las actualizaciones en este tipo de sistemas han de realizarse en horarios que no supongan una interrupción crítica del sistema.

3.14 Ficheros de inicio de sistemas operativos

Los **ficheros de inicio**, también conocidos como archivos de arranque, son componentes clave en el proceso de inicio de un sistema operativo. Estos ficheros contienen instrucciones y configuraciones que se ejecutan automáticamente al encender o reiniciar el sistema.

Los ficheros de inicio suelen tener una estructura jerárquica y están ubicados en ubicaciones específicas del sistema operativo. Por ejemplo, en sistemas basados en UNIX o Linux, el fichero de inicio principal es el "init" o "systemd", mientras que en Windows se utilizan los ficheros "boot.ini" y "ntldr".

La función principal de los ficheros de inicio es establecer el entorno de ejecución inicial del sistema operativo y cargar los componentes esenciales para el arranque del sistema. Esto incluye la inicialización de servicios, la carga de controladores de dispositivos, la configuración de variables de entorno y la ejecución de scripts o programas necesarios para el inicio del sistema.

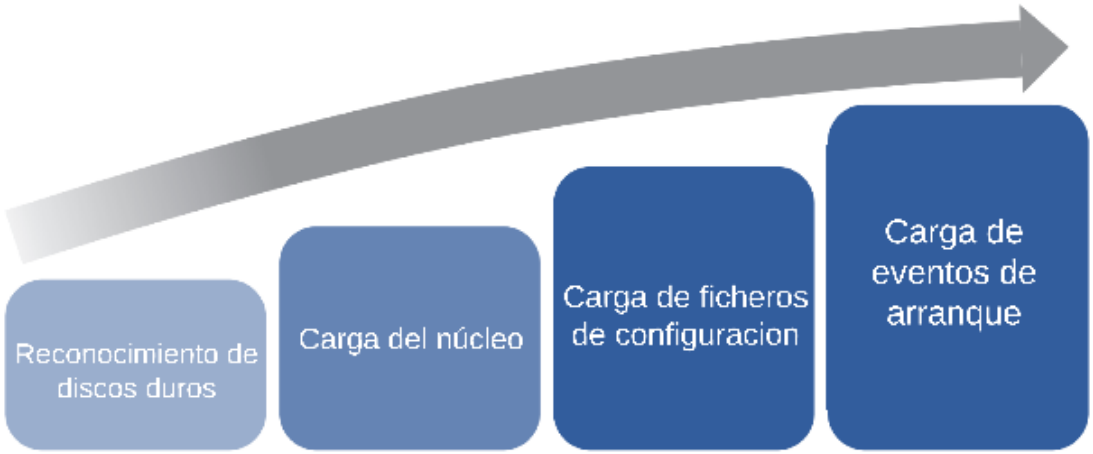
Así, al encender el ordenador, el equipo accede a una pequeña sección del disco duro donde se encuentran las instrucciones más básicas, que se encargan de reconocer las unidades de los discos duros y cargar el gestor de arranque que definirá el sistema operativo que será utilizado.

Los pasos necesarios que hace un equipo para **reconocer los discos duros** que tiene son:

- Reconocer las etiquetas de los discos.
- Localizar ficheros en el disco.
- Cargar el gestor de arranque.

Después, el ordenador cargará los siguientes ficheros que dejarán la máquina en manos del usuario:

- El núcleo del sistema operativo.
- Ficheros de configuración del arranque.
- Un fichero donde se guardan los acontecimientos del arranque.



Proceso de arranque en un ordenador.

3.15 Controladores de dispositivos

Los **sistemas operativos para arquitecturas de ordenador abiertas,** como Windows o Linux, deben poder comunicarse con miles de dispositivos de diferentes fabricantes, cada uno de ellos con sus propias prestaciones y características internas.

Esta comunicación exige que exista un programa para cada dispositivo (o, al menos, para conjuntos de dispositivos muy parecidos) que haga de intermediario entre las posibilidades de control del sistema operativo y la electrónica del dispositivo. Dichos programas se llaman drivers (controladores en inglés).

Los controladores más genéricos se integran en el núcleo del sistema, mientras que los más específicos aparecen en forma de librerías que son llamadas cuando se necesitan.

Actualmente, los sistemas operativos aprovechan la conectividad de hoy en día para obtener los drivers de un repositorio mediante la conexión de Internet. Esto supone automatizar la instalación de los dispositivos de manera que el sistema se conecte a Internet, obtenga los controladores y los instale sin necesidad de que intervenga el usuario.

4. Resumen

El sistema operativo es el conjunto de programas que controla el acceso a los dispositivos de un ordenador por parte del resto de programas. Se compone del núcleo, las bibliotecas y los programas complementarios que se utilizan para el ajuste y la programación. El acceso a los dispositivos lo realizan los controladores. En cuanto a los derechos que un usuario posee sobre un programa determinado los concede el propietario mediante una licencia; estos derechos pueden ser de uso restringido o libres.

Existen diferentes sistemas operativos según el tipo de licencia que utilizan y según el tipo de equipo en el que se instalarán; como, por ejemplo, los basados en arquitectura x86, 64bits o MAC; estos últimos cuentan con un soporte exclusivo para sistemas operativos iOS.

La selección de un sistema operativo dependerá, pues, del uso al que vaya destinado, la máquina disponible y el tipo de licencia. Antes de proceder a su instalación es preciso consultar la documentación, comprobar los requisitos de la máquina y elegir el plan de licencias apropiado. En muchos casos, la instalación de varias máquinas y las actualizaciones pueden mecanizarse y realizarse a distancia.

Las máquinas virtuales permiten la instalación de diferentes sistemas operativos mediante la utilización de la misma máquina física. Los sistemas virtuales son completamente independientes entre ellos, por lo que la arquitectura virtual determina el acceso de los recursos comunes para todos los sistemas alojados. Hoy en día estos sistemas son cada vez más utilizados, ya que reducen el coste del hardware y optimizan su utilización. Esto se debe a que, si, en un momento dado, un sistema no utiliza muchos recursos, estos pueden ser utilizados por otros sistemas.

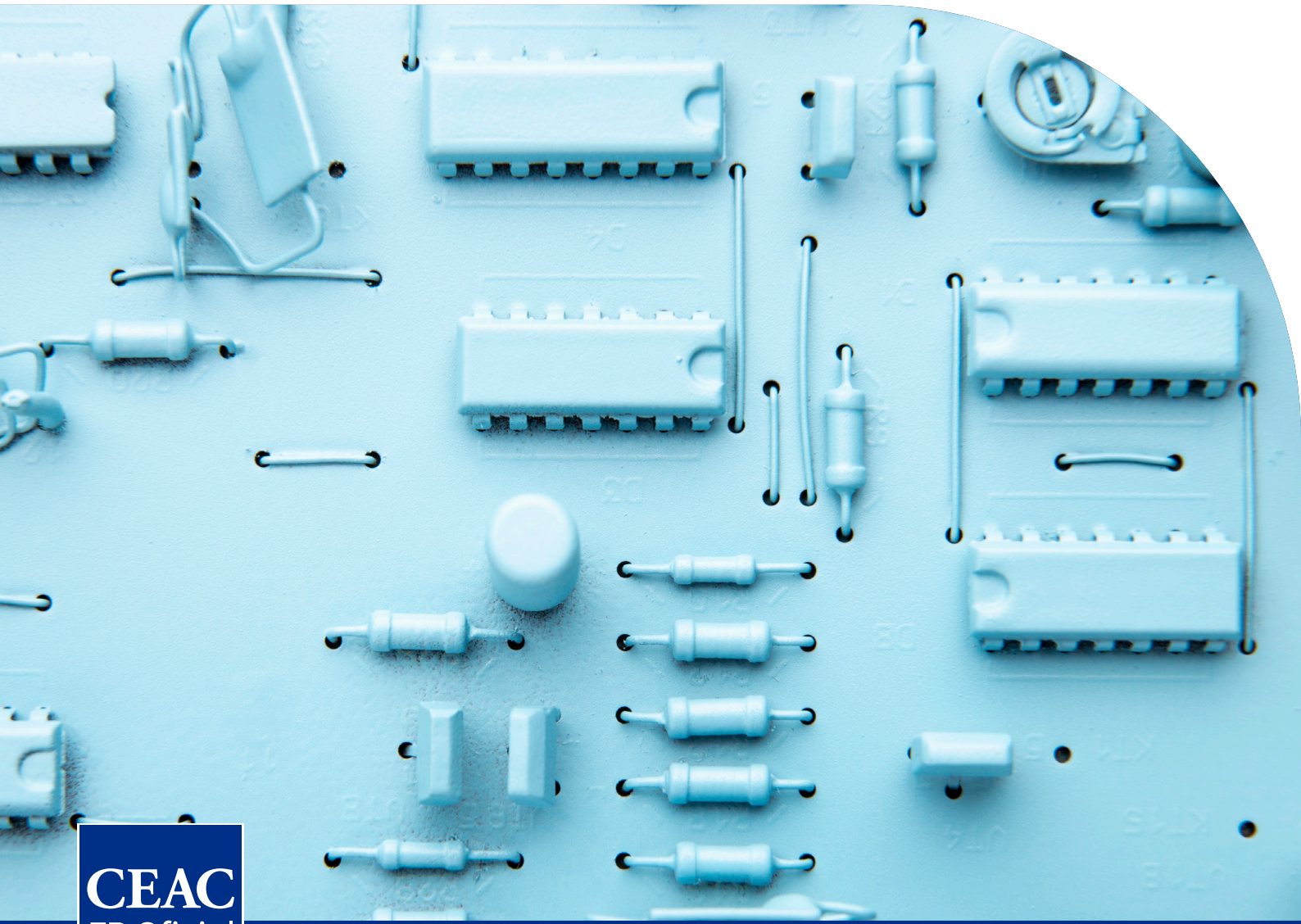
Desarrollo de aplicaciones multiplataforma

MÓDULO:

Sistemas informáticos

UNIDAD:

Gestión de información



CEAC
FP Oficial

MÓDULO:

Sistemas informáticos

UNIDAD:

Gestión de información

CEAC FP Oficial

ÍNDICE

1. Introducción

Las ideas y sensaciones humanas son efímeras por naturaleza; sin embargo, hemos sido capaces de crear un gran mapa del entorno que nos rodea, de nuestro pasado y de nuestra historia gracias a nuestra habilidad para representar esas ideas y sensaciones, utilizando diferentes códigos e inventando soportes persistentes cada vez más sofisticados donde imprimir dichos códigos.

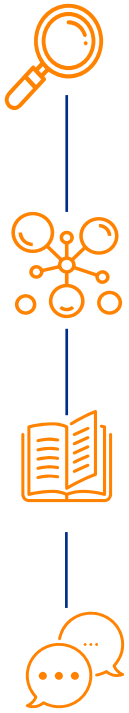
La evolución de los soportes de información ha estado marcada por saltos cualitativos. La invención del papiro hizo que en unos pocos rollos pudiesen transcribirse las leyendas orales y escritas sobre piedra de toda una civilización; la imprenta pudo realizar millones de copias de textos selectos para extenderlos por todo el mundo; de manera similar, los soportes digitales actuales, como los discos duros o las memorias de estado sólido, son capaces de almacenar una antología razonablemente buena de toda la cultura que la humanidad ha sido capaz de crear hasta la fecha, recopilando las más importantes obras literarias, científicas, pictóricas, musicales e incluso cinematográficas.

La masificación de datos en los soportes digitales obliga a distinguir entre la máquina física, donde se aglutinan billones de unidades de información, y el sistema lógico, imprescindible para poder recuperar y devolver el sentido a lo almacenado.

Las obras almacenadas en un medio digital se llaman indistintamente archivos o ficheros. En esta unidad verás cómo los archivos se almacenan en los medios digitales, así como la manera en que se integran los diferentes soportes físicos en un ordenador, cuáles son las técnicas para aumentar la integridad de la información y la eficiencia en el acceso a esta, y el modo de introducir, organizar y eliminar los ficheros. Después, verás cómo mejorar la eficiencia de la administración programando tareas en el tiempo y obteniendo estadísticas del rendimiento del sistema.

2. Objetivos pedagógicos

Los objetivos de aprendizaje que se pretenden alcanzar con esta unidad son:



- **Comprender la importancia y evolución de los soportes de información.**
- **Analizar los conceptos y códigos utilizados en la representación de ideas y sensaciones.**
- **Comprender la relación entre la máquina física y el sistema lógico en el almacenamiento de archivos digitales.**
- **Aprender técnicas para organizar y gestionar archivos digitales de manera eficiente.**

3. Gestión de información

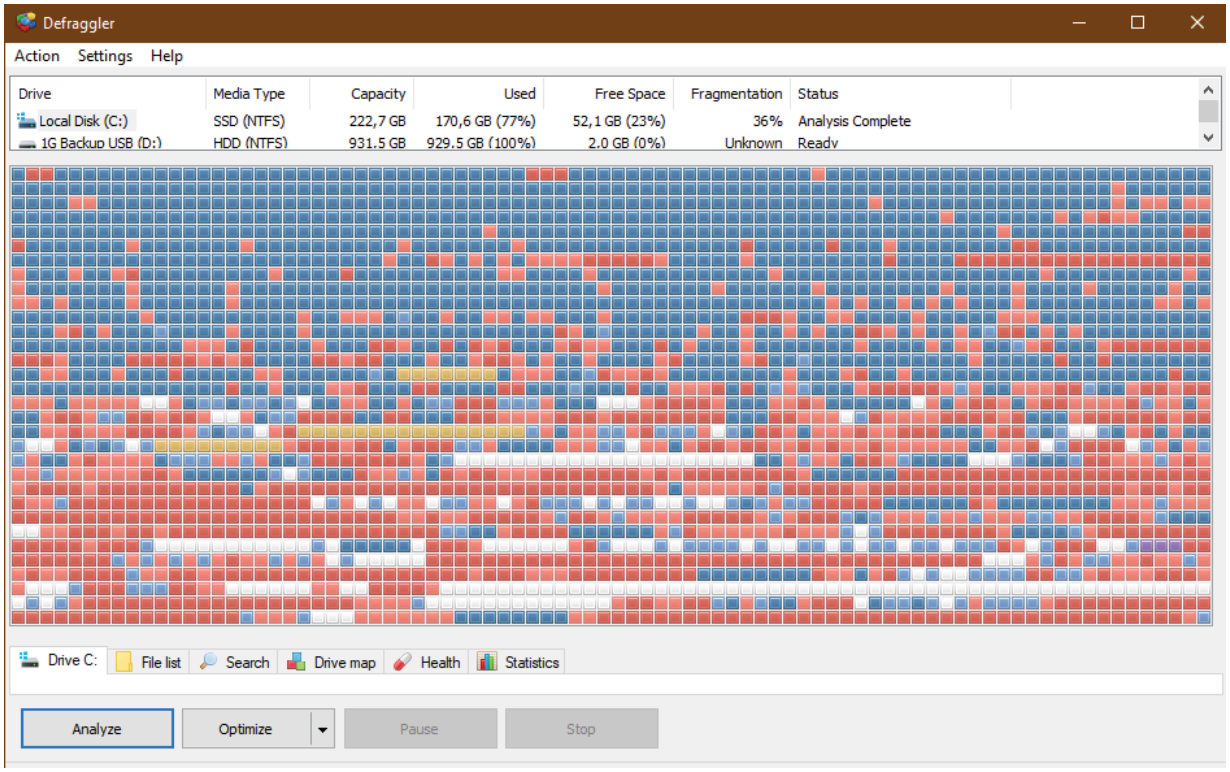
3.1. Sistemas de archivos

Un **sistema de archivos** es el conjunto de las normas y los procedimientos que debe seguir un sistema informático para poder ubicar información en un soporte físico digital, como puede ser un disco duro, un USB o un DVD, y para que el mismo sistema u otro que siga las mismas normas y procedimientos pueda recuperar dicha información. La unidad fundamental de un sistema de archivos es el archivo o fichero.

Un sistema de archivos proporciona una estructura lógica para acceder y gestionar los archivos y directorios en un dispositivo de almacenamiento. Permite al sistema operativo guardar y recuperar datos de manera eficiente, así como realizar operaciones como creación, modificación, eliminación y búsqueda de archivos.

Un **fichero es una agrupación de datos** que forman bien una obra completa o bien parte de una misma obra, como, por ejemplo, una fotografía, un texto o los primeros minutos de una película. El fichero es manejado por el sistema de archivos como una unidad, incluso cuando los datos están físicamente separados en diferentes zonas del soporte.

El sistema operativo es el responsable de implementar los sistemas de archivos en los soportes cuya maquinaria pueda controlar. Como veremos más adelante, un mismo soporte puede contener varios sistemas de archivos accesibles mediante diferentes sistemas operativos.



Un mismo archivo puede estar dividido y almacenado en diferentes secciones del disco duro generando un mapa de datos irregular, pero el sistema operativo tratará las diferentes partes del archivo como una única unidad de datos.

Las unidades lógicas han de estar formateadas con un sistema de archivos en el que el sistema operativo pueda interpretar los bits que identifican los ficheros almacenados.

Existen distintos **tipos de sistemas de archivos**:

FAT

Este sistema utiliza una **tabla de asignación de archivos** (Files Asignation Table). Los archivos almacenados en este sistema de archivos son divididos en clústeres, unidades de almacenamiento del disco, y se indica en la tabla FAT el primer y último clúster de cada archivo. Las tablas FAT y el directorio raíz han de estar siempre en la misma posición de la unidad lógica para ser localizados en el arranque del sistema y se guardan dos copias de ellos para recuperarlos en caso de errores.

No existe un orden por el que se almacena la información en el disco. Generalmente, se utiliza el primer clúster libre, lo que provoca que un mismo archivo pueda estar distribuido en diferentes partes del disco, hecho que a su vez provoca una alta latencia en el acceso y lectura de los archivos. Una técnica para unir los clústeres que corresponden a un mismo archivo es la desfragmentación, pero el tiempo del proceso es muy largo.

El **sistema FAT** es efi ciente para unidades de hasta 200 MB, pero con unidades mayores, las tablas FAT son más grandes y el rendimiento se reducirá sensiblemente. Además, en función del sistema operativo, el sistema de archivos FAT no soporta unidades de gran tamaño. Para Windows NT, por ejemplo, el límite de sistema era de 4 GB.

Pero, además de la limitación de tamaño, la mayor limitación de este sistema es la de las propiedades de los archivos. Aunque las propiedades como solo lectura, archivo oculto o los permisos de usuario se apliquen desde el sistema operativo, en realidad es en el sistema de archivos de la unidad lógica donde se aplican. En el sistema FAT solo es posible aplicar a los archivos las propiedades de solo lectura, oculto, sistema o modifi cado, dejando fuera todos los permisos de usuarios y credenciales.

Este sistema es el utilizado por sistemas operativos como Windows, es simple y compatible, pero menos eficiente y limitado en términos de tamaño máximo de archivo y partición.

NTFS

Este sistema es el más utilizado hoy en día en los sistemas Microsoft porque ofrece mejor seguridad, control de acceso y capacidad para manejar archivos grandes y particiones grandes.

Desde el punto de vista del usuario, los archivos se siguen distribuyendo en forma de árbol mediante directorios igual que en el sistema FAT. La diferencia es que no existen sectores especiales en el disco como tablas FAT ni tiene dependencias de hardware como sectores específicos o posiciones fijas.

Las ventajas fundamentales de este sistema de archivos son la eliminación del límite de tamaño soportado y el aumento en las propiedades de un archivo, añadiéndose todo el conjunto de permisos y credenciales de usuario sobre los archivos y directorios.

Otros sistemas

Además de los **sistemas de archivos para Windows FAT y NTFS**, podemos encontrar otros sistemas de archivos si trabajamos con otros sistemas operativos, como, por ejemplo Linux.

A continuación se presenta un conjunto de sistemas de archivos para Linux clasificados según su naturaleza.

- **Sistema de ficheros de disco.** Se trata de los sistemas de ficheros que encontramos en los dispositivos locales de los ordenadores. Algunos ejemplos de estos sistemas de archivos son ext2, ext3, ext4, ReiserFS, XFS, JFS e ISO9660.
- **Sistema de ficheros en red.** Este tipo de sistemas de ficheros posibilitan que ordenadores clientes, a través de una red de área local, se conecten a otro servidor y accedan a sus ficheros como si tratase de recursos locales. Algunos ejemplos de estos sistemas de archivos son ext2, ext3, ext4, vfat, NTFS, HFS e ISO9660.

3.2. Gestión de sistemas de archivos mediante comandos y entornos gráficos

Para poder acceder a la información almacenada en un sistema informático, los datos son estructurados en forma de árbol mediante archivos y carpetas. Históricamente, siempre se han utilizado los comandos de los sistemas operativos para navegar a través de los archivos y carpetas, así como tareas de mantenimiento como su creación, copiado y eliminación.

Algunos de los comandos más utilizados son:

- **"cd":** Permite cambiar de directorio.
- **"ls" (o "dir" en Windows):** Muestra el contenido de un directorio.
- **"mkdir" (o "md" en Windows):** Crea un nuevo directorio.
- **"rm" (o "del" en Windows):** Elimina un archivo.

Evidentemente, estas tareas pueden ser realizadas de manera mucho más rápida dentro del entorno gráfico proporcionado por los sistemas operativos actuales.

Además de los comandos básicos utilizados para navegar a través de los directorios, también existen comandos que nos permiten gestionar completamente los sistemas de archivos, desde sus permisos de lectura y escritura hasta dar formato a una unidad por completo.

Los **sistemas Unix** tienen un mayor control sobre los permisos aplicados sobre carpetas y archivos, y es importante conocer los comandos que se utilizan para crear dichos permisos, puesto que es mucho más común en servidores modificarlos mediante comandos que mediante el entorno gráfico del sistema operativo. La forma de aplicar permisos es una secuencia numérica de tres cifras que van del 0 al 7 según el nivel de permisos y en la que cada dígito de los tres que la componen corresponden a Administrador, Grupo y Otros, respectivamente.

En el sistema Linux, los números de los permisos se suman para indicar que se aplican a cada tipo de usuario.

3.3 Estructura de directorios de sistemas operativos libres y propietarios

Para que los **archivos guardados en un medio digital** puedan ser recuperados, es necesaria una estructura lógica que permita al usuario conocer su existencia y localizarlos: esta estructura se llama árbol de directorios y proporciona un marco lógico para almacenar y acceder a la información, facilita el mantenimiento del sistema, permite el control de acceso y seguridad, y promueve la interoperabilidad y portabilidad entre diferentes sistemas. Una estructura de directorios bien diseñada contribuye a mejorar la eficiencia, la productividad y la confiabilidad del sistema operativo en general.

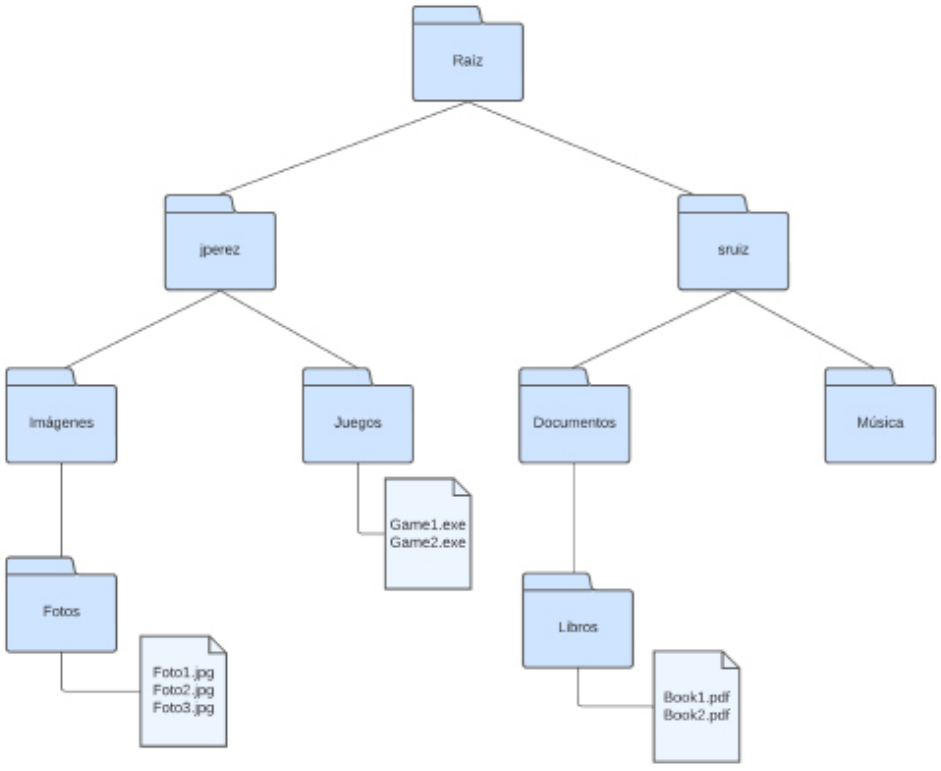
El árbol de directorios es una representación visual y jerárquica de la estructura de directorios en un sistema de archivos. Se utiliza comúnmente en sistemas operativos y sistemas de almacenamiento para organizar y gestionar los archivos y carpetas de manera lógica.

Un **árbol de directorios** se construye mediante la creación de listas, también conocidas como directorios, que pueden contener nombres de archivos y otras listas (subdirectorios). Esta estructura jerárquica se forma a partir de una lista principal llamada raíz, de la cual se derivan todas las demás listas.

Cada lista (directorio) que se deriva de otra se considera un directorio hijo de ese directorio padre. Del mismo modo, el directorio del cual se deriva una lista se conoce como directorio padre de esa lista. Así, las listas pueden tener relaciones de antecesoras y sucesoras en función de si contienen otras listas o están contenidas en ellas. Cuando varias listas y archivos comparten un directorio antecesor común, se dice que cuelgan de ese directorio.

Un árbol de directorios, por tanto, es una jerarquía de directorios (listas de archivos) que puede representarse mediante un árbol genealógico.

Un árbol de directorios está bien definido si los nombres de los diferentes directorios reflejan claramente categorías y si su jerarquía se corresponde con una jerarquía de categorías de general a particular. Si es así, un usuario que conoce algunas de las propiedades de un archivo podrá examinar primero el directorio raíz, después el directorio descendiente cuyo nombre refleje la categoría a la que debería pertenecer el archivo, y así sucesivamente, particularizando cada vez más hasta dar con el archivo que busca, siguiendo así una ruta lógica.



Representación gráfica de un árbol de directorios.usuario.

RECUERDA: Los sistemas operativos de tipo Unix pueden ser muy diferentes internamente, pero con respecto al usuario son casi idénticos porque basan su comunicación en un estándar llamado Posix.

El sistema operativo de un ordenador está grabado en un árbol de directorios, por lo que un usuario que se enfrenta por primera vez a un determinado ordenador se encontrará con nombres de ficheros y directorios que ya están definidos.

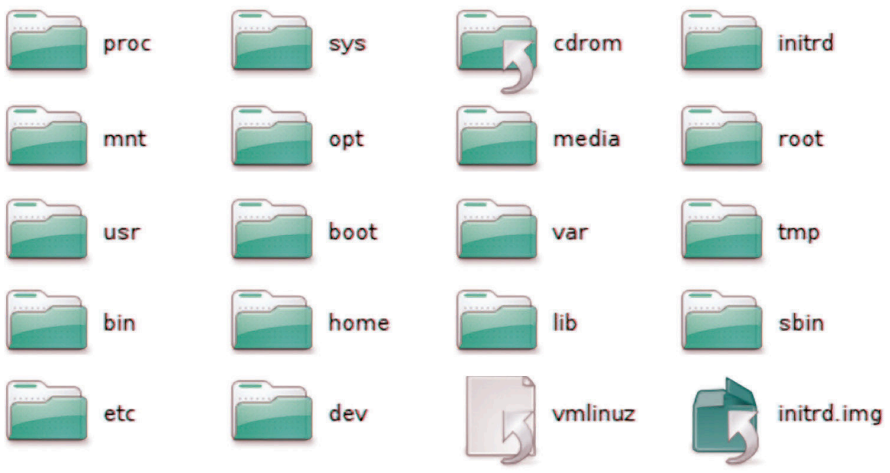
Sin embargo, cada usuario tiene asignado un directorio en el cual puede crear su propia estructura, siendo el responsable de escoger los nombres de los archivos y de los directorios que allí cree. Si es cuidadoso con la creación de dicha estructura, le será muy fácil hallar sus propios archivos.

Los volúmenes, ya sean medios completos, matrices o particiones, contienen un único sistema de archivos que se integra en los sistemas operativos, incorporándose a su estructura de directorios.

La forma como se realiza esta integración varía según el sistema operativo. Consideramos las dos siguientes por ser las más comunes:

- **Estructura normalizada FHS.** Posix es una norma internacional creada para que los usuarios y administradores de diferentes sistemas operativos puedan trabajar en un entorno muy similar. Se suele decir que dichos sistemas operativos son de tipo Unix. Esta norma aconseja un árbol de directorios predefinido para el sistema operativo con una sola raíz, llamado FHS. Para integrar un volumen se crea un directorio vacío, y en ese directorio se monta el volumen, lo cual significa que toda la jerarquía de ficheros del volumen pasa a colgar de dicho directorio.

  El directorio en el que se monta un volumen puede ser cualquiera, incluidos los directorios del sistema operativo. Para montar volúmenes temporales, como pendrives o discos extraíbles, se aconseja utilizar los directorios media o mnt.



La estructura de directorios FHS es común a todos los sistemas operativos basados en Unix.

- **Estructura NTFS.** La estructura de archivos de Microsoft, NTFS, es utilizada por todos los sistemas operativos de Microsoft desde Windows 2000. Esta estructura admite un doble comportamiento: por un lado, trabaja igual que sus antecesores, los sistemas de archivos de la familia FAT. En este caso, el sistema operativo asigna a cada volumen un nombre de unidad que consiste en una letra entre la A y la Z seguida de dos puntos (:).

  Cada volumen tiene su propio árbol de directorios y el nombre de unidad indica la raíz. El otro comportamiento posible es similar a FHS: un volumen puede ser montado en un directorio cualquiera de otro volumen.

3.3.1 Sistema de archivos Unix

A diferencia de los sistemas Microsoft, Unix utiliza el sistema de archivos para albergar no solo los ficheros y las carpetas, sino también binarios que son utilizados para administrar las herramientas del sistema y los periféricos conectados. Para un usuario sin experiencia puede ser confuso no saber dónde poder encontrar algún directorio del sistema, pero Unix tiene una distribución intuitiva fácil de comprender con un poco de práctica. Para empezar, existen cuatro tipos de directorios según su contenido:

- **Estáticos**. Contienen binarios, bibliotecas, documentación y otros ficheros que no cambian sin intervención del administrador. Pueden estar en dispositivos de solo lectura (read-only) y no necesitan que se hagan copias de seguridad tan a menudo como con ficheros dinámicos.
- **Dinámicos**. Estos directorios contienen archivos que no son estáticos y pueden cambiar con mayor frecuencia. Deben encontrarse en dispositivos de lectura-escritura (read-write) para permitir modificaciones y actualizaciones. Necesitan que se hagan copias de seguridad a menudo debido a su naturaleza cambiante.
- **Compartibles**. Contienen ficheros que se pueden encontrar en un ordenador y utilizarse en otro. Estos archivos son compartidos y accesibles por múltiples usuarios o sistemas en una red. Permiten compartir recursos y datos entre diferentes sistemas y usuarios.
- **No compartibles.** Contienen ficheros que no son compartibles. Pueden ser archivos confidenciales, específicos de un usuario o sistema, que no están destinados a ser compartidos con otros usuarios o sistemas. Estos archivos suelen ser de uso privado y restringido a un contexto específico.

Por ejemplo:

- **Estáticos**

  /bin, /sbin, /opt, /boot, /usr/bin

- **Dinámicos**

  /var/mail, /var/spool, /var/run, /var/lock, /home

- **Compartibles**

  /usr/bin, /opt

- **No compartibles**

  /etc, /boot, /var/run, /var/lock

RECUERDA: Todos los directorios dependen del directorio raíz "/" incluso cuando se trata de unidades lógicas separadas o periféricos acoplados al equipo. A diferencia de Microsoft, no existen diferentes unidades (c:, d:, e:).

A continuación, veamos una lista de los directorios más importantes, en un sistema Unix/Linux:

- /bin/ Comandos/. Programas binarios esenciales (cp, mv, ls, rm, etc).
- /boot/. Ficheros utilizados durante el arranque del sistema (núcleo y discos RAM).
- /dev/. Dispositivos esenciales, discos duros, terminales, sonido, vídeo, lectores DVD / CD, etc.
- /etc/. Ficheros de confi guración utilizados en todo el sistema y que son específi cos del ordenador.
- /etc/opt/. Ficheros de configuración utilizados por programas alojados dentro de /opt/.
- /etc/X11/. Ficheros de configuración para el sistema X Window.
- /etc/sgml/. Ficheros de configuración para SGML (Opcional).
- /etc/xml/. Ficheros de configuración para XML (Opcional).
- /home/. Directorios de inicios de los usuarios (Opcional).
- /lib/. Bibliotecas compartidas esenciales para los binarios de /bin/, /sbin/ y el núcleo del sistema.
- /mnt/. Sistemas de ficheros montados temporalmente.
- /media/. Puntos de montaje para dispositivos de medios como unidades
- lectoras de discos compactos. Nota: Ubuntu monta en este directorio las particiones Windows caso de existir.
- /opt/. Paquetes de aplicaciones estáticas.
- /proc/. Sistema de ficheros virtual que documenta sucesos y estados del
- núcleo. Contiene principalmente ficheros de texto.
- /root/. Directorio de inicio del usuario root
- /sbin/. Comandos/programas binarios de administración de sistema.
- /tmp/. Ficheros temporales
- /srv/. Datos específicos de sitios servidos por el sistema.
- /usr/. Jerarquía secundaria para datos compartidos de solo lectura (Unix
- system resources). Este directorio puede ser compartido por múltiples ordenadores y no debe contener datos específicos del ordenador que los comparte.

- /usr/bin/. Comandos/programas binarios.
- /usr/include/. Ficheros de inclusión estándar (cabeceras de cabecera utilizados para desarrollo).
- /usr/lib/. Bibliotecas compartidas.
- /usr/share/. Datos compartidos independientes de la arquitectura del sistema. Imágenes, ficheros de texto, etc.
- /usr/src/. Códigos fuente (Opcional).
- /usr/X11R6/. Sistema X Window, versión 11, lanzamiento 6 (Opcional).
- /usr/local/. Jerarquía terciaria para datos compartidos de solo lectura específicos del ordenador que los comparte.
- /var/. Ficheros variables, como son logs, bases de datos, directorio raíz de servidores HTTP y FTP, colas de correo, ficheros temporales, etc.
- /var/cache/. Cache de datos de aplicaciones.
- /var/crash/. Depósito de información referente a caídas del sistema (Opcional).
- /var/games/. Datos variables de aplicaciones para juegos (Opcional).
- /var/lib/. Información de estado variable. Algunos servidores como MySQL y PostgreSQL almacenan sus bases de datos en directorios subordinados de éste.
- /var/lock/. Ficheros de bloqueo.
- /var/log/. Ficheros y directorios de registro del sistemas (logs).
- /var/mail/. Buzones de correo de usuarios (Opcional).
- /var/opt/. Datos variables de /opt/.
- /var/spool/. Colas de datos de aplicaciones.
- /var/tmp/. Ficheros temporales preservados entre reinicios.

Es importante tener en cuenta que esta lista puede variar ligeramente dependiendo de la distribución de Unix/Linux que estés utilizando. Cada distribución puede tener su propia estructura de directorios específica, pero estos directorios son comunes en la mayoría de los sistemas Unix.

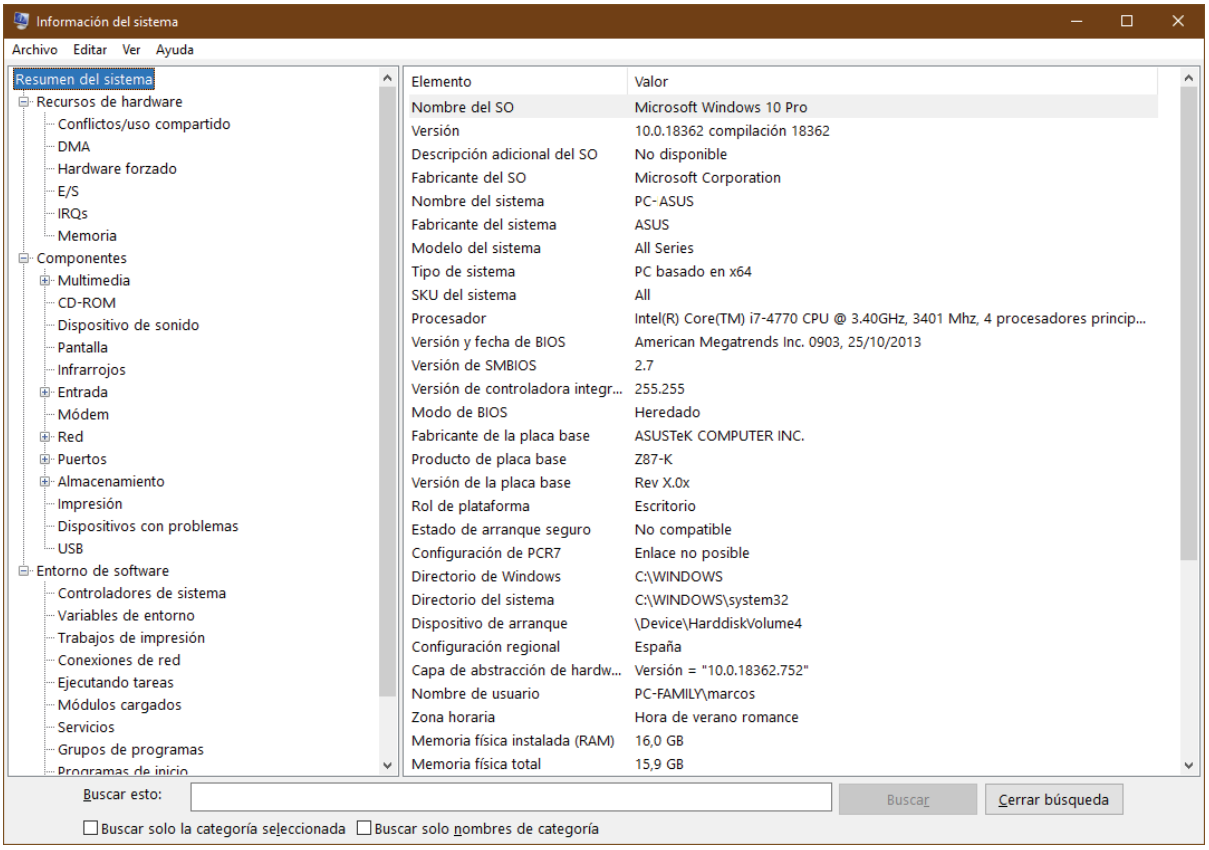
RECUERDA: El comando systeminfo del intérprete de comandos muestra información detallada del estado de un sistema Windows.

3.4 Búsqueda de información del sistema mediante comandos y herramientas gráficas

Los sistemas operativos Windows incluyen una utilidad llamada Información del sistema que ofrece cinco categorías de información:

- **Resumen del sistema.** Esta categoría muestra detalles sobre el sistema operativo instalado, incluyendo su versión, el tipo de procesador utilizado, información de la BIOS y la cantidad de memoria RAM disponible en el sistema.
- **Recursos de hardware.** Analiza las señales y recursos utilizados por los dispositivos que componen el sistema. La utilidad notifica posibles problemas o conflictos que puedan surgir entre los dispositivos, lo que puede ayudar a identificar y resolver problemas de hardware.
- **Componentes**. Proporciona información sobre los dispositivos periféricos conectados al sistema, como impresoras, tarjetas de sonido, tarjetas de red, entre otros. También se muestra información sobre los controladores utilizados por el sistema operativo para estos dispositivos.
- **Entorno de software.** Analiza los programas del sistema que están en funcionamiento. Puedes obtener detalles sobre los procesos en ejecución, servicios activos y otros componentes de software que están interactuando con el sistema operativo.
- **Red**. Proporciona información relacionada con la configuración de red del sistema. Puedes obtener detalles sobre los adaptadores de red instalados, las conexiones activas, la configuración de protocolos de red y otra información relevante para la conectividad de red.

En los sistemas operativos de tipo Unix, como Linux, la información del sistema se puede obtener a través de los archivos ubicados en los directorios /proc y /sys. Estos directorios contienen archivos virtuales que proporcionan información en tiempo real sobre diversos aspectos del sistema. Por ejemplo, el comando “cat /proc/cpuinfo” muestra información detallada sobre la CPU del sistema. De manera similar, el comando “cat /proc/meminfo” muestra información sobre el uso de la memoria RAM.



La utilidad Información del sistema de Windows proporciona información muy útil para el diagnóstico de problemas

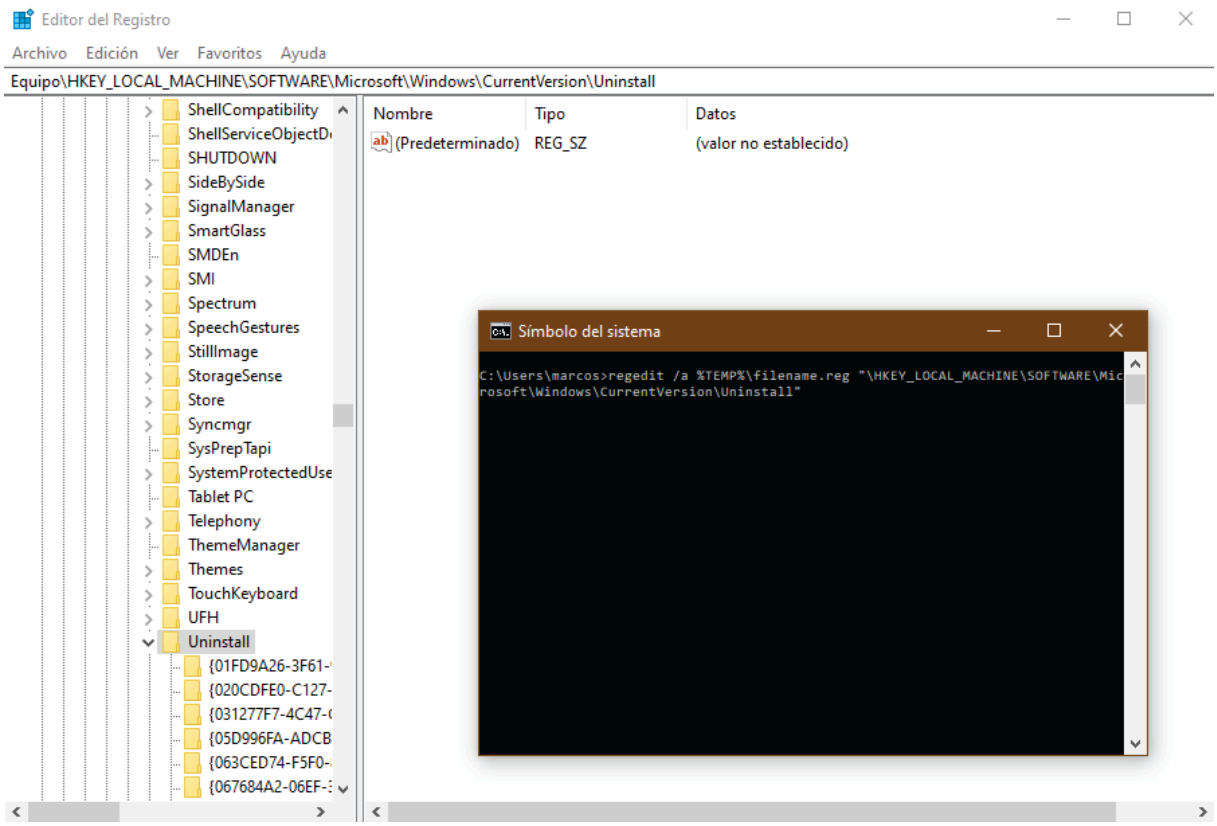
3.5 Identificación del software instalado mediante comandos y herramientas gráficas

Al i**nstalar una aplicación en un sistema**, generalmente se inscribe información del software en un registro que contiene todos aquellos programas que han sido instalados junto a información sobre versiones, directorios e instrucciones para proceder a su desinstalación.

Gracias a este registro, es posible acceder a la información para hacer un listado de todos aquellos programas que han sido instalados. Para acceder al archivo que contiene esta información, lo podemos hacer de manera manual mediante líneas de comandos o mediante el listado de registros que proporciona el sistema.

Generalmente, no es necesario recurrir a los comandos para poder **desinstalar** un programa, puesto que los sistemas operativos actuales proporcionan herramientas gráficas que permiten listar los programas instalados y desinstalarlos correctamente del sistema.

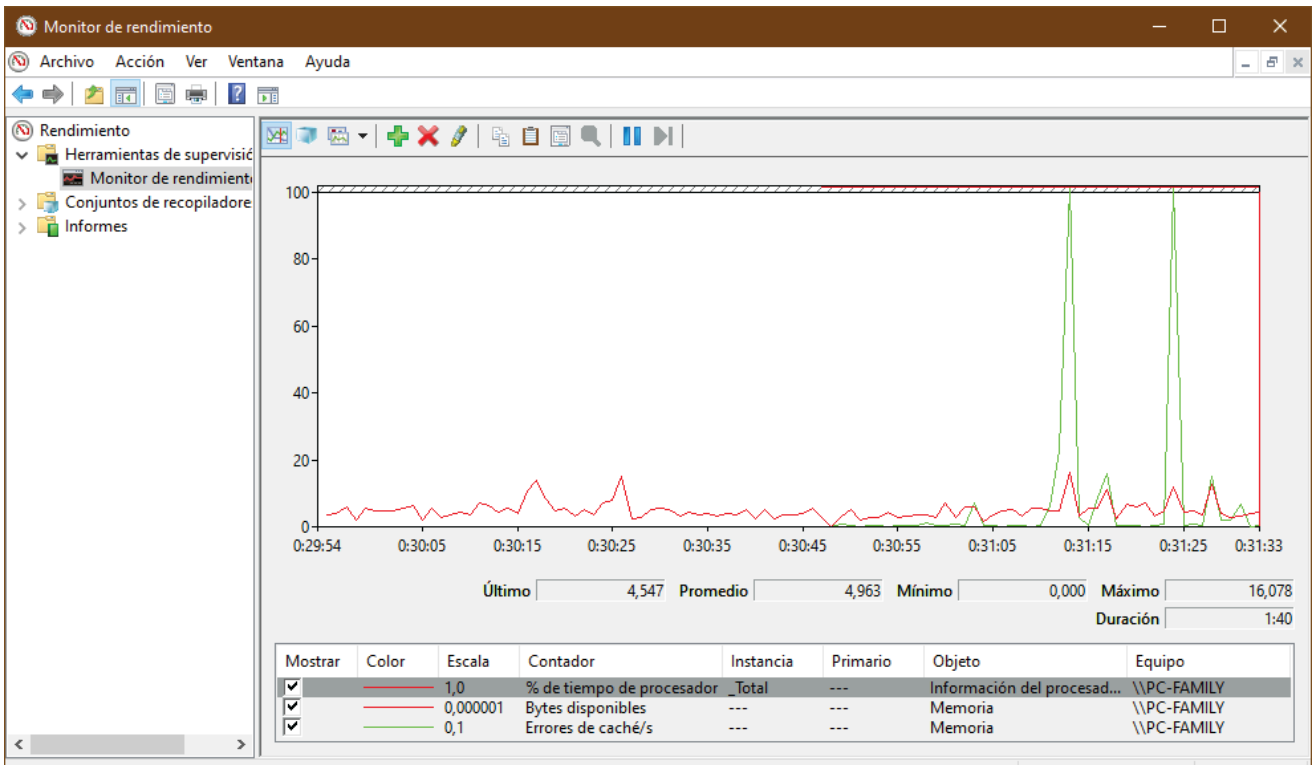
La ventaja de realizar la desinstalación manualmente podría ser la completa eliminación de todos los datos, puesto que algunos programas, a pesar de haber sido desinstalados, siguen manteniendo carpetas y archivos en nuestro sistema.



Se muestra simultáneamente la ventana de comandos donde podemos aplicar cambios a los registros y la pantalla de registros proporcionada por el sistema Windows, donde se listan todos los registros del sistema

3.6 Gestión de la información del sistema. Rendimiento. Estadísticas. Montaje y desmontaje de dispositivos en sistemas operativos

Para realizar un seguimiento estadístico del rendimiento del sistema, los sistemas operativos Windows tienen una aplicación gráfica llamada *Monitor* de rendimiento del Sistema localizada en el menú de *Inicio* > *Herramientas administrativas* > *Monitor de rendimiento*.



El monitor de rendimiento del sistema Windows muestra las estadísticas del estado del sistema a partir de las variables suministradas por el administrador.

Esta aplicación aporta varias **herramientas** que permiten al administrador hacer un seguimiento estadístico del rendimiento del sistema; es decir, proporciona numerosos indicadores que pueden ser monitorizados con diferentes tipos de contadores: instantáneos sobre gráfica, de frecuencia, de tiempo transcurrido, de promedio y otros. Puede mostrar varios contadores simultáneamente sobre una gráfica, y, además, acepta disparadores.

Se entiende por montar un dispositivo la acción de crear un acceso desde un directorio a un dispositivo conectado a nuestro sistema operativo. No significa copiar el contenido, sino crear un enlace entre el directorio y el dispositivo conectado. Dependiendo del dispositivo y el sistema operativo, este "*acceso directo*" será creado en un lugar determinado. En Windows, un dispositivo de almacenamiento es accesible desde *Este equipo*, mientras que a un escáner o a una impresora se accede desde *Configuración* > *Dispositivos*.

Los **sistemas Unix,** por otro lado, incorporan los montajes de los dispositivos en su estructura de directorios de manera que, para acceder a un pendrive conectado a la máquina, deberemos ir a la ruta */dev/sdb*. Este proceso se ha automatizado para la mayoría de casos, pero siguen existiendo dispositivos que requieren de un montaje manual; por ejemplo, cargar una imagen de DVD que tiene el formato ISO: primero se crea el directorio desde el cual se accederá al contenido del DVD, *mkdir /mnt/iso*, y posteriormente se montará el dispositivo (en este caso un archivo) en el directorio creado: *mount -t iso9660 imagenDVD.iso /mnt/iso*. A partir de este momento, podremos acceder al contenido de la imagen del DVD a través del directorio */mnt/iso*.

Los sistemas de tipo Unix utilizan, sin embargo, una utilidad estándar llamada Sysstat que provee varios comandos del sistema que se encargan de realizar informes estadísticos sobre el rendimiento del sistema. El comando sar permite imprimir los informes estadísticos. Existen, además, muchas aplicaciones creadas por desarrolladores independientes libres y comerciales. Por ejemplo, SYSSTAT GRAPH.

3.7 Herramientas de administración de discos. Particiones y volúmenes. Desfragmentación y chequeo

La **gestión de volúmenes** se produce en varios niveles: el conexionado a un ordenador de los medios físicos y su reconocimiento por parte de la memoria BIOS o la UEFI; el establecimiento de particiones y matrices RAID; el reconocimiento por parte del sistema operativo de los volúmenes (particiones) durante el proceso de arranque o con el ordenador en funcionamiento; el montaje inicial de los sistemas de archivos de dichos volúmenes en el árbol o árboles de directorios; el formateado de los sistemas de archivos, y las operaciones de reparticionado y copia de seguridad.

El **conexionado físico** se realiza utilizando conectores normalizados. Antes de adquirir una unidad de almacenamiento, es necesario buscar la documentación del fabricante del ordenador y comparar con los catálogos para averiguar qué dispositivos son compatibles.

Entre las tecnologías actuales más comunes para conexiones internas y profesionales están SATA (I, II y III), SCSI (I, II, III e iSCSI), SAS, SSA, FC-AL y otras. Para dispositivos externos removibles, son más comunes USB (2.0/3.0/3.1/3.2) y FireWire.

El segundo paso es el reconocimiento del medio por los programas del fabricante del ordenador. Mientras que los discos más estándar son reconocidos automáticamente por la memoria BIOS o la UEFI de la mayoría de los ordenadores, los discos profesionales suelen tener un dispositivo adicional que debe instalarse en el interior del ordenador y que tienen su propia memoria para el manejo básico y configuración.

La configuración de la bios o de la memoria de control (firmware) del dispositivo se realiza pulsando alguna tecla poco después de comenzar la puesta en marcha de un ordenador y, por lo general, la propia pantalla del ordenador indica cuál es esa tecla durante un periodo muy corto de tiempo (uno o dos segundos).

En tercer lugar se debe definir y configurar la tabla de particiones, la cual es un conjunto de datos que indica al ordenador cuáles son los volúmenes instalados, si pueden utilizarse para poner en marcha el sistema operativo, en qué parte del medio se encuentran ubicados (si el medio es un disco duro se expresa en sectores), el tipo de sistema de ficheros utilizado, y, en sistemas Unix, el punto de montaje.

Tradicionalmente, la **tabla de particiones** se guarda en el primer sector de cada medio, llamado registro maestro de arranque o MBR, por sus siglas en inglés. Este sector es lo primero y lo único que es capaz de leer una memoria BIOS clásica. Desde la aparición de UEFI, el encargado de realizar esta tarea es GPT o tabla de particiones GUID. Tanto MBR con arranque múltiple como GPT pueden redirigir el arranque a una de las particiones del medio en el que está escrito o al MBR de otro medio.

Una **tabla de particiones tradicional** puede guardar los datos de hasta cuatro particiones, llamadas primarias. Después, la información de particiones se puede ampliar para tener más (particiones extendidas). GPT no tiene límites en el número de particiones, más allá de las del propio sistema operativo.

Actualmente, en los ordenadores de empresa la gestión de particiones de MBR a través de la memoria BIOS se halla al borde de la desaparición, y está siendo sustituida por UEFI, que realiza una gestión de particiones prácticamente desasistida, sin necesidad de buscar la información en el MBR. Aun así, existen muchas aplicaciones para administrar la tabla de particiones de un ordenador.

Las más básicas son los programas fdisk, disponibles para varios sistemas operativos. Más sofisticados y actuales son los programas cfdisk, gdisk y parted para sistemas operativos de tipo Unix, y bootrec /fi xmbr desde la consola de recuperación de Windows para este sistema.

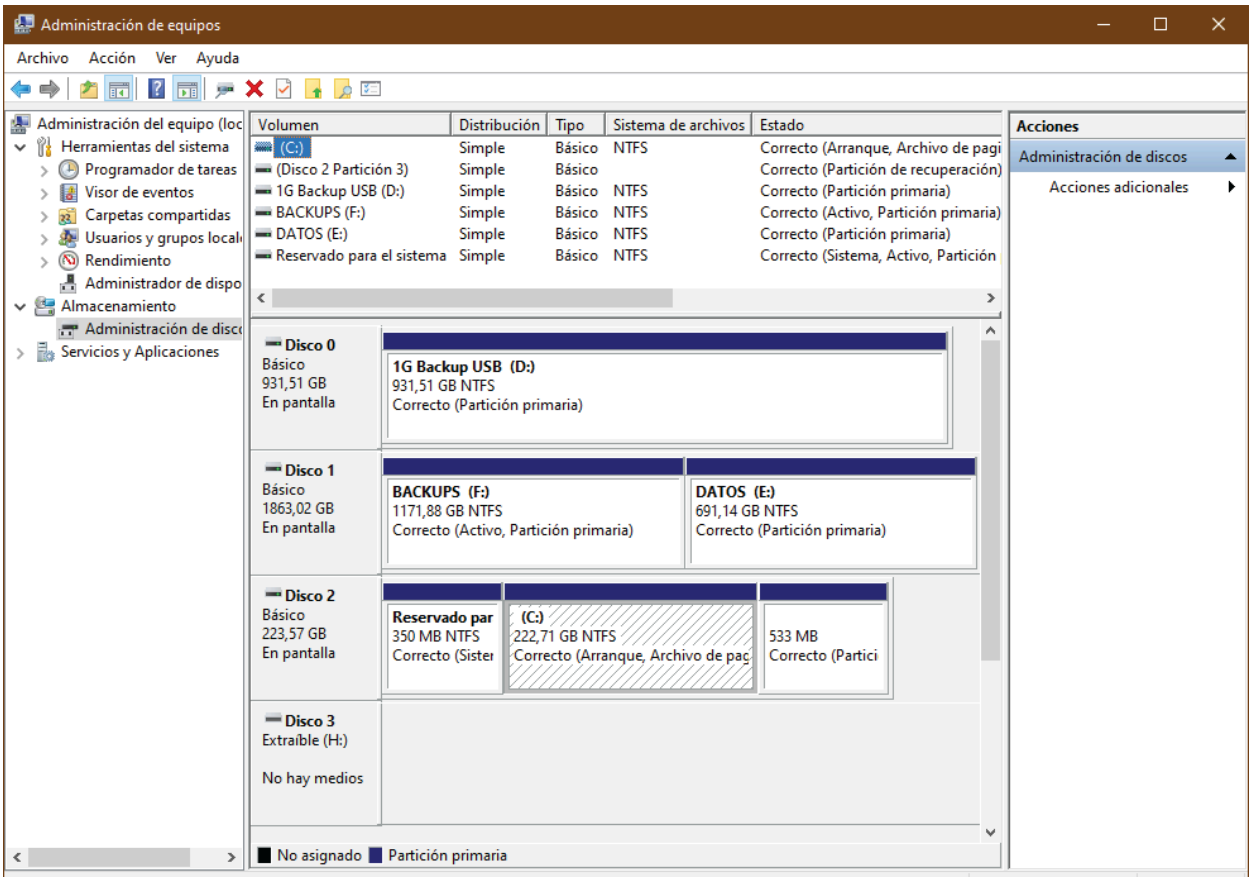
Una vez instalados los volúmenes y reconocidos en la tabla de particiones, hay que proceder a su formateado. Los sistemas de tipo Unix pueden formatear un volumen en una amplia diversidad de sistemas de archivos utilizando la utilidad comando mkfs desde el intérprete comandos -los sistemas Windows lo hacen desde el programa de instalación o desde el escritorio-, formateando en sistemas de archivos NTFS o, según el medio, en FAT32 –ahora en desuso mediante la herramienta de administración de discos.

Una vez particionado un disco es necesario montarlo. Los sistemas operativos orientados a usuarios personales hacen esto automáticamente, algunos sistemas de tipo Unix obligan a utilizar las instrucciones del intérprete de comandos mount, para montar, y umount para desmontar unidades.

Existen **muchas herramientas que permiten realizar de manera gráfica** y sencilla las operaciones de gestión de la tabla de particiones (el particionado) y otras más sofisticadas, como el cambio de tamaño de particiones sin borrar los contenidos o la copia de seguridad de volúmenes completos.

Windows cuenta con la herramienta de administración de discos que se encuentra en el escritorio siguiendo la secuencia *Inicio > Herramientas administrativas > Administración de equipos > Almacenamiento > Administración de discos*. En sistemas de tipo Unix, están gparted y kparted. Algunas herramientas de este tipo vienen en formato USB o CD-ROM autoarrancable, por lo que no dependen del sistema operativo instalado. Cabe destacar la herramienta libre Gparted Live, basada en gparted, y la herramienta propietaria Paragon Partition Manager.

PARA SABER MÁS: Los servidores de archivos utilizan por lo general el protocolo SMB.



La herramienta Administración de discos de Windows integra todas las funciones de gestión de los volúmenes principalmente con sistemas de

3.8 Sistemas de archivos de red y matrices de discos RAID

Los **sistemas de archivos de red** permiten compartir archivos y recursos entre diferentes dispositivos a través de una red. Estos sistemas se basan en un servidor central que almacena los archivos y los clientes que acceden a ellos a través de la red.

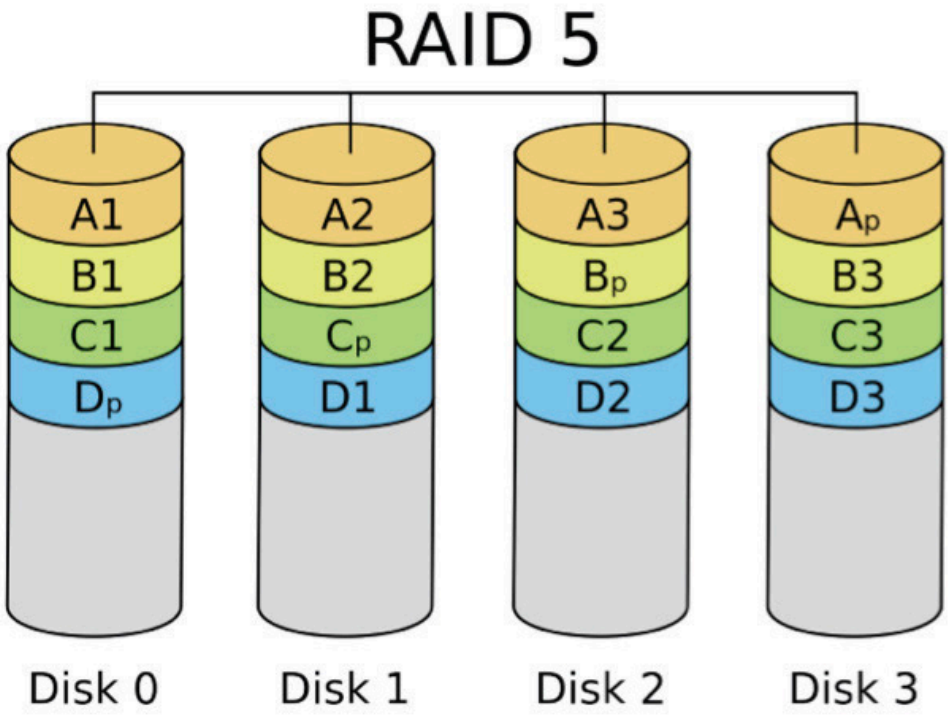
Algunos ejemplos populares de sistemas de archivos de red son el Protocolo de Sistema de Archivos en Red (Network File System, NFS), el Sistema de Archivos Distribuido (Distributed File System, DFS) y el Servicio de Archivos de Windows (Windows File Service).

La ventaja principal de los sistemas de archivos de red es la capacidad de acceder y compartir archivos de manera centralizada, lo que facilita la colaboración y el intercambio de información en entornos de red. Además, estos sistemas suelen ofrecer funcionalidades avanzadas como la gestión de permisos de acceso, la replicación de datos y la tolerancia a fallos, lo que garantiza la disponibilidad y la integridad de los archivos.

Así, los archivos de toda una sede o empresa se guardan generalmente en una cabina de discos, la cual provee los medios físicos de almacenamiento, además de una electrónica especial para administrar esos medios controlando los errores y optimizando la velocidad.

Los volúmenes de dicha cabina son montados en un servidor de archivos, que es un ordenador que cuenta con el software apropiado para poner sus archivos a disposición de los ordenadores de oficina a través de la red local.

Centralizar la información en un único punto reduce drásticamente el tiempo y los medios necesarios para su gestión, pero también introduce nuevos retos. Existe un único punto de fallo, por tanto, y este punto debe ser lo más fiable posible, tanto en disponibilidad como a la hora de asegurar la integridad de los datos. Es muy importante contar con un segundo sistema de almacenamiento de respaldo para actuar en caso de desastre.



Ejemplo de cómo se distribuye la información en un RAID 5. Aunque deje de funcionar un disco, siempre se puede recuperar su información.

La velocidad del sistema debe ser suficiente para cubrir la demanda de información de los usuarios. Para satisfacer estas demandas, los discos de la cabina pueden trabajar solidariamente en distintas configuraciones.

Estas configuraciones se llaman RAID. Las matrices de discos RAID son una tecnología que combina múltiples discos duros en un solo sistema lógico para mejorar el rendimiento y la fiabilidad del almacenamiento. RAID (Redundant Array of Independent Disks) utiliza diferentes técnicas para distribuir y duplicar los datos en los discos, lo que proporciona mayor velocidad de lectura/escritura y protección contra fallos.

Existen varios niveles de RAID, cada uno con su propia configuración y características. Algunos de los niveles de RAID más comunes son:

- **RAID 0.** Los datos se reparten entrelazados entre varios discos. Esta configuración multiplica la velocidad por el número de discos, pero también multiplica por el mismo factor la probabilidad de desastre por el fallo de un disco. Se trata de una configuración que se utiliza en aplicaciones de cálculo intensivo que requieren una muy alta velocidad y que no guardan datos críticos para la supervivencia de una empresa.
- **RAID 1.** Los datos se copian idénticos en dos discos. Si uno de ellos se avería, la matriz seguirá funcionando. Esta configuración apenas afecta a la velocidad, pero mejora muy notablemente la seguridad de los datos ante la avería de un disco. Se usa en pequeñas empresas por ser una manera barata de mejorar la fiabilidad del sistema.
- **RAID 5.** Distribuye la información de paridad entre todos los discos que forman parte del RAID. RAID 5 necesita un mínimo de tres discos para ser implementado y, generalmente, se implementa con soporte hardware para realizar el cálculo de la paridad. Si falla uno de los discos del RAID, con los que quedan se puede seguir accediendo a la información. Tiene una gran implantación, ya que sólo desperdicia un disco del conjunto para ofrecer la redundancia.

Las matrices de discos RAID son utilizadas en entornos donde se requiere un alto rendimiento y una mayor seguridad de los datos. Se utilizan en servidores y sistemas de almacenamiento para aplicaciones críticas que necesitan acceso rápido a los datos y protección contra la pérdida de información en caso de fallos del disco.

3.9 Gestión de archivos

Un sistema de gestión de archivos proporciona servicios para el uso y acceso de archivos y directorios.

3.9.1 Rutas

Todo archivo almacenado en un medio se distingue por un nombre y una posición en el árbol de directorios. La combinación de estos dos datos se llama ruta del archivo. No puede haber dos archivos ni directorios con la misma ruta, pero sí con el mismo nombre mientras la ruta sea diferente.

Las aplicaciones que permiten gestionar archivos tienen marcada la ruta de un directorio como activa. En un gestor de archivos gráfico, también llamado navegador de archivos, el directorio que aparece en pantalla es el directorio activo. En un intérprete de comandos, el directorio activo es el que aparece al solicitar un listado sin parámetros, con el comando ls en sistemas de tipo Unix o dir en sistemas Windows. La ruta del directorio activo puede mostrarse usando el comando pwd en Unix o cd (sin argumentos) en Windows.

Una ruta se puede expresar de dos maneras diferentes: desde la raíz del árbol de directorios se llama ruta absoluta y desde el directorio activo se llama ruta relativa.

Los sistemas operativos de tipo Unix expresan las rutas utilizando el caracter "/" como separador. Las rutas absolutas comienzan con /, indicando la raíz, mientras que las rutas relativas comienzan directamente con un nombre de archivo. De izquierda a derecha se listan todos los nombres de directorio que hay que recorrer hasta llegar al directorio o archivo que se quiere referenciar, separándolos con una barra de división (/).

Otro indicador importante son dos puntos sucesivos "..", los cuales indican el directorio padre del activo o del último referenciado en la ruta. Hay diversos caracteres que no se pueden utilizar en un nombre de ruta, entre ellos el espacio. Para superar esta limitación, se puede escribir la ruta entre comillas o utilizar el símbolo de contrabarra (\) seguido del caracter "prohibido".

PARA SABER MÁS: El intérprete de comandos es menos intuitivo que los sistemas gráficos, pero en manos de un profesional es mucho más eficiente a la hora de hacer tareas complejas.

A continuación podemos ver un ejemplo de ruta absoluta en Unix:

/home/fotos/arbol.jpg

Y esto un ejemplo de ruta relativa:

fotos/arbol.jpg

En los sistemas operativos Windows, las rutas también se representan de izquierda a derecha. Para indicar una ruta absoluta, se indica la letra del volumen donde nace el árbol seguida de dos puntos (A:, B:); y después se indican los nombres de los directorios hasta llegar al directorio o archivo al que se quiere hacer referencia, separados por contrabarras. Las rutas relativas comienzan directamente con el nombre de un directorio o archivo contenido en el directorio activo.

Una ruta absoluta en Windows puede ser:

c:\documentos\fotos\arbol.jpg

y una ruta relativa:

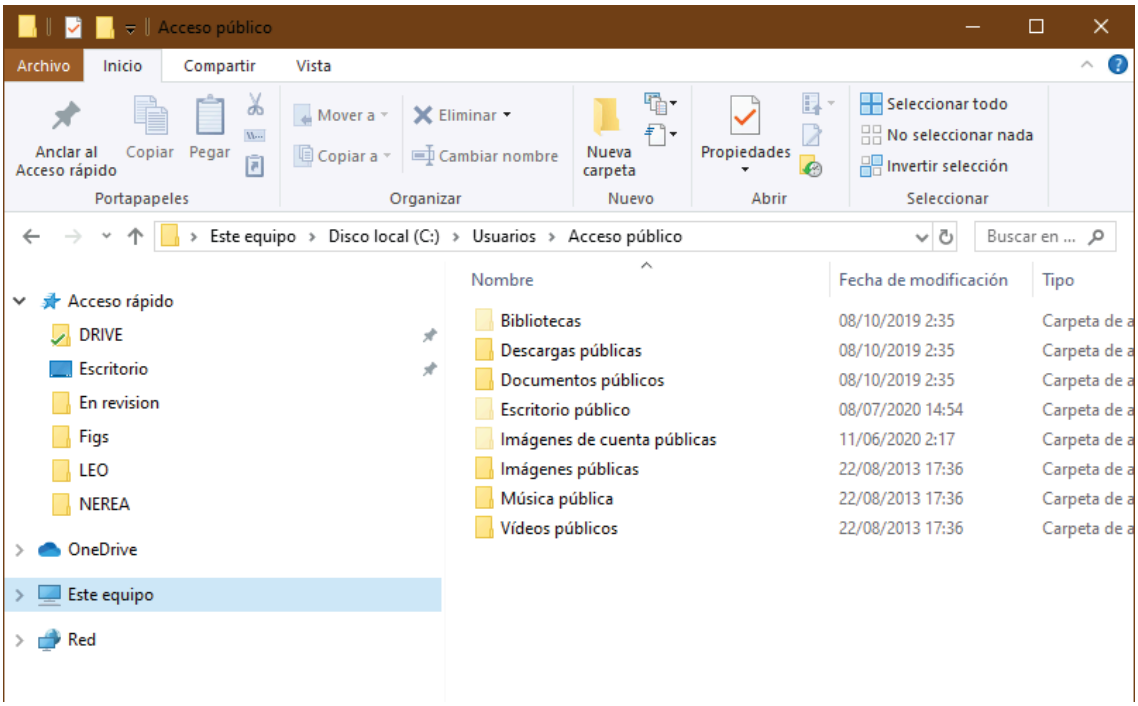
fotos\arbol.jpg

3.9.2 Herramientas de gestión de archivos

Veamos a continuación cuáles son las principales herramientas de gestión de archivos:

- **Administrador de archivos.** Muestra una o varias vistas con iconos en forma de carpeta que representan a los directorios y con otros iconos que representan a los archivos. Las operaciones básicas son:
  - *Desplazarse por el árbol de directorios.* Para cambiar el directorio activo a un hijo del actual pulsamos dos veces seguidas el botón principal del ratón sobre un icono de carpeta. Para cambiar al padre pulsa mos dos veces sobre el icono de padre, que suele ser el primer icono del listado.
  - *Ejecutar un programa o abrir un documento.* Pulsamos dos veces el botón principal del ratón con la flecha sobre el icono del archivo.
  - *Copiar y pegar un archivo.* Con la flecha sobre el icono del archivo a copiar, seleccionamos la opción Copiar, después cambiamos a otro directorio activo y seleccionamos la opción Pegar. En Windows, las opciones aparecen pulsando el botón secundario del ratón.

- *Cortar y pegar un archivo.* Análogamente, seleccionamos la opción.
- *Cortar con la flecha sobre un icono*, cambiamos el directorio activo y lo pegamos en éste.
- *Renombrar*. Con la flecha sobre el icono, seleccionamos la opción de cambiar de nombre y tecleamos el nuevo nombre para el archivo o directorio.



Un gestor de archivos permite administrar.

- **Intérprete de comandos.** Las operaciones más básicas son:
  - *Cambiar el directorio activo.* CD archivo.
  - *Copiar archivos*:
    - En Unix: cp archivo_a_copiar archivo_copiado.
    - En Windows: copy archivo_a_copiar archivo_copiado.
  - **Mover archivos:**
  - *En Unix:* mv archivo_a_mover archivo_movido.
  - *En Windows:* move archivo_a_mover archivo_movido.
- **Renombrar archivos:**
  - *En Unix:* mv archivo_a_renombrar archivo_renombrado.
  - *En Windows:* rename archivo_a_renombrar archivo_renombrado.

3.10 Montar volúmenes en carpetas

El **montaje de volúmenes** se refiere al proceso de vincular un dispositivo de almacenamiento, como un disco duro o una partición, a una carpeta o directorio específico en el sistema de archivos. Al montar un volumen en una carpeta, se le asigna una ubicación lógica que permite acceder a los archivos y directorios almacenados en ese dispositivo.

El montaje de volúmenes es esencial para acceder y utilizar dispositivos de almacenamiento en un sistema operativo. Permite al sistema reconocer y utilizar los datos almacenados en el dispositivo como si fueran parte del sistema de archivos principal.

Una unidad montada es una unidad asignada a una carpeta vacía de un volumen que utiliza el sistema de archivos NTFS. Las unidades montadas funcionan como cualquier otra unidad, pero son rutas de acceso de unidad asignadas en lugar de letras de unidad.

Cuando vemos una unidad montada, en el Explorador de Windows, aparece como un icono de unidad en la ruta de acceso en la que está montada. Como las unidades montadas no están sujetas al límite de 26 letras para las unidades locales y las conexiones de red asignadas, utilizamos unidades montadas cuando deseamos tener acceso a más de 26 unidades del equipo.

Por ejemplo, si tenemos una unidad de CD-ROM con la letra E y un volumen NTFS con la letra F, montamos la unidad de CD-ROM como F:\CD-ROM. Podemos liberar la letra de unidad E y tener acceso directamente a la unidad de CD-ROM mediante F:\CD-ROM.

También podemos utilizar **unidades montadas** cuando necesitemos espacio de almacenamiento adicional en un volumen. Si asignamos una carpeta de ese volumen a otro volumen con espacio de disco disponible (por ejemplo, 2 gigabytes), ampliará el espacio de almacenamiento del volumen en 2 gigabytes. Con las unidades montadas no está limitado por el tamaño del volumen donde se creó la carpeta.

Las unidades montadas hacen que los datos sean más accesibles y ofrecen flexibilidad para administrar el almacenamiento de datos basándose en el entorno de trabajo y la utilización del sistema.

Los siguientes son otros ejemplos en los que podemos utilizar unidades montadas:

- Para ofrecer espacio de disco adicional para los archivos temporales, podemos convertir la carpeta C:\Temp en una unidad montada.
- Cuando empiece a quedar poco espacio en la unidad C, podemos mover la carpeta Mis documentos a otra unidad que tenga más espacio de disco disponible y, después, montarla como C:\Mis documentos.

Utilizamos el complemento Administración de discos o el comando mountvol para montar una unidad en una carpeta de un volumen local. La carpeta en la que montemos la unidad debe estar vacía y debe encontrarse en un volumen NTFS básico o dinámico.

3.11 Tolerancia a fallos

En los sistemas profesionales en los que es vital el mantenimiento de la información almacenada, es importante tener en cuenta la tolerancia a fallos de los sistemas. Entendemos por tolerancia a fallos la capacidad de un servidor o sistema de almacenamiento para continuar funcionando correctamente a pesar de la presencia de fallos o errores. En otras palabras, implica la capacidad de un sistema para resistir y recuperarse de fallas sin interrumpir sus operaciones normales.

En términos más técnicos, la tolerancia a fallos implica la implementación de mecanismos y técnicas que permiten detectar, mitigar y recuperarse de fallos de hardware, software o comunicación, evitando así la interrupción de los servicios y la pérdida de datos.

Existen diversas estrategias y técnicas utilizadas en la tolerancia a fallos para garantizar la continuidad y la disponibilidad de los sistemas. Algunas de las más comunes son:

- **Redundancia**: Consiste en la duplicación de componentes críticos, como discos duros, fuentes de alimentación o servidores, de modo que si uno de ellos falla, el sistema pueda seguir funcionando sin interrupciones. La redundancia puede implementarse a nivel de hardware o software. Los sistemas RAID (Redundant Array of Independent Disks), por ejemplo, ofrecen una forma de almacenamiento que combina varios discos duros en un solo sistema lógico.

  El objetivo principal de un sistema RAID es proporcionar redundancia y aumentar la fiabilidad y el rendimiento de los datos. Existen varios niveles de RAID, como RAID 0, RAID 1, RAID 5, entre otros, cada uno con sus propias características y beneficios. Al utilizar RAID, se distribuyen los datos a través de los discos y se generan copias redundantes de los mismos, de modo que si uno de los discos falla, los datos pueden recuperarse de los discos restantes. Esto mejora la tolerancia a fallos y la disponibilidad de los datos, ya que el sistema puede seguir funcionando incluso si uno o varios discos fallan.

- **Balanceo de carga:** Esta estrategia consiste en distribuir la carga de trabajo entre varios servidores o recursos para evitar la sobrecarga y mejorar la eficiencia del sistema. Si uno de los servidores falla, los demás pueden hacerse cargo de su carga de trabajo sin interrupciones.

- **Tolerancia a fallos en tiempo real:** Se refiere a la capacidad de un sistema para detectar y responder rápidamente a los fallos en tiempo real. Esto implica el uso de algoritmos y técnicas que permiten la recuperación instantánea frente a fallos, minimizando el impacto en el rendimiento y la disponibilidad del sistema.

- **Respaldo y recuperación de datos:** Esta técnica implica la implementación de sistemas de respaldo y recuperación de datos, como copias de seguridad periódicas y procedimientos de recuperación en caso de fallos. Esto asegura que los datos críticos estén protegidos y se puedan restaurar en caso de pérdida o corrupción.

  Los backups consisten en realizar copias periódicas de los archivos y sistemas críticos, almacenándolos en un medio seguro y accesible. En caso de que ocurra un fallo, se puede restaurar la información desde el backup, minimizando la pérdida de datos y facilitando la recuperación del sistema. Es importante realizar backups de manera regular y asegurarse de que los datos se encuentren en ubicaciones externas o sistemas de almacenamiento independientes para garantizar su integridad.

- **Detección y recuperación automática de fallos:** Consiste en utilizar mecanismos y algoritmos de detección de fallos en tiempo real para identificar problemas y activar automáticamente procesos de recuperación. Estos procesos pueden incluir la reinicialización de servicios, la restauración de configuraciones o la migración de tareas a otros recursos.

3.12 Tareas automáticas

La a**utomatización de tareas en la gestión de información** es un enfoque que busca simplificar y agilizar las tareas recurrentes y rutinarias relacionadas con la administración de la información. Consiste en utilizar herramientas y tecnologías que permiten programar la ejecución automática de estas tareas, liberando tiempo y recursos para otras actividades más críticas.

La automatización de tareas puede aplicarse a diversas áreas de la gestión de información, como el procesamiento de archivos, la organización de datos, la generación de informes, la copia de seguridad y la sincronización de datos, entre otras. Al automatizar estas tareas, se pueden evitar errores humanos, reducir los tiempos de respuesta y optimizar el flujo de trabajo. La programación de tareas automáticas es un aspecto fundamental de la automatización de tareas en la gestión de información. Consiste en establecer un programa o calendario para la ejecución automática de ciertas tareas en momentos específicos o según eventos predefinidos.

Existen varias herramientas y tecnologías que permiten programar tareas automáticas en diferentes sistemas operativos. Por ejemplo, en Windows se utiliza el Programador de tareas, que permite programar la ejecución de scripts, programas o comandos en momentos específicos o con una periodicidad determinada. En sistemas basados en Unix/Linux, se utiliza el cron, un servicio que permite programar la ejecución de comandos o scripts en función de la hora, el día, la semana o el mes.

La **programación de tareas automáticas** ofrece numerosos beneficios en la gestión de información. Permite establecer horarios regulares para la ejecución de tareas de mantenimiento, como la limpieza de archivos temporales, la optimización de bases de datos o la copia de seguridad de datos críticos. También facilita la generación automática de informes periódicos, la actualización de datos en tiempo real y la sincronización automática de información entre diferentes sistemas.

En sistemas operativos como Windows, Mac OS X y Unix, se incluyen herramientas específicas para programar y realizar tareas automáticas de mantenimiento. Estas herramientas facilitan la ejecución automática de tareas recurrentes y rutinarias, como copias de seguridad, sincronización de archivos y otras actividades relacionadas con la gestión de información.

En Windows, se utiliza el Administrador de tareas para programar y controlar tareas automáticas. Esta herramienta permite establecer horarios y condiciones para la ejecución de programas, scripts o comandos. También proporciona información detallada sobre los recursos del sistema utilizados por cada tarea.

En Mac OS X, se utiliza la aplicación iCal, que funciona como un calendario y permite programar tareas automáticas. A través de iCal, los usuarios pueden establecer eventos periódicos para ejecutar scripts o programas en momentos específicos.

En sistemas Unix, como Linux, se utiliza el servicio Crontab para programar tareas automáticas. Crontab permite establecer horarios y fechas para la ejecución de comandos o scripts, y es ampliamente utilizado para automatizar tareas de mantenimiento y gestión de información.

En cuanto a las tareas de copia de seguridad o backup, existen programas especializados que ofrecen funcionalidades avanzadas para esta tarea. Algunos ejemplos de programas de copia de seguridad son rsync, Acronis, VmWare vCenter Server, Veeam y Veritas Backup Exec. Estas herramientas permiten realizar copias de seguridad completas, incrementales o diferenciales, programar horarios de ejecución, restaurar datos y garantizar la integridad y disponibilidad de la información.

4. Resumen

La información es almacenada en los equipos informáticos a través de ficheros organizados por carpetas, lo que permite crear un sistema en forma de árbol. Cada archivo tiene asociado una extensión que determina al sistema operativo mediante qué programa ha de ser ejecutado para proceder a su lectura.

Originalmente, el acceso a los archivos se realizaba a través de comandos que recorrían el sistema de carpetas hasta encontrar el archivo, al que se le asignaba, también mediante comandos, el programa que lo ejecutaría. Dicho sistema sigue estando vigente en los sistemas actuales, aunque ha sido reemplazado progresivamente por un modelo más grafico que permite al usuario acceder a la información sin necesidad de escribir la ruta en la que se almacena, sobre todo por lo que respecta a los sistemas operativos Windows e iOS.

Para instalar periféricos en un ordenador es necesario realizar la instalación de los controladores, que son los que permitirán al sistema operativo que accione los nuevos dispositivos. Su instalación, igual que en la gestión de archivos, puede llevarse a cabo mediante comandos o a través de la interfaz grafica. En este sentido, es frecuente, en equipos Linux, realizar la instalación mediante comandos, mientras que en los sistemas operativos Windows o iOS se realiza mediante las herramientas graficas.

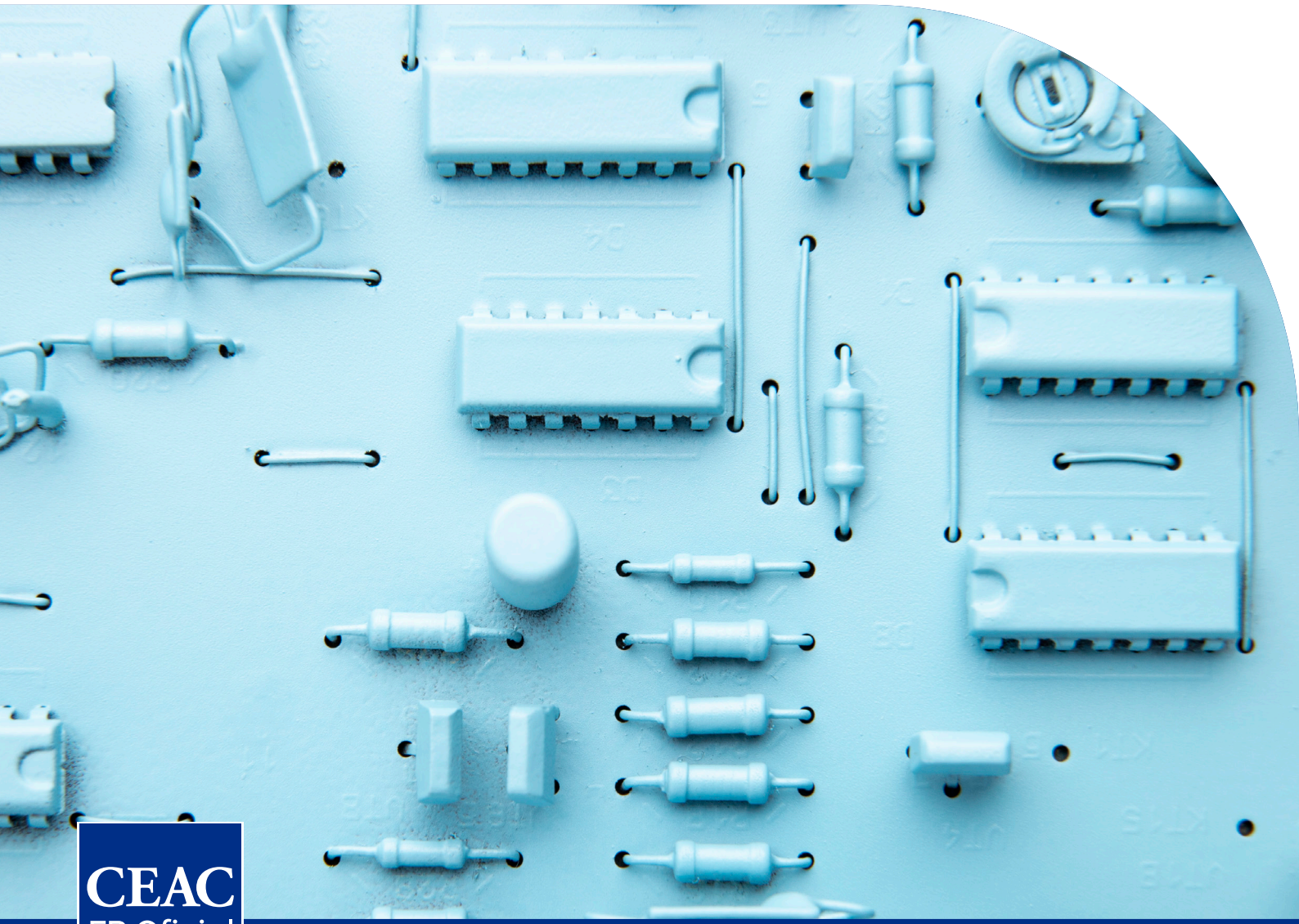
Desarrollo de aplicaciones multiplataforma

MÓDULO:

Sistemas informáticos

UNIDAD:

Configuración de sistemas operativos



CEAC
FP Oficial

MÓDULO:

Sistemas informáticos

UNIDAD:

Configuración de sistemas operativos

CEAC FP Oficial

ÍNDICE

1. Introducción

Los ordenadores son elementos críticos para la supervivencia de instituciones y empresas. Su capacidad de convertir en conocimiento útil la información procedente del entorno, de los colaboradores, de los adversarios y de la propia institución los hace imprescindibles para elaborar estrategias competitivas; pero si la información se pierde, se falsea o va a parar a manos equivocadas, los resultados pueden ser catastróficos.

Los sistemas informáticos modernos siguen un esquema de seguridad llamado AAA, que son las siglas de autenticación, autorización y auditoría. Comprueban la identidad de los usuarios que entran en el sistema (autenticación), sean estas personas o aplicaciones. Siempre que un usuario intenta acceder a los recursos del sistema, como programas, ficheros de datos o periféricos, se comprueba si ese usuario tiene permisos para acceder a dicho recurso (autorización).

Las operaciones de autenticación y acceso a los recursos quedan registradas para su análisis (auditoría). En esta unidad verás cómo se configura la seguridad en los sistemas operativos más comunes. Conocerás cómo se crean y administran los usuarios y grupos de usuarios, qué usuarios y qué grupos vienen preconfigurados en los sistemas operativos y cuál es su función. Aprenderás también a asegurar la identidad de los usuarios en la máquina y en el mundo real y cómo deben agruparse para facilitar su administración. Del mismo modo, conocerás cómo se asocian los recursos del sistema informático a los usuarios y la manera de administrar eficazmente dichas asociaciones.

Por último, aprenderás a tratar los programas del sistema operativo y cómo llevar a la práctica la administración de la información mediante el uso de comandos y herramientas de software.

2. Objetivos pedagógicos

Los objetivos de aprendizaje que se pretenden alcanzar con esta unidad son:

Comprender la importancia estratégica de los ordenadores y sistemas informáticos en la supervivencia y competitividad de instituciones y empresas.

Familiarizarse con el esquema de seguridad AAA (Autenticación, Autorización y Auditoría) y su aplicación en los sistemas informáticos modernos.

Asegurar la identidad de los usuarios en el entorno de la máquina y en el mundo real, aplicando prácticas adecuadas de agrupación de usuarios para facilitar su gestión.

Desarrollar competencias en el manejo de programas del sistema operativo y herramientas de software para llevar a cabo una efectiva administración de la información en el entorno informático.

3. Configuración de sistemas operativos

3.1. Configuración de usuarios y grupos locales

La **creación y gestión** de cuentas de usuario es una tarea fundamental en la configuración de sistemas operativos. Permite establecer perfiles individuales para cada usuario, lo que garantiza la seguridad y la personalización de la experiencia de uso. Algunas acciones importantes en la creación y gestión de cuentas de usuario incluyen:

Creación de cuentas de usuario: En esta etapa se definen los datos básicos de cada cuenta, como el nombre de usuario y la contraseña. También se pueden especificar otras configuraciones, como la imagen de perfil y las opciones de inicio de sesión.

Configuración de permisos: Las cuentas de usuario pueden tener diferentes niveles de privilegios y permisos en el sistema. Es posible asignar permisos de administrador, limitar el acceso a determinados recursos o definir permisos específicos para cada usuario.

Gestión de contraseñas: La seguridad de las cuentas de usuario es crucial. Se deben establecer políticas de contraseñas sólidas, que incluyan requisitos de longitud, complejidad y periodicidad de cambio. Además, es importante educar a los usuarios sobre buenas prácticas de seguridad y la importancia de proteger sus contraseñas.

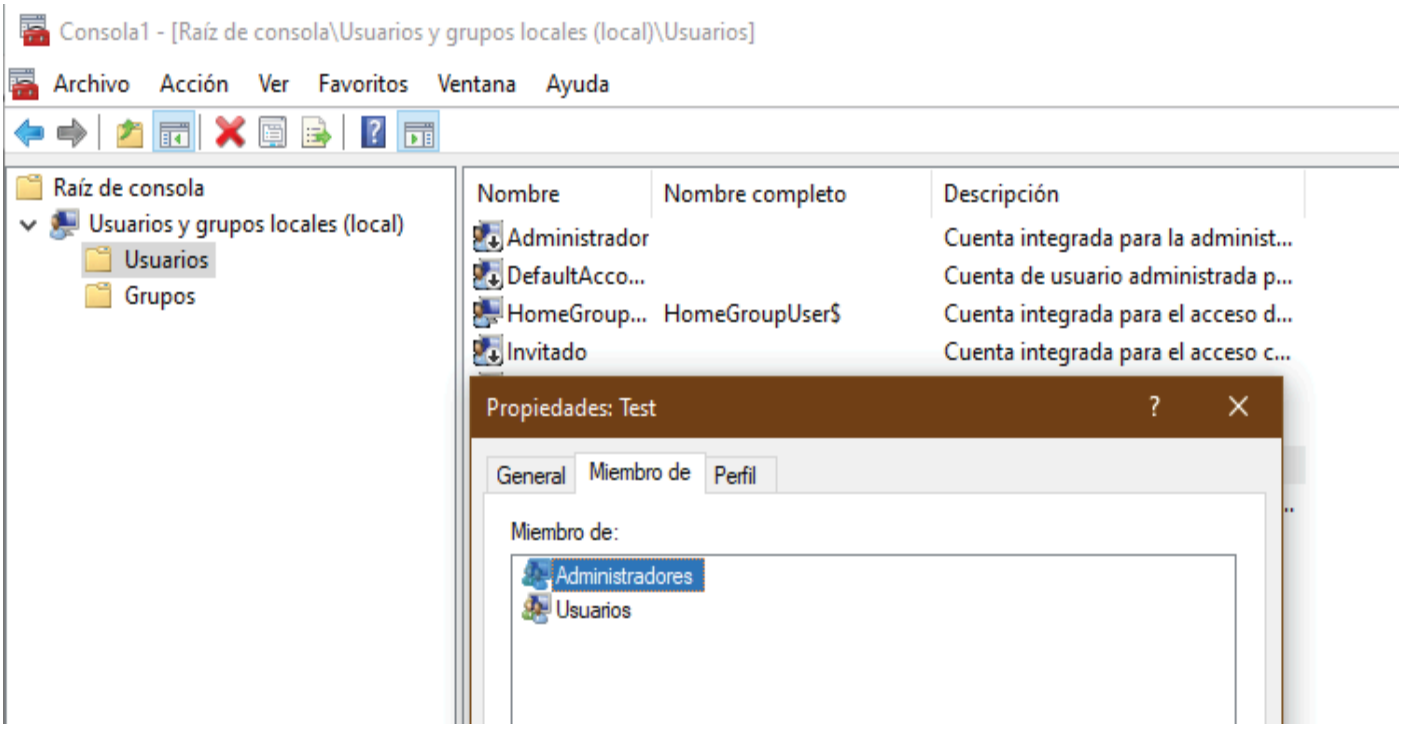
La condición más importante para poder crear usuarios y grupos locales en un sistema es ingresar en este con una cuenta de usuario que tenga los privilegios suficientes. Generalmente esta es la cuenta del usuario llamado Administrador (Windows) o root (Unix), aunque en sistemas complejos es habitual asignar estas funciones a un usuario con privilegios más limitados. En los sistemas operativos Windows, la administración de usuarios y grupos se realiza mediante la consola de administración de Microsoft. En Windows 7 o 2008 los pasos a seguir son los siguientes:

1. Inicio > Escribir **mmc** y pulsar **Entrar**.
2. Introducir la contraseña de administrador y agregar el complemento de **Usuarios** y **grupos locales**. Aquí pueden configurarse las características de los usuarios y grupos existentes, o crear uno nuevo pulsando el menú Acción.

PARA SABER MÁS: En un sistema operativo Unix, los detalles de los comandos pueden conocerse utilizando el comando man seguido del nombre del comando sobre el que se desea información.

En los sistemas operativos de tipo Unix, la administración de grupos, usuarios y privilegios puede realizarse desde el intérprete de comandos utilizando las siguientes órdenes:

- useradd. Añadir una cuenta de usuario al sistema local.
- usermod. Modificar las características de una cuenta de usuario.
- userdel. Borrar una cuenta de usuario.
- passwd. Activar un usuario nuevo asignándole una contraseña.
- groupadd. Añadir un grupo de usuarios al sistema local.
- groupmod. Modificar las características de un grupo.
- groupdel. Borrar un grupo del sistema local.



En un sistema operativo Windows, la aplicación Usuarios y grupos locales de la consola MMC configura las características de la cuenta de un usuario.

En los sistemas operativos Unix, la gestión de usuarios y grupos locales también es esencial para la administración de la seguridad y los accesos.

En un sistema operativo Unix, los detalles de los comandos pueden conocerse utilizando el comando ***man.*** seguido del nombre del comando sobre el que se desea información.

3.2 Usuarios y grupos predeterminados

Los **sistemas operativos y los controladores** de dominio tienen definidos algunos usuarios y grupos desde el mismo momento de su instalación.

3.2.1. Usuarios y grupos predeterminados en entornos Windows

Windows es un sistema operativo diseñado para admitir múltiples usuarios en un mismo ordenador, manteniendo sus documentos y configuraciones aislados entre sí. Para lograr esto, Windows clasifica a los usuarios en tres categorías predefinidas: administradores, usuarios limitados (estándar) e invitados, cada una con diferentes niveles de permisos y restricciones en el sistema.

El usuario estándar tiene la capacidad de modificar ciertas configuraciones del sistema operativo, pero estas modificaciones no afectan a otros usuarios ni comprometen la seguridad general. Sin embargo, tienen pleno acceso y pueden ejecutar todos los programas instalados en el equipo.

El usuario inicial es una cuenta especial que se asemeja al usuario estándar, pero con permisos adicionales, como la capacidad de convertirse en administrador en momentos específicos o para aplicaciones particulares, como las consolas. Esto permite realizar tareas específicas que requieren permisos elevados, pero sin comprometer la seguridad global del sistema.

El usuario administrador no tiene restricciones y puede realizar todo tipo de tareas. Esto incluye realizar cambios que afecten a otros usuarios, como limitar sus permisos, aplicar políticas de seguridad (como establecer requisitos para las contraseñas de otros usuarios) o gestionar la instalación de programas en el sistema.

Por otro lado, el usuario invitado es el tipo de cuenta con mayores restricciones, destinada a personas desconocidas o visitantes ocasionales. Está diseñada principalmente para usuarios que desean acceder al ordenador de forma esporádica, como para navegar por la web o consultar el correo electrónico. A los usuarios invitados no se les permite realizar acciones que afecten al sistema, como instalar o desinstalar programas existentes o realizar cambios en la configuración del equipo.

3.2.2 Usuarios y grupos predeterminados en entornos Unix

En Unix, incluyendo sistemas basados en Unix como Linux, el concepto de usuarios y grupos es fundamental para gestionar el acceso y los permisos en el sistema operativo.

En Unix, cada usuario tiene una identificación única conocida como UID (User ID), que se utiliza para identificar y autenticar al usuario en el sistema. Además, los usuarios se agrupan en conjuntos lógicos conocidos como grupos. Cada grupo tiene una identificación única conocida como GID (Group ID) y puede incluir uno o varios usuarios.

Al igual que en Linux, Unix utiliza un usuario especial llamado "root" que tiene privilegios de superusuario. El usuario root tiene acceso completo y control absoluto sobre el sistema, pudiendo realizar cualquier acción y modificar cualquier configuración en el sistema operativo. Sin embargo, se recomienda utilizar la cuenta root con precaución, ya que cualquier error o acción incorrecta puede tener consecuencias graves para la seguridad y estabilidad del sistema.

Los usuarios regulares en Unix tienen sus propios directorios de inicio, donde pueden almacenar sus archivos personales y configuraciones. Cada usuario tiene permisos de lectura, escritura y ejecución sobre su propio directorio de inicio, pero no tiene acceso directo a los directorios y archivos de otros usuarios, a menos que se les otorguen permisos explícitos.

Los permisos en Unix se gestionan mediante el sistema de permisos basado en propietarios, grupos y otros. Cada archivo y directorio tiene permisos asociados que especifican qué acciones pueden realizar los diferentes usuarios y grupos. Estos permisos se establecen mediante la combinación de las tres categorías: propietario, grupo y otros, y se pueden configurar para permitir o restringir la lectura, escritura y ejecución de archivos y directorios.

```
marcos@debian:~$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:marcos
floppy:x:25:marcos
tape:x:26:
sudo:x:27:
audio:x:29:pulse,marcos
dip:x:30:marcos
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
```

nombre_grupo:password:nº grupo:usuarios

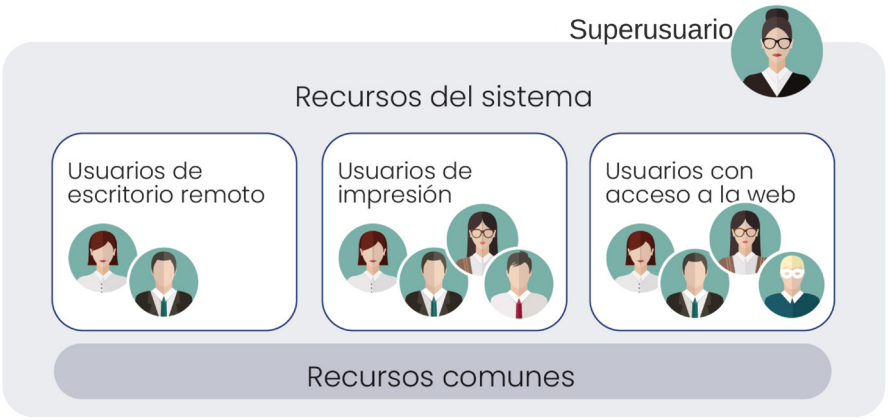
Un sistema operativo Unix crea cuentas de usuario y grupos para su propio uso.

3.3 Seguridad de cuentas de usuario

El usuario de un sistema informático es aquella persona o programa que accede a un sistema informático para que este le ayude a resolver un problema. El sistema asigna a cada usuario unas credenciales, formadas por un nombre único y una contraseña (u otro sistema de autenticación) y el derecho a utilizar ciertos recursos. Esta asignación se llama cuenta de usuario.

Los recursos se organizan de dos posibles maneras:

- **Equipo local.** Un ordenador pone sus recursos a disposición de los usuarios a través de sus propios periféricos o de un terminal de red. La persona que instala el sistema operativo debe escoger la contraseña del primer usuario, llamado superusuario o administrador local. El superusuario tiene acceso a todos los recursos. Una de sus funciones será crear y administrar las cuentas del resto de usuarios. En una organización, asignar los privilegios usuario por usuario podría requerir un esfuerzo titánico. Por ello, para abordar esta tarea las cuentas de



Cada usuario puede acceder a los recursos de un sistema informático en la medida en que disponga de privilegios propios y pertenezca a grupos.

- **Dominio**. Los recursos están distribuidos en una red de ordenadores. Uno o más ordenadores, llamados controladores de dominio, centralizan todas las cuentas de usuario y administran la visibilidad y el acceso a los recursos. Al instalar un controlador de dominio, se crea la cuenta del administrador de dominio, cuyo papel y privilegios son similares a los del administrador local, pero para los recursos que forman el dominio.

  El usuario de un dominio se identifica ante cualquiera de los ordenadores que participan en el dominio con el usuario y contraseña de su cuenta de usuario de dominio, la cual es independiente de la cuenta local. Al igual que en un entorno local, en los dominios también existen los grupos de usuarios.

RECUERDA: Lo más importante de una política de contraseñas es que toda la empresa la conozca y la aplique.

3.4 Seguridad de contraseñas

La mayoría de los ataques contra la **seguridad informática** de las empresas e instituciones provienen de empleados o exempleados descontentos, y la mayor vulnerabilidad de las empresas frente a dichos ataques es una política de contraseñas poco rigurosa.

Lo más importante de una política de contraseñas es que toda la empresa la conozca y la aplique. Los empleados deben estar concienciados para mantener sus contraseñas en secreto. No deben dejarlas anotadas ni en el ordenador ni cerca de este. No deben proporcionárselas absolutamente a nadie, ni siquiera los administradores tienen por qué conocerlas. Si alguien las reclama alegando motivos técnicos o de política de seguridad, primero habrá que pedir permiso a un supervisor conocido.

Los administradores, por su parte, deben configurar el sistema informático para que sólo acepte contraseñas con un mínimo de complejidad, para que bloquee la entrada de un usuario si ha intentado varias veces identificarse con una contraseña no correcta, y para que las contraseñas de cada usuario expiren periódicamente.

```
marcos@debian:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nolog
in
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
tss:x:105:111:TPM2 software stack,,,:/var/lib/tpm:/bin/false
dnsmasq:x:106:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
usbmux:x:107:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
```

Listado del archivo de contraseñas en Linux y el comando para obtenerlo. Las contraseñas aparecen sustituidas por la letra x.

Algunos aspectos comunes de las políticas de contraseñas incluyen:

- **Longitud mínima de contraseña:** Se establece una longitud mínima para las contraseñas, generalmente de al menos 8 caracteres, para garantizar una mayor complejidad.
- **Complejidad de caracteres:** Se requiere que las contraseñas contengan una combinación de letras mayúsculas y minúsculas, números y caracteres especiales. Esto aumenta la seguridad al hacer que las contraseñas sean más difíciles de adivinar o descifrar.
- **Cambio periódico de contraseñas:** Se establece un intervalo de tiempo después del cual los usuarios deben cambiar sus contraseñas. Esto ayuda a evitar el uso continuo de contraseñas comprometidas o débiles.
- **Restricciones de reutilización:** Se prohíbe el uso de contraseñas anteriores, evitando que los usuarios utilicen contraseñas previamente comprometidas o fácilmente adivinables.

También deben asegurarse de que el sistema operativo guarda las contraseñas cifradas.

Si un empleado o colaborador cesa su relación con la organización, todas sus cuentas en el sistema informático deberán ser eliminadas inmediatamente. El administrador debe mantener un registro de todas las cuentas que proporcionan accesos al sistema por motivos provisionales y utilizarlo para eliminarlas en cuanto dejen de ser necesarias.

La seguridad informática se rompe por el eslabón más débil y la presencia de contraseñas obvias es ese eslabón. Pueden utilizarse programas de ataques de diccionario, como Jacktheripper, para comprobar periódicamente que en el sistema no hay contraseñas demasiado fáciles de averiguar.

3.4.1 Acceso a los recursos. Permisos locales

Cuando hablamos del acceso a los **recursos**, debemos diferenciar entre las dos plataformas más importantes, Windows y Unix, puesto que cada una de ellas accede de manera diferente a los recursos.

3.4.2 Acceso a los recursos del sistema en Unix

En un sistema operativo de tipo Unix todos los recursos son representados en forma de ficheros en el árbol de directorios, ya sean datos, programas, directorios o incluso dispositivos físicos. Cada archivo puede ser accedido de tres maneras diferentes:

- **Lectura**. El contenido del fichero es consultado y utilizado por un programa, pero el fi chero no se modifica.
- **Escritura**. El contenido del fichero es modificado.
- **Ejecución**. El contenido del fichero es reconocido como un programa y se pone en la cola de ejecución para dar instrucciones a la CPU.

Cada archivo está marcado como propiedad de un usuario y de un grupo. En el momento en que se crea el archivo, el usuario creador es su propietario y el grupo principal del propietario es el grupo propietario. Solamente el superusuario puede cambiar los propietarios y grupos a los que pertenece un archivo, usando el comando chown.

Un archivo puede ser accedido por tres tipos de usuarios: su propietario, los usuarios que pertenecen al grupo propietario del archivo y el resto de usuarios. El archivo está marcado con seis bits que indican, respectivamente, si se permite la lectura, la escritura o la ejecución al propietario; si se permite la lectura, escritura o ejecución a los usuarios del grupo propietario; y si se permite la lectura, escritura o ejecución al resto de usuarios.

El usuario propietario de un archivo y el superusuario pueden cambiar los permisos para cada tipo de usuario con la orden chmod.

RECUERDA: Windows representa a los usuarios grupos y recursos con iconos.
Una vez localizado un icono, sus propiedades pueden cambiarse pulsando sobre él con el botón secundario del ratón y buscando la opción en el menú de contexto.

Los **atributos** de los archivos pueden visualizarse con la orden ls -l. La primera letra es una d si el archivo es un directorio y las siguientes tres letras indican los permisos del propietario: r significa que tiene permiso de lectura, w indica permiso de escritura y x permiso de ejecución; si falta una de las tres letras, entonces el propietario carece del permiso correspondiente.

A continuación, y de manera análoga, aparecen los permisos para el grupo propietario y los permisos para el resto de usuarios del sistema

```
marcos@debian:/$ ls -l
total 68
lrwxrwxrwx   1 root root     7 jul  8 12:01 bin -> usr/bin
drwxr-xr-x   3 root root  4096 jul  8 12:31 boot
drwxr-xr-x  17 root root  3180 jul  9 13:16 dev
drwxr-xr-x 129 root root 12288 jul  9 13:16 etc
drwxr-xr-x   3 root root  4096 jul  8 12:33 home
lrwxrwxrwx   1 root root    30 jul  8 12:02 initrd.img -> boot/initrd.img-4.19.0-9-amd6
4
lrwxrwxrwx   1 root root    30 jul  8 12:02 initrd.img.old -> boot/initrd.img-4.19.0-9-
amd64
lrwxrwxrwx   1 root root     7 jul  8 12:01 lib -> usr/lib
lrwxrwxrwx   1 root root     9 jul  8 12:01 lib32 -> usr/lib32
lrwxrwxrwx   1 root root     9 jul  8 12:01 lib64 -> usr/lib64
lrwxrwxrwx   1 root root    10 jul  8 12:01 libx32 -> usr/libx32
drwx------   2 root root 16384 jul  8 12:01 lost+found
drwxr-xr-x   3 root root  4096 jul  8 12:01 media
drwxr-xr-x   2 root root  4096 jul  8 12:01 mnt
drwxr-xr-x   2 root root  4096 jul  8 12:01 opt
dr-xr-xr-x 144 root root     0 jul  9 13:16 proc
drwx------   3 root root  4096 jul  8 12:34 root
drwxr-xr-x  24 root root   640 jul  9 13:20 run
lrwxrwxrwx   1 root root     8 jul  8 12:01 sbin -> usr/sbin
drwxr-xr-x   2 root root  4096 jul  8 12:01 srv
dr-xr-xr-x  13 root root     0 jul  9 13:16 sys
drwxrwxrwt  15 root root  4096 jul  9 22:04 tmp
drwxr-xr-x  14 root root  4096 jul  8 12:23 usr
drwxr-xr-x  11 root root  4096 jul  8 12:01 var
```

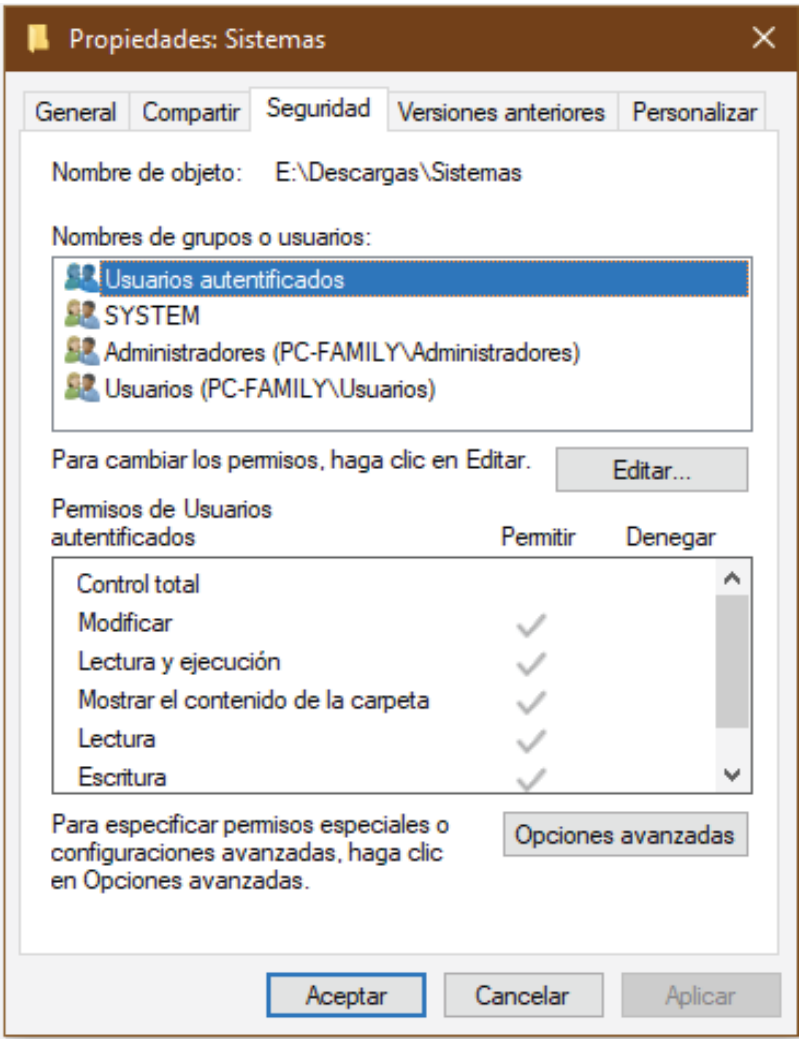
El comando ls -lista los archivos del directorio activo y muestra sus propiedades.

3.4.3 Acceso a los recursos del sistema en Windows

Los sistemas operativos de marca Windows permiten administrar el acceso a los recursos, ya sean locales o de un dominio, a través de su interfaz gráfica. En este contexto, cada recurso es un objeto cuyos atributos pueden ser modificados, y se representa mediante un icono cuyas propiedades pueden ser modificadas pulsando el botón secundario del ratón con la flecha sobre él. También los usuarios y grupos son objetos que se representan en forma de iconos y se acceden de igual manera.

Windows distingue diferentes tipos de recursos, como ficheros, impresoras o discos compartidos, que son representados por objetos de diferentes clases con diferentes privilegios. El acceso a un recurso se controla mediante sus propiedades, que pueden ser cambiadas exclusivamente por el propietario, el cual decide qué privilegios otorga a qué usuarios o grupos . En Windows no hay límite sobre la cantidad de usuarios y grupos que pueden tener acceso a un fichero.

Un recurso puede contener otros que dependan de él; por ejemplo, una carpeta puede contener ficheros. Los recursos dependientes siempre heredan todas las propiedades del recurso contenedor, tanto en el momento de ser creados como cuando se cambian las propiedades del contenedor, aunque se pueden personalizar cambiando uno a uno sus atributos.



En un sistema operativo Windows pueden concederse privilegios personalizados sobre un recurso a múltiples grupos y usuarios.

Además del control del acceso a recursos particulares, Windows utiliza unas reglas llamadas directivas locales, que afectan a todos los usuarios y controlan el acceso a los recursos generales del sistema. Estas reglas determinan qué funciones de seguridad se habilitan, qué sucesos del sistema son registrados y qué privilegios tiene un usuario o grupo sobre las funciones principales del sistema.

3.5 Directivas locales

Un perfil de usuario es un **conjunto de recursos asociados** a una cuenta de usuario que proporcionan a su propietario un entorno de trabajo personalizado e independiente, dentro del cual sus acciones no afectarán al resto de usuarios del sistema.

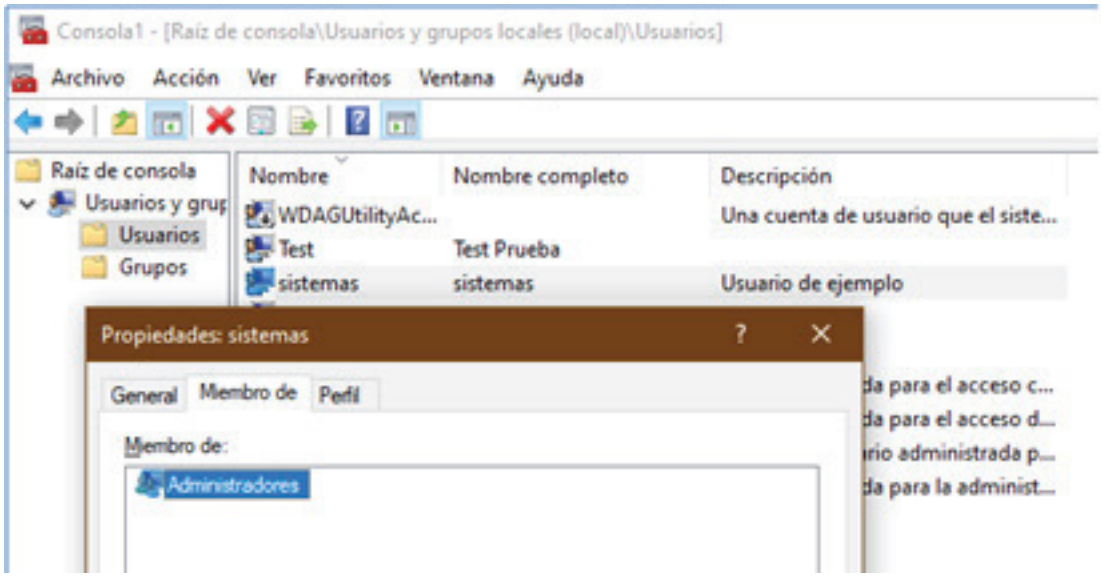
Al crear un usuario local, el administrador puede darle unos permisos para que pueda acceder únicamente a unos recursos del sistema determinados. Para no tener que aplicar los mismos permisos a unos usuarios que tienen los mismos privilegios, se aplican directivas locales para asignar los permisos automáticamente en función del grupo al que pertenezcan los usuarios.

Un perfil de usuario se crea automáticamente cuando se da de alta la cuenta. Incluye un directorio bajo el cual el usuario puede crear su propio árbol, programas que se ejecutan cuando el usuario activa su cuenta y que pueden ser muy útiles; por ejemplo, para establecer conexiones con recursos remotos; y en sistemas gráficos de escritorio incluye un escritorio propio, con iconos, menú de inicio, estilo gráfico y fondo de pantalla personalizables.

El perfil tiene una parte **obligatoria**, formada por ficheros del administrador que son impuestos al usuario; y una parte que puede ser cambiada por el usuario, formada por archivos y carpetas a su nombre o creadas por él.

Un perfil de usuario puede ser local, si reside en un ordenador de escritorio, o móvil, si está guardado en un dominio. Un perfil móvil permite al usuario trabajar en el mismo entorno aunque utilice ordenadores diferentes, siempre que lo haga dentro del mismo dominio.

En Windows el perfil de usuario incluye un escritorio y menú de inicio configurables, la conexión a recursos compartidos y la puesta en marcha de scripts.



La consola de administración de Microsoft permite diseñar un perfil local para cada usuario.

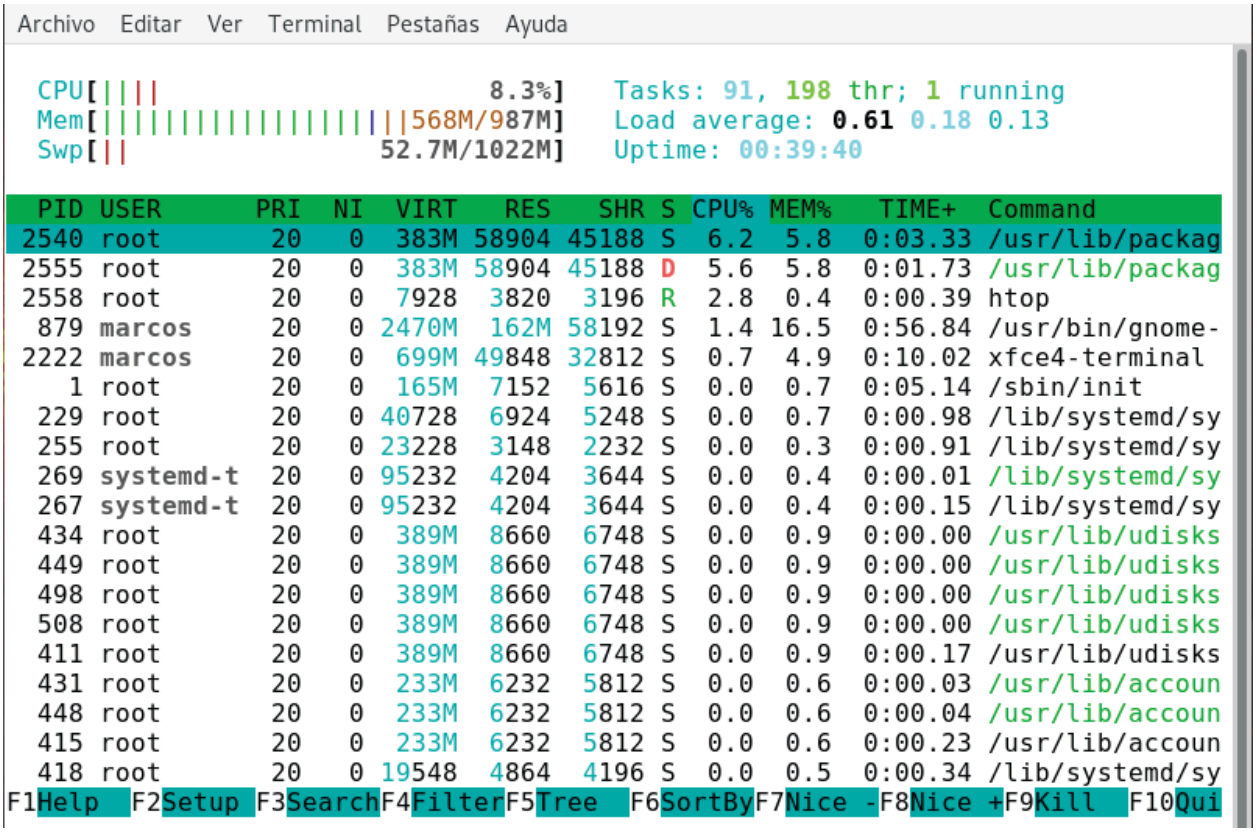
En Unix el concepto de perfil no está definido como tal, pero en la práctica también existe. Cuando el **administrador** crea una cuenta de usuario le asigna un directorio prototipo, con todos los directorios, archivos de configuración y programas necesarios. El administrador puede tener tantos directorios prototipos como desee, aunque mientras no indique lo contrario, todos los usuarios se crean con el perfil del directorio /etc/skel.

Para que el usuario tenga un entorno de escritorio debe ser creado desde alguno de losentornos de escritorio, disponibles para Unix, como Gnome, KDE o XFCE. En este caso el usuario también podrá tener un escritorio con un menú de inicio, iconos, carpetas y apariencia personalizables.

3.6 Servicios y procesos

Los **servicios** y **procesos** son las partes de un programa ejecutado dentro del sistema que ofrecen un servicio al usuario o a la propia máquina y que, en estado de ejecución, consumen recursos del sistema. Cada uno de estos servicios suelen ser independientes y son arrancados por el sistema operativo para poder llevar a cabo las funciones necesarias dentro del sistema.

Muchos programas que necesitan ser ejecutados de manera constante crean procesos en la máquina en vez de estar instanciados como software que el usuario deba ejecutar manualmente. Una característica de los servicios es que, al trabajar a bajo nivel consumen menos recursos que un programa normal en ejecución. A pesar de esto, un administrador de sistemas siempre debe controlar los servicios que se están ejecutando, para asegurarse que solo están en proceso los necesarios, puesto que ejecutar procesos innecesarios supondría una pérdida en los recursos.



Htop permite monitorizar el estado de todos los procesos del sistema y realizar operaciones sobre ellos.

La configuración de servicios implica definir cómo deben comportarse, qué recursos utilizar y qué opciones de configuración deben aplicarse. Esto puede incluir la especificación de puertos de red, ajustes de seguridad, configuración de bases de datos, entre otros aspectos. La gestión de servicios implica supervisar su funcionamiento, realizar cambios en su configuración, iniciar o detener su ejecución, y asegurarse de que estén disponibles y funcionando correctamente.

El **monitoreo** de procesos implica obtener información sobre el estado, uso de recursos y rendimiento de los procesos en ejecución. Esto puede incluir la visualización de información como el consumo de CPU, memoria y disco, el seguimiento de la actividad de red, y la identificación de posibles cuellos de botella o problemas de rendimiento. Las herramientas de monitoreo pueden proporcionar gráficos, alertas y registros para facilitar el análisis de la actividad del sistema.

Otra característica de servicios y procesos es que pueden asignarse permisos para que funcionen dependiendo del usuario que utilice la máquina. De esta manera, el servicio cola de impresión necesario para imprimir tendría un acceso libre pero el proceso Antivirus solo podría ser ejecutado por el sistema y administrado por el administrador.

RECUERDA: Los servicios o daemons son programas que se ejecutan en el ordenador de forma transparente al usuario para dar servicio a otros programas.

3.6.1 La comunicación de los procesos

En ocasiones, los servicios no pueden realizar una tarea por sí solos y es necesaria la comunicación entre varios procesos para llevarla a cabo. Existen varios tipos de comunicación entre procesos: uno de ellos es el sistema emisor-receptor, en el que un servicio emisor proporciona datos a otro servicio receptor. Para poder llevar a cabo esta comunicación, debe haber un canal entre los procesos por el que se pueda transmitir la información.

Este **canal** ha de ser capaz no solo de transmitir los datos, sino también de gestionar la comunicación, bloqueando la transmisión del emisor si el receptor está ocupado procesando el mensaje anterior. Estas vías de comunicación son los pipes (tuberías en inglés) y son proporcionadas por el sistema operativo.

Los pipes también realizan funciones de sincronización entre las partes y son capaces de administrar multitud de procesos. Es el caso de los sistemas lectura-escritura, en los que se administra el acceso a un archivo para que pueda ser leído por varios procesos, pero solo escrito por uno al mismo tiempo.

Este modelo en el que existen varios lectores, pero donde solo puede haber un servicio que modifique los datos, es el utilizado por la comunicación cliente-servidor. Algunas de las aplicaciones que usan este sistema son la de compartición de archivos o el correo electrónico.

RECUERDA: Los pipes son los recursos más utilizados para gestionar los recursos de memoria y procesador de un sistema

Los pipes soportan una comunicación unidireccional y FIFO (en inglés, First In First Out); esto quiere decir que los datos escritos en el pipe se leen en el mismo orden en que se escribieron. Los procesos deben respetar esta secuencia para garantizar una comunicación correcta.

- **Creación de un pipe.** El servicio que permite crear un pipe es el siguiente:

```
int pipe(int fd[2]);
```

Esta llamada devuelve dos descriptores que representarán la entrada y la salida de la tubería:

- **fd[0],** descriptor de archivo que se emplea para leer en el pipe.
- **fd[1],** descriptor de archivo que se utiliza para escribir en el pipe.

  La llamada pipe devuelve 0 si fue bien y –1 en caso de error.

- **Cierre de un pipe.** Cuando un proceso finaliza su escritura o lectura en el pipe, debe cerrar el extremo correspondiente para indicar que ya no se utilizará. Esto es importante para evitar bloqueos y liberar los recursos asociados con el pipe. Para cerrar un pipe y todas sus comunicaciones, debe utilizarse la siguiente función.

```
int close(int fd);
```

  El argumento de close indica el descriptor de archivo que se desea cerrar. La llamada devuelve 0 si se ejecutó con éxito. En caso de error, devuelve –1.

- **Escritura en un pipe.** El servicio de escritura cuando se usa un pipe se realiza de la siguiente manera:

```
int write(int fd, char *buffer, int n);
```

Donde el primer parámetro representa el descriptor del archivo que se utilizará en la escritura y el segundo argumento define el buffer por el que entrarán los datos, por ejemplo el teclado u otro servicio. El último parámetro define el tamaño de los datos que serán escritos. El proceso de escritura está definido por los pasos y controles de sincronización siguientes:

1. Si la tubería está llena o se llena durante el proceso de escritura, la operación bloqueará el proceso emisor hasta que se pueda completar.

2. Si no hay ningún proceso leyendo la tubería, esta devuelve el mensaje de error SIGPIPE al proceso que está realizando la escritura.

3. El proceso de escritura sobre una lectura es atómica; es decir, en el caso de que varios procesos intenten escribir en una misma tubería, solo uno de ellos lo hará y los otros se bloquearán hasta que haya terminado el proceso de escritura del primero.

- **Lectura de un pipe.** Para leer datos de un pipe se utiliza el siguiente servicio, también empleado para leer datos de un archivo:

```
int read(int fd, char *buffer, int n);
```

El primer parámetro define el descriptor de lectura del pipe. El segundo argumento define el buffer del usuario donde se realizará la lectura; por ejemplo, un archivo de salida o incluso por pantalla. El último parámetro definirá el número de bytes que se leerán a través del pipe. La llamada devuelve el número de bytes leídos. En caso de error, la llamada devuelve –1.

Así como en la escritura del pipe, la lectura también sigue una serie de pasos para asegurarse de que todo el proceso se realiza correctamente:

- Si la tubería está vacía, la llamada bloquea el proceso en la operación de lectura hasta que algún proceso escriba datos en la misma.
- Si la tubería almacena M bytes y se quieren leer n bytes, entonces:
  - Si **M > n**, la llamada devuelve n bytes y elimina de la tubería los datos solicitados.
  - Si **M < n**, la llamada devuelve M bytes y elimina los datos disponibles en la tubería.
- Si no hay escritores y la tubería está vacía, la operación devuelve fin de archivo (la llamada read devuelve cero). En este caso, la operación no bloquea el proceso.
- Al igual que las escrituras, las operaciones de lectura sobre una tubería son atómicas. En general, la atomicidad en las operaciones de lectura y escritura sobre una tubería asegura siempre que el número de datos involucrados en las anteriores operaciones sea menor que el tamaño de la misma.

3.6.2 Semáforos

Los semáforos son mecanismos de sincronización que permiten al sistema bloquear servicios para ordenar la capacidad de procesamiento del hardware. Se inicializan con un número entero no negativo que representa el número de procesos que hay que ejecutar en un mismo momento, y se definen por dos instrucciones atómicas: wait y signal (espera y señal), que determinan si un proceso puede ejecutarse o ha de esperar la señal. Un proceso se pone en espera si el número absoluto del semáforo es negativo; si no, se desbloqueará uno de los procesos que están esperando. Las estructuras de las funciones wait y signal son:

```
wait(s){
  s = s - 1;
  if (s < 0)
     Bloquear el proceso;

}
signal(s){
  s = s + 1;
  if ( s >= 0)
     Desbloquear un proceso bloqueado en la operación wait;
}
```

3.6.3 Mutex

Los mutex son mecanismos de los sistemas operativos especialmente diseñados para la sincronización de los procesos ligeros. El mutex es el mecanismo de sincronización más sencillo y ligero, y es empleado para proporcionar a un proceso el uso exclusivo sobre algún recurso, de manera que ningún otro servicio puede acceder a él ni en forma de lectura ni escritura.

El mutex es definido mediante dos sentencias:

- **lock**. Un hilo o proceso solicita adquirir el mutex mediante la operación de bloqueo. Si el mutex está libre, el hilo o proceso adquiere el mutex y continúa ejecutando la sección crítica del código. Si el mutex está ocupado por otro hilo o proceso, el hilo o proceso se bloquea y espera hasta que el mutex esté disponible.
- **unlock**. Desbloquea el mutex. Si existen procesos bloqueados en él, se desbloqueará uno de ellos, que será el nuevo proceso que adquiera el mutex. La operación unlock sobre un mutex debe ejecutarla el proceso ligero que adquirió con anterioridad el mutex mediante la operación lock. Esto es diferente a lo que ocurre con las operaciones wait y signal sobre un semáforo.

Una variable condicional es una variable de sincronización asociada a un mutex que se utiliza para bloquear un proceso hasta que ocurra algún suceso. Las variables condicionales tienen dos operaciones atómicas para esperar y señalizar:

- **c_wait.** Bloquea al proceso que ejecuta la llamada y le expulsa del mutex dentro del cual se ejecuta y al que está asociado la variable condicional, permitiendo que algún otro proceso adquiera el mutex. El bloqueo del proceso y la liberación del mutex se realizan de forma atómica.
- **c_signal.** Desbloquea uno o varios procesos suspendidos en la variable condicional. El proceso que se despierta compite de nuevo por el mutex.

3.7 Comandos de sistemas libres y propietarios

Los entornos gráficos de usuario utilizan iconos para crear una metáfora del mundo real, haciendo más intuitivo el manejo básico de los ordenadores. Sin embargo, cuando se trata de administrar un sistema, buscar paralelismos con el mundo exterior no hace sino poner barreras entre la máquina y el administrador, que necesita un método de trabajo directo y eficaz como el que proporcionan los comandos.

PASSWD:
fichero de Usuarios
SHADOW Contrasdeñas

Passwd Crear nueva contraseña

Intérprete de comandos de los sistemas basados en Unix	
su	Cambiar la cuenta de usuario.
man	Solicita información sobre los comandos del sistema.
is	Lista el contenido de un directorio
cd	Cambia el directorio de trabajo
touch	Crea un archivo vacío
cp	Copia un archivo
mv	Cambia un archivo de directorio o de nombre
mkdir	Crea un directorio
rm	Borra un fichero
rmdir	Borra un directorio
find	Busca un fi chero en el sistema
cat	Muestra el contenido de un fichero
Intérprete de comandos de Windows	
help	Solicita información sobre los comandos del sistema
dir	Lista el contenido de un directorio
cd	Cambia el directorio de trabajo
copy	Copia un archivo
move	Cambia un archivo de directorio
mkdir	Crea un directorio
del	Borra un fi chero
rd	Borra un directorio
type	Muestra el contenido de un fichero

3.8 Herramientas de monitorización del sistema

Los sistemas operativos incluyen herramientas de monitorización de sucesos, realizando así la función de auditoría para prevenir o corregir problemas en el acceso a los recursos. La auditoría se realiza en los siguientes tres pasos:

1. Configuramos los servicios de monitorización para indicarles qué tipo de acontecimientos queremos que registren.

2. Los servicios de monitorización recopilan los datos en un archivo llamado registro.

3. Se utiliza una aplicación para interpretar los sucesos recogidos en el registro.

3.8.1 Monitorización en Windows

En Windows, la configuración de los servicios de monitorización se realiza con la Directiva de auditoría, que se habilita siguiendo la secuencia Inicio> Herramientas administrativas de W**indows > Directiva de seguridad local:**

"Configuración de seguridad\Directivas locales\Directiva de auditoría".

A partir de Windows server 2012 y Windows 8, existe además una Directiva de auditoría avanzada que permite recopilar datos aún más específicos. Se activa con la secuencia Inicio > Herramientas administrativas de Windows > Directiva de seguridad local: "Configuración de seguridad\Configuración de directiva de auditoría avanzada\Directivas de auditoría del sistema".

En el intérprete de comandos, la instrucción auditpol.exe /get /category muestra una lista detallada de las operaciones (políticas) de auditoría disponibles, indicando cuáles están habilitadas. Para analizar los eventos se utiliza el Visor de sucesos, que se encuentra en Herramientas administrativas. El visor de sucesos muestra todos los eventos registrados por la directiva de auditoría.

3.8.2 Monitorización en Unix

En sistemas operativos de tipo Unix, el sistema operativo, los servidores y las aplicaciones pueden generar eventos. La mayoría de los desarrolladores de programas siguen la recomendación de guardar sus registros en el directorio /var/log. Estos archivos suelen tener forma de texto, por lo que sólo necesitan un visor de texto genérico como More para ser leídos y son muy fáciles de manipular para su análisis.

El comando tail -f /var/log/NombreDelFichero muestra las últimas líneas de un fichero conforme se van escribiendo, por lo que es muy útil para seguir en tiempo real los eventos que se van registrando en un determinado archivo.

El servicio principal de registro de eventos es syslogd, que registra los mensajes del hardware, de parte del sistema operativo y de muchos servicios asociados al sistema; mantiene el archivo de eventos /var/log/syslog y actúa junto al servicio klogd enviando mensajes a /var/log/messages.

El fichero /etc/syslog.conf permite configurar qué tipos de eventos serán auditados por syslogd y a qué archivos será enviado cada tipo de evento.

Un archivo de eventos muy útil para la seguridad es /var/log/auth.log, que registra todas las conexiones de usuarios al sistema, indicando si han sido exitosas o no, y a través de qué terminal se han realizado.

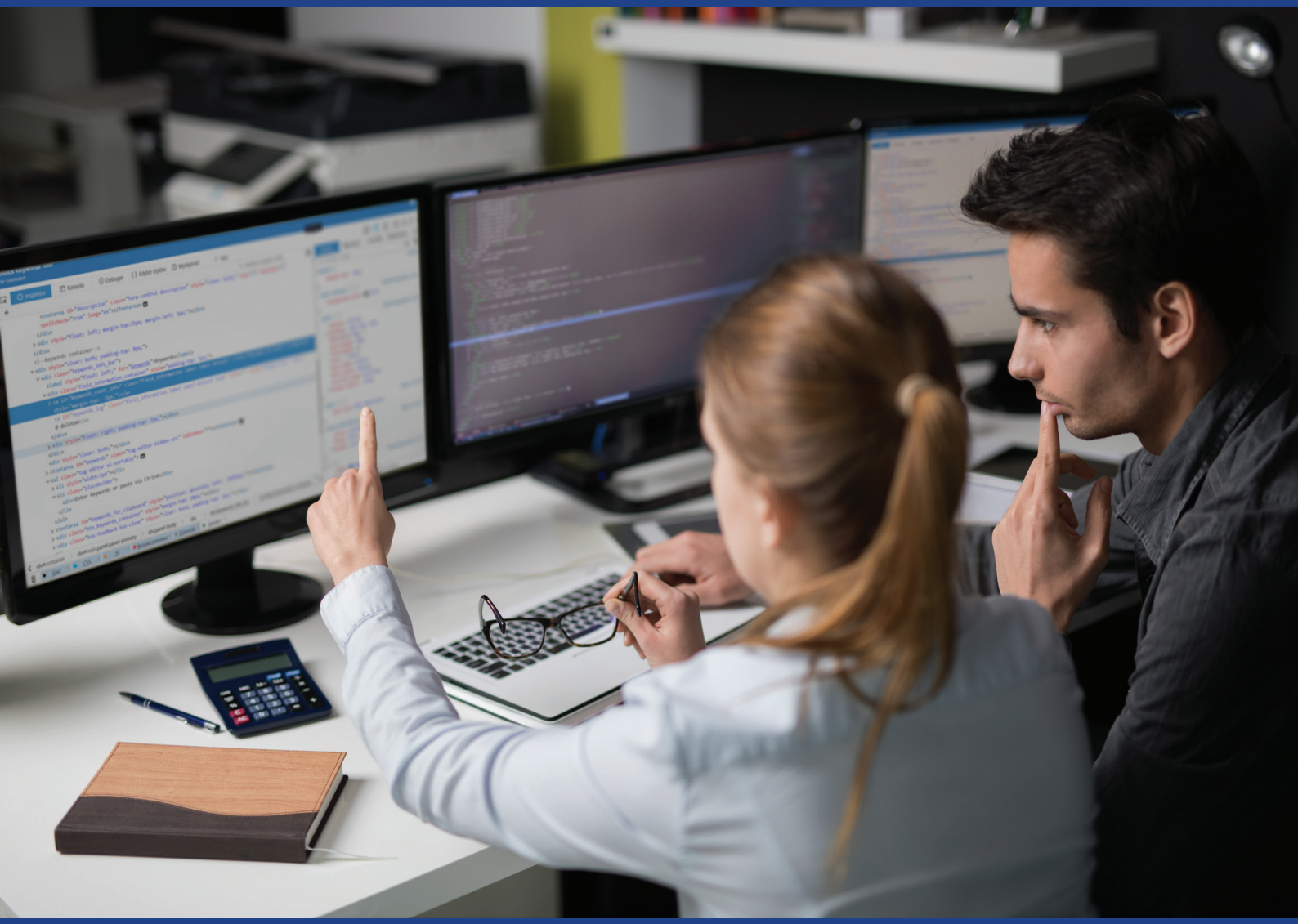
4. Resumen

En los sistemas operativos, es posible definir políticas de seguridad y asignarlas según el usuario que inicie la sesión en el equipo. Por ejemplo, hay grupos a los que se les puede asignar una serie de permisos y políticas que serán heredadas por todos aquellos usuarios que pertenezcan a dicho grupo sin necesidad de aplicar los permisos de forma individual.

Las políticas de seguridad se basan fundamentalmente en las acciones que el usuario puede realizar sobre los archivos y carpetas del sistema operativo. De esta manera, entre las políticas más comunes existen las de lectura, ejecución o modificación de los archivos. También pueden aplicarse restricciones de uso con el fin de evitar modificaciones en la configuración del sistema, o la utilización de recursos, como impresoras, que no forman parte de los permisos de ficheros y carpetas.

Las contraseñas pueden ser descifradas por software que analiza las posibles combinaciones de letras o el propio sistema en busca de indicios que permitan descubrirlas. Para evitarlo, las contraseñas son almacenadas en el sistema después de ser encriptadas con la finalidad de que, incluso pudiendo acceder al registro de usuarios, no puedan ser descifradas. Una política recomendable a los usuarios es la utilización de combinaciones de letras, números y símbolos que no formen ninguna palabra que esté en el diccionario, pues son éstas las primeras que se utilizan para intentar romper la seguridad de un sistema.

DESARROLLO DE APLICACIONES MULTIPLATAFORMA



CEAC

Formación Profesional Oficial

Módulo: Sistemas informáticos

Unidad: Conexión de sistemas en red

INICIATIVA Y COORDINACIÓN
Centro de Estudios CEAC

COLABORADORES
Realización:
ITACA (Interactive Training Advanced Computer Aplications, S.L.)

Elaboración de contenidos:
Dan Triano
Ingeniero Técnico en Informática de Sistemas por la Universidad Autónoma de Barcelona

Actualización de contenidos:
ISCA Training & Consulting, S.L.
Amparo Sota
Responsable de la creación y gestión de las páginas de venta online de diferentes productos y servicios (Habemus, Knownet, Merioliva, Fotos y bodas). Responsable del proyecto “talleres de compra online página web Eroski.es”.

Supervisión técnica y pedagógica:
Departamento de Enseñanza de Centro de Estudios CEAC

Coordinación editorial:
Departamento de Producto de Centro de Estudios CEAC

Primera edición, primera reimpresión: mayo 2021

ISBN: 978-84-1300-607-9 (Obra completa)
ISBN: 978-84-1300-608-6 (Sistemas informáticos)

Depósito Legal: B 2081-2021

Impreso por:
SERVINFORM
Avenida de los Premios Nobel, 37
Polígono Casablanca
28850 Torrejón de Ardoz (Madrid)

Printed in Spain
Impreso en España

Índice

5. CONEXIÓN DE SISTEMAS EN RED

En esta unidad verás todos los aspectos relacionados con la configuración de los equipos para formar parte de una red de área local. Aprenderemos a configurar un PC para poder ser conectado a una red, repasando aspectos como la dirección IP, DNS, puerta de enlace residencial o máscara de subred.

Analizaremos la estructura y los estándares que hacen funcionar la comunicación TCP/IP, permitiendo que los equipos puedan mantener una comunicación independientemente del fabricante o modelo.

Veremos los diferentes tipos de red divididas por su topología física, es decir, la manera en la que están distribuidas mediante el cableado, y veremos los diferentes métodos que se utilizan para enviar los paquetes de información. Hablaremos de las diferencias entre las redes cableadas y las inalámbricas, así como la seguridad que hay que tener en cuenta en cada una de ellas.

Explicaremos los tipos de ataques que pueden sufrir las redes por parte de terceros y la manera de encriptar los datos en las redes inalámbricas para evitar que las comunicaciones sean escuchadas o suplantadas.

Por último, daremos algunas pautas a seguir, sobre todo en empresas, para minimizar los riesgos de sufrir un ataque. Estas pautas deberán de ser seguidas no solo por el administrador del sistema, sino por todos los usuarios de la red, implicando la necesidad de concienciar a los usuarios para evitar acciones que pongan en peligro la privacidad de los datos.

5.1 Configuración del protocolo TCP/IP en un cliente de red

A la hora de incorporar una máquina en una red, es necesario tener unas consideraciones previas y configurar el nuevo equipo para que pueda comunicarse correctamente con el resto de nodos de la red, incluido el servidor.

5.1.1 Configuración del protocolo TCP/IP en un cliente de red

Para que pueda realizarse la comunicación, cada dispositivo conectado a una red, debe disponer de un identificador único que lo diferencia del resto. A este identificador se le denomina IP, que es una combinación numérica de

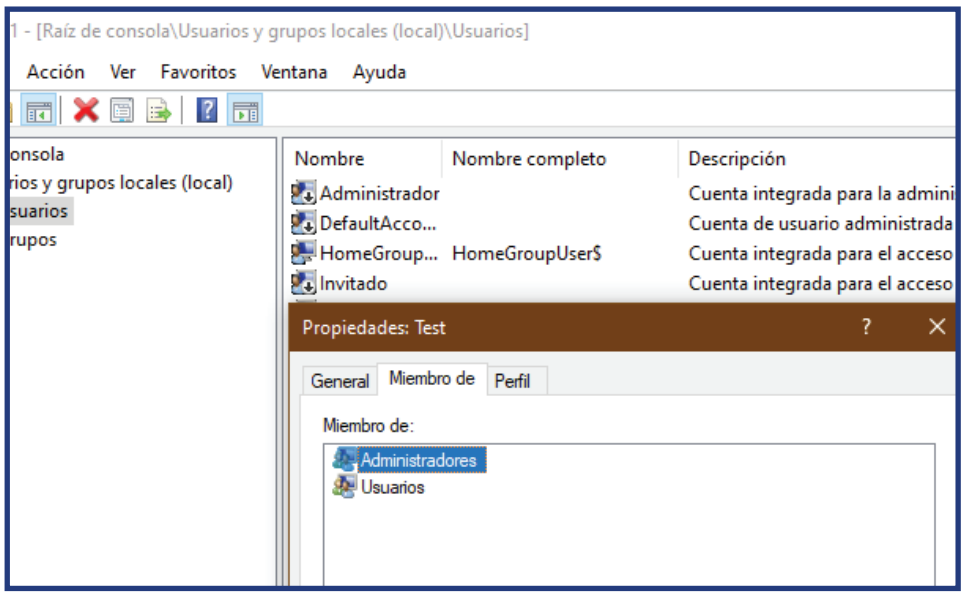


Figura 5.1
Asignación manual de la dirección IP de un equipo.

32 bits, aunque generalmente se representa de manera decimal, separando cada octeto de bits por un punto (Figura 5.1).

5.1.2 Direcciones IP

Una dirección IP es un número que identifica, de manera lógica y jerárquica, una interfaz de un dispositivo dentro de una red que utilice el protocolo IP. Los sitios de Internet que, por su naturaleza, necesitan estar permanentemente conectados, generalmente, tienen una dirección IP fija (comúnmente, IP fija o IP estática). Esta no cambia con el tiempo. Los servidores de correo, DNS, FTP públicos y servidores de páginas web necesariamente deben contar con una dirección IP fija o estática, ya que de esta forma se permite su localización en la red.

Las direcciones IP deben ser diferentes para cada equipo conectado en una red ya que es el sistema que utilizan el resto de máquinas para poder enviar un mensaje a su destinatario. Si existiesen dos equipos con la misma IP, se produciría un error de duplicidad en la red y esas máquinas no podrían estar conectadas correctamente.

5.1.3 Máscaras de subred

La máscara de subred es un elemento imprescindible a la hora de interpretar una dirección IP, ya que a partir de la combinación de dirección IP y máscara podemos determinar que la parte de la dirección IP identifica a la red y que parte a la IP identifica al host. Una máscara de red es un número de 32 bits (representado en formato decimal por cuatro octetos separados por punto) en el que todos los valores que estén a uno identifican la parte

de red de la dirección IP, y todos los bits que estén a cero identifican la parte de host. En la máscara de red, el primer bit empezando por la izquierda siempre es uno y el resto de bits consecutivos se mantiene a uno mientras identifiquen la parte de red. Cuando modifiquemos el valor de un bit de uno a cero se debe mantener el resto de bits hasta el final de la dirección a cero, ya que en la máscara de red no pueden existir alternancias de unos y ceros.

De esta manera, si tenemos, por ejemplo, una dirección de red 192.168.1.152 con máscara 255.255.255.0 podemos deducir que la dirección de esta red es 192.168.1.0 y la dirección de host es 192.168.1.152.

La fórmula que nos permite saber cuál es la dirección de red a partir de una dirección de red y una máscara es: dirección IP "and" máscara = dirección de red.

"And" es una operación entre bits en la que el resultado es uno solo cuando los dos bits son uno.

Aplicando esta fórmula si, por ejemplo, tenemos la dirección IP 192.168.100.6, que en binario es 11000000.10101000.01100100.00000110, con máscara de red 255.255.255.252, que en binario es 11111111.11111111.11111111.11111100, podemos calcular su dirección de red, que es 192.168.100.4, que en binario es 11000000.10101000.01100100.00000100.

5.1.4 IPv4. IPv6

Desde el nacimiento del protocolo TCP/IP, utilizado por la mayoría de redes, la dirección IPv4 basada en cuatro octetos ha sido la única utilizada.

Sin embargo, debido al gran tamaño que están alcanzando las redes de comunicación, los 32 bits que conforman el IPv4 no son suficientes para representar las direcciones de Internet que existen actualmente en todo el mundo.

Por ello, en 1996 se empezaron a plantear nuevos estándares de comunicación que pudiesen dar solución a la gran demanda de direcciones IP creando el IPv6, una extensión de la actual versión IP compuesta por seis octetos que permiten la creación de 6,7 × 1017 (670 mil billones) de direcciones.

5.1.5 Configuración estática

En pequeñas redes que no dispongan de servidor central, es común asignar las direcciones IP manualmente, lo que se denomina **configuración estática**, ya que una vez configurada una dirección es mantenida en el equipo indefinidamente hasta que es cambiada por el usuario.

5.2 Configuración dinámica automática

Los servidores que proporcionan los servicios de conectividad, resolución de nombres y enrutamiento, también pueden ser configurados para proporcionar direcciones IP a los hosts conectados mediante el servicio **DHCP** (en inglés de *Dynamic Host* Configuration Protocol - (**Protocolo de configuración dinámica de host)**. Este servicio crea una tabla que relaciona una IP con las direcciones MAC de las tarjetas de red conectadas a una red. La dirección MAC es única, y no puede ser repetida por ningún otro dispositivo de red en el mercado. Con esta información crea una tabla que utiliza para asignar la dirección IP a un equipo cuando se conecta a la red (Figura 5.2).

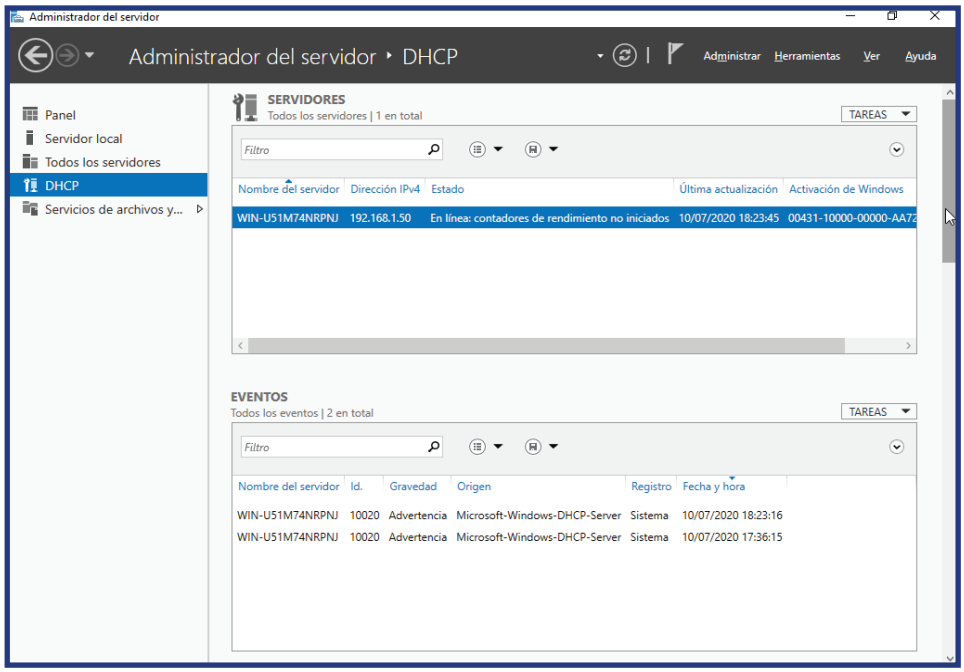


Figura 5.2
Pantalla del servicio DHCP de Windows Server.

5.2.1 Direcciones dinámicas

Es posible utilizar una asignación de IP dinámica dentro de un rango de direcciones que serán utilizadas por los equipos a medida que son conectados a la red. En la tabla DHCP se pueden asignar fechas de caducidad de las asignaciones de manera que un ***host***, al no estar conectado durante un largo período de tiempo, pierda la dirección que se le había establecido

originalmente. Esto es especialmente útil en conexiones en las que se conecten y desconecten muchos equipos, por ejemplo una Wi-Fi pública. En este caso podríamos no considerar la fecha de caducidad de la asignación, sino simplemente asignar diferentes IP a los dispositivos cada vez que se conectasen.

5.2.2. Direcciones fijas

Algunos dispositivos conectados a la red necesitan de una IP fija para poder funcionar correctamente. Este es el caso de recursos compartidos como impresoras o discos duros, en los que un cambio de dirección IP, provocaría que el resto de usuarios tuviesen problemas para encontrarlos en la red. Por ello, el DHCP reserva, direcciones o rangos IP para ser asignados a direcciones MAC de manera permanente. De esta manera, una impresora con dirección 192.168.1.10 tendrá la misma dirección aunque se desconecte durante un largo periodo de tiempo.

5.3 Configuración de la resolución de nombres

La dirección IP de una máquina es un número decimal de 32 bits de cuatro números entre 0 y 255 separados por punto, lo cual es difícil de memorizar e identificar por un humano. Para ello, además de las direcciones IP se asignan nombres utilizando nuestro alfabeto para que sean fáciles de recordar por las personas. Así, se pueden aplicar nombres como PC1, PC-Marta, Servidor1, ServidorCorreo, etc.

Todas las redes necesitan de un sistema de resolución de nombres para que los usuarios puedan compartir recursos utilizando el nombre del recurso y no su dirección IP. Los servidores que se encargan de realizar la traducción de nombre de recursos se llaman servidores DNS. El administrador de estos servidores DNS se encarga de definir las zonas DNS que se han de utilizar, así como los registros que necesitamos dentro de esas zonas para que las resoluciones de nombres funcionen. Algunos ejemplos de registros que nos podemos encontrar dentro de las zonas en un servidor DNS son:

- **Registro de tipo A.** Proviene de la abreviación de la palabra inglesa address y sirve para transformar los nombres de host de un dominio a direcciones IP.

- **Registro de tipo MX.** Proviene del inglés mail exchange y sirve para dar de alta nuestro servidor de correo; es decir, cada vez que un usuario intente enviar un correo a nuestra empresa deberá de preguntar al servidor DNS por el registro MX que apunte a nuestro servidor de correo.

- **Registro de tipo PTR.** Proviene de inglés pointer y es un registro de recurso de un dominio que define las direcciones IP de todos los sistemas en una notación invertida. Se utiliza para encontrar en nombre de un recurso DNS a partir de su dirección IP realizando una resolución inversa de nombre DNS.

Para poder proporcionar una tolerancia a errores y un balanceo de carga en los servidores DNS, nos encontramos los siguientes tipos de servidores DNS:

- **Primarios.** Guardan los datos de un espacio de nombres en sus ficheros en formato de lectura/escritura.

- **Secundarios.** Obtienen los datos de los servidores primarios a través de una transferencia de zona y tienen los datos en un formato de solo lectura.

- **Locales o caché.** No contienen zona para realizar la resolución de nombres. Cuando se les realiza una consulta, estos servidores DNS consultan a los servidores DNS correspondientes, almacenando la respuesta en su base de datos para agilizar la repetición de estas peticiones que en el futuro les realicen sus clientes sobre el mismo recurso.

5.4 Ficheros de configuración de red

En ocasiones, los servidores de red no son capaces de proporcionar de manera automática la información sobre enrutamiento o la resolución de nombres. En estas ocasiones es necesario que el administrador del sistema modifique los archivos que leerá el servidor para realizar estas funciones. En los sistemas Microsoft disponemos generalmente de herramientas gráficas que nos permiten aplicar estas configuraciones manuales mediante una interfaz. Para los sistemas Unix/Linux, en cambio, es necesario modificar los archivos manualmente. Algunos de ellos son:

Figura 5.3
Ejemplo de un archivo resolv.conf.

- **/etc/hosts. L**a función de este archivo es la de resolver los nombres de los hosts que no pueden ser resueltos de manera automática. También se utiliza para resolver nombres en redes que no dispongan de servidor DNS. El archivo está compuesto por varias líneas, cada una de ellas con la dirección IP y el nombre de host al que pertenece.

- **/etc/resolv.conf.** Este archivo especifica las direcciones IP de los servidores DNS y el dominio de búsqueda (Figura 5.3).

- **/etc/sysconfig/network.** Especifica el enrutamiento que se ha de seguir en caso de mantener comunicaciones entre diferentes redes. Es decir, escribiremos las IP de los router de cada red.

5.5 Tablas de enrutamientos

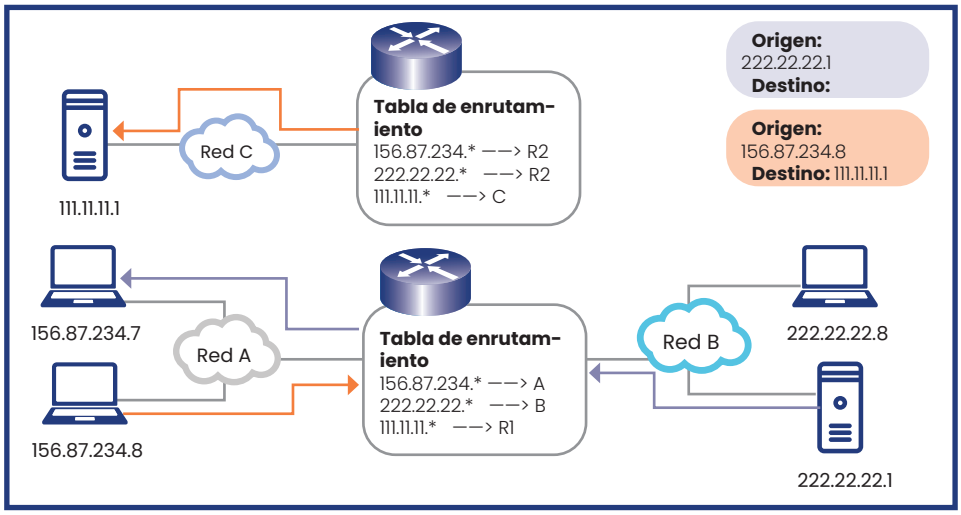


Figura 5.4
Enrutamiento entre tres redes diferentes y las tablas de enrutamiento en cada router.

Cuando debe existir una comunicación entre equipos que forman parte de diferentes redes es necesario un enrutamiento para redirigir los paquetes de información al destino, ya que, al pertenecer a diferentes redes, los ordenadores configurados dentro de una red no pueden comunicarse directamente con los ordenadores de otras redes. Para ellos se crean tablas de enrutamiento que contienen la dirección IP del router de cada red. Esto permite que la información de una red pueda viajar hasta el router de otra red. El router, en ese momento, leerá el paquete y decidirá a qué host de su red va dirigido. En caso de no encontrar el nodo destino devolverá al origen un mensaje de error y cortará la comunicación (Figura 5.4).

5.5.1 Determinísticos o estáticos

El enrutamiento determinístico consiste en configurar los **routers**, que son los dispositivos encargados de dirigir los paquetes dentro y fuera de la red, de manera manual, definiendo en una tabla la dirección IP del router de las otras redes. Esto es una configuración muy sencilla, pero que debe realizarse únicamente en redes pequeñas, puesto que el mantenimiento para redes con muchos routers sería muy costoso. El inconveniente de esta tipología es su rigidez, pues un cambio en el nombre de un **router** provocaría el cambio en las tablas de enrutamiento del resto de dispositivos.

5.5.2 Adaptativos o dinámicos

Son los más utilizados por su dinamismo en redes medianas o de gran tamaño. Se utiliza un servidor para gestionar el enrutamiento dentro de la red. Pueden ser de tres tipos:

- **Adaptativo centralizado.** Todos los nodos de la red son iguales, excepto un nodo central que recoge toda la información de los demás equipos y construye su propia tabla de enrutamiento para servir a los demás.

- **Adaptativo distribuido.** La información de enrutamiento es distribuida a todos los nodos que comparan la tabla con su base de datos y la actualizan en caso de modificaciones.

- **Adaptativo aislado.** Es el más efectivo ante cambios de tipología y de tráfico en la red. Se basa en el envío de la información a todos los nodos, excepto al emisor. Aunque es eficaz, este sistema tiene un evidente abuso en el uso de recursos de red.

5.6 Gestión de puertos

Los **puertos** son un concepto lógico que se utiliza para definir el acceso de la información a una máquina dentro de una red. La máquina destino decide, a bajo nivel, el tratamiento que le dará a los paquetes que entren por un puerto determinado. De esta manera, la información puede ser filtrada, excepto la que entre por un determinado puerto, o puede ser redirigida, a un programa que esté escuchando por un puerto determinado.

En redes privadas es habitual tener todos los puertos cerrados para aquellas comunicaciones procedentes del exterior de la red; aunque, en ocasiones, se abre un puerto por el que está permitido acceder. En las comunicaciones de Internet, el protocolo http utiliza el puerto 80 para enviar y recibir la información, por lo que los servidores que alojan las páginas web deben permitir la conexión por ese puerto para que pueda existir comunicación.

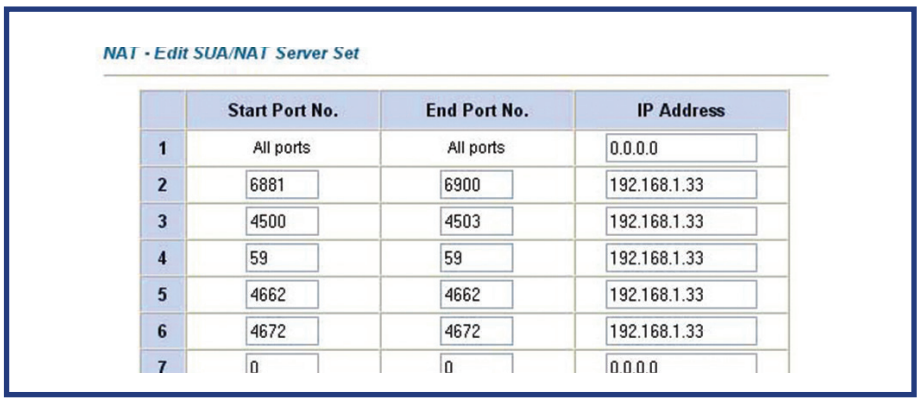


Figura 5.5
Ejemplo en el que se abren los puertos. En este caso, se abren rangos de puertos del 6881 al 6900 para la dirección 192.168.1.33.

Para saber más

Puedes obtener más información sobre los comandos de control de red si en la consola escribes el comando seguido de /help.

Además de las conexiones externas, también es necesario abrir los puertos de salida a aplicaciones que utilicen recursos de interés que se encuentren fuera de nuestra red. Este uso es muy común en aplicaciones **P2P** (del inglés *Peer to Peer*). Los programas P2P utilizan unos puertos específicos, por lo que, para que pueda existir comunicación, hay que abrirlos en el router para que nuestra máquina (y, por consiguiente, su IP) pueda enviar y recibir información por dichos puertos hacia y desde el exterior (Figura 5.5).

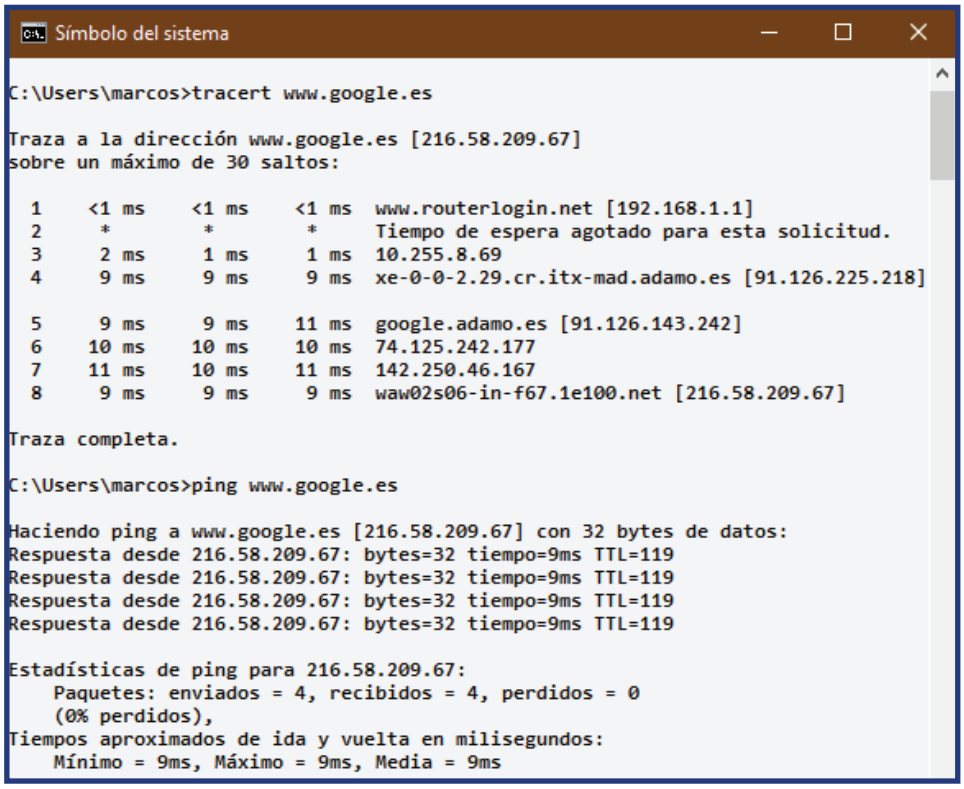


Figura 5.6
Respuesta a los comandos ping y tracert de la dirección de la página web de Google.

5.7 Verificación del funcionamiento de una red mediante el uso de comandos

La manera más rápida de comprobar el correcto funcionamiento de una red, y la más utilizada por los administradores de sistema, es mediante el uso de comandos que envían pequeños paquetes de información y devuelven información sobre la transmisión de los datos, desde los tiempos hasta la ruta recorrida por el archivo.
Los comandos más conocidos son (Figura 5.6):

- **PING.** Muestra información básica sobre el envío de los paquetes de información. También informa de la dirección de destino, previamente resuelta por un DNS y el tiempo que ha tardado el paquete desde el origen hasta su llegada al destino.
- **TRACERT.** Muestra una lista ordenada de los enrutadores intermedios por los que ha pasado el paquete. Es muy interesante observar el listado de máquinas para ver el recorrido y detectar aquellos nodos por los que pasa, como servidores, routers, etc., hasta llegar al destino demandado.

5.8 Resolución de problemas de conectividad en sistemas operativos en red

En las redes informáticas, al estar distribuidas en su mayoría de forma genérica, se tiene la posibilidad de identificar los nodos que producen los errores de comunicación mediante los comandos de red.

Utilizando comandos como tracert, podemos ver el camino que recorren los paquetes enviados entre el origen y el destino. De esta manera, podremos ver en qué nodo de la red se interrumpe la comunicación en caso de

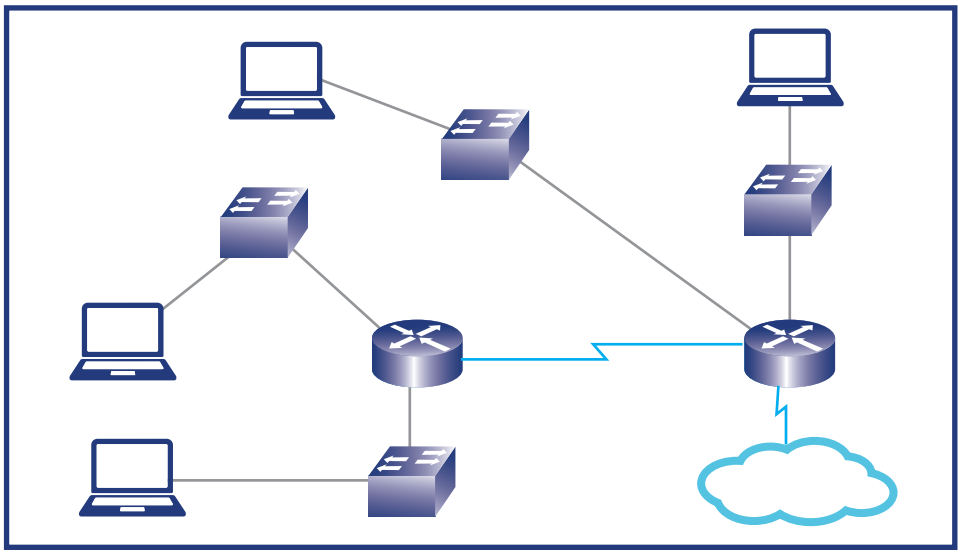


Figura 5.7
Estructura de una red donde intervienen varios nodos de conexión.

producirse un error en la transmisión de los datos. Estos retrasos reciben el nombre de lag (en inglés, retraso).

En ocasiones, los problemas de comunicación son originados en la propia máquina sin que ningún otro elemento de la red esté implicado en el mal funcionamiento. En estos casos, podría deberse a una mala configuración de los equipos que impida la correcta comunicación con el resto de la red (Figura 5.7):

- **Duplicidad en la red.** Este error es debido a una asignación repetida de la misma IP entre varios equipos de la misma red. Para solucionar este problema, basta con modificar la IP que tiene asignada el equipo o configurarlo para recibir automáticamente la IP por parte del servidor.

- **Máscara de subred incorrecta.** Al realizar una incorrecta configuración de la máscara de subred es posible que el equipo no sea reconocido por el resto dentro de una red porque, a pesar de pertenecer a la misma estructura física, conceptualmente estaría accediendo a una red diferente a la que no tendría acceso.

5.9 Comandos utilizados en sistemas operativos libres y propietarios

Como en la mayoría de funcionalidades, los diferentes sistemas operativos tienen diferentes comandos para comprobar el estado de la red, a pesar de que las funcionalidades son similares o idénticas. Es importante conocerlos bien tanto en sistemas operativos libres como en sistemas operativos propietarios.

- **Microsoft:**

  - **IPCONFIG.** Es una aplicación de consola que muestra los valores de configuración de red de TCP/IP actuales y actualiza la configuración del protocolo DHCP y el sistema de nombres de dominio (DNS).
  - **NETSTAT.** Muestra las conexiones actuales del equipo. Podemos visualizar toda la información de las conexiones como direcciones IP, DNS, máscaras de red, etc.
  - **PING.** Envía una serie de paquetes a través de la red y devuelve el estado de la recepción por parte del destinatario.
  - **TRACERT.** Genera el recorrido realizado por un paquete de información desde el origen hasta el destino.

- **UNIX/Linux:**

- **IFCONFIG.** Es una aplicación de consola que muestra los valores de configuración de red de TCP/IP actuales y actualiza la configuración del protocolo DHCP y el sistema de nombres de dominio (DNS).
- **NETSTAT.** Muestra las conexiones actuales del equipo. Podemos visualizar toda la información de las conexiones como direcciones IP, DNS, máscaras de red, etc.
- **PING.** Envía una serie de paquetes a través de la red y devuelve el estado de la recepción por parte del destinatario.
- **TRACEROUTE.** Genera el recorrido realizado por un paquete de información desde el origen hasta el destino.

Como podemos ver, las funcionalidades en sí son las mismas, pero utilizan nombres de comandos diferentes. Podríamos ver más diferencias entre los comandos al utilizar sus funcionalidades avanzadas. En NetSat de Unix, por ejemplo, además de la información de las conexiones, tiene opciones para que muestre los puertos abiertos en esas conexiones.

5.10 Monitorización de redes

Para comprobar el estado de nuestra red y detectar cualquier nodo que pudiera estar experimentando un mal funcionamiento, es necesario monitorizar todas las conexiones y dispositivos de la red. Esto se realiza generalmente con software instalado en el servidor que, de manera frecuente, va enviando paquetes de datos a todas las partes de red y calculando la respuesta, tanto en tiempo como eficacia, para, de esta manera, informar al administrador del sistema en caso de encontrar cualquier error. Son sistemas vitales para servidores que proporcionan un servicio continuo, como

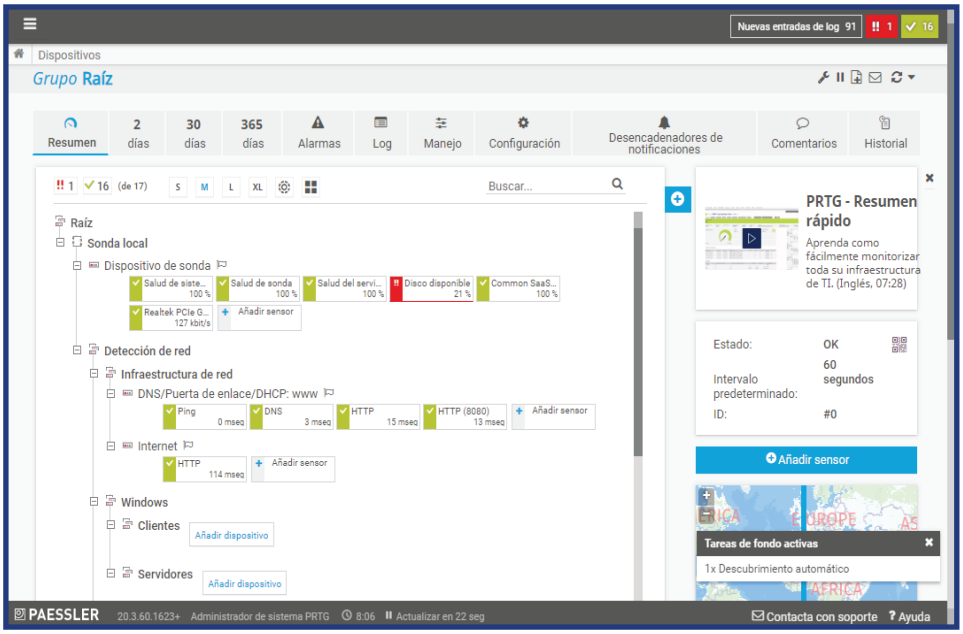


Figura 5.8
Software de monitorización de una red.

Para saber más

Un software multiplataforma para monitorizar redes es OverLook (http://overlooksoft.com/)

pueden ser los servidores web. En caso de producirse una caída en el sistema que afecte a la conectividad o en la resolución de peticiones, el programa enviará un correo electrónico para que pueda realizar las operaciones oportunas. Una característica extra que tienen estos programas es que, al mismo tiempo que se puede controlar el funcionamiento de la red, también es posible obtener datos estadísticos de las conexiones, horarios, velocidades, peticiones, etc. Datos que pueden ser utilizados para demostrar la necesidad de ampliar los recursos utilizados (Figura 5.8).

5.11 Protocolos TCP/IP

El modelo TCP/IP es el conjunto de protocolos utilizados para poder realizar las conexiones de red. Fue creado en la década de 1970 por DARPA, una agencia de Departamento de Defensa de los Estados Unidos y se desarrolló a partir de ARPANET, la tecnología predecesora de Internet.

El modelo TCP/IP es básicamente un conjunto de protocolos, o normas, que deben seguir todos los implicados en la comunicación para poder realizarse la conexión. Define la manera en la que los datos deben ser divididos, encapsulados, codificados y transmitidos. Además, define cómo deben ser recibidos, decodificados, desencapsulados y unidos en el destino. Solo de esta manera puede existir la comunicación entre dos máquinas.

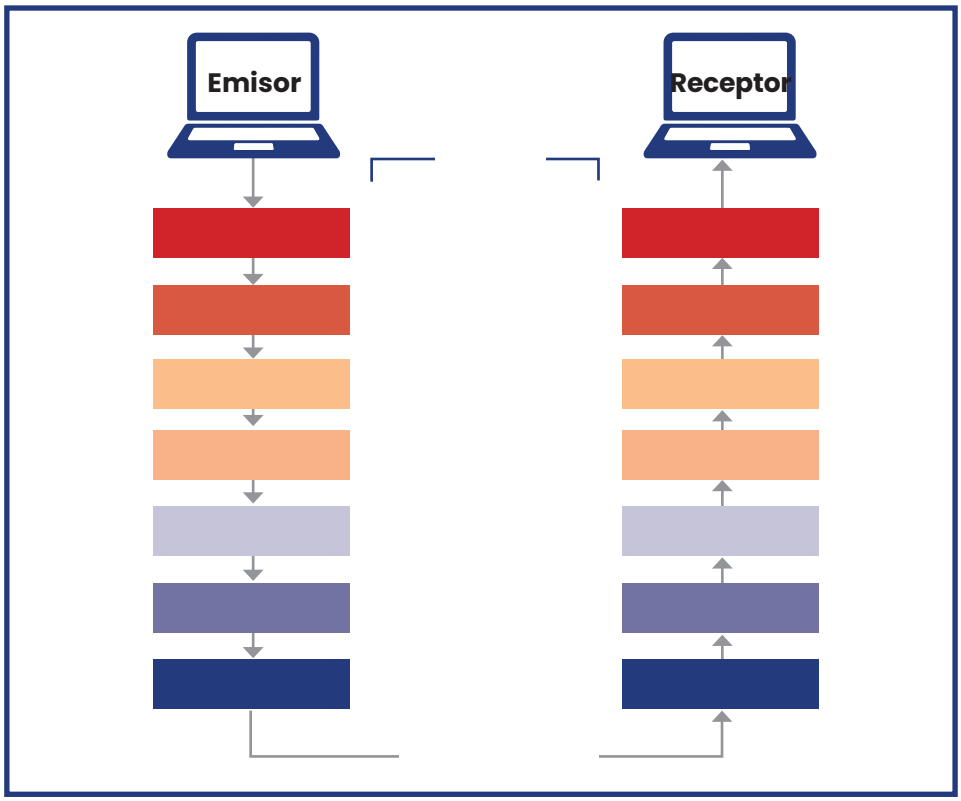


Figura 5.9
Comunicación entre dos ordenadores utilizando el modelo de comunicación con capas OSI.

La complejidad del proceso de comunicación requiere que se lleve a cabo por procedimientos separados. Por ello, se utiliza conceptualmente un modelo de capas en el que cada una de ellas realiza una tarea dentro del proceso de comunicación. A pesar de existir un modelo de siete capas estándar llamado OSI (Figura 5.9) y creado por la Organización Internacional para la Estandarización, lo cierto es que TCP/IP utiliza el modelo de cuatro capas:

Capa 4 o capa de aplicación. Su función es la de mantener la comunicación entre los equipos, así como representar la información recibida y proporcionar al software de la máquina acceso a la conexión. Esta capa es comparable a las capas de aplicación, presentación y sesión del modelo OSI.

- **Capa 3 o capa de transporte.** Es la encargada de realizar el transporte de los paquetes independientemente del tipo de hardware de red que posean emisor y receptor. Los protocolos que utiliza son TCP y UDP. Esta capa es comparable a la capa de transporte del modelo OSI.

- **Capa 2 o capa de red.** Se encarga de dirigir los paquetes de información a través de diferentes redes aunque no estén conectadas de manera directa. Tienen la información de la ruta que deben seguir los paquetes con tal de llegar al destino. Esta capa es comparable a la capa de red del modelo OSI.

- **Capa 1 o capa de enlace.** Su función es la de dividir los datos y encapsularlos de manera ordenada, incluyendo en los datos que se envían la manera en la que se ha realizado la división y encapsulamiento, para que el destino pueda reconstruir la información. Esta capa también es la encargada de controlar los errores que puedan existir en los datos antes de enviarlos y de la sincronización entre las partes de la comunicación. Esta capa es comparable a la capa de enlace de datos del modelo OSI.

Para saber más

Existe una capa en el modelo OSI que no está referenciada en el modelo TCP/IP. Esta es la capa física, que se encarga de los componentes electrónicos y la codificación en impulsos eléctricos de la información binaria.

5.12 Configuración de los adaptadores de red en sistemas operativos libres y propietarios

A pesar de las diferencias entre los sistemas operativos libres y propietarios, las configuraciones que se realizan en los adaptadores deben ser las mismas para que pueda llevarse a cabo la comunicación. A continuación, veremos el listado de especificaciones básicas que deberemos configurar para conectar un equipo a una red. Algunas de estas configuraciones ya las hemos visto anteriormente:

- **Dirección IP.** Definiremos la dirección que identificará el equipo dentro de la red. No es lo habitual en máquinas cliente, pero en equipos servidores es posible que tengan instaladas más de una tarjeta de

red. En ese caso, cada tarjeta de red deberá identificarse por una IP y funcionarán como elementos independientes dentro de la red.

- **Máscara de subred.** Definiremos mediante la máscara de subred la parte de la dirección IP que pertenece a la dirección de red y la parte que corresponde con la identificación del host.

- **Gateway o puerta de enlace.** Será la IP del equipo que nos proporcione los servicios de red como la conectividad, el enrutamiento de los datos e incluso el servicio DNS. En redes pequeñas deberemos introducir la IP del router que hace de nodo central de todas las conexiones y en redes más grandes introduciremos la IP del servidor que nos proporcione los servicios de red.

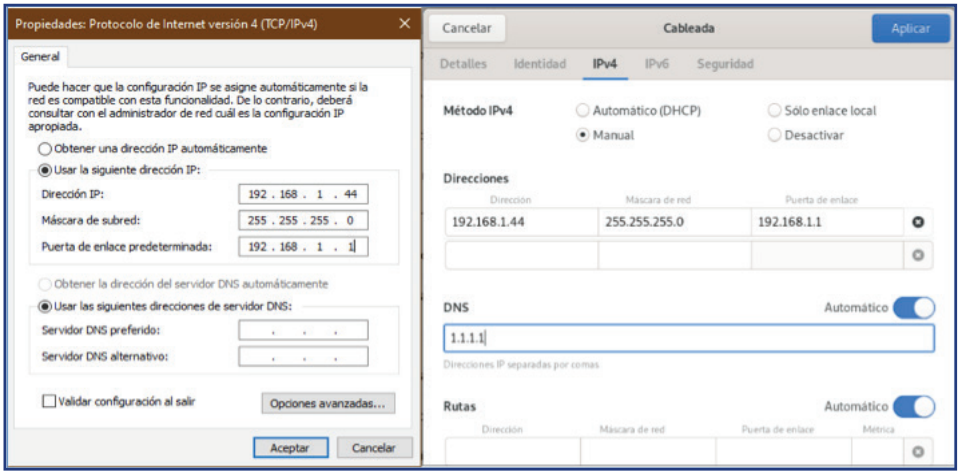


Figura 5.10
Comparación de las interfaces de Microsoft y Linux para configurar los adaptadores de red.

- **DNS.** En muchas ocasiones, en este espacio introduciremos la misma dirección que la puerta de enlace, puesto que la mayoría de veces se trata del mismo dispositivo. Pero en redes grandes, en las que tengamos un equipo diferente dedicado a dar el servicio DNS, deberemos introducir la IP de este otro servidor.

Estas especificaciones son las mismas independientemente del sistema operativo que estemos utilizando; en cualquier caso la interfaz será diferente, pero no debería suponer ningún problema a la hora de configurarlo (Figura 5.10).

5.13 Software de configuración de los dispositivos de red

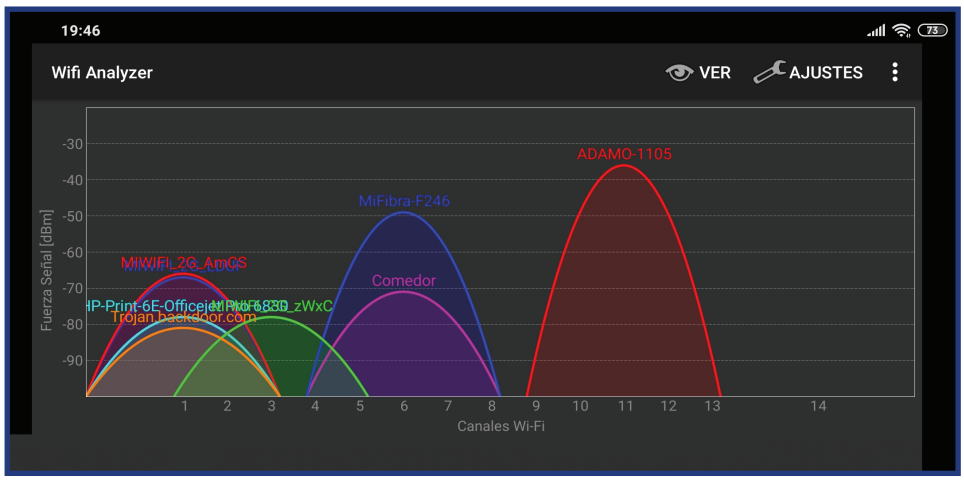


Figura 5.11
Pantalla de una app analizadora de señales Wi-Fi.

Habitualmente los dispositivos de red son configurados mediante los propios sistemas operativos, pero es posible instalar software para configurarlos que, en ocasiones, añade nuevas funcionalidades como la creación de estadísticas, monitorización de conexiones o simplemente una visualización más atractiva que la proporcionada por la interfaz del sistema operativo. Por ejemplo, Config+.

Cuando empezaron a utilizarse dispositivos inalámbricos, los sistemas operativos no permitían la configuración de redes inalámbricas de forma nativa y fue necesario un software específico del fabricante para poder utilizarlos.

Para saber más

Cada adaptador de red que se vende en el mercado es identificado por un numero único en todo el mundo. Los servidores utilizan esta identificación para relacionarla con la IP y el nombre de un equipo.

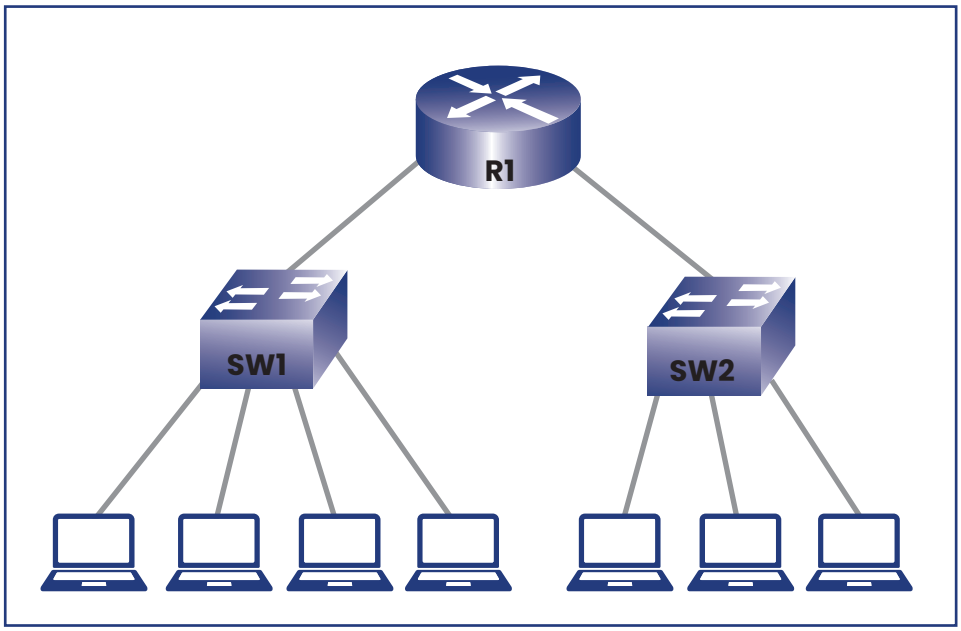


Figura 5.12
Ejemplo de interconexión que permite conectar más de un equipo al mismo puerto del router utilizando el switch como dispositivo intermedio de conexión.

Ahora, cualquier móvil con la app apropiada puede convertirse en un analizador de espectro (Figura 5.11).

5.14 Interconexión de redes: adaptadores de red y dispositivos de interconexión

Las limitaciones físicas y estructurales en ocasiones nos impiden que los equipos puedan tener una conexión directa a la red. Es muy común en oficinas en las que el número de equipos conectados a la red (PC, impresoras, portátiles) aumenta con el tiempo, mientras que las tomas donde conectarlos no lo hacen por el coste que supondría la ampliación de las instalaciones (Figura 5.12). En estas situaciones, la mejor solución es utilizar un dispositivo de interconexión que permita conectar varios equipos a una misma toma de red. Por ejemplo:

***Hub* (concentrador).** Es un dispositivo que centraliza el cableado en un mismo punto para permitir la ampliación de una red. Cuando recibe un paquete de información, automáticamente lo reenvía a todos los equipos que estén conectados con él. Cada uno de los equipos se encargará de aceptar o rechazar la conexión dependiendo de si es o no el destinatario. Actualmente está en desuso en favor de los switches.

***Switch* (conmutador).** Este dispositivo recibe la información desde el lado de la toma y lo envía al destinatario correspondiente guiado por la dirección MAC del equipo destino. A diferencia del hub, el switch envía la información solo al destinatario disminuyendo considerablemente la saturación de la red para el resto de los nodos.

***Router* (enrutador).** Es un dispositivo más avanzado que los anteriores, puesto que no solo se encarga de entregar el paquete, sino que calcula la ruta más corta para realizar el envío, ya que tiene la tabla de enrutamiento donde almacena la situación de todas las máquinas que están conectadas a él. Generalmente se están utilizando para conectar un gran número de equipos, incluidos otros enrutadores, ya que pueden ser utilizados como nodo central de una red.

5.15 Redes cableadas. Tipos y características. Adaptadores de red. Conmutadores, enrutadores, entre otros

Las redes cableadas se pueden dividir según su estructura física y su estructura lógica.

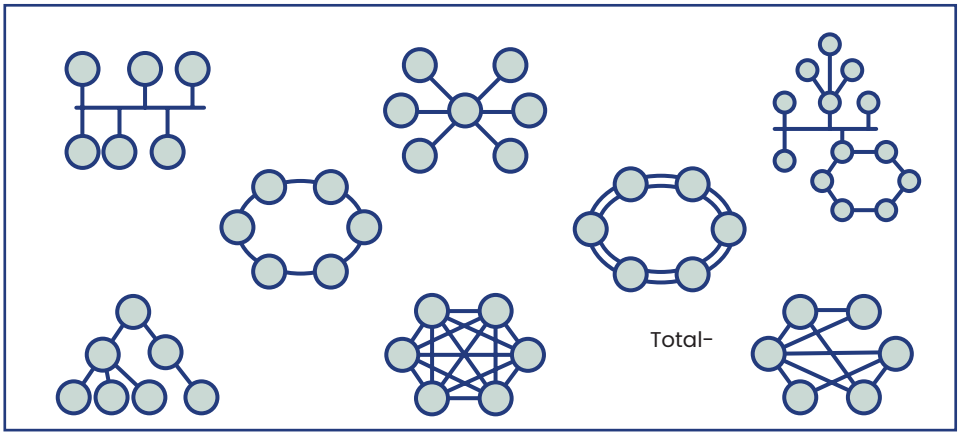


Figura 5.13
Tipologías físicas de una red de área local.

Las topologías físicas representan la manera en la que se realizan la conexiones físicas entre los diferentes nodos de una red. Dentro de esta categoría existen diferentes topologías (Figura 5.13):

- Una **topología de bus circular** usa un cable llamado backbone que termina en ambos extremos donde se conectan todos los equipos de la red.

- La **topología de anillo** conecta cada uno de los host de la red consecutivamente hasta llegar al último, el cual se conecta con el primero, creando así un anillo cerrado que conecta todos los equipos.

- La **topología en estrella** conecta todos los cables con un punto central de concentración.

- Una **topología en estrella** extendida crea varias conexiones utilizando topología de estrella, y las conecta entre sí mediante dispositivos de interconexión como hubs o switches.

- Una **topología jerárquica** es similar a una estrella extendida con la diferencia que no se conectan mediante dispositivos de interconexión, sino mediante un servidor que controla el trafico de la comunicación.

- La **topología de malla** es un sistema de red que interconecta todos los equipos con todos los demás. Esto asegura la comunicación creando vías alternativas cuando alguna pueda fallar. Este sistema es utilizado en entornos donde es vital que no falle la comunicación bajo ninguna circunstancia, como sistemas de vigilancia militar o centrales nucleares. Los sistemas que tienen vías alternativas pero que no conectan todos sus nodos entre sí se denominan de topología de malla parcial.

- En **la topología de árbol** se conectan los nodos de la red de manera que exista un servidor base desde donde salen todas las ramificaciones.

- Las **topologías lógicas** representan la manera en que los hosts, de una red se comunican entre sí decidiendo el camino que recorren los datos. Los dos tipos existentes son broadcast y el sistema de tokens.

Para saber más

Las redes Ethernet son el estándar de las redes de área local utilizadas actualmente en la mayoría de redes.

- La **topología broadcast** (difusión) se basa en enviar la información a todos los nodos de la red, haciendo que el receptor lo acepte y el resto de hosts lo rechacen si no son los destinatarios. Los mensajes son depositados en una cola de recepción en los hosts, que los van administrando por orden de llegada. Esto sucede porque dentro de la red todos los hosts pueden enviar mensajes sin pedir turno al resto. Este sistema es el medio utilizado por las redes Ethernet.
- La **topología transmisión de tokens** (fichas) se utiliza un mecanismo de turnos llamado token para controlar el acceso a la red por parte de los host que desean transmitir datos. Solo existe un token en cada red, que va pasando de equipo en equipo. Cuando un host recibe el token, se le permite enviar un número determinado de paquetes a su destinatario y envía el token al siguiente host. De esta manera, el sistema se asegura que ningún emisor satura la red.

5.16 Redes inalámbricas. Tipos y características

Las redes inalámbricas (en inglés ***wireless***) son aquellas que permiten la interconexión de los equipos sin necesidad de cableado. Por ello, las tipologías en las que se dividen las redes inalámbricas no se basan en los tipos de interconexiones como en las redes cableadas, sino que se dividen en el método de transferencia y el tipo de señal utilizados, así como la **distancia** de comunicación que soportan (Figura 5.14).

Figura 5.14
Cada uno de los tipos de señales organizados según su alcance.

- ***Wireless Personal Area Network (WPAN).*** Este tipo de conexiones están basadas en la conectividad a corta distancia de pequeños equipos como

móviles o aparatos de domótica. Tiene como base fundamental el bajo consumo para maximizar el uso de baterías y la transferencia de una pequeña cantidad de datos. Algunos dispositivos que utilizan esta categoría son las especificaciones IEEE 802.15.1 conocidas como **Bluetooth**.

- ***Wireless Local Area Network (WLAN).*** Es la más utilizada en hogares y oficinas, está basada en un alcance medio de la señal para la conexión de diferentes equipos a un nodo central. Una de las especificaciones que están en esta categoría es el estándar IEEE 802.11, conocido como **Wi-Fi.**

- ***Wireless Metropolitan Area Network (WMAN).*** Son utilizadas para una distribución de la señal a largas distancias para proporcionar cobertura en áreas metropolitanas. Una de las especificaciones más usadas es la IEEE 802.16, muy parecida al Wi-Fi y conocida con el nombre de ***WiMax.***

- ***Wireless Wide Area Network (WWAN).*** Utiliza conexiones basadas en tecnología móvil para conectar los equipos de una manera parecida a la WLAN. Es una de las tecnologías que mas rápido ha evolucionado debido a la necesidad del mercado de proporcionar una conectividad cada vez mejor a los dispositivos móviles. En el listado de especificaciones más usadas están G**PRS, EDGE, 3G y 4G.**

5.17 Seguridad básica en redes cableadas e inalámbricas

Tanto las redes cableadas como las inalámbricas son susceptibles de tener brechas de seguridad si no se toman las medidas adecuadas. Cualquier persona que se conecte a nuestra red puede utilizar herramientas de software para realizar ataques a las comunicaciones de los otros usuarios dentro de la red. En las redes cableadas es necesario que la persona que realice el ataque esté físicamente conectado dentro de nuestra red y que el sistema le otorgue conexión, mientras que en las redes inalámbricas será necesario que conozca la clave mediante la que el dispositivo encripta las comunicaciones emitidas.

Generalmente, la información es retransmitida a todos los nodos de una red, quienes filtran aquella información que no va destinada a ellos. En estos casos, es posible adquirir software que monitorice las comunicaciones de la red para poder leer la información que se envía entre dos nodos de la red. Los tipos de ataques que pueden recibir los usuarios de una red son:

- **Ataques de intromisión.** Se basa en acceder a los archivos almacenados en un ordenador que, por una mala configuración, son compartidos por el resto de usuarios. El atacante tendrá acceso a estos archivos e incluso eliminarlos del ordenador.

- **Ataque de espionaje en líneas.** Es común en redes Wireless en las que la comunicación es enviada a todo el entorno sin necesidad de estar conectado físicamente a ningún dispositivo. Se basa en recibir la información de la que no se es destinatario.

- **Ataque de intercepción.** Utilizando el software instalado, es posible acceder al flujo de información de la red para poder acceder a los documentos, archivos y conversaciones que circulan por la red.

- **Ataque de modificación.** Si el atacante está en el camino entre el emisor y el receptor, es posible que se utilice ese factor para recibir los datos del emisor, modificarlos y reenviar la información manipulada al destinatario de una manera totalmente transparente para los implicados.

- **Ataque de denegación de servicio.** Son ataques que se realizan enviando un gran número de peticiones a un servidor hasta saturar su capacidad. Hay que tener en cuenta que, a pesar de estar preparados para recibir una gran cantidad de peticiones, los servidores tienen limitaciones físicas que no le permiten atender a un número infinito de peticiones. Estos ataques no necesitan de grandes conocimientos técnicos por parte de los atacantes, puesto que necesitan únicamente un software que de manera repetida realice peticiones a un mismo equipo servidor.

- Ataque de suplantación. Este ataque se basa en falsear la identificación de un equipo para hacerse pasar por otro nodo de la red. A efectos prácticos, la red identificará ese equipo con otra identidad, lo que permitirá

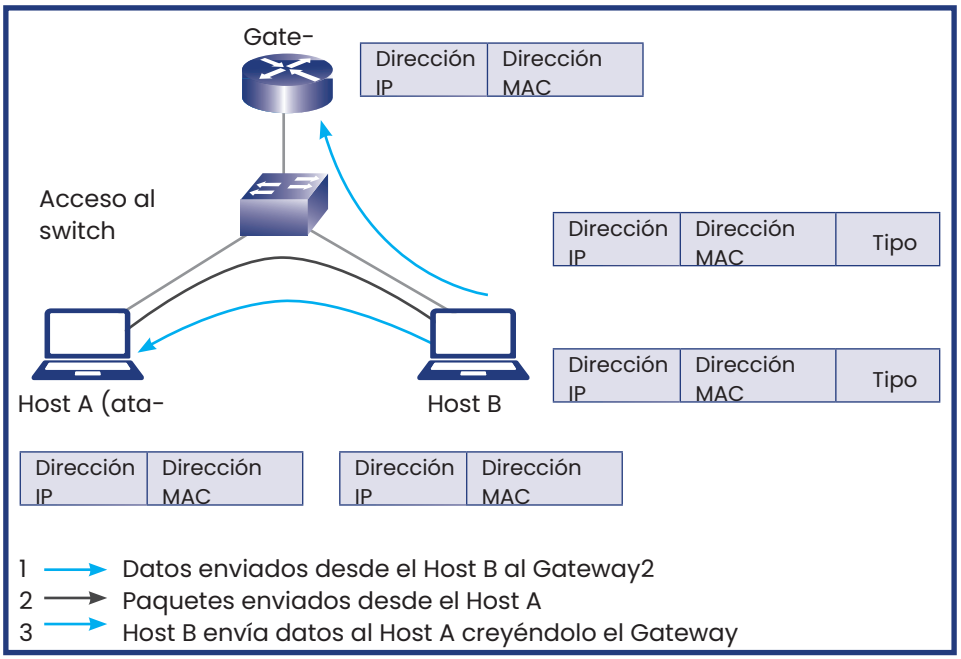


Figura 5.15
Suplantación de identidad por parte de un atacante para que la víctima le envíe toda la información.

recibir y enviar mensajes como si fuera otra persona de la red. Estos ataques son comunes en los robos de la información de las tarjetas de crédito, donde los ladrones se hacen pasar por el banco para que los usuarios les faciliten sus datos bancarios (Figura 5.15).

5.18 Seguridad en la comunicación de redes inalámbricas

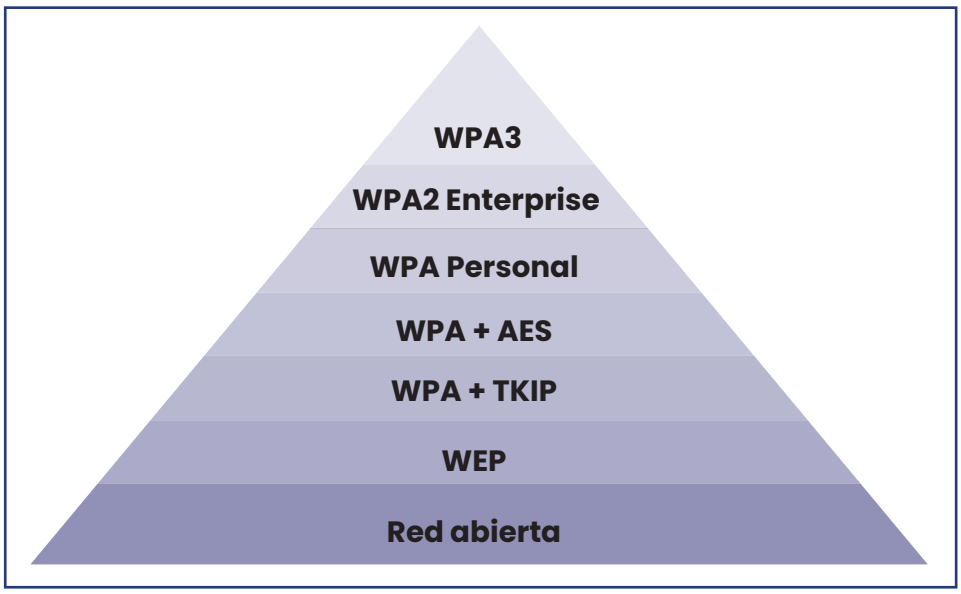


Figura 5.16
Protocolos de seguridad ordenados por su seguridad, de menor (abajo) a mayor (arriba).

En redes inalámbricas donde no es necesario que un equipo esté conectado físicamente a la red, es necesario utilizar medidas de seguridad adicionales para preservar la privacidad de la información y el acceso a la red. Para ello, se utilizan códigos de cifrado conocidos por el dispositivo inalámbrico y los equipos autorizados y que se utilizan para encriptar la información de manera que, aunque sea interceptada por terceros, no pueda ser descifrada sin el código correcto (Figura 5.16).

Algunos de estas encriptaciones son:

- **WEP (Wired Equivalent Privacy o Privacidad Equivalente a Cableado):** es el cifrado de 64 y 128 bits que codifica los datos mediante la clave de cifrado. Este tipo de seguridad es el menos recomendado debido a su facilidad por parte de un cracker (del inglés crack, romper) para descubrir el código.

- **WPA (*Wi-Fi Protected Access* o Acceso protegido a Wi-Fi):** es un sistema basado en el anterior WEP, pero mejorando el algoritmo de encriptación, haciendo más difícil por parte de un atacante descubrir la clave secreta. De todos modos, se conocen vulnerabilidades en este sistema que hacen que pueda ser descifrado.

- **WPA2 (*Wi-Fi Protected Access* o Acceso protegido a Wi-Fi):** es la segunda versión del sistema WPA, que utiliza el algoritmo de cifrado AES (Advanced Encryption Standard) haciendo de este sistema uno de los más seguros existentes hoy en día.

El término **PSK** es la utilización de la misma clave de acceso para todos los usuarios que se conecten a un mismo dispositivo, reduciendo de esta manera la seguridad de la red. En entornos profesionales es un pro-blema la utilización de este sistema, puesto que un empleado que no per-tenezca ya a la empresa puede seguir utilizando la red al conocer la clave. La única alternativa que tiene la empresa es cambiar el código de acceso del dispositivo inalámbrico (y el de todos los equipos conectados) o utilizar un servidor **RADIUS** que permita el acceso a la red inalámbrica en función del usuario del sistema operativo. A pesar de las medidas de seguridad, las claves de encriptación, incluso las más seguras, no son totalmente fi ables porque pueden ser vulneradas mediante software que analiza los paquetes que se envían y descifra el código de seguridad mediante algoritmos.

5.19 Acceso a redes WAN. Tecnologías

Una red WAN (del inglés Wide Area Network) es una red de gran tamaño que puede abarcar desde los 100 Km hasta los 1.000 Km y que se utiliza para dar servicio a un país o continente. Internet sería el ejemplo más sig-nificativo de una red WAN. Normalmente, la WAN es una Routerred punto a punto, es decir, red de paquetes conmutados. Las redes WAN pueden usar sistemas de comunicación vía satélite o de radio.

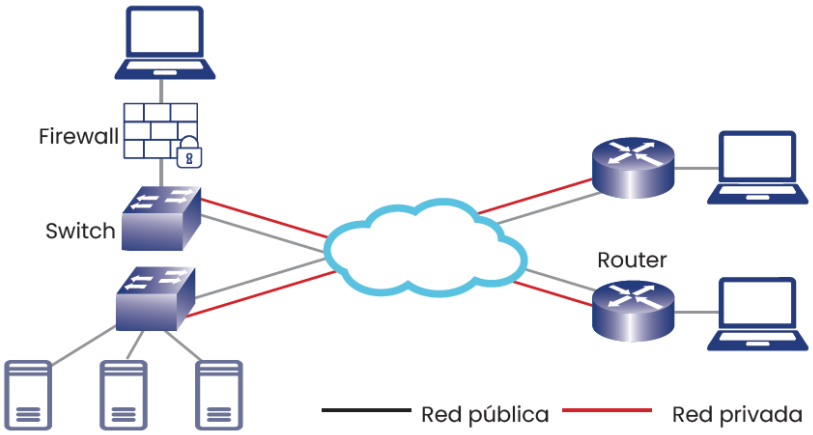


Figura 5.17
Esquema de Internet.

Para conectarse a este tipo de redes es necesario un proveedor de servicio que te permita conectarte dándote una dirección IP única dentro de la WAN, así como proporcionarte el servicio de DNS y enrutamiento necesarios para entablar la comunicación con el resto de la WAN. El funcionamiento y la estructura son muy similares a una red LAN; la única diferencia reside en su gran tamaño y en su estructura de malla parcial en la que existen diferentes caminos para llegar al mismo punto (Figura 5.17).

El ATM (en inglés ***Asynchronous Transfer Mode*** o Modo de Transferencia Asíncrona) es una tecnología de telecomunicación que se basa en la divi-sión de la información en cortos paquetes (celdas ATM) de longitud cons-tante, que no son enviados por un mismo canal asignado, sino que son enrutados por canales virtuales hacia el destino. Este sistema permite ha-cer frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones.

Las líneas xDSL están basadas en una familia de tecnologías que utilizan técnicas de modulación junto a procesamientos digitales de la señal, para mejorar el ancho de banda que proporciona el par de cobre utilizado como canal para la comunicación en Internet.

5.20 Seguridad de comunicaciones

Para poder preservar la seguridad de las comunicaciones, es indispen-sable una correcta confi guración del sistema que difi culte los ataques de terceros que podrían afectar al funcionamiento de la red o poner en peligro la confi dencialidad de los datos.

Para ello, será necesario establecer una política de seguridad y difundirla a todos los usuarios de la red con tal de preservar la seguridad de la red. La mejor opción es limitar el acceso de los usuarios a los recursos de sus equipos para evitar que modifi quen las confi guraciones de cortafue-gos o conexiones de Internet indispensables para evitar ataques a partir de los equipos clientes.

En cuanto al servidor, hay que identifi car la información más sensible para almacenarla, si es necesario, en un dispositivo aislado de la red ex-terior y al que solo se pueda acceder desde los equipos conectados a la red previa autentifi cación de los usuarios.

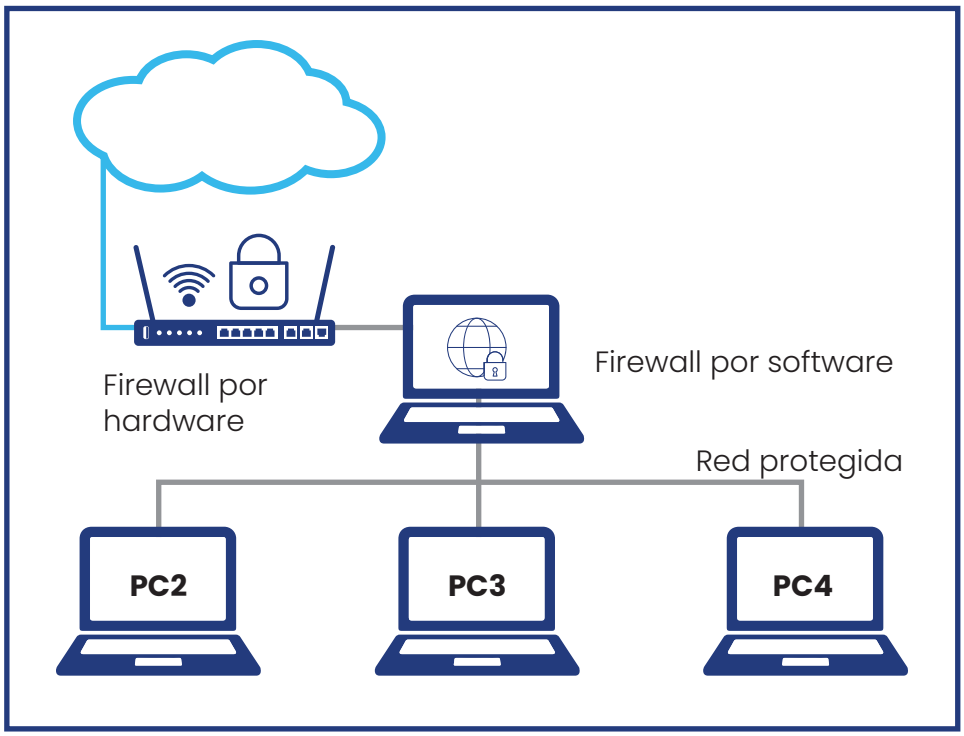


Figura 5.18
Esquema de una red con un dispositivo cortafuegos a la entrada de Internet y un software cortafuegos en el servidor central.

El **cortafuegos** (en inglés, *firewall*) es el *software* o *hardware* mediante el cual se aíslan los intentos de conexión entrantes desde cualquier puerto que no sea el autorizado. Además, de las peticiones entrantes, se puede identificar la procedencia y denegar su acceso según su dirección IP. Esta acción se produce cuando el administrador ha elaborado una **lista negra** de direcciones a las que el cortafuegos ha de denegar el acceso (Figura 5.18).

Una de las consideraciones a tener en cuenta, sobre todo en equipos servidor, es la de no realizar instalaciones de software poco conocido, puesto que podrían contener código para divulgar la información de tu ordenador a terceros. También evitar contraseñas demasiado evidentes o que conformen palabras de diccionario. En su lugar, una combinación de letras, mayúsculas y minúsculas, números y símbolos es la mejor opción para usuarios administradores.

Actualizar el sistema operativo y el software que requiere de conexión a Internet es fundamental para solucionar problemas de seguridad que constantemente se descubren en cualquier sistema operativo. Un mantenimiento deficiente en las actualizaciones del sistema operativo hace vulnerable un sistema conforme pasa más tiempo sin realizarse correctamente.

Resumen

Los equipos que conforman una red informática necesitan estar configurados para poder ser identificados por el resto de equipos con el fin de que pueda establecerse la comunicación entre ellos. Esto se consigue asignándole una dirección IP, un número binario de 32 bits representado de forma decimal por cuatro octetos separados por punto que no solo define el nombre de la máquina, sino también la dirección de la red a la que pertenece.

Para poderse establecer la comunicación en una red, no basta con interconectar físicamente los equipos, sino que es preciso, además, configurarlos para que todos formen parte de la misma red. Esto se realiza con la máscara de red, con la que se definen los bits de la IP que se utilizan para identificar la red, mientras que los restantes bits se utilizan para identificar al equipo.

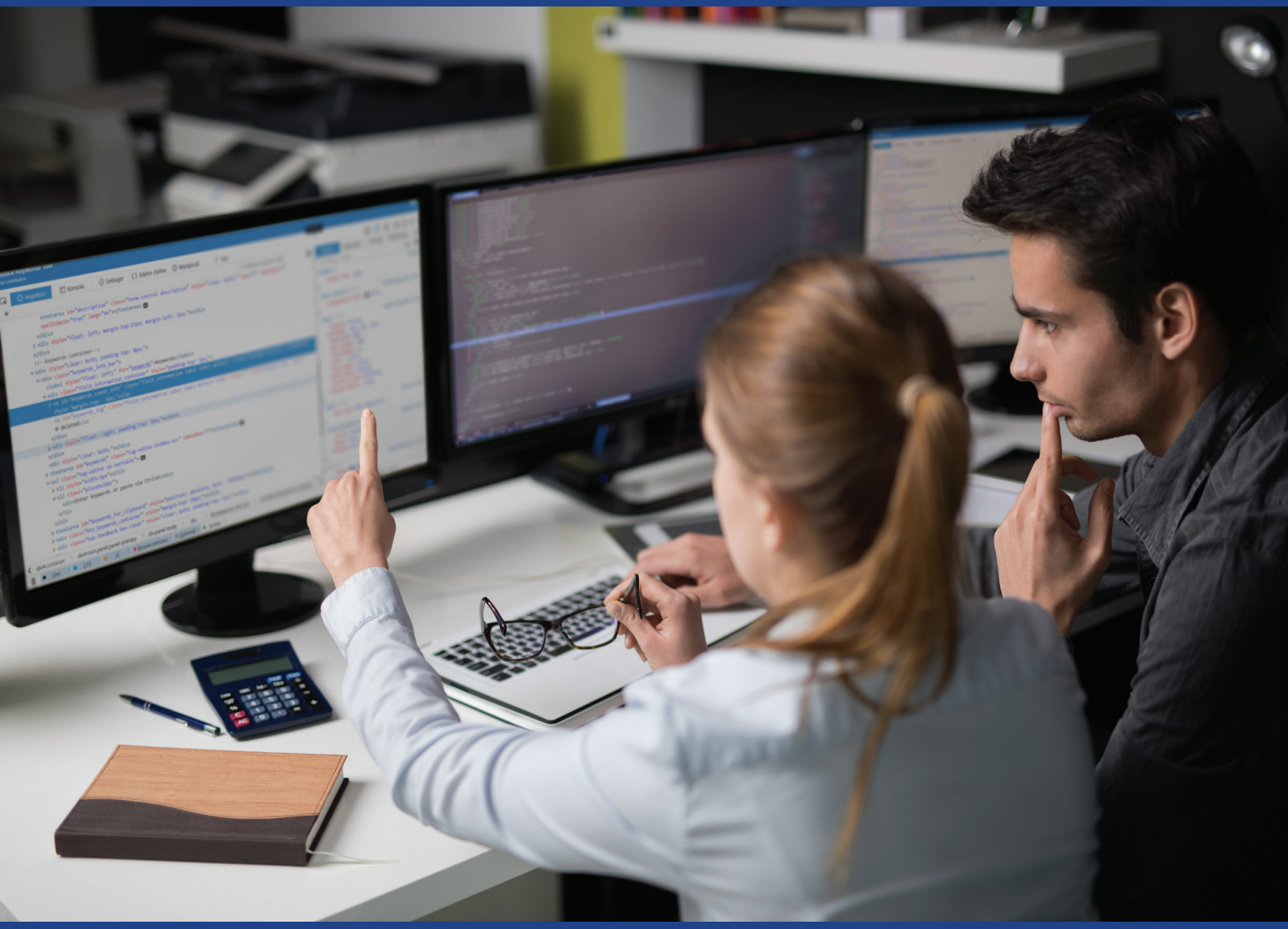
Los dispositivos de interconexión se emplean para conectar diferentes equipos a una misma sección de la red, lo que, sin duda, favorece la comunicación, puesto que filtran aquellos paquetes que circulan por la red y no están destinados a ninguno de los equipos conectados a esa parte de la red.

Los paquetes de datos son enviados y recibidos a través de los puertos de comunicación, que forman parte, a su vez, de una de las capas de comunicación TCP/IP. Estos puertos, por defecto están cerrados con el fin de aumentar la seguridad de la conexión, por lo que es preciso abrirlos para poder recibir datos a través de ellos.

Existen aplicaciones que permiten monitorizar el estado de las redes, su tráfico, la velocidad, los errores de conexión, etcétera. Sin embargo, los sistemas operativos proporcionan, a través de los comandos, las herramientas básicas que permiten obtener información de los paquetes que son enviados o recibidos y hacernos una idea del estado de la red.

Las redes han ido tradicionalmente por vía cableado, como Ethernet, coaxial o fibra óptica. Actualmente, sin embargo, es más frecuente ver redes inalámbricas, ya que proporcionan una mayor movilidad de los equipos y suponen un ahorro en la instalación de cableado. A pesar de las ventajas, las conexiones Wi-Fi se enfrentan a problemas de seguridad, por estar basadas en dispositivos que emiten la información a través del espacio, pudiendo ser ésta interceptada por cualquiera que se halle dentro del radio del emisor. Para evitar que terceros puedan obtener la información de los usuarios de la red, los dispositivos inalámbricos incorporan una clave de encriptación que es necesaria para poderse conectar y poder descifrar los datos recibidos.

DESARROLLO DE APLICACIONES MULTIPLATAFORMA



CEAC

Formación Profesional Oficial

Módulo: Sistemas informáticos

Unidad: Gestión de recursos en una red

INICIATIVA Y COORDINACIÓN
Centro de Estudios CEAC

COLABORADORES
Realización:
ITACA (Interactive Training Advanced Computer Aplications, S.L.)

Elaboración de contenidos:
Dan Triano
Ingeniero Técnico en Informática de Sistemas por la Universidad Autónoma de Barcelona

Actualización de contenidos:
ISCA Training & Consulting, S.L.
Amparo Sota
Responsable de la creación y gestión de las páginas de venta online de diferentes productos y servicios (Habemus, Knownet, Merioliva, Fotos y bodas). Responsable del proyecto "talleres de compra online página web Eroski.es".

Supervisión técnica y pedagógica:
Departamento de Enseñanza de Centro de Estudios CEAC

Coordinación editorial:
Departamento de Producto de Centro de Estudios CEAC

Primera edición, primera reimpresión: mayo 2021

ISBN: 978-84-1300-607-9 (Obra completa)
ISBN: 978-84-1300-608-6 (Sistemas informáticos)

Depósito Legal: B 2081-2021

Impreso por:
SERVINFORM
Avenida de los Premios Nobel, 37
Polígono Casablanca
28850 Torrejón de Ardoz (Madrid)

Printed in Spain
Impreso en España

ÍNDICE

6. GESTIÓN DE RECURSOS EN UNA RED

En esta unidad verás las configuraciones disponibles para poder gestionar aquellos recursos que normalmente son compartidos en una red de área local. Una de las principales funciones por las que se utilizan las redes de información es para compartir documentación entre los diferentes usuarios. Veremos que esto es posible fácilmente interconectando los ordenadores entre sí, pero es importante tener en cuenta aspectos de seguridad, como permisos y accesos para asegurar la confidencialidad de la información y que solo pueda ser accedida por las personas autorizadas.

Explicaremos los recursos que proporcionan los sistemas operativos, tanto servidor como local, para proporcionar la seguridad necesaria a los documentos compartidos. Explicaremos las diferencias entre los permisos de carpetas y archivos, y los derechos en la utilización de los sistemas a los que se accede por parte del usuario.

También veremos cómo crear conexiones a una red local desde el exterior, conservando la seguridad e integridad de la conexión y teniendo acceso a todos los recursos disponibles de la misma manera que si se realizase la conexión físicamente desde el mismo entorno. Hablaremos entonces de conexión VPN.

Por último, haremos especial hincapié en todos los temas de seguridad existentes en una red, desde los mencionados permisos de carpetas hasta los dispositivos cortafuegos y de control de tráfico y los programas de encriptación de la información, para evitar intrusiones externas a nuestro sistema.

6.1 Diferencias entre permisos y derechos. Permisos de red. Permisos locales. Herencia. Permisos efectivos. Denegación de permisos

En este apartado veremos las diferentes formas de las que disponemos para poder acceder a los recursos compartidos en red.

6.1.1 Diferencias entre permisos y derechos

En una red de área local, las máquinas interconectadas pueden compartir información con el resto de equipos conectados a la misma red. Para poder asegurar la confidencialidad de los archivos almacenados en cada ordenador, es necesario definir las **políticas de seguridad.**

Entendemos por **permisos**, la viabilidad de los usuarios o equipos de acceder y utilizar un recurso compartido: carpetas, archivos, discos duros, etc. En cambio, los derechos de usuario son las tareas que puede llevar a cabo un usuario dentro de una red o dominio, como puede ser iniciar sesión con un usuario y contraseña en un equipo de la red. Los administradores y, en ocasiones, los usuarios pueden establecer los permisos de las carpetas y ficheros para que puedan ser accedidos por otros equipos de la red. Depende del sistema operativo utilizado, podemos establecer diferentes permisos, los más comunes son: lectura, escritura, modificación y ejecución. Y pueden ser aplicados a equipos, usuarios y grupos (Figura 6.1).

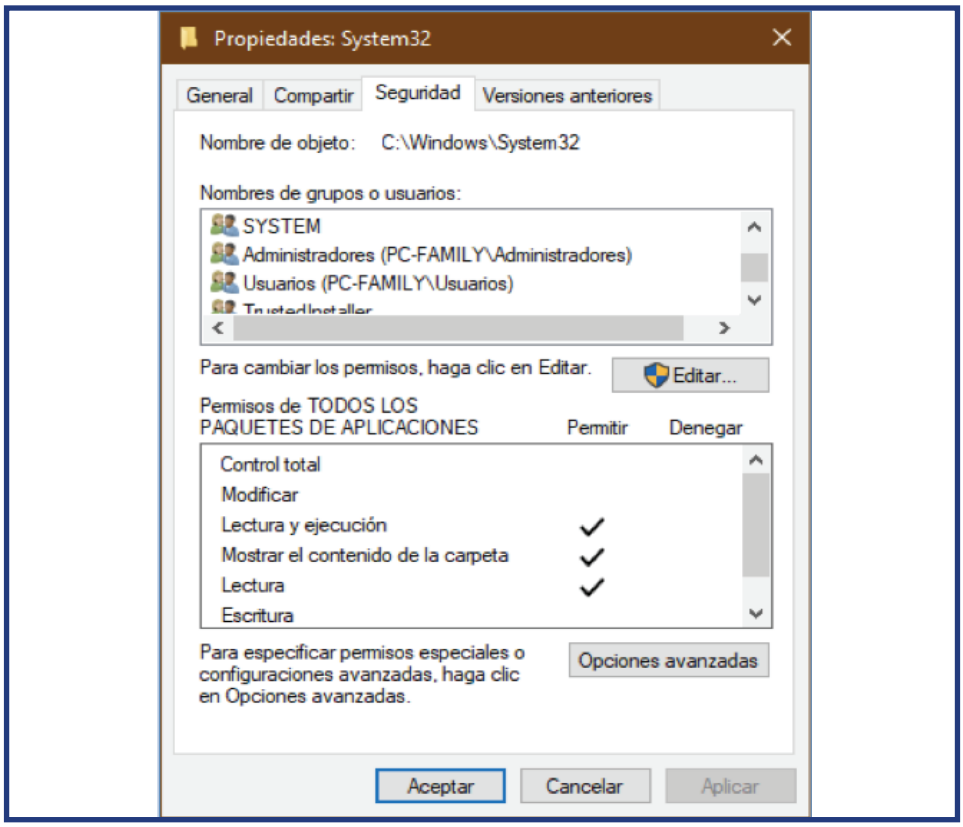


Figura 6.1
Pantalla para definir los permisos de una carpeta en el sistema operativo Windows.

6.1.2 Permisos de red

Los **permisos de red** son las credenciales que solicita un servidor para poder dar servicio a un *host* conectado a la red. Se pueden configurar los servidores para que den servicio de red (enrutamiento, DNS, conectividad) únicamente a los equipos que hayan sido iniciados con un nombre de usuario y contraseña reconocidos por el propio servidor. De esta manera, se limita el acceso a la red de cualquier equipo que se pueda conectar físicamente, pero que no tenga el permiso del administrador.

6.1.3 Permisos locales

Los **permisos locales,** así como los permisos de red, son las credenciales de los usuarios para poder acceder a recursos del sistema. La diferencia reside en que el ámbito de aplicación de estas políticas se limita al equipo que se está utilizando independientemente de si está conectado en red.

Cuando un usuario accede a un equipo, debe especificar si lo hará con un nombre de usuario de red o un nombre de usuario local, por lo que no es posible que existan incompatibilidades entre ambas políticas.

6.1.4 Herencia

Entendemos por **herencia** la propagación de los permisos, aplicados previamente a una carpeta, a todos los archivos y subcarpetas que contenga. De otra manera, obligaría al administrador a dar permisos archivo por archivo de manera individualizada. Esta herencia también se hace efectiva sobre los archivos y carpetas creados o movidos a una carpeta con permisos.

Al incorporar archivos o carpetas en una carpeta con la propiedad de herencia, todos los permisos serán aplicados automáticamente.

6.1.5 Permisos efectivos

Los **permisos efectivos** son aquellos en los que en caso de conflicto de permisos, se mantienen los más restrictivos. Imaginemos que una carpeta tiene políticas de lectura y escritura, y estos permisos son heredados a todos los archivos y subcarpetas que contiene. Podemos entonces aplicar a uno de estos archivos denegación de escritura. Existiría un conflicto entre el derecho de escritura heredado y la denegación de escritura asignado. La política más restrictiva, en este caso la denegación de escritura, se haría efectiva.

6.1.6 Denegación de permisos

La **denegación de permisos** es crear políticas restrictivas sobre un grupo de usuarios. Esto es utilizado cuando la mayoría de usuarios, pero no todos, pueden tener acceso a un recurso compartido. Es más rápido crear el recurso abierto, y denegar el acceso únicamente a aquellas personas que no deban tener acceso.

6.2 Derechos de usuarios. Directivas de seguridad. Objetos de directiva. Ámbitos de las directivas. Plantillas

Existen dos tipos de **derechos de usuario**, los derechos de inicio de sesión y los privilegios. Los derechos de inicio de sesión son, como indica su nombre, el derecho de un usuario a poder iniciar sesión dentro de un equipo conectado a la red. Suele hacerse para que solo las personas autorizadas puedan utilizar los equipos conectados a la red y para poder aplicar políticas de seguridad sobre los diferentes usuarios.

Los **privilegios**, en cambio, controlan el uso de los recursos del sistema por parte del usuario. Un ejemplo claro es impedir que el usuario, una vez haya iniciado sesión en una máquina, no pueda modificar la configuración del sistema (configuración de red, dispositivos, firewall, etc.) o instalar ningún tipo de software.

Las **directivas de seguridad** son configuradas en el servidor que proporciona conectividad a los equipos y define los derechos, permisos y privilegios de cada uno de los usuarios. Generalmente se utilizan grupos de usuarios a los que se les asigna dichas directivas de seguridad, que son heredadas a todos los usuarios que pertenezcan al grupo.

Los **objetos de directiva** son los elementos y servicios del dominio a los que se les aplica las políticas de seguridad. Un objeto de directiva podría ser la carpeta favoritos de un equipo, el panel de control, la cola de impresión, la fecha y la hora, etc.

Los **ámbitos de las directivas** son aquellos lugares dentro de la estructura organizativa del directorio donde se quiere aplicar las políticas de seguridad. Por ejemplo, un sitio web, un dominio o una subcarpeta del Active Directory.

Existen centenares de políticas y objetos de directiva, lo que hace difícil configurar todas ellas cuando contamos con un gran número de usuario o grupos. Los sistemas operativos servidor permiten crear **plantillas** que relacionen los objetos de directiva con los permisos que se desean asignar, de manera que podemos aplicar esta plantilla a los nuevos usuarios o grupos y aplicar únicamente los cambios necesarios.

6.3 Requisitos de seguridad del sistema y de los datos

Es necesario en cualquier red en la que se compartan datos mantener una estricta política de seguridad que no permita el acceso de terceros a la información. Una buena creación de políticas de seguridad aplicada a grupos y usuarios facilita al administrador del sistema el correcto mantenimiento de la seguridad sin necesidad de realizar modificaciones en los permisos.

Por **políticas de seguridad** entendemos todas aquellas normas de buen uso de los recursos que tengan acceso a Internet como, por ejemplo, no abrir correos de remitentes desconocidos, no acceder a páginas web que no sean fiables, analizar los dispositivos ***pendrive*** con el antivirus antes de abrirlos, etc.

Así como seguir una buena política de seguridad para los usuarios, también es necesario que los ficheros tengan correctamente asignados los permisos de lectura, escritura y modificación, y que ningún otro usuario pueda modificarlos intencionadamente o por error. Para proteger los datos del sistema local, como la carpeta c:/Windows, es conveniente aplicarles una política de solo lectura a todos los usuarios excepto el administrador. A esa carpeta no es posible aplicarle una política más estricta, puesto que, al ser archivos de sistema, será necesario su acceso para utilizar los servicios del sistema operativo.

Por otro lado, los archivos del usuario deberán estar concentrados en una única carpeta para facilitar su mantenimiento y copia de seguridad. Si no es posible guardar los documentos en un servidor de archivos, que sería la mejor opción, es recomendable guardarlos en ***Mis Documentos***, o incluso en una unidad diferente especialmente creada para almacenar datos "D:/". De esta manera, aunque falle el sistema los archivos, los documentos estarán a salvo en la otra unidad.

En cuanto a las instalaciones, una de las cosas más importantes es preparar el entorno para evitar que se puedan realizar intrusiones desde el exterior. Los dispositivos cortafuegos permiten que la comunicación fluya entre la red de área local y el exterior, al mismo tiempo que evita que entidades externas puedan acceder a nuestro sistema sin nuestro consentimiento.

Además, internamente, un usuario que reciba un correo electrónico infectado en su cuenta personal puede propagar el virus mediante el correo interno; por ello, es conveniente aplicar análisis de antivirus en el servidor de correo para que detecte y neutralice cualquier correo que pueda contener amenazas para el sistema. Por estas razones, es conveniente tener diferentes servidores para cada uno de los servicios de correo, archivos, comunicaciones, permisos de usuario, etc.; para que, en caso de fallo en el sistema o infección de un virus o intrusión, la amenaza no pueda traspasarse al resto de sistemas.

6.4 Seguridad a nivel de usuarios y seguridad a nivel de equipos

Hemos hablado de las políticas de seguridad que se aplican a los usuarios y a los grupos para poder utilizar los recursos de la red. Pero los sistemas operativos actuales permiten, además, crear políticas de seguridad aplicadas no solo a los **usuarios** que se identifican, sino también a los **equipos** conectados físicamente a la red (Figura 6.2).

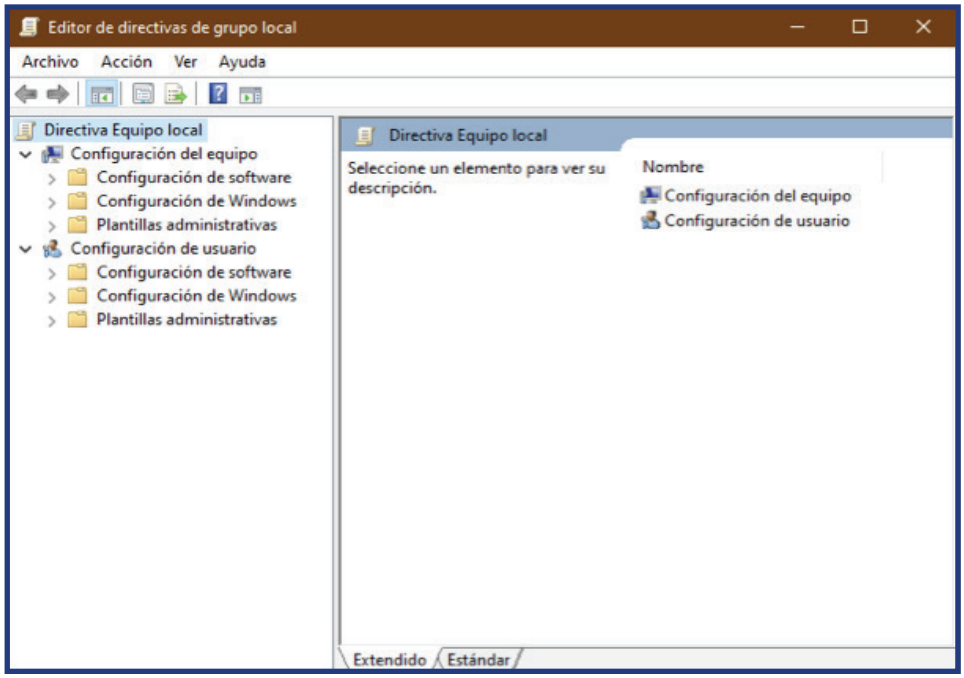


Figura 6.2
Pantalla en la que se visualizan las políticas de privacidad que se pueden aplicar al equipo o al usuario.

Por ejemplo, deseamos que los equipos que están en el área personal puedan tener acceso a la impresora de personal independientemente de los usuarios que estén utilizando los equipos. En la pantalla en la que definimos las políticas de seguridad, veremos que podemos definir los permisos de los usuarios, de los equipos físicos o de ambos. En este caso, seleccionaremos cada uno de los equipos de personal y les daremos acceso a la cola de la impresión de personal. Cuando existe una incompatibilidad entre los permisos aplicados a un equipo y los otorgados a un usuario, se aplica la norma de los permisos efectivos, aplicando aquellas políticas más restrictivas.

Si un equipo nuevo es configurado para pertenecer a un Dominio, los permisos locales y de red son automáticamente aplicados al equipo; esta funcionalidad permite una rápida configuración para los equipos nuevos o formateados.

6.5 Servidores de archivos

Es común en empresas centralizar los **archivos** en un servidor que almacene toda la información. Esto es debido a que los equipos locales son más susceptibles de estropearse o incluso ser robados, mientras que el servidor tiene la capacidad de realizar copias de seguridad periódicamente.

Cualquier ordenador conectado a una red tiene la capacidad de convertirse en un servidor de ficheros, basta con aplicar políticas de seguridad sobre una carpeta y dar acceso a otros equipos. Pero, como hemos dicho anteriormente, el modelo a utilizar comúnmente es el del servidor de ficheros centralizados por las numerosas ventajas que proporciona (Figura 6.3).

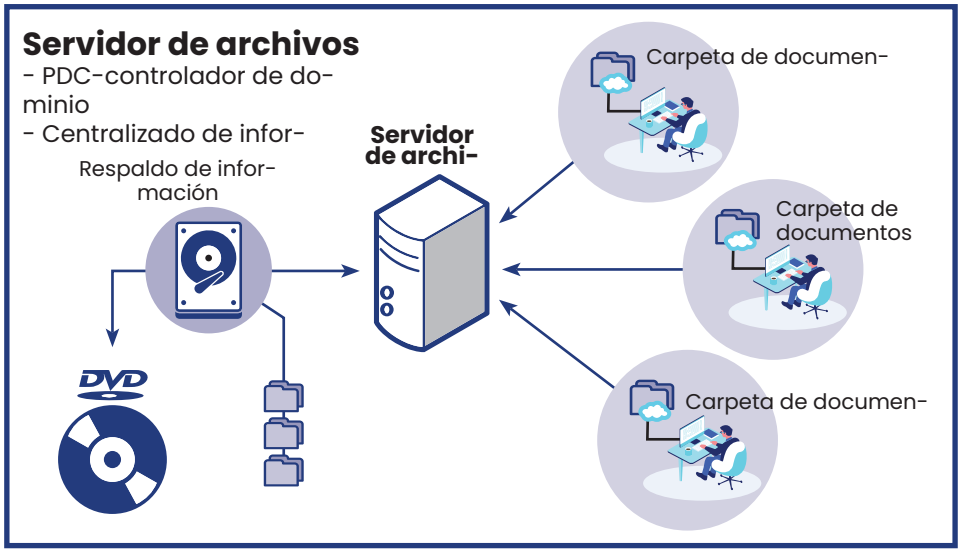


Figura 6.3
Esquema de una red que utiliza un servidor centralizado donde almacenar los archivos.

Existen problemas cuando almacenamos la información en servidores que tienen instalado un sistema operativo diferente al del cliente. Esto es debido a que la manera en la que se estructuran los directorios en un sistema Linux (montaje de unidades) no es la misma que en un sistema Windows (D:/Documentos). Esto provoca que los servidores Linux que deban dar servicio a equipos Windows deberán tener instalado un paquete de compatibilidad para dar servicio a los PC con sistemas operativos Microsoft. El paquete más utilizado actualmente para los servidores de archivos Linux es Samba (http://www.samba.org/).

Varios de los problemas que conlleva el uso de servidores clásicos de ficheros han hecho que en los últimos años cambie la forma de alojar los ficheros y acceder a ellos. El uso de dispositivos NAS primero y más tarde el alojamiento directamente en la nube han sido los dos métodos más utilizados para alojar información y ganar en seguridad y accesibilidad. Aun así, el uso de un servidor de archivos centralizado tiene ventajas frente a la dispersión en estaciones de usuario:

- **Compartición de la información.** Centralizar los archivos en una ubicación accesible para todos es una manera fácil de poder compartir la información a todos los usuarios sin necesidad de configurar permisos de red, ya que basta con copiar los archivos a las carpetas comunes del servidor.

- **Movilidad del usuario.** Normalmente, en una empresa cada empleado tiene su propio ordenador y, cuanto mayor sea el número de equipos, mayor es la posibilidad de que falle alguno de ellos. Tener centralizada la información supone no perderla en caso de que un equipo cliente deje de funcionar, ya que le bastará con cambiar el equipo y el usuario podrá acceder a la información que tenía anteriormente. Además, los servidores pueden ser configurados para ser accedidos desde fuera de la red a través de Internet, por lo que es posible acceder a la información desde cualquier parte del mundo.

- **Copias de seguridad y antivirus.** Tener centralizada toda la información supone un bajo coste en antivirus, puesto que, al no tener información sensible en los equipos locales, es posible adquirir las licencias únicamente para el servidor. Además, es mucho más factible realizar copias de seguridad de un solo equipo que de todos los de la empresa.

6.5.1 Tipos de servidores de archivos

Existen tres tipos de servidores de archivos en función de la administración de estos:

- **Servidor de discos virtuales.** Cada usuario dispone de una cuota de espacio reservado en el disco servidor. El servidor se encarga de emular la lectura y escritura del disco, mientras que el cliente tiene su propio administrador de archivos. La ventaja que supone este sistema es su fácil implementación, así como un espacio garantizado para cada usuario, ya que cada uno tendrá un tamaño asignado independiente de los demás otorgando mayor seguridad y privacidad a los documentos del usuario. El inconveniente es que, al estar los espacios aislados, no es posible compartir información con otros usuarios de manera sencilla y rápida. Además, es difícil gestionar la asignación de tamaños si se quiere modificar luego.

- **Servidor de archivos físicos.** Este tipo de servidores no soporta estructuras de directorios ni operaciones sobre el sistema de archivos. Las operaciones del usuario se basan en la creación, eliminación y modificación del contenido. Los archivos se van almacenando en el servidor y se guardan las referencias de la posición de disco donde se almacena. La ventaja de este sistema es que el tamaño de un usuario ya no es fijo

y puede ir utilizando los recursos de almacenamiento que vaya necesitando; el inconveniente sigue siendo el aislamiento de los usuarios, que no facilita la compartición de la información.

- **Servidor de archivos lógicos.** Este sistema es el más eficiente para compartir archivos a través de una red por su optimización en el tráfico de información. El sistema de archivos está definido en el servidor, por lo que no importa el sistema operativo que utilicen los clientes, ya que todos podrán acceder a la información de la misma manera.

  Además, a diferencia de los otros sistemas, con el servidor de archivos lógicos se puedan compartir los archivos entre los usuarios de manera sencilla. El inconveniente es que el servidor soporta una carga de trabajo mucho mayor, ya que se encarga de gestionar todo el sistema de archivos y sus permisos, así como las peticiones de acceso, lectura y escritura de todos los usuarios.

6.5.2 Sistemas múltiples

Generalmente, los equipos locales tienen sus propios discos locales en los que almacenar la información, por lo que es habitual trabajar de manera local en las tareas continuas y guardar los archivos en el servidor una vez finalizado el trabajo. Los sistemas operativos permiten acceder a los discos lógicos del servidor de dos maneras distintas:

• **Identificación de archivos ampliados:**

```
\\servidor\directorio\archivo
```

• **Discos remotos:** una funcionalidad de los sistemas operativos que permite enlazar una ubicación en el disco servidor con una unidad local, virtualizando el espacio del servidor y conceptualizándolo para que el usuario lo vea como una unidad local más:

```
F:/directio/archivo
```

6.5.3 Medidas de seguridad y problemas en el sistema de archivos

Cuando se almacena la información en servidores pueden existir numerosos problemas debido a la transmisión de los datos o errores en sistemas internos del servidor.

- **Actualización indivisible.** Si un programa abre un archivo directamente desde el servidor para modificarlo, es posible que, al realizar la actualización de los datos, exista algún problema en la comunicación o en el propio programa que provoque que no se guarde bien la información, provocando, además, que el archivo quede defectuoso y no puedan recuperarse los datos. Para solventar esto, se crea un archivo de versión múltiple. Al abrir un archivo se crea una copia que permanece oculta hasta el momento en el que se vuelve a cerrar el archivo. Si el archivo se ha cerrado correctamente, la copia es eliminada; por el contrario, si el programa genera algún error y no se corrige correctamente el archivo original, este es eliminado y sustituido por la copia. Esta práctica es habitual en los editores de texto: se puede hacer la prueba abriendo un documento de texto; verás que se crea un archivo oculto que desaparece en el momento de cerrar el editor de texto.

- **Almacenamiento estable.** Es posible que la información no se almacene bien por un error en el soporte físico del servidor. Las copias de seguridad se hacen generalmente por la noche y no pueden usarse para recuperar la información el mismo día en que se han generado, puesto que no ha habido tiempo para realizarse la copia de seguridad. Para ello se pueden utilizar dos discos idénticos para almacenar la información: un archivo es guardado en un primer disco y, si no hay errores, se copia en un segundo disco idéntico de manera que, si falla uno de los dos discos, puede ser sustituido fácilmente por otro.

- **Sistema multicopia.** El sistema multicopia se basa en la aplicación de los dos sistemas anteriores, pero utilizando un mismo soporte físico. Se realizan copias de seguridad al abrirse un archivo pero al mismo tiempo existen dos copias de cada archivo, y cada copia está en lugares diferentes del disco. Es muy difícil que se corrompan dos sectores diferentes del disco duro; pero, si la unidad completa se estropea, se perderán todos los datos.

- **Concurrencia de archivos.** Los controles de acceso múltiple permiten bloquear el archivo cuando está siendo modificado por diferentes usuarios. Los pasos para realizar el bloqueo son: bloquear, leer, actualizar, desbloquear.

  Se puede crear un límite de tiempo por el que un usuario puede realizar un bloqueo a un archivo; lo que es una práctica habitual para evitar que se monopolice un recurso compartido. Si el programa que está ejecutando un archivo se interrumpe inesperadamente, se deberá controlar para levantar el bloqueo desde el sistema. Si es un archivo local, será el administrador de archivos quien levante el bloqueo; mientras que, si es un servidor, el administrador de archivos local avisará al servidor para que realice el desbloqueo. Si la máquina local cae y no puede avisar al

servidor, este detectará la desconexión del equipo y eliminará el bloqueo sobre todos los archivos abiertos por el usuario.

- **Transacciones.** Las transacciones son un conjunto de instrucciones que funcionan de manera automática, es decir, han de ejecutarse todas o ninguna. Estas instrucciones son indivisibles y, a pesar de ejecutarse una por una, si alguna de ellas no se puede llevar a cabo, el resto de acciones realizadas hasta el momento se desharán, devolviendo los archivos a su estado original antes de iniciar la transacción.

6.6 Servidores de impresión

Actualmente, existen impresoras que pueden ser conectadas a una red de área local mediante cableado Ethernet o *Wi-Fi.* Cuando el número de impresoras es elevado y se quiere controlar su uso por parte de los usuarios, es posible centralizar el servicio de impresión de todas las impresoras a un servidor central que aplica las políticas de seguridad de los usuarios para permitir o denegar el uso de las impresoras.

Para las impresoras que no pueden ser conectadas directamente a la red, es posible conectarlas mediante USB al **servidor de impresión**, de manera que puedan tener acceso a ella todos los usuarios de la red.

Los servidores de impresión ponen a disposición de los usuarios la posibilidad de utilizar un impresora conectada a red. Para ello ha de crear una cola de impresión donde se irán situando las peticiones de los usuarios a medida que lleguen. Al tratarse de varios usuarios intentando utilizar el mismo recurso, es necesario establecer este servicio para mantener un orden de las peticiones entrantes.

En sistemas Microsoft, la creación de servidores de impresión es uno de sus servicios nativos; mientras que en sistemas operativos Linux es necesario instalar un módulo que proporcione el servicio. Actualmente, el más utilizado es CUPS (http://www.cups.org/), que proporciona conectividad a los equipos conectados, y una cola de impresión para poder administrar las conexiones.

Existen dispositivos de interconexión parecidos, los hub, en los que se conectan las impresoras vía USB a la toma Ethernet. Estas impresoras serán visibles por el resto de hosts de la red, que podrán utilizarlas como cualquier otra impresora de red sin necesidad de crear un servidor de impresión (Figura 6.4).

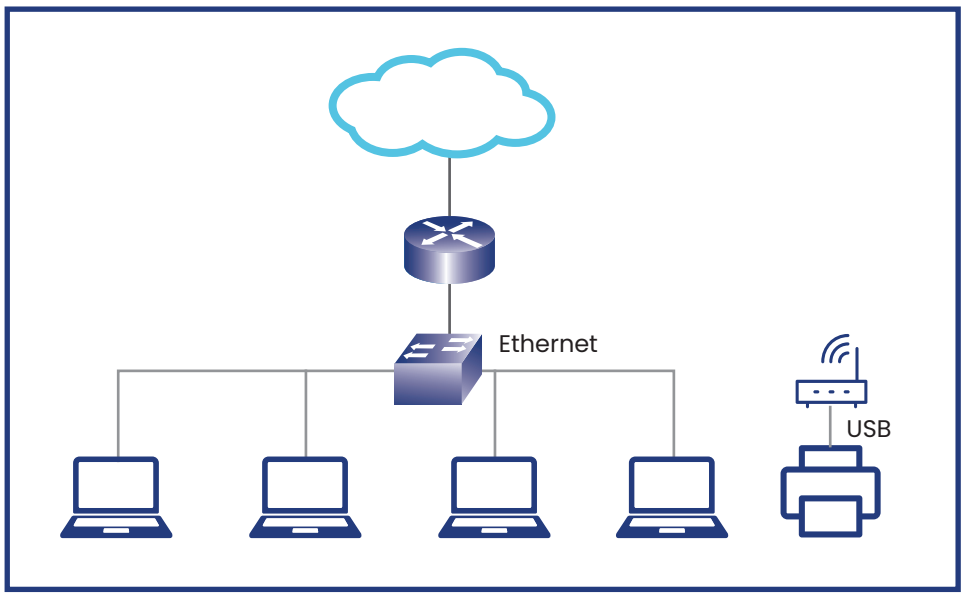


Figura 6.4
Dispositivo que conecta una impresora USB a la red mediante una conexión inalámbrica, creando un servidor de impresión accesible por el resto de usuarios.

6.7 Servidores de aplicaciones

Se llama servidores de aplicaciones a aquellos servidores que proporcionan a los usuarios de una red el acceso a una aplicación instalada en el equipo y corresponde al concepto de sistema distribuido. Esta opción es recomendable en aquellas empresas en las que un mismo software es utilizado por muchos empleados. Las ventajas de la utilización de un sistema distribuido son:

- La **alta disponibilidad,** ya que estos sistemas suelen estar funcionando veinticuatro horas al día durante todo el año.

- El **mantenimiento** es menor, ya que las actualizaciones o cambios realizados en la aplicación solo deberán efectuarse en la máquina central, mientras que en un sistema cliente habría que aplicar los cambios a todas y cada una de las máquinas en las que el software estuviese instalado. Esto incluye la escalabilidad, es decir, la ampliación del software para cumplir con nuevas necesidades.

- **Centralización** de los datos accesibles desde cualquier máquina de manera instantánea por parte de cualquier usuario (Figura 6.5).

La utilización de estos sistemas también supone algún inconveniente, como la **caída total del sistema** en caso de fallo en el servidor, tanto en la aplicación como en el resto del sistema, que supondría que todos los usuarios que utilizan la aplicación se quedarían sin servicio. Sin embargo, en una distribución local un error en una sola máquina no afecta al resto de usuarios.

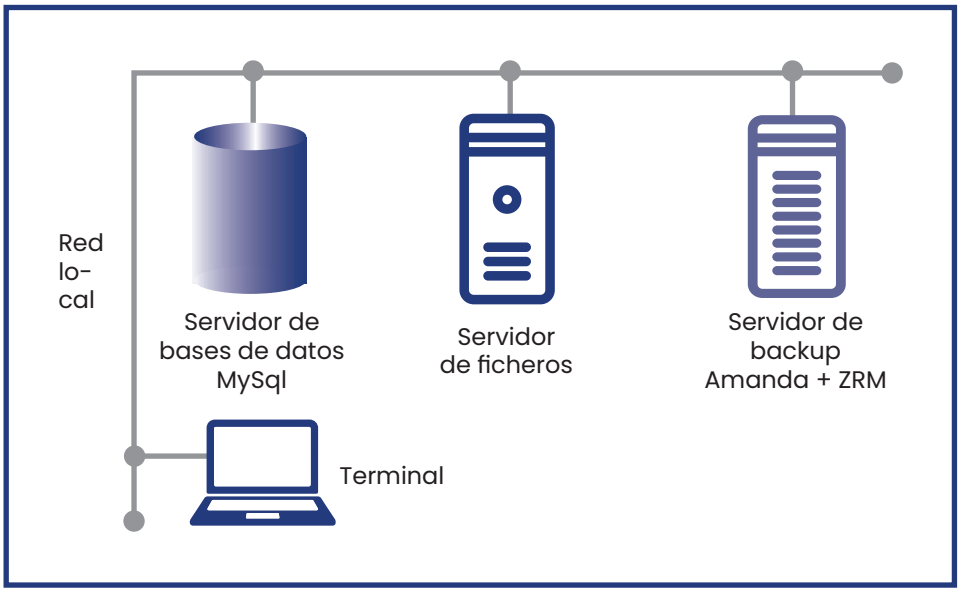


Figura 6.5
Sistema distribuido en el que los recursos de una aplicación son repartidos entre varios servidores.

6.8 Técnicas de conexión remota

Es posible facilitar el trabajo de un administrador de sistemas mediante la utilización de conexiones remotas. Este sistema permite entrar en ordenadores de manera remota a través de su IP y utilizarlo como si la persona estuviera delante. Es habitual la utilización de programas cuando se da soporte a los usuarios, haciendo que el informático no deba moverse de su puesto para solucionar casi cualquier problema en el otro equipo. Lo único que necesita es que el ordenador funcione y ejecute el servicio de control remoto de manera local.

Otra situación en la que es habitual utilizar conexiones remotas es cuando el ordenador no tiene conectado ningún periférico de entrada o salida (monitor, teclado, ratón), como, por ejemplo algunos servidores. Estos programas permiten utilizar los equipos a distancia incluso en estas situaciones y permiten solucionar problemas en los servidores a cualquier hora sin necesidad de estar en el mismo lugar que la máquina.

Existen aplicaciones que, una vez instaladas en una máquina, permiten acceder a ella desde cualquier otro equipo que esté conectado en la red simplemente conociendo las claves de acceso. Algunas de las más utilizadas son **TeamViewer** (http://www.teamviewer.com/) para asistencia técnica, ya que es de uso puntual, y **VNC** (http://www.realvnc.com/) para ordenadores de empresa en los que se puede acceder sin autorización expresa del usuario.

El sistema operativo Windows dispone de un servicio nativo que ofrece esta posibilidad llamado escritorio remoto. El protocolo que utiliza la aplicación de **escritorio remoto** de Windows se llama RDP (Remote Desktop

Protocol). RDP es un protocolo propietario desarrollado por Microsoft que permite la comunicación en la ejecución de una aplicación entre un terminal y un servidor Windows, que recibe la información en el terminal a través de la pantalla, el teclado y el ratón.

La diferencia con la otras aplicaciones similares es que no permite compartir el mismo escritorio, sino que accede a la máquina por una puerta trasera mediante un usuario y contraseña de Windows (Figura 6.6).

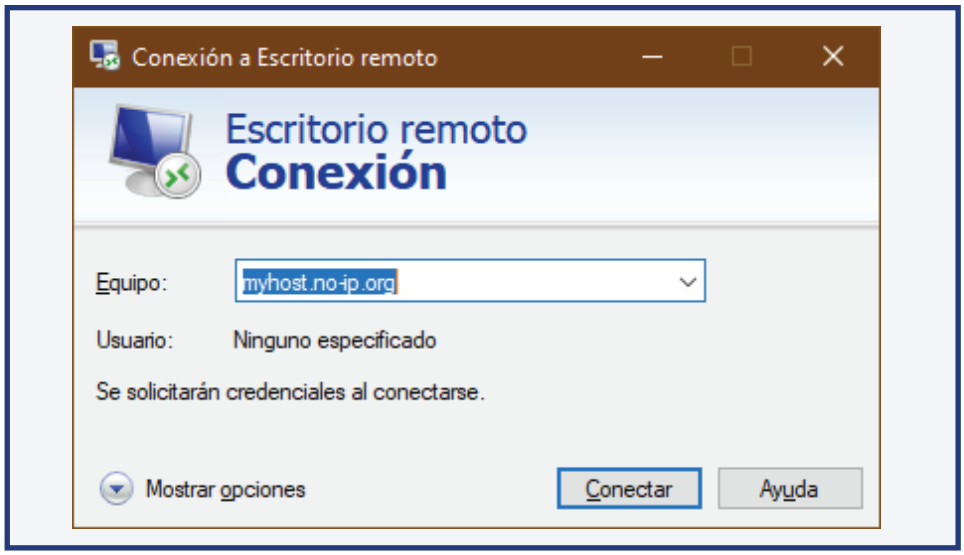


Figura 6.6
Ventana de la aplicación Escritorio remoto de Windows para acceder a un equipo mediante IP o nombre de red.

Las técnicas de conexión remota hay que utilizarlas con prudencia en equipos locales utilizados por los usuarios, puesto que hay que tener en cuenta temas como la privacidad o la protección de datos confidenciales. Es recomendable siempre avisar al usuario que se va a acceder a su equipo antes de hacerlo.

6.9 Herramientas de cifrado

Cuando es necesaria una gran seguridad en la transmisión de datos, es posible utilizar un software que encripta la información mediante un sistema de claves públicas y privadas generadas por los usuarios.

El emisor encripta toda la información con la clave privada y otorga al receptor una clave pública con la que puede descifrar los datos que vaya recibiendo. Es el sistema más efectivo que existe actualmente para poder transmitir la información de manera segura, siempre y cuando las claves privadas no sean descubiertas por terceros (Figura 6.7).

Para saber más

Una herramienta de cifrado que actualmente está integrada en muchos sistemas operativos de código libre es Gnupg (http://www.gnupg.org)

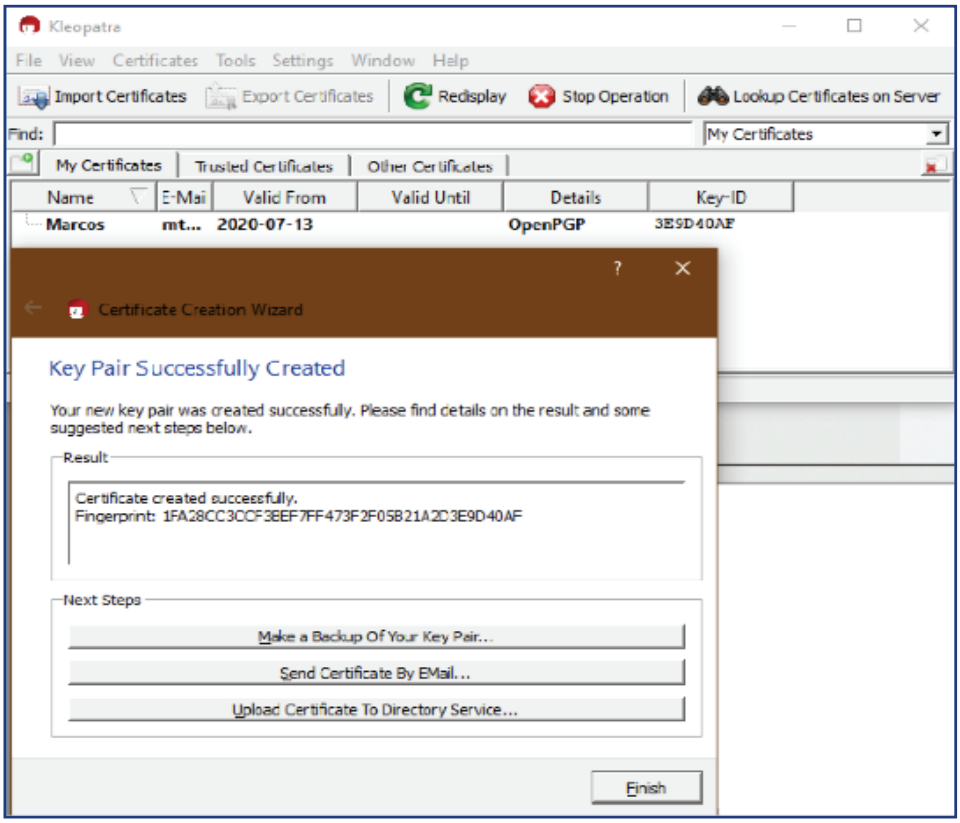


Figura 6.7
Software de cifrado en el que hay diferentes firmas para autentificar y cifrar los datos.

Hay numerosos tipos de cifrado dependiendo del algoritmo utilizado y la decisión de cuál escoge reside en el nivel de seguridad, el tiempo de codificación, la compatibilidad con el software utilizado, etc.

Las herramientas de cifrado son instaladas en los sistemas operativos servidores para encritpar toda la información que es transmitida a través de ellos. Hay software como GNU Privacy Guard, compatible con todas las plataformas que en ocasiones viene instalado y configurado de serie en algunos sistemas operativos de código libre orientados a ofrecer servicios web o de comunicación, lo que elimina el trabajo que supone su instalación y configuración por parte del administrador.

6.10 Herramientas de análisis y administración

Es importante para el administrador comprobar el rendimiento de los equipos, sobre todo del servidor, y comprobar que responde correctamente a todas las peticiones de manera eficaz y en un tiempo de respuesta aceptable.

Existen herramientas que permiten realizar un seguimiento de los recursos del sistemas y realizar un informe que detalle la forma en la que los equipos responden a las peticiones de servicio para comprobar el correcto funcio-

namiento de los sistemas. Pese a que existen herramientas nativas en los sistemas operativos (Figura 6.8), es habitual instalar software externo que realiza análisis más precisos y exhaustivos, como AVG TuneUp (https://www.avg.com/es-es/avg-pctuneup/).

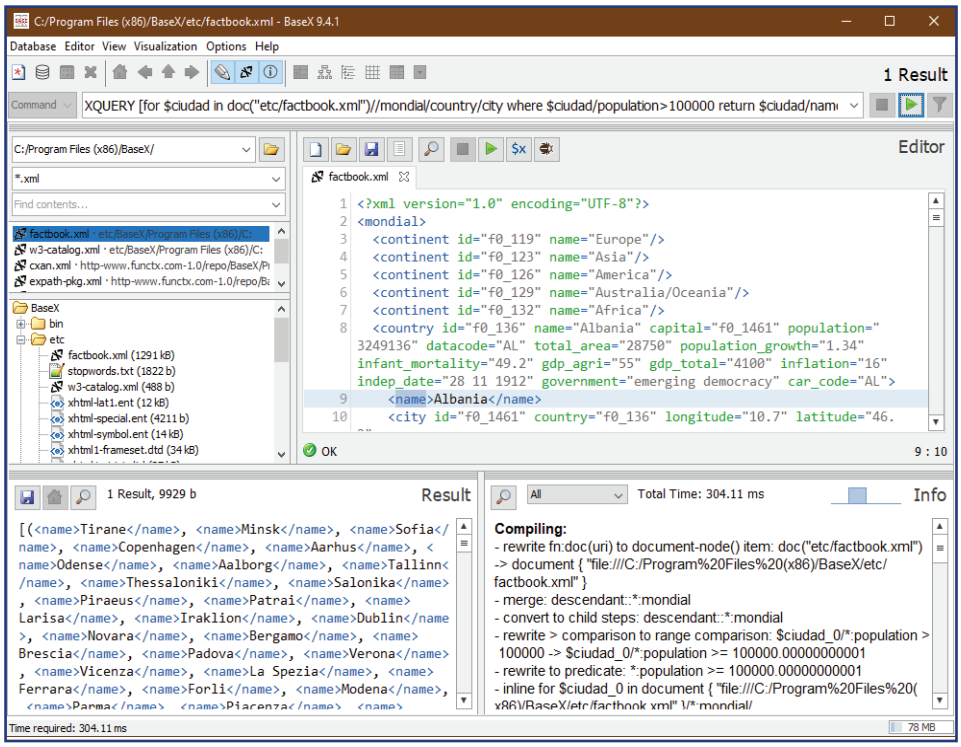


Figura 6.8
Análisis del monitor de rendimiento de Microsoft Windows.

Estos análisis son utilizados para medir el rendimiento del equipo y el uso de sus recursos. Unos resultados en los que la gráfica de procesamiento y memoria lleguen a límites muy altos pueden suponer una necesidad de aumentar el hardware para poder dar servicios a todos los procesos que necesitan ser ejecutados. Una alternativa a realizar una costosa inversión en recursos de hardware sería una limpieza de todos los programas y servicios que se están ejecutando.

En ocasiones, hay procesos que desconocemos que se están ejecutando y que muy posiblemente no sean necesarios en el equipo. Un buen mantenimiento reduce considerablemente el consumo de recursos en un equipo.

Existe otra razón por la que puedan darse altos niveles de utilización de los recursos y es un ataque exterior o un virus en el equipo. Existen virus cuya función es ejecutar servicios que requieren un alto nivel de procesamiento, lo que satura el procesador; o escriben datos en memoria hasta desbordar su capacidad. Estos virus son fácilmente detectables con un análisis de antivirus o analizando los servicios que más recursos consumen y buscar en Internet a qué programas pertenecen. Cuando el problema es la transmisión de datos, sobre todo en un servidor web, es posible que se esté sufriendo un ataque de denegación de cceso, que se basa en saturar un

servidor con un gran número de peticiones de acceso, desbordando su capacidad de procesarlas.

Por otro lado, existen herramientas para poder administrar los servidores de una manera remota mediante una interfaz web accesible insertando un usuario y una contraseña, y configuradas para poder ser utilizadas incluso desde el exterior de la red, siempre que se den los permisos adecuados.

Estas herramientas permiten administrar aspectos como usuarios, servidores, PHP, MySQL, DNS, Samba o DHCP, entre otros. Algunas de estas herramientas son **Webmin**, **Plesk** y **cPanel** (Figura 6.9).

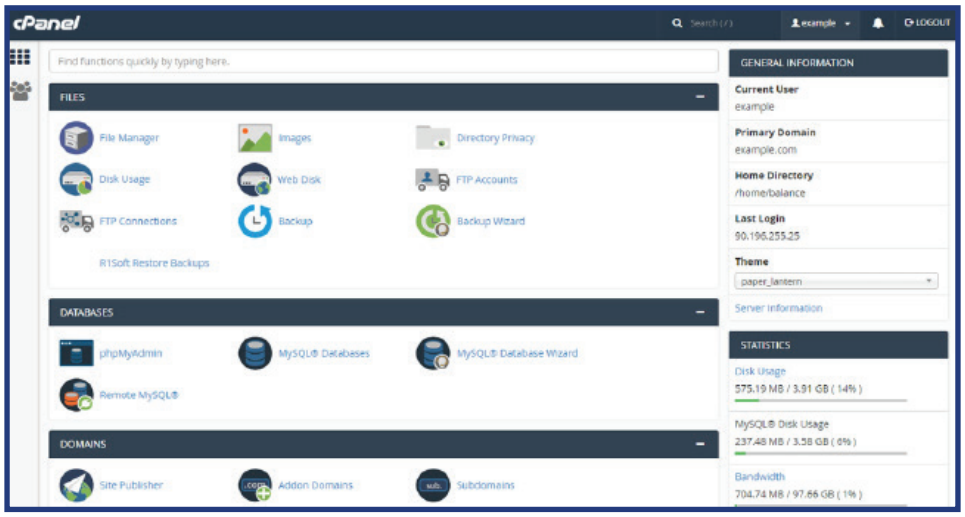


Figura 6.9
Ejemplo del panel de control cPanel.

6.11 Cortafuegos

Los cortafuegos son mecanismos que se utilizan para limitar el tráfico no deseado en una red. Suelen situarse cómo último nodo antes de salir al exterior de una red. Por ejemplo, entre el *router* y el servidor.

Un cortafuegos protege de los accesos producidos desde el exterior de una red, pero no evita los ataques o negligencias producidos por usuarios que ya existen dentro de la red. Para una mayor seguridad, es posible colocar cortafuegos en las diferentes secciones de una red, por ejemplo, situando un dispositivo cortafuego conectado a los ordenadores del departamento de personal para evitar que personas de la empresa intenten acceder a los datos de estos equipos (Figura 6.10).

Las diferencias entre los diferentes tipos de cortafuegos residen en las capas en que se aplican los filtros:

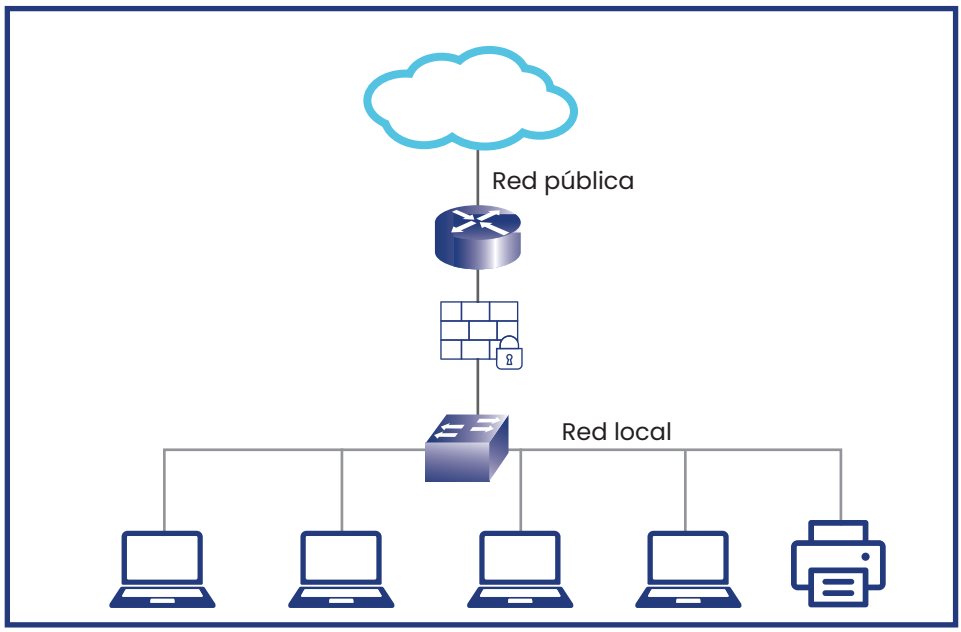


Figura 6.10
Esquema de una red aislada del exterior mediante un cortafuegos que filtra las conexiones entrantes.

- **Nivel de aplicación de pasarela**. Aplica los mecanismos de filtrado para aplicaciones especificas, como servidores FTP o Telnet.

- **Circuito a nivel de pasarela.** Aplica los mecanismos de filtrado y seguridad en conexiones, realizadas mediante TCP o UDP. Una vez establecidas las conexiones, los paquetes son transmitidos entre los nodos sin más controles por parte del cortafuegos.

- **Cortafuegos de capa de red o de filtrado de paquetes**. Analiza los paquetes IP en el nivel de red (capa 2 del modelo TCP/IP). En este nivel se pueden filtrar los paquetes recibidos según información sobre su procedencia, IP origen, IP destino, puerto de salida, MAC, etc.

- **Cortafuegos de capa de aplicación.** Trabaja en el nivel de aplicación (capa 8 del modelo TCP/IP). De esta manera se puede filtrar según las características propias a este nivel de información. Un ejemplo sería filtrar una entrada del protocolo HTTP según la URL de procedencia.

- **Cortafuegos personal.** Este cortafuegos está basado en un software instalado en la máquina cliente que filtra las conexiones entrantes en el equipo a través del software de manera personalizada.

Existen dos tipos de política basadas en la manera en la que el cortafuegos procesa las peticiones:

- **Política restrictiva.** Se niega el acceso a cualquier conexión externa excepto aquellas que han sido previamente definidas como permitidas por parte del administrador del sistema.

- **Política permisiva.** Se permite todo el tráfico excepto el que esté explícitamente denegado mediante una lista negra de direcciones IP.

6.12 Sistemas de detección de intrusión

Un sistema de detección de intrusos (o **IDS**, de sus siglas en inglés *Intrusion Detection System*) es un software que generalmente se instala en el servidor que proporciona conectividad a la red y que por lo tanto tiene acceso al exterior y se utiliza para analizar los paquetes entrantes y su procedencia para detectar si provienen de una fuente fiable y comprobar que la conexión se ha realizado por una petición desde dentro, una petición que ha sido iniciada desde un host que forma parte de nuestra red interna (Figura 6.11).

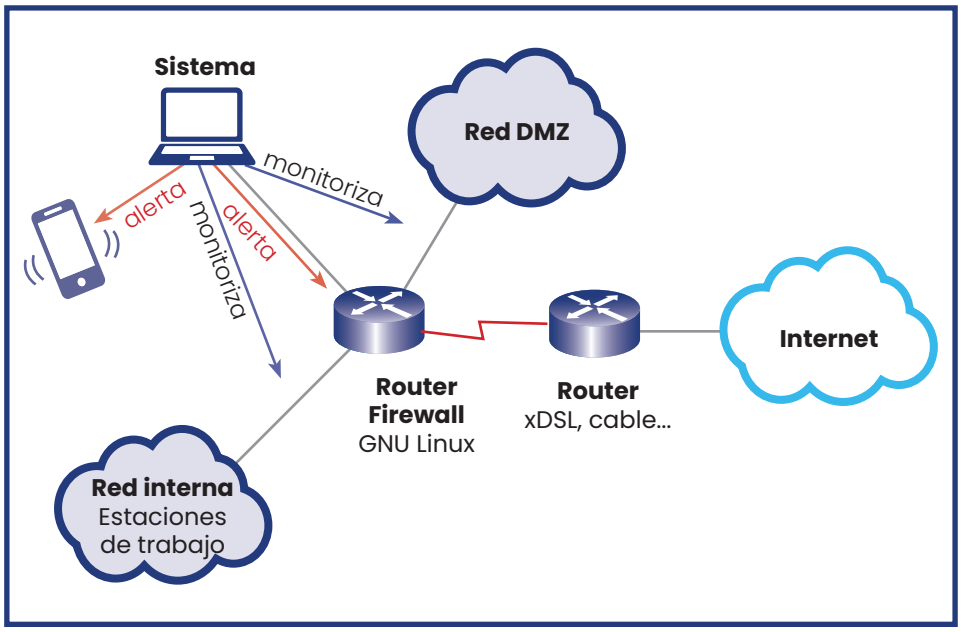


Figura 6.11
El sistema IDS avisa a los usuarios administradores cuando detecta una intrusión mediante la monitorización del tráfico.

Los IDS utilizan sensores virtuales para analizar el tráfico en busca de anomalías que pueda considerar ataques. Suele integrarse junto al firewall para que éste bloquee los accesos que el IDS identifica como inseguros.

Una parte importante de los IDS es su base de datos, en la que almacena todas las firmas de las procedencias no seguras, y que constantemente se va actualizando a medida que se reportan nuevos ataques.

Para poder diferenciar entre las conexiones autorizadas y las peligrosas, además de utilizar su base de datos, el sistema IDS utiliza una heurística

que analiza el estado habitual de la red (como, por ejemplo, ancho de banda, puertos utilizados, tamaño de los paquetes) y avisa de aquellas conexiones que no corresponden con los patrones que tiene establecidos.

Resumen

Los equipos conectados a una red han de responder a dos clases de políticas: las políticas de usuario, propias del sistema operativo, que se aplican a los archivos locales; y las políticas de seguridad y acceso a recursos, que se aplican a los equipos conectados a la red.

Debemos diferenciar entre los permisos utilizados para el acceso a archivos y carpetas, y los derechos de los usuarios, que son definidos para la utilización de los recursos de red, como pueden ser unidades de almacenamiento o impresoras que no están conectadas en local al equipo.

En una red de área local es posible configurar un servidor central para ofrecer los servicios de impresión, almacenamiento o aplicación al resto de equipos de manera centralizada. Se trata de una manera, por parte del administrador, de tener controlados los recursos de la red y facilitar la aplicación de las políticas de seguridad, sí como los derechos de los usuarios sobre estos servicios.

Las aplicaciones de control remoto permiten a los administradores y personal técnico acceder a los equipos a distancia y utilizarlos con facilidad. Se trata de un recurso muy utilizado, tanto en la reparación de ordenadores como en la administración de los servidores para su mantenimiento.

Los cortafuegos (firewall) son dispositivos físicos o software conectado entre la red de área local y la conexión al exterior. Son los encargados de filtrar todas aquellas conexiones entrantes que no son autorizadas. Generalmente, los firewall están configurados para discriminar cualquier conexión, y será el administrador quien deberá abrir los puertos por las que quiera permitir las conexiones.

Ejercicios de autocomprobación

Indica si las siguientes afirmaciones son verdaderas (V) o falsas (F):

1. Es necesario definir las políticas de seguridad para poder asegurar la confidencialidad de los archivos almacenados en cada ordenador.

2. Los administradores y los usuarios pueden establecer los permisos de lectura, escritura, modificación y ejecución de las carpetas y ficheros para que puedan ser accedidos por otros equipos de la red.

3. Se limita el acceso a la red de cualquier equipo que se pueda conectar físicamente, pero que no tenga el permiso del administrador.

4. Impedir que el usuario, una vez haya iniciado sesión en una máquina, no pueda modificar la configuración del sistema (configuración de red, dispositivos, firewall, etc.) o instalar ningún tipo de software es un ejemplo de privilegio.

5. Es necesario en cualquier red en la que se compartan datos mantener una estricta política de seguridad que no permita el acceso de terceros a la información.

6. Los sistemas operativos actuales no permiten crear políticas de seguridad aplicadas a los usuarios que se identifican, ni a los equipos conectados físicamente a la red.

7. Es común en empresas centralizar los archivos en un servidor que almacene toda la información.

8. Los cortafuegos (firewall) son dispositivos físicos o software conectado entre la red de área local y la conexión al exterior. Son los encargados de filtrar todas aquellas conexiones entrantes que no son autorizadas. Generalmente, los firewall están configurados para discriminar cualquier conexión, y será el administrador quien deberá abrir los puertos por las que quiera permitir las conexiones.

Completa las siguientes afirmaciones:

9. Centralizar los _____ en una ubicación accesible para todos es una manera fácil de poder compartir la _____ a todos los usuarios sin necesidad de configurar permisos de _____, ya que basta con copiar los archivos a las carpetas comunes _____.

10. Las aplicaciones de control remoto permiten a los _____ y personal técnico acceder a los equipos a distancia y utilizarlos con facilidad. Se trata de un _____ muy utilizado, tanto en la reparación de _____ como en la administración de los _____ para su mantenimiento.

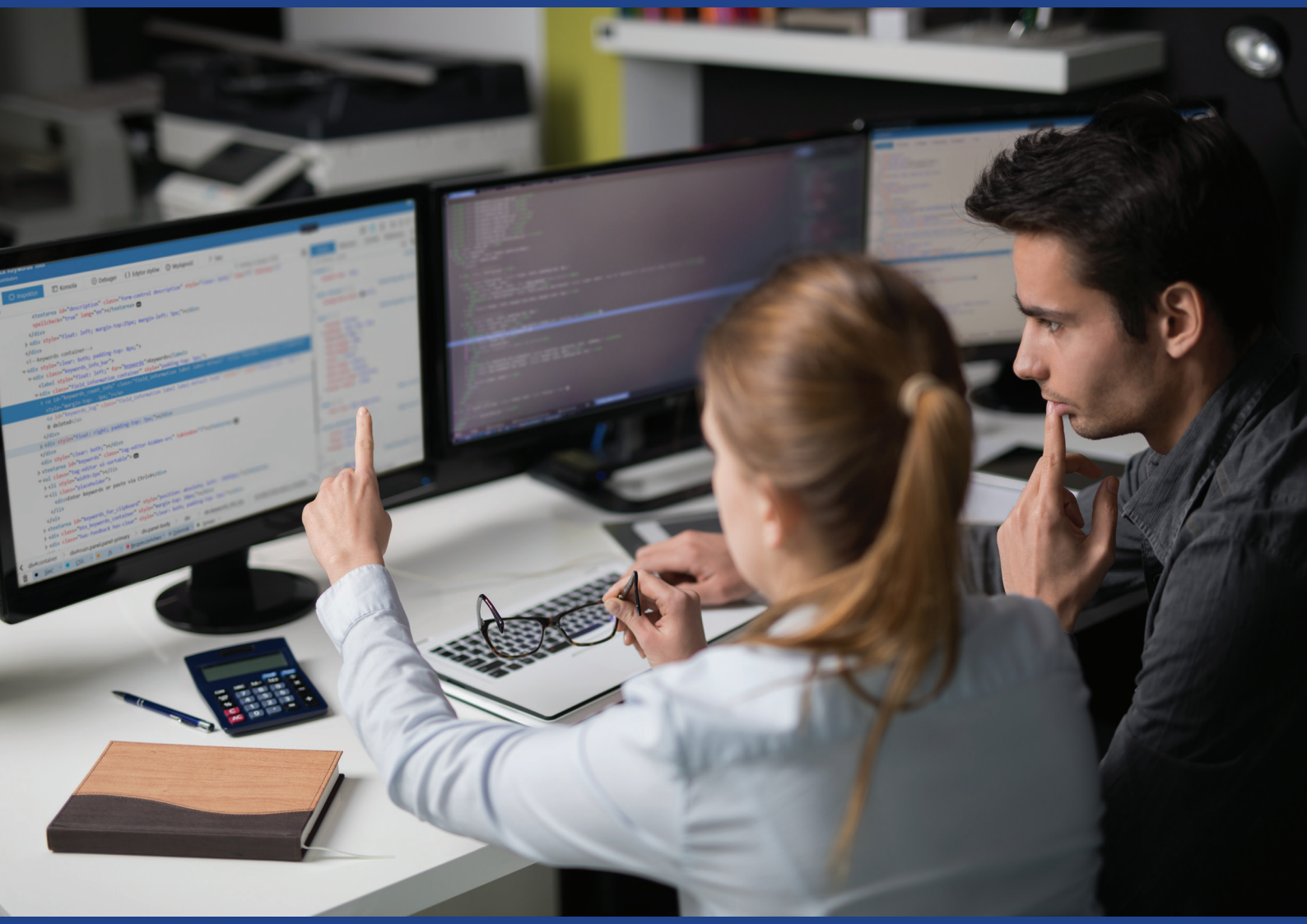
Soluciones de los ejercicios de autocomprobación

Unidad 6

1. V
2. V
3. V
4. V
5. V
6. F. Los sistemas operativos actuales permiten crear políticas de seguridad aplicadas a los usuarios que se identifican, sino también a los equipos conectados físicamente a la red.
7. V
8. V
9. archivos, información, red, servidor.
10. administradores, recurso, ordenadores, servidores.

ÍNDICE

DESARROLLO DE APLICACIONES MULTIPLATAFORMA



CEAC

Formación Profesional Oficial

Módulo: Sistemas informáticos

Unidad: Explotación de aplicaciones informáticas de propósito general

INICIATIVA Y COORDINACIÓN
Centro de Estudios CEAC

COLABORADORES
Realización:
ITACA (Interactive Training Advanced Computer Aplications, S.L.)

Elaboración de contenidos:
Dan Triano
Ingeniero Técnico en Informática de Sistemas por la Universidad Autónoma de Barcelona

Actualización de contenidos:
ISCA Training & Consulting, S.L.
Amparo Sota
Responsable de la creación y gestión de las páginas de venta online de diferentes productos y servicios (Habemus, Knownet, Merioliva, Fotos y bodas). Responsable del proyecto "talleres de compra online página web Eroski.es".

Supervisión técnica y pedagógica:
Departamento de Enseñanza de Centro de Estudios CEAC

Coordinación editorial:
Departamento de Producto de Centro de Estudios CEAC

Primera edición, primera reimpresión: mayo 2021

ISBN: 978-84-1300-607-9 (Obra completa)
ISBN: 978-84-1300-608-6 (Sistemas informáticos)

Depósito Legal: B 2081-2021

Impreso por:
SERVINFORM
Avenida de los Premios Nobel, 37
Polígono Casablanca
28850 Torrejón de Ardoz (Madrid)

Printed in Spain
Impreso en España

ÍNDICE

7. EXPLOTACIÓN DE APLICACIONES INFORMÁTICAS DE PROPÓSITO GENERAL

En esta unidad analizaremos los tipos de software existentes en el mercado y los clasificaremos según su propósito y su tipo de licencia. Veremos que existen tres tipos de software destinados a proporcionar servicio de sistema, programación o aplicación y que, a su vez, pueden dividirse entre programas de pago o de licencia libre.

Veremos los requisitos que suelen necesitar las aplicaciones para poder funcionar correctamente en un equipo y los explicaremos en profundidad para entender mejor las razones por las que en ocasiones los equipos experimentan un bajo rendimiento cuando se ejecutan algunas aplicaciones.

Dedicaremos un apartado a las herramientas ofimáticas, dada su importancia actualmente. Se trata de paquetes especialmente diseñados para cubrir las necesidades profesionales facilitando la elaboración de documentación y presentaciones, así como la creación de hojas de cálculo especialmente pensadas para el mundo de las finanzas y la contabilidad.

Explicaremos en qué consisten las herramientas que se han ido desarrollando con el tiempo basadas en Internet. Veremos cómo funcionan servicios y plataformas como redes sociales, foros, RSS, buscadores... y explicaremos qué necesidades cubren a los usuarios de Internet que las utilizan normalmente y cómo algunas de ellas están cambiando la manera de relacionarse de las personas.

Por último, analizaremos aquellas aplicaciones que son diseñadas para propósitos generales y pueden ser utilizadas en múltiples situaciones para dar servicio a las necesidades de usuarios y empresas. Podemos poner como ejemplos aplicaciones de antivirus, recuperación de datos, mantenimiento del sistema, entre otras.

7.1 Tipos de software

A pesar de poder diferenciar los tipos de software según muchos criterios diferentes, diferenciaremos tres grandes grupos en función del ámbito en el que se utilizan los programas:

- **Software de sistema**. Son los programas que funcionan a más bajo nivel para controlar el hardware y ser utilizado por el usuario, así como ofrecer los servicios más básicos de los sistemas. Dentro de esta categoría podemos encontrar los sistemas operativos, los controladores, servidores, utilidades y herramientas.

- **Software de programación.** Son las herramientas que utilizan los desarrolladores para poder crear nuevos software. Se considera un tipo de software diferente al resto por su naturaleza, ya que son programas utilizados para crear otros programas. En esta categoría podemos considerar algunos editores de texto, compiladores, depuradores, herramientas de control de versiones, etc.

- **Software de aplicación.** Son los programas que ofrecen un servicio al usuario y le permiten realizar tareas especificas. La lista de este tipo de software es realmente larga, puesto que comprende la mayoría del software existente; como aplicaciones ofimáticas, videojuegos, software de empresas, programas de diseño, etc.

Otra manera de dividir el software es el tipo de licencia con el que se adquiere. Básicamente, existen dos tipos:

- **Licencias de pago.** Son las aplicaciones desarrolladas generalmente por empresas que requieren un desembolso económico para poder ser utilizadas, ya sea en la adquisición del software o mediante una cuota periódica.

- **Licencias libres.** Existen diferentes categorías para este tipo de licencia, pero básicamente son propias de aplicaciones desarrolladas por comunidades de usuarios sin ánimo de lucro que distribuyen el software de manera gratuita, siempre y cuando se siga una política de respeto hacia los creadores de la misma y su utilización no tenga fines lucrativos. El tipo de software ligado a estas licencias puede ser de uno de estos tipos:

  - **El software libre** permite ejecutar el programa para cualquier propósito, incluida la alteración de su código fuente para adaptarlo a necesidades particulares y creando nuevas versiones con modificaciones implementadas por cualquier usuario que también pueden ponerse a disposición del público.

  - **El software de fuente abierta** permite su libre distribución siempre y cuando no se impongan restricciones o condiciones suplementarias a los productos derivados. Es decir, no se puede crear una versión derivada de un software de fuente abierta e imponer limitaciones en

su uso. Estos tipos de licencias no permiten establecer restricciones en cualquier software que dependa de ellas; por ejemplo, un sistema operativo de fuente abierta no debe poner restricciones para instalar programas aunque sean de otros desarrolladores. De igual manera, no se podrá discriminar su uso a ninguna persona, colectivo o campo de actividad.

- El software de **dominio público** es aquel que no dispone de copyright.

- El software con ***copyleft*** es el software libre que obliga a los desarrolladores que crean versiones del original a distribuirlas de manera libre sin poder imponer restricciones adicionales.

- El software **semilibre** es aquel que no es libre, pero otorga autorización para usar, copiar, distribuir o modificar a **particulares** siempre y cuando no sea con fines de lucro.

- ***Freeware*** es el software que permite su utilización y distribución gratuita, pero no la modificación. De hecho, se distribuyen los ejecutables del programa, pero nunca el código fuente.

7.1.1 Desarrollo de software libre

A pesar de resultar extraño que una empresa se dedique a la creación de software que no le reportará beneficios económicos, lo cierto es que las razones que llevan a los desarrolladores a realizar este tipo de software no están basadas en motivaciones económicas, sino en una filosofía que establece el software como una manera de conocimiento o cultura que no ha de ser restringida económicamente. Además, sistemas operativos como Linux han demostrado que la libre modificación del código por parte de los usuarios puede acabar en un avance tecnológico de una plataforma que, de otra manera, no podría haberse llevado a cabo:

- **Motivación ética.** Según la *Free Software Foundation*, el software es conocimiento; debe poderse difundir sin trabas; su ocultación es una actitud antisocial; y la posibilidad de modificar programas es una forma de libertad de expresión. Los miembros de esta asociación son defensores de la expresión ***free source*** (código libre).

- **Motivación pragmática.** Según la *Open Source Initiative*, las ventajas de un desarrollo comunitario favorecen el avance técnico y no eliminan la posibilidad de beneficios económicos mediante la distribución libre. De hecho, el termino ***fuente abierta*** fue acuñado para eliminar la palabra free (en inglés, gratis o libre) de la expresión ***free source*** (código abierto) creando la expresión ***open source*** (código abierto).

Recuerda

Las licencias libres pueden proporcionar beneficios económicos

7.2 Requisitos del software

Todo software utiliza un determinado número de recursos necesarios para su funcionamiento. Estos requisitos deben estar bien documentados cuando se adquiere el programa para compararlos con nuestro sistema y saber si podrá ser ejecutado y si su funcionamiento será óptimo:

Memoria. Los programas ejecutados en un sistema operativo deben ser almacenados en la memoria del equipo, ya que la velocidad de lectura del disco duro es demasiado lenta y no permitiría la correcta ejecución del software. El problema de la memoria es que, a pesar de la alta velocidad de acceso, lectura y escritura, su capacidad suele ser limitada, por lo que es un requisito que hay que tener muy en cuenta a la hora de utilizar un programa en nuestro sistema (Figura 7.1).

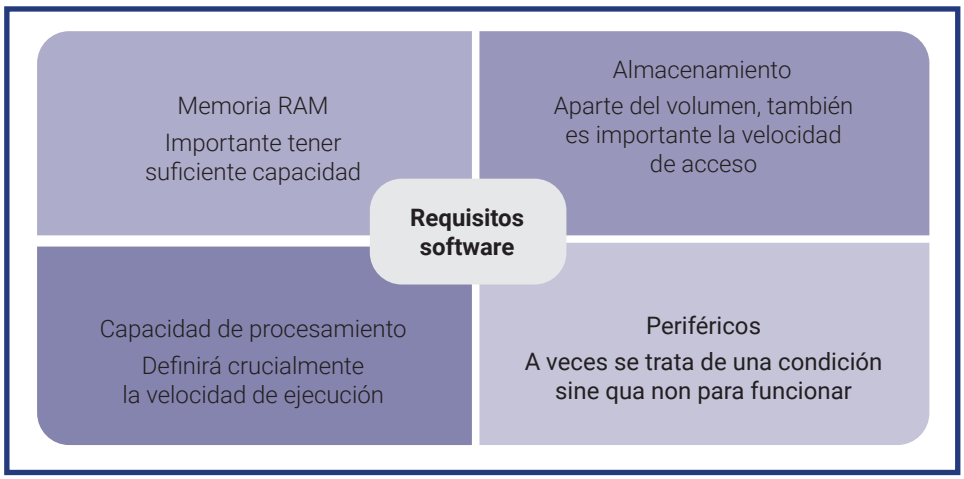


Figura 7.1
Antes del uso de un programa, deberemos verificar que va a funcionar en nuestro dispositivo.

- **Almacenamiento.** Actualmente la capacidad de almacenamiento de los equipos es muy elevada y es posible aumentarla de manera sencilla y a un bajo coste. Aún así, los programas necesitan espacio en el disco duro para almacenar sus archivos o bases de datos, por lo que, a pesar de contar hoy en día con equipos con gran capacidad de almacenamiento, es necesario especificar la cantidad de espacio que ocupará la instalación del software en nuestro sistema.

  Hoy en día se han desarrollado grandes capacidades de almacenamiento que pueden llegar al terabyte a muy bajo coste; pero, paradójicamente, la mejora de las conexiones a Internet está fomentando almacenar la información en servidores externos, ya sea guardando archivos en servicios como DropBox o visualizando películas vía ***streaming***, lo que ha conllevado la aparición de discos de menor tamaño, pero con una velocidad de acceso mucho mayor, los discos SSD.

- **Proceso.** Al igual que con el almacenamiento, los equipos actuales tienen una gran capacidad de proceso, pero este recurso es mucho más costoso de ampliar y puede volverse insuficiente cuando ejecutamos un gran número de procesos simultáneamente.

  Tanto la memoria como el proceso son requisitos que están íntimamente ligados, pues recordemos que el procesador realiza las operaciones sobre las instrucciones almacenadas en memoria. Cada vez que se procesa el conjunto de instrucciones almacenadas en memoria, se vuelca la información y se vuelven a introducir nuevas instrucciones en la memoria.

  Tener un procesador demasiado lento supone que las instrucciones son ejecutadas en mayor tiempo, pero disponer de una memoria demasiado pequeña implicaría tener que realizar más volcados de memoria; un proceso que, por lo general, requiere de tiempo extra para realizarse. Por ello, hay que analizar con detenimiento las razones por las que se produce un deterioro en la eficiencia del sistema. Si se están ejecutando muchos procesos al mismo tiempo, deberemos tener una gran capacidad de memoria; por ejemplo, servidores que ofrecen servicios de mensajería, almacenamiento de archivos, conexiones de usuarios, copias de seguridad, antivirus, etc. Pero, si ejecutamos pocos procesos que requieren una gran cantidad de cálculo, necesitaremos un procesador más potente, por ejemplo aplicaciones de modelado 3D, simuladores, generadores de gráficos, etc.

- **Periféricos.** Algunos programas necesitan dispositivos de entrada o salida para poder funcionar. Lectores de tarjetas, sensores biométricos, impresoras, teclados, etc; son algunos ejemplos. Los videojuegos; además, deben especificar la potencia gráfica que ha de soportar el equipo para poder funcionar correctamente.

Para saber más

El termino streaming es utilizado para definir la visualización de vídeos a través de Internet sin necesidad de descargarlos previamente. Youtube muestra videos vía streaming.

7.3 Herramientas ofimáticas

Son herramientas utilizadas originalmente en oficinas pero que debido a su utilidad se han implantado en cualquier ámbito tanto laboral como doméstico. Se trata de una serie de programas que son utilizados para crear, modificar, organizar, escanear, imprimir, etc; documentos y archivos. Como en la mayoría de software, existen distribuciones de pago y de código libre:

- **Editores de texto.** Son utilizados para crear documentos escritos con un formato preparado para ser imprimido. El tamaño tanto del papel como de la letra, así como la fuente y el formato, pueden ser fácilmente

modificados por el usuario para conseguir la presentación deseada. Actualmente, estos programas han incorporado un gran número de herramientas que las hacen muy potentes y capaces de ofrecer resultados profesionales.

- **Hojas de cálculo.** Son utilizadas en contabilidad ya que son una herramienta ideal para realizar operaciones matemáticas de manera sencilla y prácticamente automática. Además el formato de celdas distribuidas por filas y columnas es idóneo para conseguir documentos enfocados en la contabilidad, ventas, inventarios, etc.

- **Presentaciones.** Una funcionalidad muy interesante que incorporan la mayoría de herramientas ofimáticas es la creación de presentaciones en las que se pueden añadir comportamientos y estilos que ofrezcan un resultado atractivo y adecuado para realizarlas.

  Los programas de presentaciones añaden gran cantidad de plantillas para definir tanto el fondo de las pantallas como la distribución de los títulos y los contenidos. También incorporan efectos de movimiento para generar transiciones entre las pantallas que tengan un aspecto más atractivo para fomentar la atención del público; así como permitir la incorporación de imágenes y vídeos que pueden ser reproducidos durante la presentación. Aunque generalmente las presentaciones se utilizan de apoyo en una comparecencia pública, lo cierto es que pueden conseguir incluso más relevancia que la persona que realiza la explicación.

- **Correo electrónico.** Dada la importancia del correo electrónico para las empresas, los paquetes ofimáticos han incorporado funcionalidades para poder administrar el correo electrónico de una manera sencilla e intuitiva, además de permitir realizar copias de los mensajes y utilizar libretas de direcciones exportables.

Todas las herramientas ofimáticas están adaptadas para el uso compartido de archivos cuando se utilizan servidores de archivos. Al intentar acceder a un archivo que está siendo modificado por otro usuario, el programa lo abrirá en modo de solo lectura y avisará al usuario que tiene limitaciones para realizar modificaciones. Además, permiten establecer credenciales para limitar su lectura, creando áreas que pueden ser modificadas y otras que no. Es habitual aplicar estas restricciones en hojas de cálculo para la creación de presupuestos en los que las casillas que tienen el precio están bloqueadas para evitar que se manipulen.

Las herramientas ofimáticas han ido evolucionando y han ido proporcionando cada vez más funcionalidades a los usuarios.

Por ejemplo, los correctores ortográficos son una potente herramienta que analiza el texto en busca de errores ortográficos o sintácticos a medida que escribe el usuario. Además, proporcionan alternativas para realizar las correcciones oportunas o incluso las aplica automáticamente. Los diccionarios son instalados por idiomas según las necesidades del usuario.

El formato en la creación de los documentos está pensado para su posterior impresión, de manera que están definidos los estándares de papel y los márgenes para facilitar su lectura. Además, es posible crear encabezados en los documentos para incorporar logotipos, títulos, autores, etc.; que serán visibles en todas las páginas, así como la numeración automática de las hojas que componen el documento.

Actualmente, se están implantando herramientas ofimáticas que funcionan directamente desde la nube (término que hace referencia a contenido almacenado en servidores de Internet), sin necesidad de que el cliente deba instalar ningún tipo de software en su equipo. Este sistema permite asegurar los datos almacenados, puesto que no dependen de un soporte físico local a pesar de que actualmente la seguridad de los datos guardados no está asegurada.

Para saber más

La nube son los servidores accesibles desde Internet en los que podemos almacenar información y recuperarla en cualquier ordenador con conexión.

7.4 Herramientas de Internet

Existen aplicaciones que utilizan Internet para ofrecer sus servicios a los usuarios. Generalmente, requieren de la conexión a Internet para poder ser usados, ya que están basados en la comunicación interpersonal. Estamos hablando de programas gestores de correo electrónico o de mensajería instantánea utilizados para que varias personas se puedan comunicarse.

No podemos hablar de software de comunicación vía Internet sin hacer una mención especial a las videoconferencias. Se trata de programas que utilizan el ancho de banda del que actualmente disponen los usuarios, para poder realizar comunicaciones bidireccionales simultáneas de audio y vídeo, realizando una compresión de los datos de forma instantánea para poder ser transmitidos entre emisor y receptor.

Otro tipo de aplicaciones de Internet son las ofrecidas mediante plataformas web que ofrecen servicios a los usuarios y que sin conectividad no podrían llevarse a cabo. A continuación, explicaremos algunas de estas herramientas:

• **Redes sociales:** sistemas que actualmente están cambiando la manera en la que se relacionan las personas. Son plataformas que permiten a las personas compartir información con aquellos usuarios que tengan en sus listas de contacto o mantener el contacto con aquellos conocidos, hecho que, de manera física, no sería posible. Actualmente las redes sociales son utilizadas en muchos más ámbitos más allá de los personales y cada vez es más común ver redes sociales utilizadas por empresas para promocionarse o para buscar trabajadores. Un ejemplo de red social utilizada en el ámbito profesional es www.linkedin.com.

• **RSS:** es un sistema de comunicación que utiliza Internet para enviar a los usuarios noticias frecuentes que puedan ser de su interés. Son muy utilizados en el ámbito periodístico y divulgador como blogs, revistas, periódicos, etc. Los usuarios deberán tener un software RSS que reciba la información y la muestre de manera coherente y ordenada. Un ejemplo de servicio RSS ofrecido por un medio de comunicación es www.rtve.es/rss.

• **Buscadores:** un servicio necesario dentro de Internet por la gran cantidad de información disponible. Los buscadores utilizan algoritmos muy eficientes que devuelven aquellas páginas web que coinciden con los criterios de búsqueda. El más utilizado, con una cuota del 95% de los internautas, es www.google.es, seguido de Bing, con un 3%.

• **Foros:** los foros han sido ampliamente utilizados desde los inicios de Internet. Son plataformas en las que las personas, registradas o no según la política de seguridad, pueden publicar libremente información para expresar ideas, dudas, opiniones..., que el resto de la comunidad complementa con sus aportaciones, como si de un foro de verdad se tratase. Uno de los más utilizados por los desarrolladores de aplicaciones web es www.forosdelweb.com.

7.5 Utilidades de propósito general

Entendemos por utilidades de propósito general aquellos programas que no han sido desarrollados para ofrecer un servicio o solventar un problema concreto de una empresa, sino que son desarrollados y comercializados o distribuidos para poder dar cobertura a las necesidades que pueden ser comunes a cualquier empresa o usuario. A continuación, podríamos definir algunas de las utilidades de propósito general más utilizadas generalmente:

- **Antivirus:** para cualquier usuario, tener su equipo infectado por un virus es un problema importante que requiere de tiempo y dinero para solucionarlo. La utilización de un antivirus, que ha sido diseñado espe-

cialmente para ese propósito, ayudará a cualquier usuario o empresa a realizar una desinfección del equipo de manera fácil y rápida.

- **Recuperación de datos:** una necesidad con la que muchas empresas se han encontrado alguna vez es la de recuperar información que haya sido eliminada por error. Para ello, existen herramientas que, independientemente del entorno o el tipo de datos perdidos, pueden recuperar la información de una manera casi automática (Figura 7.2).

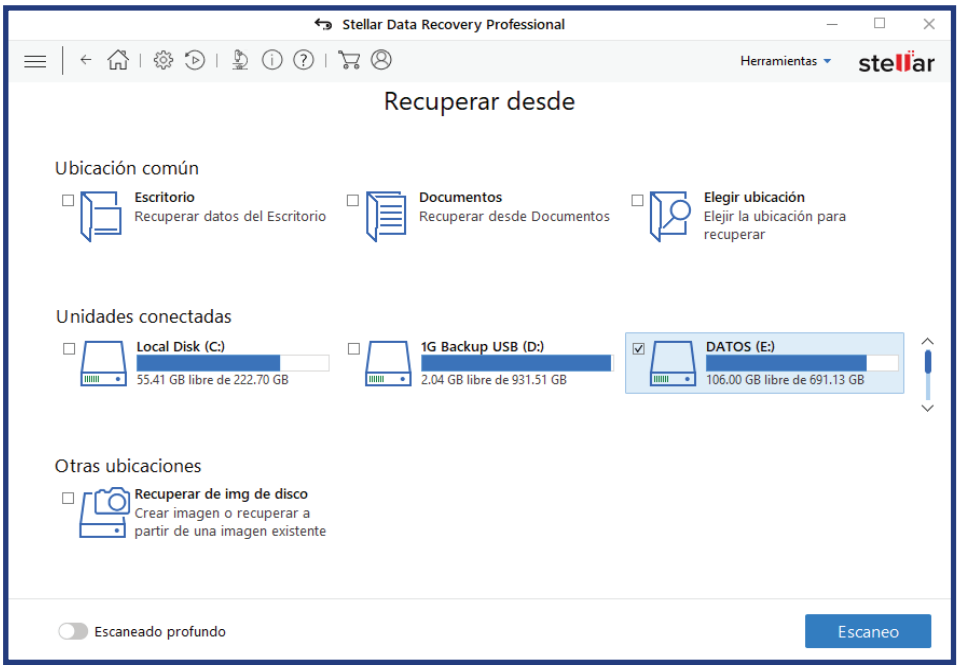


Figura 7.2
Software de recuperación de datos.

- **Mantenimiento del sistema:** existen aplicaciones que permiten monitorizar los recursos del sistema para poder llevar un control y detectar necesidades que de otra manera solo podrían ser detectadas al experimentar un mal funcionamiento del sistema. Estas herramientas previenen tener que llegar a ese punto, informando al administrador constantemente del estado del sistema (Figura 7.3).

Figura 7.3
Software de mantenimiento del sistema.

Resumen

En esta unidad hemos analizado en profundidad los aspectos relacionados con el software utilizado por usuarios, administradores y desarrolladores. Hemos clasificado el software según su función y licencia de uso.

El software utilizado actualmente cubre tres áreas de funcionalidad: sistema, programación y aplicación. Todo programa comporta un tipo de licencia, que incluye las condiciones que determina el fabricante o el programador para su utilización. Las licencias pueden dividirse básicamente en: licencias de pago, que requiere un desembolso por parte del usuario para poder utilizarlas; y las licencias libres, que suelen ser las que se aplican al software desarrollado por comunidades que no pretenden lucrarse con su distribución.

Los programas informáticos exigen que los equipos en los que vayan a ser instalados cumplan con una serie de requisitos para funcionar. Dichos requisitos suelen basarse en la capacidad de procesamiento o memoria del equipo, aunque hay casos de software que precisan de unos periféricos específicos conectados al equipo para funcionar. Hay que señalar que los diversos programas y servicios en ejecución en un equipo consumen recursos de procesamiento y memoria y, en algunos casos de manera permanente, por lo que hay que tener en cuenta no sólo las capacidades teóricas del equipo, si no la cantidad de recursos de los que disponemos a la hora de instalar el software.

El software ofimático es un paquete compuesto por diferentes programas para el procesamiento de texto y datos en el ámbito laboral, educativo, etc. Estos programas permiten, entre otras funcionalidades, la elaboración de documentos de texto y hojas de cálculo necesarias, hoy en día, en la mayoría de ámbitos profesionales.

Las herramientas de Internet es un tipo de software que requiere una conexión a Internet para funcionar. Está basado en la información que se almacena de manera local en el equipo y no en servidores externos. La naturaleza de estos programas varía notablemente, puesto que, en los últimos años, puesto que los equipos suelen estar permanentemente conectados a Internet.

Las utilidades de propósito general pretenden cubrir las necesidades que pueden surgir en cualquier equipo, independientemente del tipo de usuario que lo utilice y del sistema operativo o software instalado. Un ejemplo claro de ello son los antivirus, cuyo objetivo es eliminar cualquier amenaza del equipo.

Ejercicios de autocomprobación

Indica si las siguientes afirmaciones son verdaderas (V) o falsas (F):

1. Existen tres tipos de software destinados a proporcionar servicio de sistema, programación o aplicación y que pueden dividirse entre programas de pago o de licencia libre.

2. Las herramientas de Internet son un tipo de software que no requiere una conexión a Internet para funcionar.

3. Software de sistema son los programas que funcionan a más bajo nivel para controlar el hardware y ser utilizado por el usuario, así como ofrecer los servicios.

4. Freeware es el software que permite su utilización y distribución gratuita, pero no la modificación.

5. Los programas ejecutados en un sistema operativo deben ser almacenados en la memoria del equipo, ya que la velocidad de lectura del disco duro es demasiado lenta y no permitiría la correcta ejecución del software.

6. Redes sociales son sistemas que no cambian la manera en la que se relacionan las personas. Son plataformas que permiten a las personas compartir información con aquellos usuarios que tengan en sus listas de contacto o mantener el contacto con aquellos conocidos.

7. Para cualquier usuario, tener su equipo infectado por un virus no es un problema importante ni requiere tiempo o dinero para solucionarlo.

Completa las siguientes afirmaciones:

8. Los editores de _____ son utilizados para crear documentos escritos con un formato preparado para ser imprimido. El _____ tanto del papel como de la letra, así como la _____ y el _____, pueden ser fácilmente modificados por el usuario para conseguir la presentación deseada.

9. Los diversos programas y _____ en ejecución en un equipo consumen recursos de procesamiento y _____ y, en algunos casos de manera permanente, por lo que hay que tener en cuenta no solo las capacidades teóricas del equipo, si no la _____ recursos de los que disponemos a la hora de instalar el _____.

10. El _____ utilizado actualmente cubre tres áreas de funcionalidad: sistema, programación y aplicación. Todo _____ comporta un tipo _____, que incluye las _____ que determina el fabricante o el programador para su utilización.

Soluciones de los ejercicios de autocomprobación

Unidad 7

1. V
2. F. Las herramientas de Internet es un tipo de software que requiere una conexión a Internet para funcionar.
3. V
4. V
5. V
6. F. Redes sociales son sistemas que están cambiando la manera en la que se relacionan las personas. Son plataformas que permiten a las personas compartir información con aquellos usuarios que tengan en sus listas de contacto o mantener el contacto con aquellos conocidos.
7. F. Para cualquier usuario, tener su equipo infectado por un virus es un problema importante ni requiere tiempo o dinero para solucionarlo.
8. texto, tamaño, fuente, formato.
9. servicios, memoria, cantidad, software.
10. software, programa, licencia, condiciones.

ÍNDICE