

CURSO DE DESARROLLO DE APLICACIONES WEB



Sistemas informáticos

Quedan rigurosamente prohibidas, sin la autorización escrita de los titulares del *Copyright*, bajo las sanciones establecidas en las leyes, la reproducción total o parcial de esta obra por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares de ella mediante alquiler o préstamo públicos. Diríjase a CEDRO (Centro Español de Derechos Reprográficos, www.cedro.org) si necesita fotocopiar o escanear algún fragmento de esta obra.

INICIATIVA Y COORDINACIÓN
Centro de Estudios CEAC

COLABORADORES

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

Elaboración de contenidos:

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

Actualización de contenidos:

E-MAFE E-LEARNING SOLUTIONS, SL
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

© Planeta DeAgostini Formación, S.L.U.

Barcelona (España), 2016

Segunda edición: marzo de 2018

ISBN: 978-84-9063-804-0 (Obra completa)

ISBN: 978-84-9128-791-9 (Sistemas informáticos)

Depósito Legal: B 820-2018

Impreso por:
QPPRINT
C/ Comadrán, 7 Nave C4
08210 Barberà del Vallès
Barcelona

Printed in Spain
Impreso en España

PRESENTACIÓN DEL CURSO

El módulo que tienes en tus manos es el primero del curso de Desarrollo de Aplicaciones Web. Los conocimientos teóricos y prácticos adquiridos a lo largo de este curso te permitirán convertirte en profesional de un sector con unas elevadas expectativas de crecimiento y ser capaz de integrar servicios y contenidos distribuidos en aplicaciones web asegurando su funcionalidad tanto desde el punto de vista del cliente como desde el punto de vista del servidor.

La correcta asimilación de los contenidos del curso te capacitarán para desarrollar, implantar y mantener aplicaciones web con independencia del modelo empleado, utilizando tecnologías específicas, garantizando el acceso a los datos de forma segura y cumpliendo los criterios de accesibilidad, usabilidad y calidad exigidos en los estándares establecidos. Serás capaz de desarrollar aplicaciones web con acceso a bases de datos utilizando lenguajes de marca, objetos de acceso y herramientas de mapeo adecuados a las especificaciones a fin de desarrollar interfaces en aplicaciones web de acuerdo con un manual de estilo.

Esperamos que disfrutes estudiando y aprendiendo a lo largo de todo el curso y que disfrutes todavía más el ejercicio profesional propiamente dicho una vez completados los estudios.

INTRODUCCIÓN AL MÓDULO

"Los conocimientos de la especie humana crecen incesantemente, pero los medios que utilizamos para encontrar lo que nos interesa son los mismos que se utilizaban en la época de los barcos de vela cuadrada". En 1945, el ingeniero y científico Vannevar Bush expresaba con esta frase la necesidad de mejorar los métodos de acceso a la información. En ese sentido, planteó la construcción de una máquina que pudiese almacenar miles de libros con sus párrafos enlazados unos con otros según su temática. El sueño de Bush se llama **World Wide Web**, pero hicieron falta cuarenta y cinco años para que la electrónica, los protocolos de comunicación, los sistemas operativos, las aplicaciones informáticas y el trabajo de millones de personas hiciesen posible que ese sueño se hiciese realidad.

Desde el punto de vista de un usuario, la World Wide Web no es más que un programa en su ordenador, una ventana dentro de la cual aparece la información conforme se solicita. Pero los desarrolladores web no escriben programas para un ordenador, sino para un complejo sistema en el que se integran numerosas tecnologías. Para que una aplicación web proporcione un servicio al usuario, todas las tecnologías implicadas deben funcionar perfectamente sincronizadas.

En este módulo aprenderás a identificar las tecnologías que forman un sistema informático; a instalar, mantener y administrar los sistemas operativos que permiten que los ordenadores funcionen; a preparar los servicios y explotar las aplicaciones más comunes y a utilizar los sistemas informáticos para el procesamiento de datos, creando de esta manera sistemas de información mediante las redes de comunicación. Los conocimientos que adquirirás te permitirán desarrollar aplicaciones para un sistema informático complejo.

Esquema de contenido

1. Explotación de sistemas microinformáticos

- 1.1 Arquitectura de ordenadores
- 1.2 Componentes de un sistema informático
- 1.3 Periféricos. Adaptadores para la conexión de dispositivos
- 1.4 Chequeo y diagnóstico
- 1.5 Herramientas de monitorización
- 1.6 Normas de seguridad y prevención de riesgos laborales
- 1.7 Sistemas de comunicación
- 1.8 Características de una red: ventajas e inconvenientes
- 1.9 Tipos de redes
- 1.10 Componentes de una red informática
- 1.11 Topologías de red
- 1.12 Medios de transmisión
- 1.13 Tipos de cableado. Conectores
- 1.14 Mapa físico y mapa lógico de una red local

2. Instalación de sistemas operativos

- 2.1 Estructura de un sistema informático
- 2.2 Arquitectura de un sistema operativo
- 2.3 Funciones de un sistema operativo
- 2.4 Tipos de sistemas operativos
- 2.5 Tipos de aplicaciones
- 2.6 Licencias y tipos de licencias
- 2.7 Gestores de arranque
- 2.8 Máquinas virtuales
- 2.9 Consideraciones previas a la instalación de sistemas operativos libres y propietarios
- 2.10 Instalación de sistemas operativos. Requisitos, versiones y licencias
- 2.11 Instalación y desinstalación de aplicaciones. Requisitos, versiones y licencias

- 2.12 Uso de instalaciones desatendidas
- 2.13 Actualización de sistemas operativos y aplicaciones
- 2.14 Ficheros de inicio de sistemas operativos
- 2.15 Controladores de dispositivos

3. Gestión de información

- 3.1 Sistemas de archivos
- 3.2 Gestión de sistemas de archivos mediante comandos y entornos gráficos
- 3.3 Estructura de directorios de sistemas operativos libres y propietarios
- 3.4 Búsqueda de información del sistema mediante comandos y herramientas gráficas
- 3.5 Identificación del software instalado mediante comandos y herramientas gráficas
- 3.6 Gestión de la información del sistema. Rendimiento. Estadísticas. Montaje y desmontaje de dispositivos en sistemas operativos
- 3.7 Herramientas de administración de discos
- 3.8 Sistemas de archivos de red y matrices de discos RAID
- 3.9 Gestión de archivos
- 3.10 Montar volúmenes en carpetas
- 3.11 Tolerancia a fallos
- 3.12 Tareas automáticas

4. Configuración de sistemas operativos

- 4.1 Configuración de usuarios y grupos locales
- 4.2 Usuarios y grupos predeterminados
- 4.3 Seguridad de cuentas de usuario
- 4.4 Seguridad de contraseñas
- 4.5 Directivas locales
- 4.6 Servicios y procesos
- 4.7 Comandos de sistemas libres y propietarios
- 4.8 Herramientas de monitorización del sistema

5. Conexión de sistemas en red

- 5.1 Configuración del protocolo TCP/IP en un cliente de red
- 5.2 Configuración dinámica automática
- 5.3 Configuración de la resolución de nombres
- 5.4 Ficheros de configuración de red
- 5.5 Tablas de enrutamientos
- 5.6 Gestión de puertos
- 5.7 Verificación del funcionamiento de una red mediante el uso de comandos
- 5.8 Resolución de problemas de conectividad en sistemas operativos en red
- 5.9 Comandos utilizados en sistemas operativos libres y propietarios
- 5.10 Monitorización de redes
- 5.11 Protocolos TCP/IP
- 5.12 Configuración de los adaptadores de red en sistemas operativos libres y propietarios
- 5.13 Software de configuración de los dispositivos de red
- 5.14 Interconexión de redes: Adaptadores de red y dispositivos de interconexión
- 5.15 Redes cableadas. Tipos y características. Adaptadores de red. Comunicadores, enruteadores, entre otros
- 5.16 Redes inalámbricas. Tipos y características
- 5.17 Seguridad básica en redes cableadas e inalámbricas
- 5.18 Seguridad en la comunicación de redes inalámbricas
- 5.19 Acceso a redes WAN. Tecnologías
- 5.20 Seguridad de comunicaciones

6. Gestión de recursos en una red

- 6.1 Diferencias entre permisos y derechos. Permisos de red. Permisos locales. Herencia. Permisos efectivos. Denegación de permisos
- 6.2 Derechos de usuarios. Directivas de seguridad. Objetos de directiva. Ámbitos de las directivas. Plantillas
- 6.3 Requisitos de seguridad del sistema y de los datos

- 6.4 Seguridad a nivel de usuarios y seguridad a nivel de equipos
- 6.5 Servidores de archivos
- 6.6 Servidores de impresión
- 6.7 Servidores de aplicaciones
- 6.8 Técnicas de conexión remota
- 6.9 Herramientas de cifrado
- 6.10 Herramientas de análisis y administración
- 6.11 Cortafuegos
- 6.12 Sistemas de detección de intrusión

7. Explotación de aplicaciones informáticas de propósito general

- 7.1 Tipos de software
- 7.2 Requisitos del software
- 7.3 Herramientas ofimáticas
- 7.4 Herramientas de Internet
- 7.5 Utilidades de propósito general

1. EXPLORACIÓN DE SISTEMAS MICROINFORMÁTICOS

La creación de una aplicación web comienza con la detección de una necesidad, a la que sigue una idea original que permite resolver el problema. Este proceso requiere, en primer lugar, determinar la viabilidad de la idea, lo cual supone delimitar a quién va dirigida y cuál será su entorno de aplicación. Dicho entorno será uno de los filtros fundamentales que darán forma al proyecto.

En esta unidad aprenderás a reconocer el entorno de una aplicación web, identificando sus principales elementos y la relación existente entre ellos. En primer lugar, empezaremos por conocer qué es un sistema informático a través de sus componentes más básicos; a continuación, estudiaremos el funcionamiento de un ordenador e identificaremos sus dispositivos periféricos.

Además, nos centraremos en las redes de ordenadores. Veremos qué son los sistemas de comunicación y cuáles son las ventajas e inconvenientes de trabajar en red. Estudiaremos con detenimiento los elementos que transportan la información entre ordenadores y cómo se combinan dichos elementos al formar diferentes tipos de red y diferentes estructuras. Analizaremos también cómo debe documentarse una red de ordenadores y qué programas informáticos nos pueden facilitar su mantenimiento y explotación.

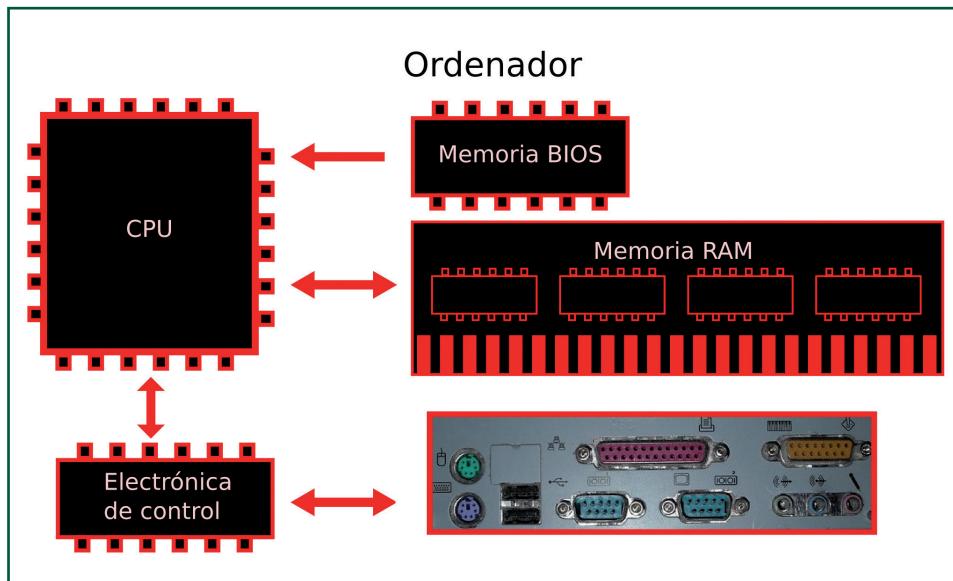
Por último, repasaremos las normas de seguridad laboral, que son de gran utilidad cuando hacemos un uso prolongado del ordenador.

1.1 Arquitectura de ordenadores

Los ordenadores están formados por dispositivos que se relacionan unos con otros formando una **arquitectura** y cada ordenador tiene su propia arquitectura; sin embargo, existen unos elementos comunes a la gran mayoría, los cuales se describen a continuación (Figura 1.1):

- **CPU (Unidad Central de Proceso).** Más conocido como *procesador* o *microprocesador* por sus reducidas dimensiones, es el componente que ejecuta las instrucciones almacenadas en memoria mediante operaciones aritmético-lógicas. Actualmente, la fabricación de los procesadores está basada en placas de circuitos integradas con miles de transistores basados en el silicio y su fabricación se realiza en grandes obleas de semiconductores de donde se obtienen varios procesadores.

Figura 1.1
Un ordenador está formado por una unidad de proceso, un conjunto de memorias, buses e interfaces.



La mayoría de los procesadores modernos realizan el procesamiento de los programas mediante cuatro etapas: **fetch** (leer), **decode** (decodificar), **execute** (ejecutar) y **writeback** (escribir).

El primer paso, **lectura**, recupera las instrucciones almacenadas en memoria. Cada programa está compuesto por una serie de instrucciones y cada una de ellas está identificada por un número llamado *Contador de Programa* (PC, del inglés *Program Counter*). Este número es leído en el proceso *fetch* para identificar la instrucción que deberá ser ejecutada. Una vez realizada la lectura, el PC es incrementado en uno para indicar que en el próximo ciclo deberá ser leída la siguiente instrucción.

El paso de **decodificación** divide la instrucción en secciones que tienen un significado propio para la arquitectura que lo está ejecutando. Una parte de la instrucción define el tipo de operación que deberá realizarse, mientras que el resto de bits de la instrucción conforman los operandos, ya sean valores inmediatos o referencias a memoria donde se guardan otros valores. De esta manera se identifican el tipo de operación por un lado y los operandos por el otro y se envían a la siguiente fase de procesamiento.

La **ejecución** realiza las operaciones procedentes de la decodificación y las aplica a los valores incluidos en la instrucción o en la memoria si se trata de valores referenciados. En este proceso interviene la ALU (Unidad Aritmético-Lógica), que es el verdadero núcleo del procesador. La ALU recibe una serie de valores en la entrada y, después de procesarlos mediante operaciones aritméticas o lógicas, el resultado es enviado a una salida.

Existen dos alternativas para la escritura de los resultados. Por un lado, el resultado de las operaciones puede ser escrito en pequeñas memorias internas de la CPU llamadas **registros**. Los registros están conectados a las entradas de la ALU, por lo que esta opción es utilizada en aquellos resultados que serán utilizados en la siguiente instrucción. Por ejemplo, imaginemos un bucle en el que una instrucción va incrementando una variable. El resultado de una iteración será utilizado como valor para incrementar en uno en la siguiente instrucción. Por otro lado, si el valor resultante de la operación no va a ser utilizado en las siguientes instrucciones, la escritura se realizará sobre la memoria principal.

Una vez realizados los procesos de lectura, decodificación, ejecución y escritura, el proceso vuelve a repetirse para las siguientes instrucciones hasta finalizar el programa.

- **BIOS.** La BIOS es un programa con una serie de instrucciones instalado en un componente del circuito integrado de la placa. Al arrancar el equipo, estas instrucciones son copiadas a la memoria principal para ser ejecutadas por el sistema durante el arranque. Este programa proporciona las funcionalidades básicas para el arranque, como el chequeo de la memoria principal, procesador, interfaz con el usuario como monitor o teclado y la ejecución de los sectores de arranque de los sistemas operativos.

Las BIOS realizan comprobaciones de hardware durante el arranque. En ocasiones, el cambio de un componente, como un procesador nuevo, hace que la BIOS no disponga de los controladores necesarios para identificar el nuevo dispositivo y provoque errores en el arranque. Para estos casos, es habitual que el fabricante lance actualizaciones de la BIOS para solventar problemas de hardware nuevo o incluso que optimice la BIOS utilizada en los primeros lotes de fabricación.

- **RAM.** La **memoria de acceso aleatorio** (en inglés, *random-access memory*) es una memoria de trabajo utilizada para almacenar las instrucciones de los programas que se están ejecutando, así como los procesos del sistema operativo. Se denomina *de acceso aleatorio* porque su principal característica es que tiene el mismo tiempo de acceso, independientemente de la posición en la que sus datos estén almacenados.

Del tamaño de almacenamiento de la memoria, así como de su velocidad de lectura y escritura, depende la cantidad de aplicaciones que un equipo puede estar ejecutando al mismo tiempo. Es posible tener una gran cantidad de programas instalados ocupando espacio en disco duro, pero es solo al ser ejecutados que entra en juego la memoria RAM, que es de donde el procesador obtiene la información.

Dada la rápida evolución del software y sus necesidades de rendimiento, es habitual encontrar equipos que puedan soportar las necesidades de procesamiento de un programa, pero que no tengan memoria RAM suficiente. Esto también sucede cuando se ejecutan varios programas al mismo tiempo. Las memorias son fabricadas como componentes independientes del resto del equipo para que en estas situaciones sea posible cambiarlas o insertar nuevos módulos en la placa base con el fin de que se sumen sus capacidades sin necesidad de cambiar todo el resto del equipo.

- **Interfaces.** Son el medio por el que un usuario establece comunicación con un equipo. Las interfaces han ido evolucionando para proporcionar una mejor experiencia al usuario, facilitando su utilización y haciéndolas más intuitivas para cualquier usuario.

Existen dos tipos de interfaces:

-Interfaz de hardware. Son aquellos dispositivos que permiten realizar un proceso de entrada y salida de la información entre el usuario y la máquina. Algunos de los periféricos más conocidos son el teclado, ratón, pantalla, impresora, pantalla táctil... También se pueden considerar interfaces de hardware los conectores por los que se conectan los dispositivos al equipo: USB, PS/2, HDMI, etc.

-Interfaz de software. Es el formato mediante el cual los programas y sistemas operativos muestran la información al usuario, así como permitirle interactuar con las funcionalidades del programa. Una interfaz gráfica ha de ser atractiva visualmente e intuitiva de utilizar. Es la ventana que tiene el usuario de poder utilizar las funcionalidades de un programa sin necesidad de tener conocimientos de programación.

- **Buses.** Son los canales mediante los cuales se comunican los diferentes componentes de un equipo o entre diferentes ordenadores. Están formados por cable o por pistas en un circuito impreso. Son componentes conductores que transmiten información lógica a través de impulsos eléctricos.

La capacidad de los buses es definida mediante su frecuencia y su ancho de banda. La frecuencia es la velocidad en la que se transmiten los datos, mientras que el ancho de banda es la cantidad de datos enviados simultáneamente. Generalmente, los buses con una alta frecuencia deben tener un ancho de banda proporcionalmente más pequeño. Esto es debido a que las frecuencias altas son más susceptibles de producir interferencias entre las diferentes señales, por lo que tener un ancho de banda grande en estas circunstancias provocaría un número mayor de interferencias.

Los buses se dividen en dos tipos fundamentalmente:

- **Bus serie.** Los datos son enviados bit a bit a través del hilo conductor. En este caso, el ancho de banda depende de la frecuencia de la señal. Son utilizados para componentes como el procesador o para buses internos del disco duro.

- **Bus paralelo.** Son los buses que envían la información por bytes utilizando varias líneas paralelas que conforman una única conexión. Han sido muy utilizados para conectar dispositivos de todo tipo. Un ejemplo muy común son las impresoras que hasta hace unos años se conectaban mediante un puerto paralelo.

Algunas de las líneas del bus paralelo tienen funcionalidades específicas dentro de la comunicación:

- △ Las **líneas de dirección** establecen la posición de memoria o el dispositivo al que se quiere establecer la conexión.
- △ Las **líneas de control** se encargan de enviar las señales que sirven para administrar la comunicación entre los dispositivos, entre los que se encuentran líneas de interrupción y de estado, que se encargan de detener la comunicación o informar del estado de un dispositivo respectivamente.
- △ Las **líneas de datos** son las que circulan la información bit a bit.

En conjunto, todos los elementos conforman la estructura necesaria para el funcionamiento de un equipo informático.

1.2 Componentes de un sistema informático

Un **sistema informático** es un conjunto de medios que permite resolver un problema abstracto siguiendo unas instrucciones determinadas. Está formado por los siguientes elementos:

- **Usuarios.** Los usuarios son las personas que plantean el problema al sistema informático para que éste les proporcione una solución.
- **Programadores.** Los programadores son personas que describen los procedimientos que debe seguir el sistema informático para dar solución a las demandas de los usuarios.

Recuerda

Un ordenador está formado por la memoria, la CPU, los buses y las interfaces.

- **Maquinaria (hardware).** El hardware es el conjunto de máquinas que permiten, directa o indirectamente, automatizar la resolución del problema siguiendo las instrucciones de los programadores.
- **Administradores.** Los administradores son las personas encargadas de la puesta en marcha, mantenimiento y evolución del sistema informático (Figura 1.2).
- **Programas (software).** Los programas son las instrucciones que los programadores proporcionan a la maquinaria para describir cómo se comunicará ésta con los usuarios y qué procedimientos seguirá para la solución de los problemas planteados por aquellos.
- **Protocolos.** Los protocolos son normas que establecen cómo debe realizarse la comunicación entre máquinas, entre las personas o entre la maquinaria y las personas que forman un sistema informático.
- **Políticas.** Las políticas son normas que rigen la relación entre los diferentes elementos de un sistema informático, describiendo qué acciones están permitidas y cuáles no.



Figura 1.2

Personal en un departamento de informática dedicado al mantenimiento y el desarrollo del sistema.

1.3 Periféricos. Adaptadores para la conexión de dispositivos

Los periféricos son aquellos dispositivos que se conectan directamente a un ordenador para que éste pueda comunicarse con el mundo exterior, recibiendo, enviando o almacenando información (Figura 1.3). Se dividen en tres clases:

- **Periféricos de entrada.** Son los que permiten al ordenador recabar información del exterior. Algunos, como el teclado o el ratón, necesitan de la intervención humana, ya que están creados para que una persona pueda dar instrucciones a la máquina; otros, como las webcams o los micrófonos, captan información del entorno sin importar su procedencia.

- **Periféricos de salida.** Muestran los datos en forma de información que puede ser interpretada por un ser humano. Sirvan como ejemplo los monitores, altavoces, impresoras, etc.

- **De entrada / salida.** Realizan operaciones tanto de entrada como de salida de datos. Los tipos más comunes son los siguientes:

- **Medios de almacenamiento masivo.** Son dispositivos que permiten almacenar información permanentemente. Se utilizan para guardar los programas que indican al ordenador lo que tiene que hacer, datos que necesitan los programas para funcionar o datos de interés para el usuario, como textos, fotografías o vídeos. Estos datos son intercambiados entre los medios de almacenamiento y la memoria RAM del ordenador. Entre los medios más comunes están los discos duros, los *pendrives* y, en desuso, los discos ópticos (CD-ROM, DVD, Blu-ray).

- **Adaptadores de red.** Son periféricos que actúan de interfaz de conexión entre aparatos o dispositivos posibilitando la compartición de recursos (discos duros, impresoras, etcétera) entre dos o más dispositivos de una red. Ejemplos de estos dispositivos son los módems, las tarjetas de red Ethernet o los adaptadores para red inalámbrica WiFi.

Para saber más

En la lista de los lenguajes de programación más utilizados que ha publicado Gartner podemos ver que, en primera posición, se encuentra Java y, en segundo lugar, está JavaScript, que le está pisando los talones a través de HTML5 y su importancia en el mundo de la movilidad.



Figura 1.3

Tipos de periféricos más utilizados hoy en día: Monitor (de salida), teclado (de entrada) y pendrive (de almacenamiento masivo).

1.4 Chequeo y diagnóstico

Los errores en un sistema informático pueden ser fruto de distintas causas, entre ellas:

- Fallo físico de la máquina afectada.
- Defectos en el software de la máquina afectada.
- Mala configuración de la máquina afectada.
- Deterioro o mala conexión del cableado.
- Fallo físico o mala configuración de la electrónica de red.
- Servidor con software inapropiado o mal configurado.
- Fallo físico en un servidor.
- Pérdida del suministro eléctrico.
- Pérdida del servicio de telecomunicaciones de un proveedor externo.
- Ataques intencionados.

1.5 Herramientas de monitorización

Las aplicaciones de monitorización son aquellos programas de ordenador que se utilizan para gestionar sistemas informáticos complejos. Se dividen en (Figura 1.4):

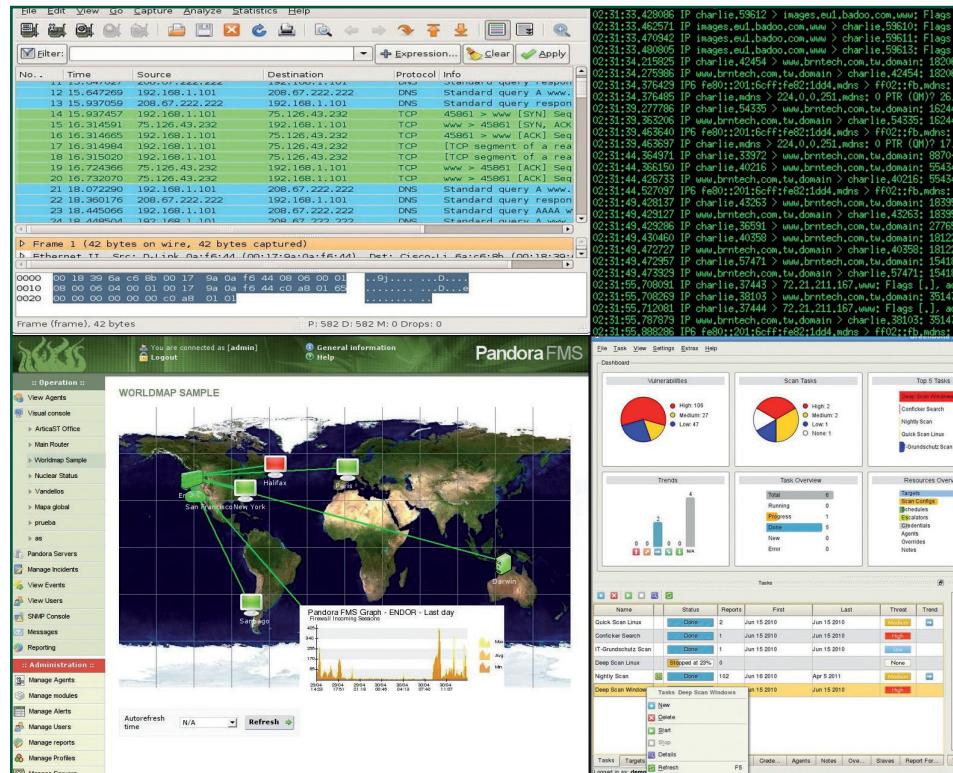


Figura 1.4

Herramientas de monitorización: Dos sniffer (arriba); un monitor de disponibilidad (abajo a la izquierda) y un gestor de amenazas (derecha).

- **Gestores de inventario.** Programas para la administración del parque de ordenadores y programas instalados. Por ejemplo: Lansweeper, IT-Inventory, OCS Inventory NG, Spiceworks GLPI, Free Network Management o Softperfect Network Scanner.
- **Monitores de estado de la red.** Programas que comprueban periódicamente que la electrónica de red esté operativa, que los servicios de la red estén en funcionamiento y que los niveles de tráfico no sean excesivos. Muestran alarmas en caso de que se produzca una anormalidad, almacenan historiales y generan gráficos y estadísticas para prevenir o rastrear problemas. Ejemplos de estos programas son Cacti, Nagios, Pandora, Hewlett Packard OpenView o CiscoWorks.
- **Gestores de amenazas (UTM).** Previenen o detectan los ataques al sistema. Comprueban el software instalado, lo comparan con listas de vulnerabilidades conocidas y sugieren mejoras y cambios, detectan contraseñas triviales, falta de software fundamental de seguridad y configuraciones poco recomendables. Descubren posibles ataques e identifican su naturaleza y procedencia. Algunos ejemplos de estos programas son Nessus, OpenVAS, Snort, Cisco MARS, Securepoint UTM for VMWare o Endian UTM Software.
- **Analizadores de protocolo (sniffers).** Analizan los mensajes y toda la información de protocolo que los acompaña en un punto determinado de una red. Los más utilizados son TCPDump, Wireshark, Cocoa Packet Analyzer y Packet Peeker.

1.6 Normas de seguridad y prevención de riesgos laborales

Si se trabaja con ordenadores es preciso tener en cuenta las siguientes **recomendaciones de seguridad** (Figura 1.5):

- La posición adecuada frente al ordenador es con la espalda recta y apoyada sobre las lumbares en el respaldo de la silla, los brazos y antebrazos formando ángulos rectos -igual que los muslos y pantorrillas-, los pies apoyados en el suelo, ayudándose si es necesario de un reposapiés, el monitor con la parte superior de la pantalla a la altura de los ojos de forma que no haya que levantar la cabeza para mirar y a una distancia mínima de 40 cm, las manos rectas respecto a los antebrazos, el teclado y el ratón como mínimo a 10 cm del borde de la mesa. Si el teclado es alto usar una almohadilla para apoyar las muñecas.
- Es importante evitar los contrastes fuertes de color, especialmente los brillos y colores chillones. El brillo y el contraste del monitor deben estar a niveles moderados.

Levantarse y tomarse un descanso al menos cada hora, aprovechar para hacer algunos ejercicios de estiramiento y para relacionarse con los compañeros. El aislamiento social es también un riesgo laboral importante cuando se trabaja con ordenadores una jornada completa.



Cuando se trata de entornos en los que hay instalados sistemas avanzados, como en los CPD (Centro de Control de Datos), donde se instalan los servidores y equipos de alto voltaje, es muy importante para el personal que trabaja con esos equipos que existan instalaciones eléctricas aisladas del resto y con dispositivos que eviten picos de tensión como los SAI (Sistema de Alimentación Ininterrumpida) que se conectan entre las tomas de corriente y los equipos. Los SAI son dispositivos que regulan la tensión eléctrica que reciben los equipos, con lo que en caso de un pico de tensión el equipo, PC o servidor, quedará a salvo.

Una característica interesante de estos equipos es que tienen una batería autónoma de la corriente eléctrica, con lo que en caso de apagarse la luz seguirá dando corriente al equipo durante un periodo de tiempo.

1.7 Sistemas de comunicación

Un sistema de comunicación es el conjunto de todos los elementos que participan en la transmisión de un mensaje: emisor, receptor, medio y código (Figura 1.6).

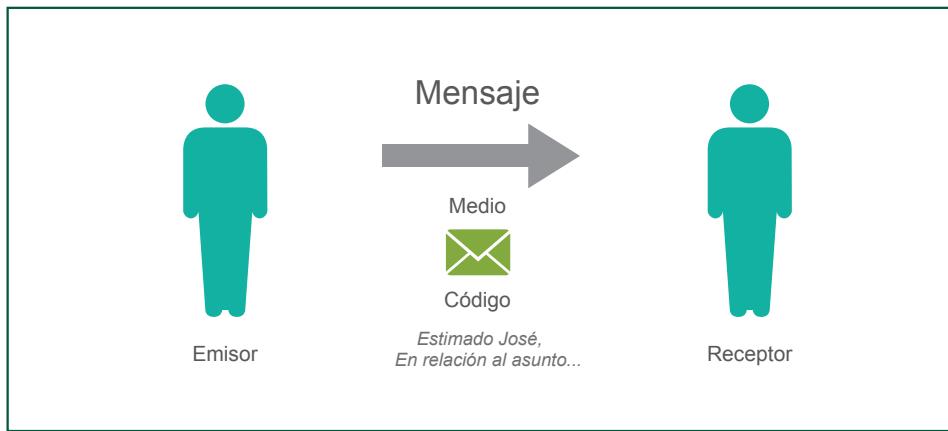


Figura 1.6
Comunicación es el acto de transmitir un mensaje de un emisor a un receptor mediante un código conocido por ambos a través de un medio.

En el ámbito de las aplicaciones web nos interesan los sistemas que pueden enviar mensajes a distancias largas y en intervalos muy cortos de tiempo. Estos sistemas se llaman **sistemas de telecomunicación**.

Cuando hablamos de sistemas informáticos, el esquema sobre la comunicación se extrae a los medios digitales, siendo el medio el sistema de cableado o redes inalámbricas, el mensaje viaja de manera encapsulada, comprimida y codificado en forma de bits que son emitidos y recibidos por equipos informáticos que hacen el papel de emisor y receptor de la información.

Este esquema, que en principio parece simple, puede llegar a ser más complejo cuando entran en juego las redes LAN (Red de Área Local) en las que la comunicación es ordenada, filtrada y distribuida para que en un entorno en el que hay varios emisores y receptores la información pueda llegar correctamente a su destino.

Para saber más

En los sistemas de comunicación, la manifestación física de un mensaje en un determinado código se conoce como señal.

1.8 Características de una red: ventajas e inconvenientes

Una **red informática** es un conjunto de dispositivos o sistemas informáticos que pueden cooperar entre ellos intercambiando información a través de un sistema de telecomunicaciones.

El uso de redes informáticas tiene numerosas ventajas que se resumen en la reducción drástica del tiempo necesario para conseguir cualquier tipo de información.

En las empresas, las redes informáticas ahorran tiempo y dinero en desplazamientos y viajes, generan oportunidades de negocio al proporcionar nuevas formas de contactar con clientes y colaboradores, agilizan el cierre de los negocios al poner informaciones complejas al alcance de los empleados inmediatamente y en cualquier lugar, reducen muy notablemente el coste de las comunicaciones al usar una única infraestructura para todos los servicios y reducen también el coste del sistema informático al concentrar la inteligencia de la red en unos pocos puntos, evitando así horas de mano de obra en mantenimiento y minimizando los requisitos de los costosos ordenadores de oficina.

Las redes informáticas también tienen inconvenientes. El más importante es el aumento del riesgo de que datos importantes para la organización puedan ser destruidos, alterados o robados. Cuanto más largo es el recorrido de la información, mayor es el riesgo de intercepción; y cuanto más centralizada esté, más graves serían las consecuencias de un desastre en caso de producirse.

1.9 Tipos de redes

Las redes, debido a su alcance, pueden clasificarse en cinco tipos fundamentales (Figura 1.7):

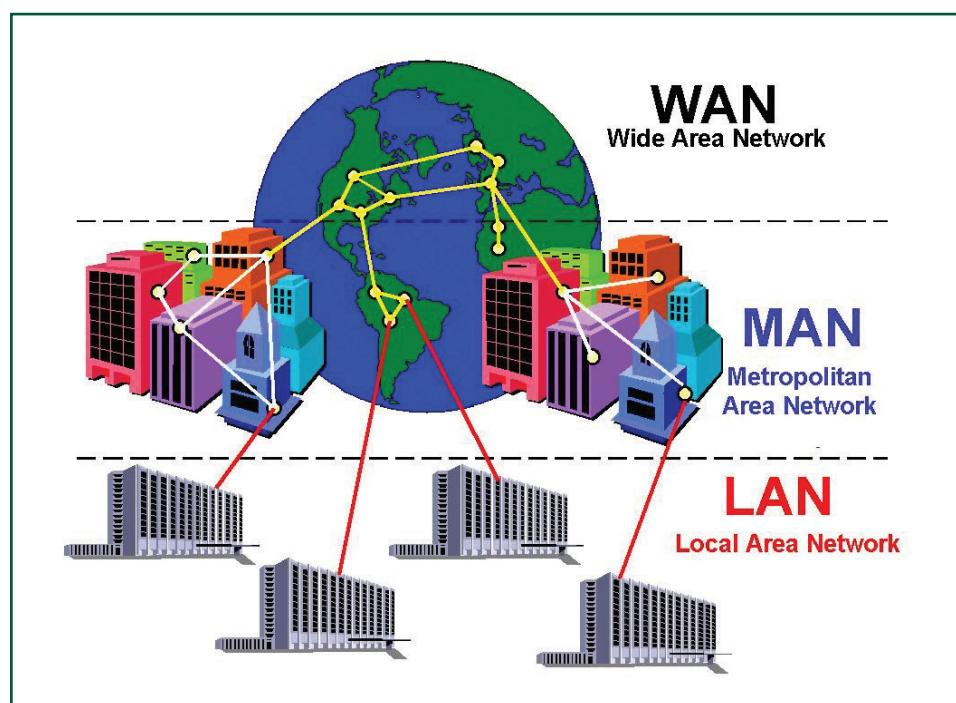


Figura 1.7

Conexión entre redes de diferentes tipos según su extensión geográfica

- **PAN (Red de Área Personal).** Son redes de muy corto alcance (hasta unos tres metros) que sustituyen al cable en la conexión entre dos dispositivos móviles, o entre un dispositivo móvil y otro fijo. La tecnología más utilizada para estas redes es Bluetooth.
- **LAN (Red de Área Local).** Son las redes que abarcan una sala o un edificio. Se utilizan en todo tipo de lugares de trabajo, y es habitual que estén disponibles en forma de redes inalámbricas en lugares de residencia. Es habitual llamar LAN a redes más grandes siempre y cuando cubran un área perteneciente a una única organización. Las tecnologías más utilizadas en redes de área local son Ethernet 10BaseT, 100BaseT o 1000BaseT (cable eléctrico de pares trenzados) para el cableado de plantas; WiFi b, g o n para las conexiones inalámbricas y Ethernet 1000BaseSX (fibra óptica multimodo) para las conexiones entre plantas.
- **CAN (Red de Área de Campus).** Son aquellas redes que abarcan varios edificios pertenecientes a una misma urbanización. Se utilizan típicamente tecnologías de fibra óptica monomodo o multimodo, como 1000BaseLX.
- **MAN (Red de Área Metropolitana).** Son redes con infraestructura propia que permiten la comunicación entre diferentes sedes de una misma organización dentro de una misma localidad. Se utilizan fibras ópticas monomodo y enlaces punto a punto ópticos o de microondas.
- **WAN (Red de Área Amplia).** Son todas aquellas redes que permiten a diferentes equipos informáticos conectarse en un área mayor que una localidad. Generalmente están administradas por empresas registradas como proveedoras de servicios de telecomunicaciones. Se utilizan medios pasivos diversos para una misma red, siendo la fibra óptica el más utilizado.

1.10 Componentes de una red informática

Una red informática se compone principalmente de tres tipos de dispositivos:

- **Hosts o Dispositivos finales.** Son los dispositivos que originan la información (emisores) y los que finalmente la reciben (receptores). Pueden ser ordenadores o dispositivos personales, ordenadores de empresa, servidores o dispositivos informáticos de servicio, como impresoras, cámaras de vídeo en red, sistemas de autenticación, sensores de alarmas, teléfonos IP, etc.
- **Medios de transmisión pasivos.** Son los medios a través de los cuales se transmite la información sin que se produzca ninguna alteración intencionada de la señal. Básicamente se utilizan los tres siguientes:

- **Cable eléctrico.** Cable coaxial o de par trenzado homologado según la misma normativa que cumplen los equipos que conecta.
 - **Fibra óptica.** Cable de fibra de vidrio para el transporte de luz homologado según la normativa de los equipos que conecta y según de la red en cuanto a distancia y velocidad.
 - **Ondas electromagnéticas.** Ondas de luz, radiofrecuencia o microondas transmitidas en el vacío o en la atmósfera.
- **Electrónica de red o medios de transmisión activos.** Son dispositivos electrónicos que adaptan, modifican o dirigen las señales para asegurar que los mensajes llegan a sus destinatarios de la mejor manera posible.

1.11 Topologías de red

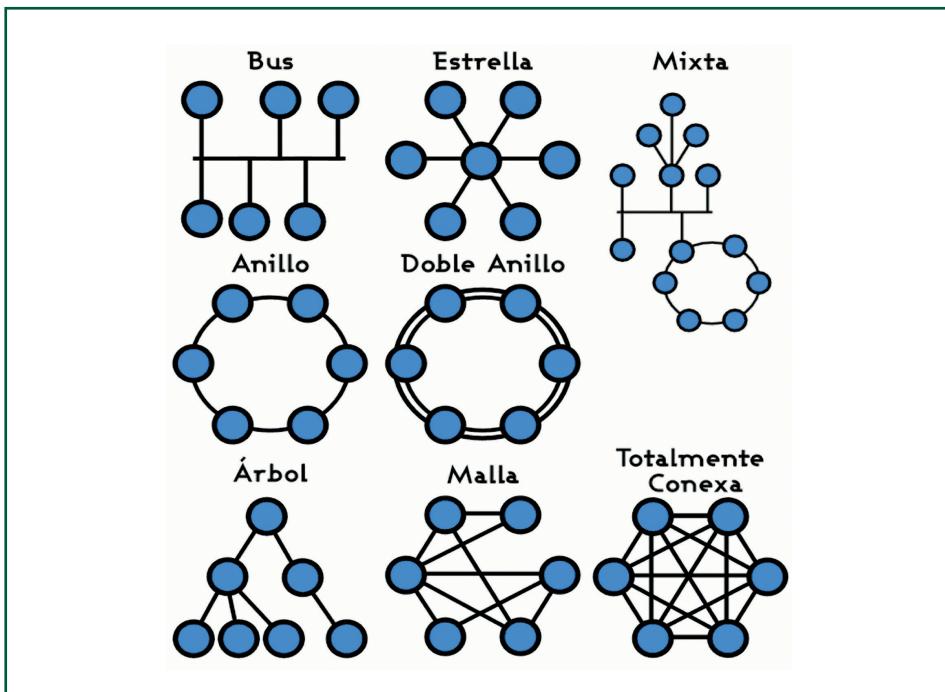
Una topología es una representación de cómo se conecta una red de telecomunicación mediante dos tipos de elementos: **nodos**, que representan a los dispositivos, sean *hosts* o medios de transmisión activos; y **enlaces**, que representan a los medios de transmisión pasivos.

Para saber más

Antiguamente, era necesario crear una red diferente para cada servicio de comunicaciones que se quisiera implantar en la sede de una empresa, ya fuese de telefonía, alarmas, control de acceso al edificio, hilo musical, etc. En la actualidad, sólo es necesaria una única infraestructura digital, la misma que comunica a los sistemas informáticos, para poder transportar todos los servicios de comunicaciones presentes y futuros en un edificio empresarial.

Las topologías básicas son (Figura 1.8):

- **Bus.** Redes en las que todos los nodos comparten un único enlace.
- **Estrella.** Redes en las que todos los nodos convergen en un nodo central y cada nodo tiene un enlace dedicado con el nodo central.
- **Anillo.** Redes en las que los nodos están conectados sucesivamente, y el primero con el último formando un anillo. Entre cada nodo y el sucesivo hay un enlace.
- **Doble anillo.** Redes las que los nodos están conectados sucesivamente, y el primero con el último formando un anillo. Entre cada nodo y el sucesivo hay **dos enlaces**.
- **Árbol o estrella extendida.** Redes jerárquicas con un nodo principal al que están conectados unos nodos secundarios, a los cuales pueden estar conectados otros nodos, y así sucesivamente.
- **Malla.** Redes en las que cada nodo tiene un enlace al menos con otro nodo, y puede tener enlaces con varios nodos.

**Figura 1.8**

Representación gráfica de diferentes topologías de red, donde se distinguen los nodos (círculos) y los enlaces (líneas).

1.12 Medios de transmisión

La forma física que adquiere un mensaje durante el camino recorrido entre el emisor y el receptor es una **onda electromagnética** llamada **señal**. El camino recorrido por esa señal se llama **medio de transmisión**. Existen diferentes tipos de medios de Transmisión. Los siguientes son los principales:

- **Medios de transmisión pasivos guiados.** Son cables por cuyo interior se desplazan las señales.
 - **Cables eléctricos.** Cables especialmente diseñados para la transmisión y que cumplen normativas para asegurar la calidad y las prestaciones.
 - **Fibra óptica.** La señal viaja en forma de luz, emitida por un diodo o por un láser, a través de una fibra de vidrio.
- **Medios de transmisión pasivos no guiados.** La propia señal es el medio. Se emite al espacio utilizando una antena, un led o un láser.
 - **Enlaces punto a punto.** La señal se emite en una sola dirección desde un emisor a un receptor mediante láser o antena parabólica. De esta manera se minimizan las pérdidas de señal y las interferencias, y lo que es aún más importante, se deja libre el espacio radioeléctrico para otras emisiones.

Recuerda

Los mensajes se propagan de un lugar a otro a través de medios pasivos, pero pueden ser procesados por medios activos para que el envío sea más eficiente.

- **Difusión.** La señal se emite en todas las direcciones mediante una antena y puede ser recibida por cualquier *host* que se encuentre dentro de la distancia de alcance de dicha señal.

• **Medios de transmisión activos.** Son equipos electrónicos que manipulan las señales para una transmisión más eficiente. Algunos ejemplos son los siguientes:

- **Transceptores.** Adaptan la señal para pasar de un medio a otro medio diferente.

- **Pasarelas de red.** Adaptan la señal y los protocolos para pasar de una red a otra diferente.

- **Enrutadores o routers.** Pasarelas que conectan varias redes y envían los mensajes a la red apropiada para que llegue a su destino. Trabajan en la capa de red del modelo OSI.

- **Repetidores.** Restablecen la señal que llega débil de un emisor lejano antes de que empiece a deteriorarse.

- **Repetidores multipuerto o hubs.** Tienen varias tomas (puertos) de conexión. La señal que reciben por una toma la reenvían por todas las demás, ya que trabajan en la capa física del modelo OSI.

- **Conmutadores o switches.** Tienen varios puertos de conexión. La señal que reciben por un puerto la reenvían únicamente por el puerto al que está conectado el destinatario, ya que trabajan en la capa de enlace de datos del modelo OSI.

- **Multiplexores.** Reciben señales procedentes de varias entradas y las reenvían por una única salida.

- **Demultiplexores.** Reciben varias señales multiplexadas en una única entrada y las reenvían por una salida diferente para cada señal.

1.13 Tipos de cableado. Conectores

Las **redes informáticas** conectan dispositivos de numerosos fabricantes. Para permitir la operación entre ellos, los cables y las clavijas de conexión (conectores) deben seguir unas normas rigurosas que determinan tamaños, formas y tensiones, así como requisitos de calidad técnica, como la máxima distancia a la que pueden transmitir una señal sin problemas o la velocidad de transmisión expresada en bits por segundo. En redes cableadas, las normas más utilizadas son las Ethernet (Figura 1.9) y algunas de ellas son:

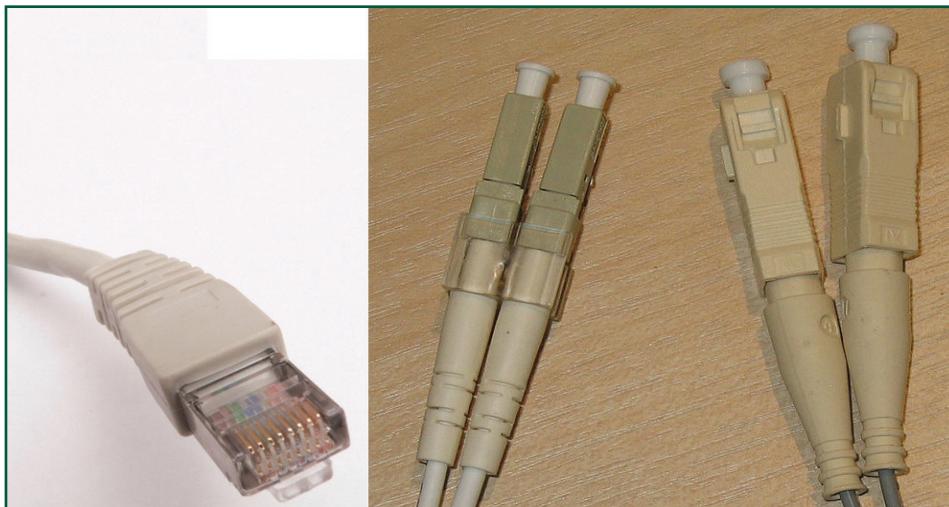


Figura 1.9

Conectores usados en redes Ethernet. De izquierda a derecha, RJ45 (cobre), LC (fibra óptica monomodo) y SC (fibra multimodo).

• **Cable eléctrico Ethernet:**

- **10Base2.** 10 Mbps sobre cable coaxial fino, hasta 185 m.
- **10BaseT.** 10 Mbps sobre cable de par trenzado y conector RJ-45, hasta 100 m.
- **100BaseT.** 100 Mbps sobre cable de par trenzado y conector RJ-45, hasta 100 m.
- **1000BaseT.** 1 Gbps sobre cable de par trenzado y conector RJ-45, hasta 100 m.
- **10GBaseT.** 2 x 5 Gbps sobre cable de par trenzado y conector RJ-45, hasta 100 m.

• **Fibra óptica Ethernet:**

- **1000BaseSX.** 1 Gbps sobre fibra óptica multimodo, hasta 550 m con fibra de 50/125 μ m.
- **1000BaseLX.** 1 Gbps sobre fibra óptica monomodo y multimodo, hasta 5 km con fibra monomodo de 10 μ m.
- **10GBaseSR.** 10 Gbps sobre fibra óptica multimodo, hasta 400 m con cable OM4.
- **10GBaseLR.** 10 Gbps sobre fibra óptica monomodo, hasta 10 km.

• **Conectores:**

- **RJ45.** Es el conector utilizado en todas las normas Ethernet para cable eléctrico con par trenzado.

- **SC.** Conector muy común para fibras ópticas multimodo.

- **LC.** Conector fácil de insertar y de pequeño tamaño para fibras ópticas monomodo y multimodo.

1.14 Mapa físico y mapa lógico de una red local

El **mapa físico** de una red local es un esquema en el que se identifican todos los hosts y medios que componen una red de ordenadores, se ubican en el espacio y se detallan conector a conector todas las conexiones de datos (Figura 1.10).

El **mapa lógico** de una red local es un esquema que identifica a cada host ante el resto de la red asignándole una dirección. La dirección de un host sigue una normativa según la tecnología de red instalada y limita con qué otros hosts puede comunicarse. En un mapa lógico, aquellos equipos de electrónica de red que pueden actuar como servidores o como clientes de servicios se consideran *hosts*.

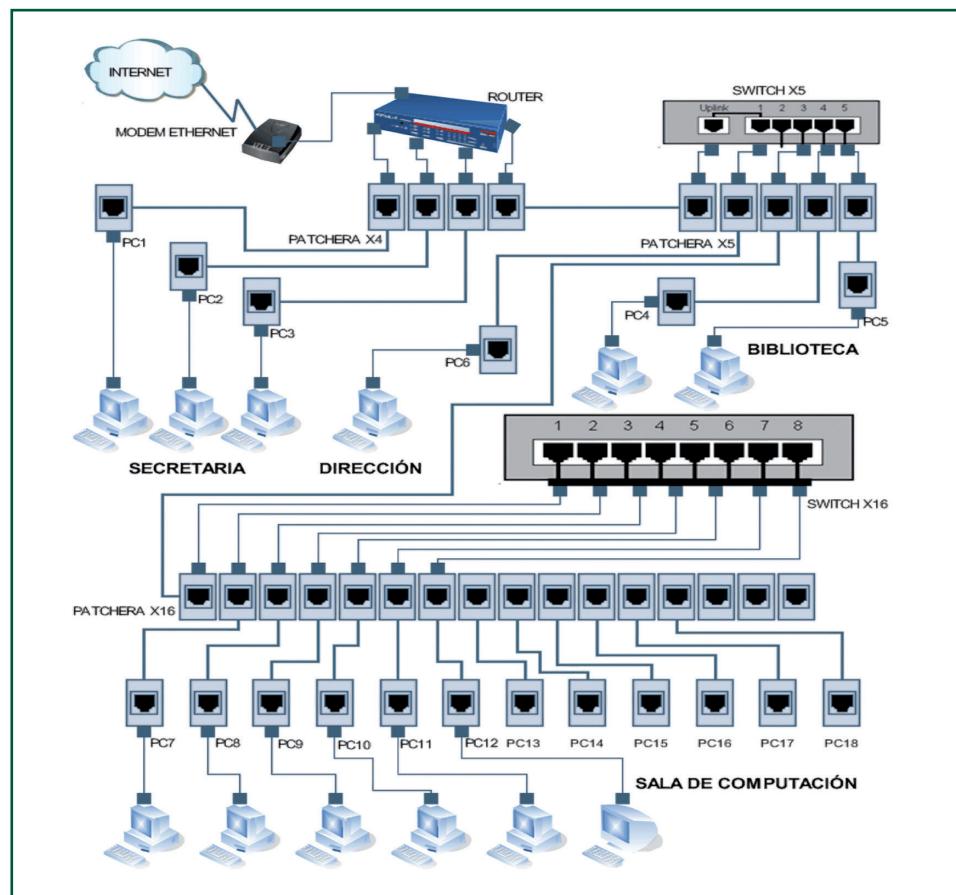


Figura 1.10

Mapa físico de una red local en el que se muestran los ordenadores, las tomas de red de cada PC numeradas, las conexiones entre los paneles de parcheo (*patch panel*), switches, router y módem de Internet.

Resumen

Los ordenadores están compuestos básicamente por una unidad de procesamiento que realiza cálculos sobre los datos almacenados en la memoria; ésta tiene la capacidad de leer y escribir datos de manera más rápida que las unidades de almacenamiento, como los discos duros, en los que se almacenan los archivos de los programas.

Un sistema informático son todos los elementos, físicos y humanos, necesarios para que puedan funcionar los equipos informáticos. Son tan importantes los ordenadores como los programas instalados, así como también los programadores que los desarrollan o los administradores y usuarios que los utilizan a diario. En definitiva, todos estos elementos conforman el sistema informático.

Una red informática es la interconexión de varios dispositivos informáticos que comparten información o funcionalidades a través de un medio físico, ya sea cableado o inalámbrico.

Las redes pueden clasificarse según la estructura en la que se interconectan sus diferentes nodos, de los que cabe destacar las topologías: bus, estrella, malla o anillo. Asimismo, mientras la disposición de los elementos de una red conforma el mapa físico (conexiones cableadas), el modo en el que los paquetes de información viajan a través de la red se denomina mapa lógico.

Ejercicios de autocomprobación

Indica si las siguientes afirmaciones son verdaderas (V) o falsas (F):

1. Los ordenadores están formados por dispositivos que se relacionan unos con otros formando una arquitectura y cada ordenador tiene su propia arquitectura; sin embargo, elementos como CPU, BIOS, RAM, interfaces y buses son comunes a la gran mayoría.
2. La cantidad de aplicaciones que un equipo puede estar ejecutando al mismo tiempo depende del tamaño de almacenamiento de la memoria, así como de su velocidad de lectura y escritura.
3. Dada la rápida evolución del software y sus necesidades de rendimiento, no es habitual encontrar equipos que no puedan soportar las necesidades de procesamiento de un programa, y que no tengan memoria RAM suficiente.
4. El hardware es el conjunto de máquinas que permite, directa o indirectamente, automatizar la resolución del problema siguiendo las instrucciones de los programas.
5. Fallo físico o mala configuración de la electrónica de red y defectos en el software de la máquina afectada pueden, entre otros, ser la causa de los errores en un sistema informático.
6. En la actualidad, solo es necesaria una única infraestructura digital, la misma que comunica a los sistemas informáticos para poder transportar todos los servicios de comunicaciones presentes y futuros en un edificio empresarial.

Completa las siguientes afirmaciones:

7. La memoria de acceso aleatorio (en inglés, *random-access memory*) es una memoria de _____ utilizada para almacenar las _____ de los _____ que se están ejecutando, así como los procesos del sistema _____. Se denomina de acceso aleatorio porque su principal característica es que tiene el mismo tiempo de acceso independientemente de la posición en la que están los _____ almacenados.

8. Una topología es una _____ de cómo se conecta una red de _____ mediante dos tipos de elementos: _____, que representan a los _____, sean hosts o medios de transmisión activos; y _____, que representan a los medios de transmisión pasivos.
9. Las _____ informáticas conectan dispositivos de numerosos fabricantes. Para permitir la operación entre ellos, los _____ y las clavijas de conexión (conectores) deben seguir unas normas rigurosas que determinan tamaños, formas y _____, así como requisitos de calidad técnica, como la máxima _____ a la que pueden transmitir una señal sin problemas o la velocidad de transmisión expresada en _____ por segundo.
10. El mapa lógico de una _____ local es un _____ que identifica a cada host ante el resto de la red asignándole una _____ que sigue una normativa según la tecnología de red instalada y limita con que otros hosts puede comunicarse. En un mapa lógico, aquellos equipos de _____ de red que pueden actuar como _____ o como clientes de servicios se consideran hosts.

Las soluciones a los ejercicios de autocomprobación se encuentran al final de este módulo. En caso de que no los hayas contestado correctamente, repasa la parte de la lección correspondiente.

2. INSTALACIÓN DE SISTEMAS OPERATIVOS

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.

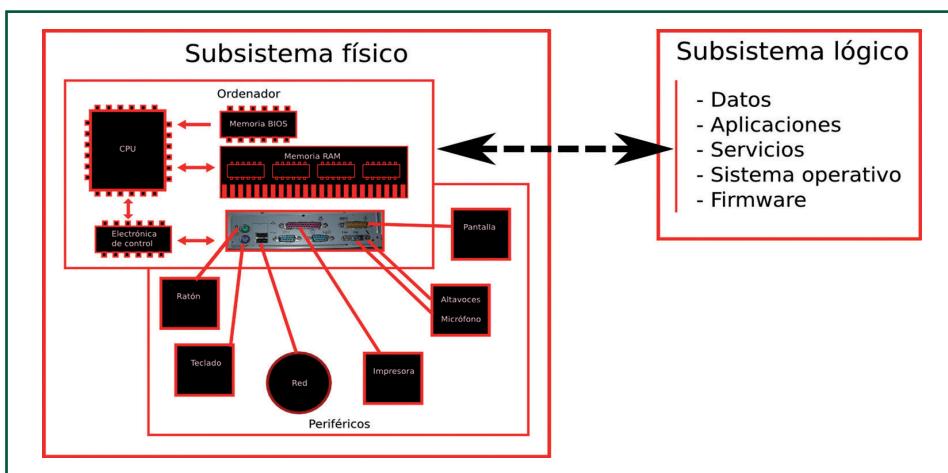
En esta unidad aprenderás a distinguir los diferentes tipos de programas que componen la inteligencia de un ordenador; también conocerás la funcionalidad de un sistema operativo, cuáles son los programas que la llevan a cabo y cómo se relacionan entre ellos. Verás, además, las principales características 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 extensos, que permiten aprovechar los recursos de una máquina compartiendo el hardware entre varios sistemas.

2.1 Estructura de un sistema informático

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 (Figura 2.1).

**Figura 2.1**

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:

- **Programas.** Los programas son los elementos de software que contienen las instrucciones para que la CPU sepa qué operaciones debe realizar en cada momento.
- **Firmware.** Se trata de un software grabado permanentemente en un chip de la computadora y proporcionado por el fabricante de ésta. Contiene las primeras instrucciones que lee CPU al encender el ordenador, las cuales sirven para comprobar cuáles son los dispositivos que forman el ordenador y en qué estado se encuentran, para proporcionar una configuración básica a estos dispositivos y para iniciar la carga de instrucciones a la memoria RAM desde uno de los dispositivos de almacenamiento masivo, generalmente el disco duro.
- **Sistema operativo.** Es el grupo de programas responsables de controlar el funcionamiento de la máquina, eliminando la necesidad de que cada uno del resto de programas instalados en el ordenador tengan que realizar por sí mismos dicha tarea.
- **Servicios.** Son programas que realizan tareas para facilitar el funcionamiento de otros programas. Estas tareas se realizan sin que el usuario de la computadora necesite intervenir ni ser informado de que se están realizando.
- **Aplicaciones.** Son todos aquellos programas que resuelven de forma directa los problemas planteados por el usuario.
- **Datos.** Los datos son informaciones manejadas o procesadas por el ordenador, pero que en ningún caso le dicen a éste lo que tiene que hacer para resolver un problema.

2.2 Arquitectura de un sistema operativo

Un sistema operativo se caracteriza por los siguientes elementos:

- **Núcleo o Kernel.** El núcleo es el programa que realiza las funciones principales del sistema operativo. Existen diferentes tipos de núcleo:

- **Monolíticos.** 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.

- **Micronúcleos.** Un micronúcleo se limita a albergar y coordinar procesos independientes que realizan las funciones del sistema operativo en forma de servicios. 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.

- **Monolíticos con módulos dinámicos.** Son núcleos más flexibles y pequeños que los monolíticos puros al añadir la posibilidad de cargar y descargar partes del programa en la memoria externa mientras están funcionando.

- **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.

- **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 éste.

- **Otros programas del sistema base:**

- **Intérprete de comandos o Shell.** Es una aplicación que permite al usuario pedir al sistema operativo prácticamente cualquier cosa que éste pueda realizar mediante la escritura de órdenes en forma de texto llamadas comandos.

- **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.** Un compilador es un programa que convierte textos, escritos en un lenguaje similar a un lenguaje humano natural, a programas que entiende la CPU.

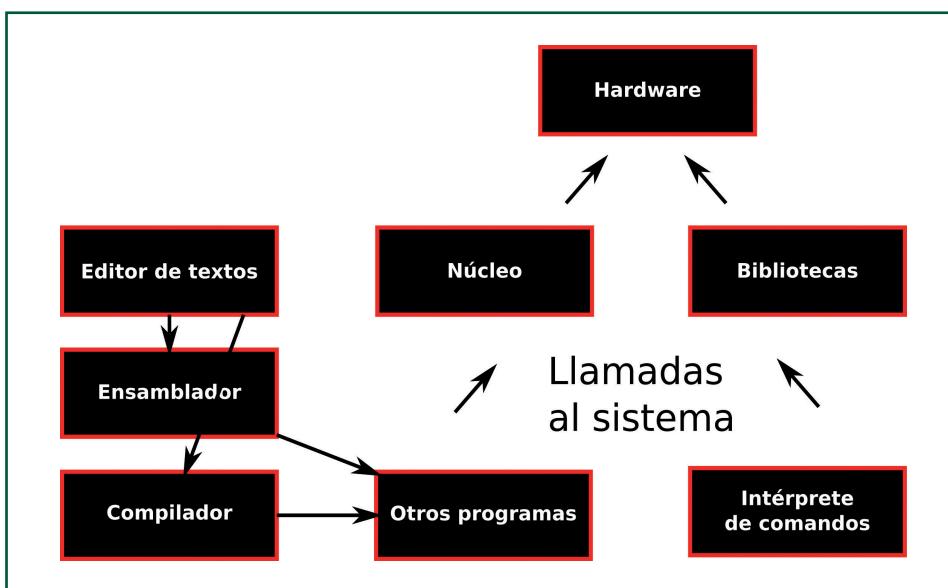


Figura 2.2

El sistema operativo está formado por el núcleo, las bibliotecas, el intérprete de comandos y programas accesorios, como un editor de textos, un ensamblador o compiladores de diversos lenguajes de programación.

2.3 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 (Figura 2.3):

- **Gestión de tareas.** Los sistemas operativos actuales son multitarea, lo cual significa que la CPU debe repartir su tiempo de trabajo entre varios programas ac-

Recuerda

El sistema operativo es el conjunto de programas que gestiona los recursos físicos de un ordenador.

tivos 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.

- **Gestión de dispositivos.** Un sistema operativo conoce cuáles son las operaciones que debe realizar sobre un dispositivo físico para que éste cumpla su propósito, proporciona al resto de programas herramientas de comunicación para que éstos 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.
- **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 ésta 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.

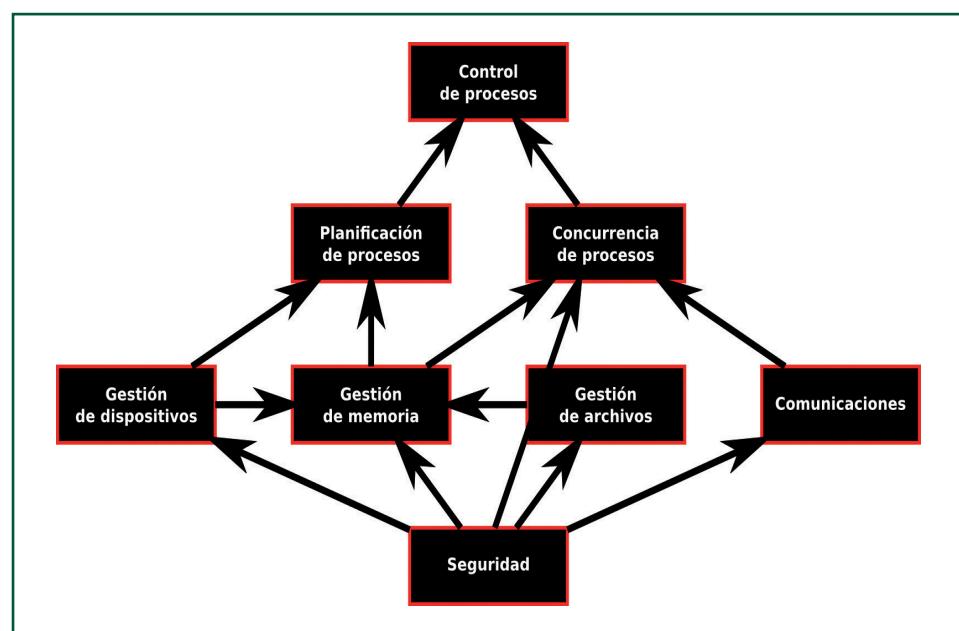


Figura 2.3

El sistema operativo gestiona los recursos mediante tareas interdependientes.

2.4 Tipos de sistemas operativos

Los sistemas operativos se clasifican según los siguientes criterios:

- **Usuarios simultáneos:**

- **Monousuario.** El sistema sólo admite un único terminal, es decir, un usuario con una pantalla, un teclado y un ratón.
- **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.
- **Bits.** Los fabricantes de microprocesadores han ido creando diferentes CPU con prestaciones cada vez mayores. El salto generacional más importante entre dos diseños se produce al aumentar el número de bits que el procesador maneja en una sola operación, que va desde 4 hasta 128. El número de bits de un sistema operativo hace referencia al tamaño de palabra que maneja la CPU para la que ha sido compilado.

- **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.
- **Multitarea.** El sistema operativo mantiene el control de la CPU enviándole programas que se ejecutan por fragmentos, dando la sensación de que todos están trabajando a la vez.

- **Arquitectura del núcleo:**

- **Monolítico.** Es una arquitectura de sistema operativo donde éste, en su totalidad, trabaja en el espacio del núcleo. Difiere de otras arquitecturas en que sólo 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.

- **Microkernel.** Es un tipo de núcleo de un sistema operativo que provee un conjunto de primitivas o llamadas mínimas al sistema para implementar servicios básicos, como espacios de direcciones, comunicación entre procesos y planificación básica. Todos los otros servicios (gestión de memoria, sistema de archivos, operaciones de E/S, etc.), que en general son provistos por el núcleo, se ejecutan como procesos servidores en espacio de usuario. En sus orígenes, el microkernel pretendía ser una solución a la creciente complejidad de los sistemas operativos. Las principales ventajas de su utilización son la reducción de la complejidad, la descentralización de los fallos (un fallo en una parte del sistema no se propagaría al sistema entero) y la facilidad para crear y depurar controladores de dispositivos, lo que produce una mejora en la tolerancia a los fallos y eleva la portabilidad entre plataformas de hardware. Los principales inconvenientes del microkernel son:

- Mayor complejidad en la sincronización de todos los módulos que lo componen.
- Su acceso a la memoria.
- Mayor complejidad en el código.
- Menor rendimiento.
- Limitaciones en diversas funciones.

• **Comunicación con el usuario:**

- **Gráfico.** El sistema operativo tiene integrado un entorno gráfico para el usuario (GUI). Por ejemplo, el escritorio de Windows o el Mac OS de los ordenadores de Apple.

- **No gráfico.** 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 X-Window System.

2.5 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:

- **Personales.** Programas diseñados para resolver problemas de una sola persona.

En esta categoría entran las aplicaciones de agenda, de comunicación individual, de reproducción de contenidos audiovisuales, programas didácticos de cultura general o de enseñanza reglada, videojuegos o programas para el ocio. En la medida en que se utilizan para atender necesidades personales también se pueden considerar los programas de ofimática.

- **Profesionales.** Son programas destinados a satisfacer las necesidades de usuarios profesionales ayudando a la elaboración de productos, como los programas de Diseño Asistido por Ordenador (CAD) para arquitectura e ingeniería, ayuda al diagnóstico en medicina, consulta de leyes en forma de hipertexto para juristas o programas profesionales de creación artística. También forman parte de esta categoría los programas de gestión enfocados a profesiones específicas o a microempresas.

- **Industriales.** Esta categoría la forman los programas destinados al control de procesos industriales, los cuales se caracterizan por ser muy estables y estar creados a la medida del usuario. Se incluyen los programas de control de maquinaria industrial, de seguridad, de procesos químicos, de tráfico portuario y aeroportuario, y un largo etcétera.

- **Gestión empresarial.** Se incluyen en esta categoría los sistemas de planificación de recursos empresariales (ERP), ya sean personalizados o hechos a medida, los programas para la gestión de pequeñas y medianas empresas y los programas de ofimática.

- **Científicas.** Son las aplicaciones que se utilizan para la asistencia a la investigación científica.

- **Herramientas.** Las herramientas son los programas que realizan tareas de mantenimiento y personalización del sistema a petición del usuario.

2.6 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.

Ese permiso se concede en forma de licencia. Se muestran a continuación las modalidades más comunes de licencia aplicables a un programa de ordenador (Figura 2.4):

Figura 2.4

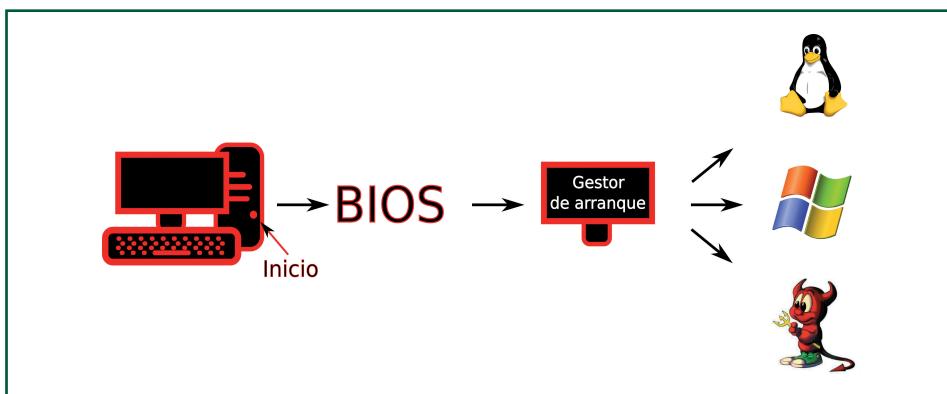
Las licencias pueden ser de uso restringido, de prueba, *freeware*, libre con *copyleft* y libre permisiva.

	Uso Restringido	Prueba	Freeware	Libre <i>Copyleft</i>	Libre Permisiva
Acceso a todas las características.	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 modificado.				Sí	Sí
Cambio de licencia por otra más restrictiva.					Sí

- **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.
- **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.** Licencias de uso restringido que se conceden gratuitamente.
- **Libre.** 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.** El redistribuidor no puede cambiar la licencia por otra si ésta reduce los derechos del usuario.
 - **Libre Permisiva.** El redistribuidor puede cambiar la licencia sin límites.

2.7 Gestores de arranque

Cuando un ordenador se pone en marcha, la CPU va a buscar su primera orden a la memoria Bios, 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 éste el control de la CPU (Figura 2.5).

**Figura 2.5**

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

La función del gestor de arranque más atractiva para el desarrollador web es la posibilidad de escoger entre diferentes sistemas operativos en una misma máquina. Existen muchos gestores de arranque diferentes; los principales son los siguientes:

- **Microsoft:** NTLoader, WBM.
- **Libres:** LILO, GRUB.
- **Independientes:** Paragon, BootMagic.

2.8 Máquinas virtuales

Una máquina virtual es un programa de ordenador que emula el funcionamiento de otro sistema informático completo, pudiendo realizar en él todas las operaciones que haríamos en un hardware real. Existen varios tipos (Figura 2.6):

Nombre	Tipo	Descripción
VWWare	Replicación de hardware.	Entorno muy utilizado en empresas.
Hyper-V	Replicación de hardware.	Entorno de Microsoft 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.

Figura 2.6

Ejemplos de máquinas virtuales de replicación, de emulación y de proceso.

- **De sistema.** Emulan un ordenador real:

- **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 el alojamiento de servicios que no pueden convivir con otros en una misma máquina y la creación de entornos virtuales que replican la red de la empresa para el desarrollo y para las pruebas. Las máquinas virtuales pueden ser fácil y rápidamente copiadas y restablecidas, conservando íntegramente su estado, por lo que son ideales para la experimentación. Pueden ser apagadas, dejando de consumir recursos de CPU, y destruirse liberando completamente al 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 ésta 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 VMWare, que se mantiene como líder del sector, y Hyper-V, que cada vez tiene una implantación más alta. Al decidir virtualizar nuestros equipos, deberemos conocer las ventajas e inconvenientes que esto implica.

Las principales ventajas de la virtualización son:

- Reduce el coste y los riesgos al tiempo que aumenta la calidad y el aprovechamiento de los equipos.
- Permite crear diferentes sistemas operativos totalmente independientes entre ellos en una misma máquina. Esto supone prescindir de tener que comprar un equipo nuevo por cada sistema operativo que necesitemos utilizar.
- Permite un mejor aislamiento y administración de los recursos.

Entre sus principales inconvenientes, se incluyen los siguientes:

- Un fallo en el hardware supondría la caída de todos los sistemas virtuales ejecutados en esa máquina.
- Para dar un servicio óptimo a los equipos virtualizados, es necesario un hardware de gran potencia y, por lo tanto, más caro.

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? El paso...

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



Para ampliar este tema, puedes ver el videotutorial **Creación de una máquina virtual**, que encontrarás en el Campus online.

llaman *VMWare Tools* y es recomendable instalarlas en todos los sistemas operativos virtuales.

La virtualización de los sistemas, cada vez más utilizada, pone en conflicto, las compañías desarrolladoras de software, que ven que su sistema de licencias por usuario carece de sentido, porque los programas dejan de estar vinculados a un único equipo.

2.9 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:

- **El uso al que van destinados:** personal, profesional o servidor:
 - **Uso personal.** Las alternativas son Windows, MacOS y algunas colecciones de software con licencia libre.
 - **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 colecciones 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 gráfico y producción musical por su fiabilidad; y Linux es valorado en ambientes académicos y de investigación por su versatilidad.
 - **Uso como servidor.** 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 cualificado 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 personal técnico dentro de la empresa para poderla llevar a cabo.
- **Requisitos de hardware.** Cada sistema operativo se adapta sólo a determinadas máquinas; por tanto, el sistema operativo y el hardware deben escogerse conjuntamente.
- **Licencia libre o propietaria.** Los sistemas operativos con licencia libre permiten planificar y desarrollar un sistema informático sin depender de intereses externos y sin coste por licencias; por tanto, a largo plazo, son preferibles a sistemas con licencia propietaria. Sin embargo, los sistemas informáticos ya presentes en la mayoría de las empresas están basados en soluciones con licencia propietaria, las cuales utilizan protocolos y formatos de datos exclusivos que obstaculizan sustancialmente la introducción de software libre. Este obstáculo es mayor cuanto más compleja es una organización y se agrava con el hecho de que el personal está formado para aplicar soluciones propietarias.

2.10 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 el tipo de usuario final, las aplicaciones que se ejecutarán y los recursos de la empresa, tanto económicos como técnicos.

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 Vista, que fue substituido por una versión más reciente, Windows 7, siendo este último mucho más eficiente y rápido que el 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 siguientes pasos:

- 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 (Figura 2.7) siguiendo paso a paso la guía de instalación.



Figura 2.7

Ejemplo de escritorio del sistema operativo Debian.

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

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 seguridad para el equipo.

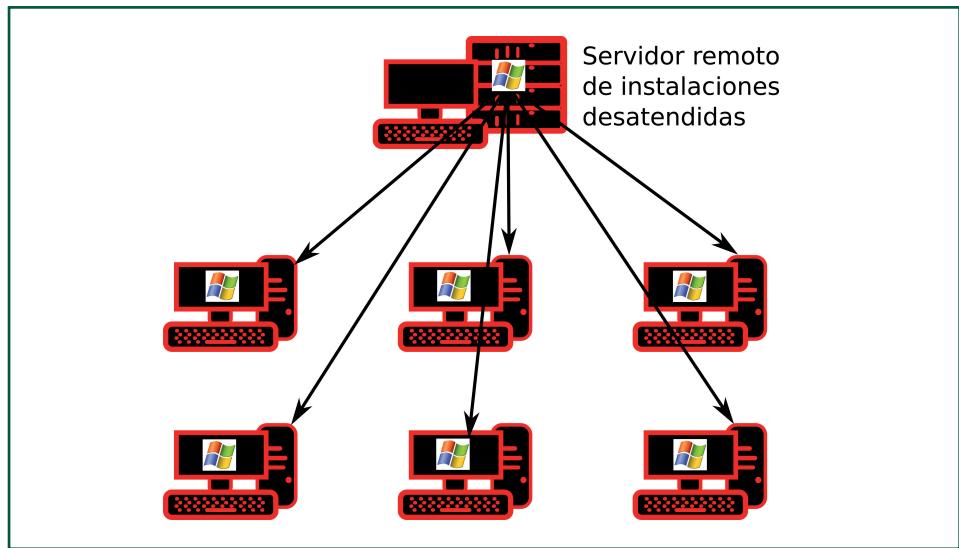
La instalación de las diferentes versiones de un programa no requiere de una reinstalación del software. Generalmente, basta con ejecutar un archivo de actualización para que los cambios se apliquen a los archivos ya instalados. Es cada vez más común que los programas se conecten a Internet en segundo 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.

2.12 Uso de instalaciones desatendidas

Instalar sistemas operativos en un entorno empresarial puede suponer muchas horas de trabajo. Las siguientes técnicas (Figura 2.8) pueden facilitarnos bastante la tarea:

- **Instalación desatendida.** Se graba en un fichero todas las respuestas a las preguntas que el sistema operativo hace cuando se está instalando. El programa instalador utilizará ese fichero 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.

Figura 2.8
Instalación remota de un sistema operativo en varios ordenadores desde un servidor central.



2.13 Actualización de sistemas operativos y aplicaciones

Es preciso actualizar los programas de nuestro ordenador para tener mayor estabilidad, más funciones o menos vulnerabilidad a posibles ataques. 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 (Figura 2.9).

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.

```

charlie:/home/chas# apt-get dist-upgrade
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Calculando la actualización... Listo
Se instalarán los siguientes paquetes NUEVOS:
  libx264-118
Se actualizarán los siguientes paquetes:
  acpid acroread acroread-data acroread-debian-files acroread-dictio
  calendar-google-provider calendar-timezones cpufrequtils cups cups
  evince-common exim4 exim4-base exim4-config exim4-daemon-light ffm
  isc-dhcp-common kdelibs-bin kdelibs5-data kdelibs5-plugins kdoctoo
  libbind9-60 libburn4 libc-bin libc-dev-bin libc6 libc6-dev libc6-i
  libdbus-1-3 libdns69 libevince2 libfreetype6 libfreetype6-dev libg
  libkde3support4 libkdecorc5 libkdesu5 libkdeui5 libkdnsd4 libkf
  libkparts4 libkpty4 libkrb5-3 libkrb5support0 libkrosscor
  libpam-modules libpam-runtime libpam0g libpcap0.8 libperl5.10 libp
  libsmclient libsndfile1 libsolid4 libsoup-gnome2.4-1 libsoup2.4-1
  libxml2-utils linux-base linux-image-2.6.32-5-686 linux-libc-dev l
  openoffice.org-base-core openoffice.org-calc openoffice.org-common
  openoffice.org-java-common openoffice.org-l10n-es openoffice.org-w
  perl perl-base perl-doc perl-modules policykit-1 python-apt python
  update-inetd ure usbutils x11-common x11-xserver-utils xbase-clien
  xulrunner-1.9.1
223 actualizados, 1 se instalarán, 0 para eliminar y 0 no actualizad
Necesito descargar 472 MB de archivos.
Se utilizarán 11,0 MB de espacio de disco adicional después de esta
Operación.
Desea continuar [S/n]? []

```

Figura 2.9

Ejemplo de orden de actualización de todos los programas en el intérprete de comandos de Debian (Linux).

- **En entornos Windows.** El sistema operativo se actualiza automáticamente con 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.

2.14 Ficheros de inicio de sistemas operativos

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:

Para saber más

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

- 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 (Figura 2.10):

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

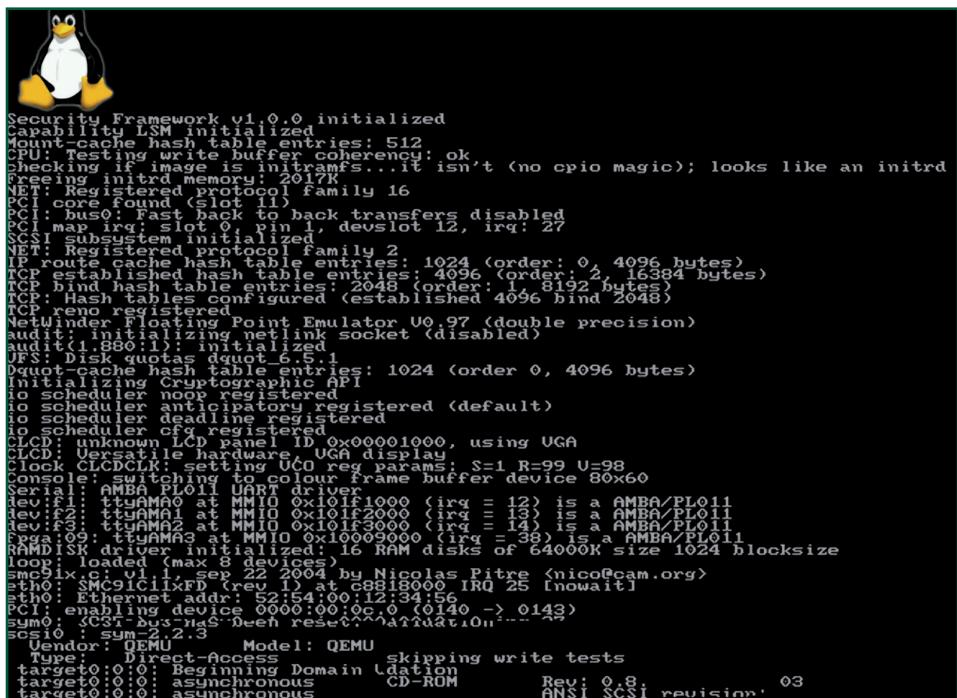


Figura 2.10

Ejemplo de carga y habilitación del hardware en el intérprete de comandos de Debian (Linux)

2.15 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.

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 maquinas virtuales permiten la instalación de diferentes sistemas operativos mediante la utilización de la misma maquina 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. Estos sistemas son, hoy en día, cada vez más utilizados, ya que reducen el coste de hardware y optimiza su utilización, pues si en un momento dado un sistema no utiliza muchos recursos, éstos pueden ser utilizados por otros sistemas.

Ejercicios de autocomprobación

Indica si las siguientes afirmaciones son verdaderas (V) o falsas (F):

1. El sistema operativo es un conjunto de programas responsable de la gestión de los recursos que proporciona el software.
2. El editor de textos es una aplicación para crear o modificar textos, que no debe confundirse con un procesador de textos, ya que un editor no cambia la apariencia de un texto, sino solamente su contenido.
3. Monolítico 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.
4. Según las leyes internacionales de propiedad intelectual, ninguna persona puede hacer uso de un programa de ordenador sin el permiso explícito de su autor. Ese permiso se concede en forma de licencia.
5. El paso menos importante al virtualizar un sistema operativo es definir los parámetros, como la cantidad de memoria o el tamaño de disco duro que se dedicarán exclusivamente a ese sistema.
6. Cada sistema operativo se adapta solo a determinadas máquinas; por lo tanto, el sistema operativo y el hardware deben escogerse separadamente.
7. 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.

Completa las siguientes afirmaciones:

8. Los _____ técnicos son las especificaciones de un sistema operativo para poder funcionar de manera óptima. Normalmente, cuanto más moderna es una _____ de un sistema operativo, más _____ necesitará en cuanto a _____ y cantidad de _____ del equipo, pero no siempre es así.
9. Las licencias definen el tipo de _____ que podrá darse a un sistema operativo. Generalmente, las licencias limitan el _____ de un sistema

operativo a una _____ o un _____ únicamente. Esto sucede en los sistemas operativos _____, en los que cada copia tiene asociado un número de identificación único.

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

Las soluciones a los ejercicios de autocomprobación se encuentran al final de este módulo. En caso de que no los hayas contestado correctamente, repasa la parte de la lección correspondiente.

3. GESTIÓN DE INFORMACIÓN

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 aglutan 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 ésta, 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.

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 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 pri-

meros 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 (Figura 3.1).

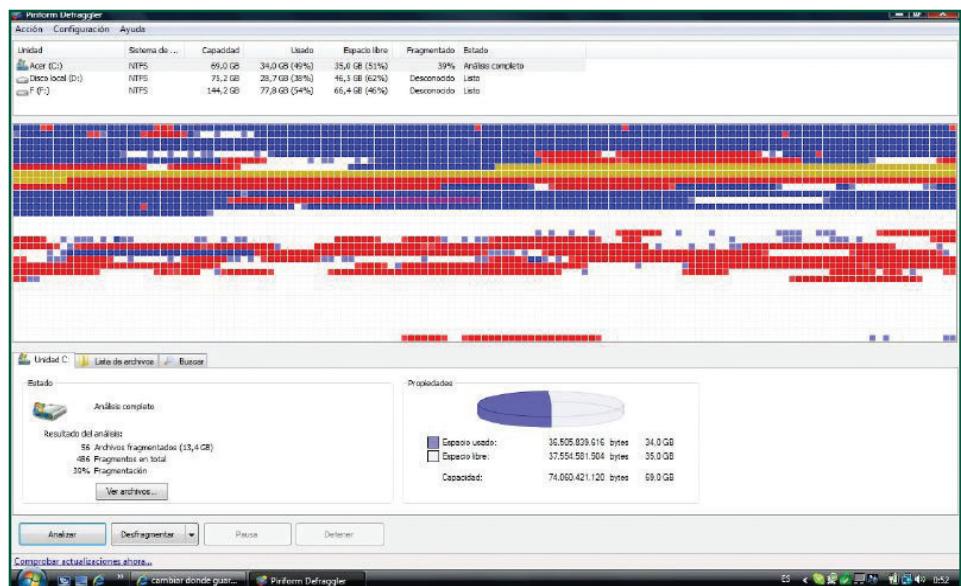


Figura 3.1
Un mismo archivo puede estar dividido y almacenado en diferentes secciones del disco duro generando un mapa de datos irregular, pero el sistema operativo tratará las diferentes partes del archivo como una única unidad de datos.

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.

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. El sistema de archivos más utilizado en los sistemas Microsoft fue FAT, que ha ido siendo sustituido por el NTFS en los equipos actuales.

3.1.1 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 herramienta 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 el más fácil y eficiente para unidades de hasta 200 MB, pero con unidades más grandes el rendimiento se reducirá, ya que necesitará tablas FAT más grandes. Además, según el sistema operativo, el sistema de archivos FAT no soporta unidades de gran tamaño. En Windows NT el límite para este sistema era de 4 GB.

Pero la mayor limitación de este sistema, además de la limitación de espacio, es el 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 se aplican en el sistema de archivos de la unidad lógica. En el sistema FAT solo es posible aplicar a los archivos las propiedades de solo lectura, oculto, sistema o modificado, dejando fuera todos los permisos de usuarios y credenciales.

3.1.2 NTFS

Este sistema es el más utilizado hoy en día en los sistemas Microsoft por la gran capacidad de almacenamiento de las unidades lógicas actuales. 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.

3.1.3. 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: NFS (network filesystem) y CIFS (common internet filesystem).

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.

Por ejemplo, algunos de los comandos más utilizados en sistemas Unix son:

- **dir o ls.** Lista el contenido de un directorio.
- **cd.** Accede a un directorio. Permite adentrarse un nivel dentro del árbol de ficheros.
- **md.** Crea un directorio.
- **rd.** Elimina un directorio.

Evidentemente, estas tareas pueden ser realizadas de manera mucho más rápida dentro del entorno grafico 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 (Figura 3.2).



Figura 3.2

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.

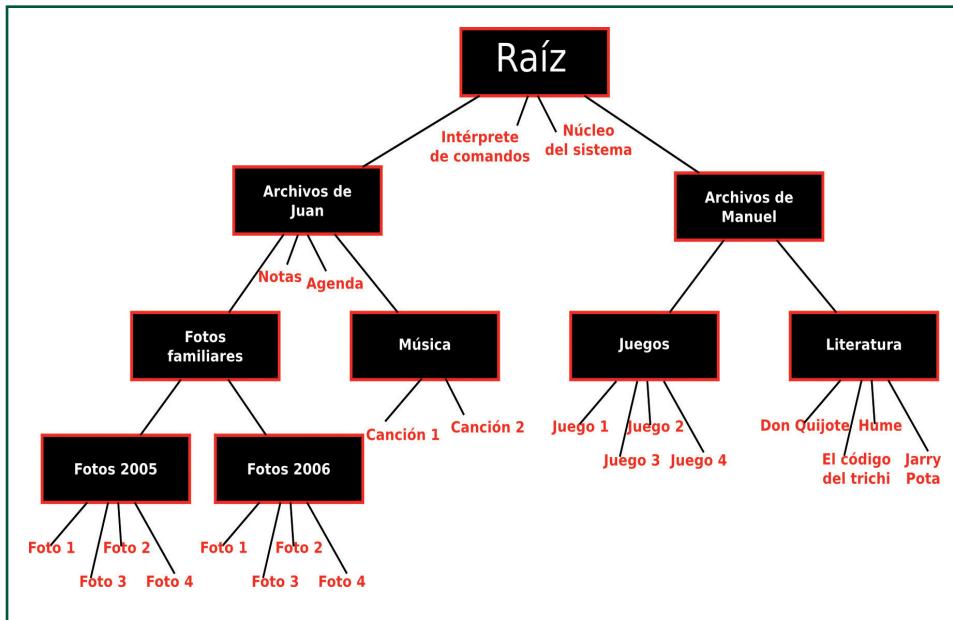
Un árbol de directorios es una lista, llamada **directorio**, que puede contener nombres de ficheros y también otras listas. De esta manera se forma una estructura jerárquica en la que, de una lista principal, llamada **raíz**, se derivan todas las demás listas, que son sus sucesoras. A la lista que deriva de otra se la llama **directorio hijo** de esa otra; y a la lista de la cual deriva una, **directorio padre** de esa una. Analogamente, las listas pueden ser antecesoras o sucesoras según contengan o estén contenidas en otras. De las listas y ficheros que comparten una antecesora común suele decirse que *cuelgan* de la antecesora.

Un árbol de directorios, por tanto, es una jerarquía de directorios (listas de archivos) que puede representarse mediante un árbol genealógico (Figura 3.3).

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.

Figura 3.3

Los directorios permiten organizar los ficheros en diversas categorías.



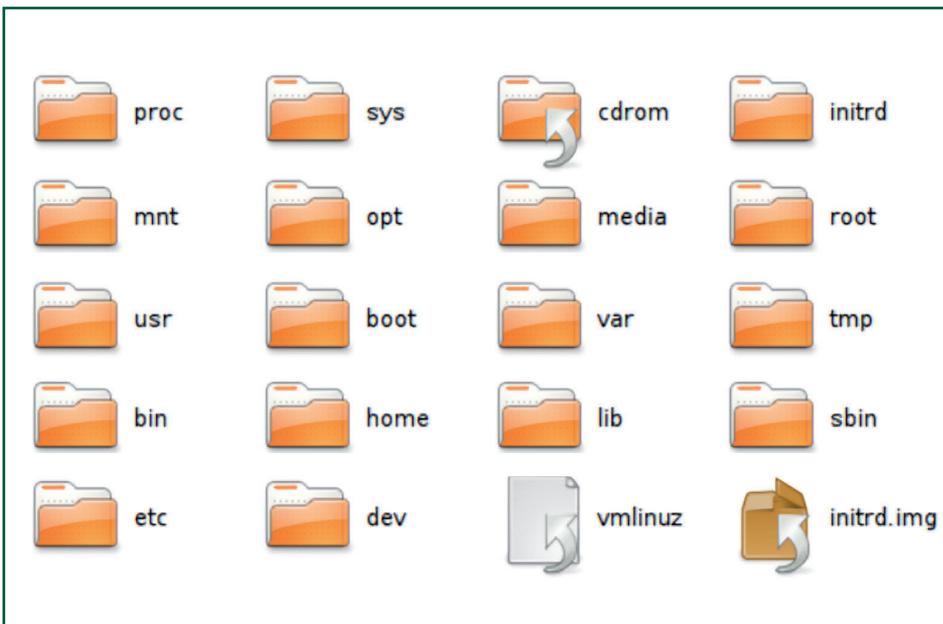
Recuerda

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 (Figura 3.4). 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.

**Figura 3.4**

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.

A diferencia de los sistemas Microsoft, Unix utiliza el sistema de archivos para albergar no solo los ficheros y las carpetas, sino también aquellos binarios que son utilizados para administrar las herramientas del sistema o 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.** Contienen ficheros que no son estáticos. Deben encontrarse en dispositivos de lectura-escritura (*read-write*). Necesitan que se hagan copias de seguridad a menudo.

- **Compartibles.** Contienen ficheros que se pueden encontrar en un ordenador y utilizarse en otro.
- **No compatibles.** Contienen ficheros que no son compatibles.

Por ejemplo:

- Estáticos:
/bin, /sbin, /opt, /boot, /usr/bin

- Dinámicos:
/var/mail, /var/spool, /var/run, /var/lock, /home

- Compartibles:
/usr/bin, /opt
- No compatibles:
/etc, /boot, /var/run, /var/lock

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:

- /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 configuración utilizados en todo el sistema y que son específicos 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.

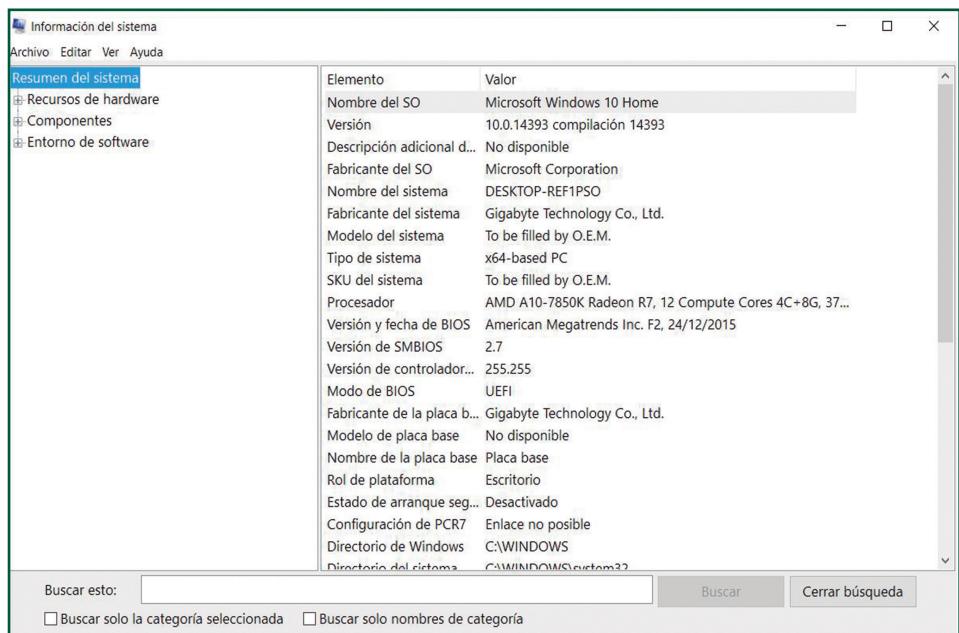
Recuerda

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 (Figura 3.5):

- **Resumen del sistema.** Identifica el sistema operativo, el microprocesador, la Bios y la memoria RAM del sistema.
- **Recursos de hardware.** Analiza las señales enviadas entre los dispositivos que componen la máquina y notifica posibles problemas o conflictos.
- **Componentes.** Muestra información sobre los dispositivos periféricos y los controladores del sistema operativo para esos periféricos.
- **Entorno de software.** Analiza los programas del sistema que están en funcionamiento.
- **Aplicaciones.** Muestra información sobre los programas del paquete Office.
- **Internet Explorer.** Muestra información sobre el navegador de Internet de Microsoft.

**Figura 3.5**

La utilidad *Información del sistema* de Windows proporciona información muy útil para el diagnóstico de problemas de los sistemas físico y lógico.

Usando el intérprete de comandos, el comando *systeminfo* muestra información similar. En los sistemas operativos de tipo Unix, la información sobre la configuración del sistema puede obtenerse mostrando en pantalla el contenido de los ficheros de los directorios */proc* y */sys*. Por ejemplo: *cat /proc/cpuinfo* muestra información sobre la CPU; *cat /proc/meminfo* muestra información sobre el uso de la memoria RAM.

3.5 Identificación del software instalado mediante comandos y herramientas gráficas

Al instalar 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 (Figura 3.6).

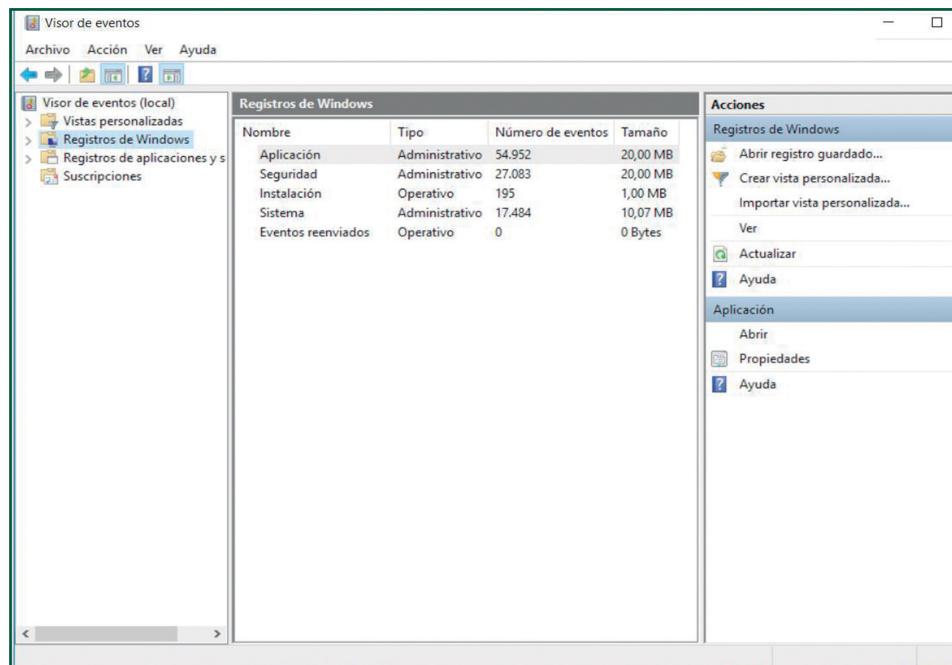


Figura 3.6

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**, a la cual se accede tecleando *monitor de rendimiento* en el buscador de la barra horizontal inferior del escritorio.

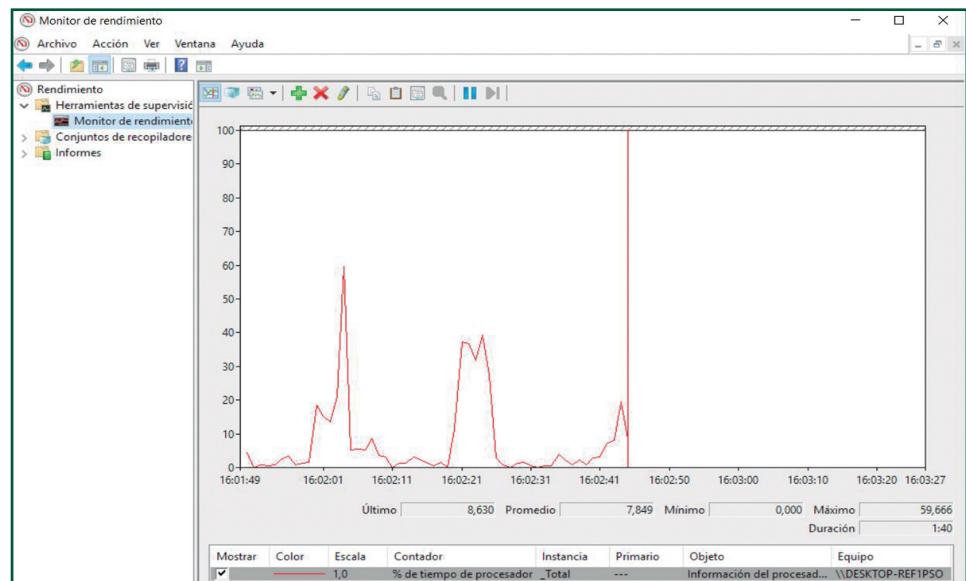


Figura 3.7

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 Mi PC, mientras que a un escáner o a una impresora se accede desde el panel de control.

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, **mk-dir /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

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; 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 más comunes para conexiones internas y profesionales están **IDE** (ATA, 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** (I, II y III) y FireWire.

El segundo paso es el reconocimiento del medio por los programas del fabricante del ordenador. Los discos más estándar son reconocidos automáticamente por la memoria **Bios** 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 por sus siglas en inglés, **MBR**. Este sector es lo primero y lo único que es capaz de leer una memoria Bios clásica. En algunas ocasiones, lo que se guarda en el MBR es un programa de arranque múltiple, que permite al usuario elegir iniciar el ordenador desde varios dispositivos. Este programa redirigirá 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**).

En los ordenadores más avanzados es habitual que la memoria **Bios** sea capaz de leer por sí misma particiones del tipo FAT, lo que permite un reconocimiento de las particiones mucho más elaborado y prácticamente automático sin necesidad de buscar la información en el MBR. 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** y **parted** para sistemas operativos de tipo Unix, y **MBRFix.exe** para los sistemas operativos de marca Windows.

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** usando 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 dispositivos (Figura 3.8), que se inicializa tecleando el texto *administración de dispositivos* en el buscador de la barra horizontal inferior del escritorio. En sistemas de tipo Unix están **gparted** y **kparted**. Algunas herramientas de este tipo vienen en formato CD-ROM autoarrancable, por lo que no dependen del sistema operativo instalado. Destacan 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.

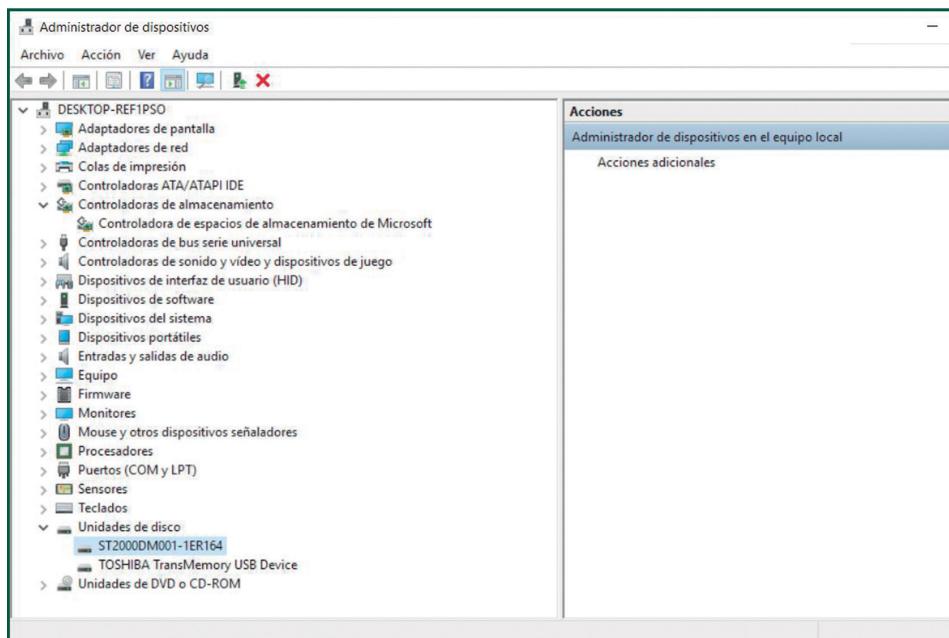


Figura 3.8

La herramienta *Administración de discos* de Windows integra todas las funciones de gestión de los volúmenes con sistemas de archivos NTFS y FAT32.

3.8 Sistemas de archivos de red y matrices de discos RAID

Los sistemas informáticos de las empresas son costosos de mantener. Una de las estrategias para reducir el gasto consiste en centralizar el almacenamiento de la información. Los archivos de toda una sede o empresa se guardan generalmente en una cabina de discos (Figura 3.9), 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.

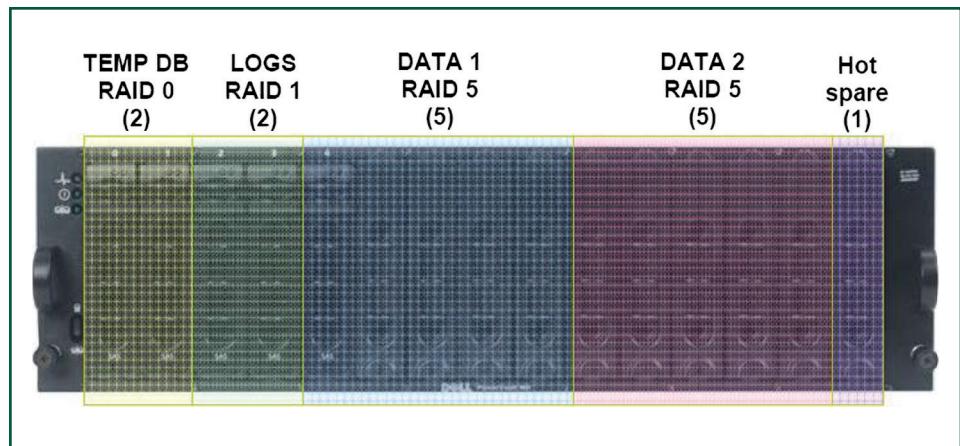


Figura 3.9

Una cabina de discos combina varios discos duros con el fin de cumplir los requisitos de almacenamiento de una empresa en cuanto a capacidad, velocidad y fiabilidad

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 y algunas de las más comunes son las siguientes:

- **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.

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 carácter "/" 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 emplear caracteres de escape; por ejemplo, el símbolo de contrabarra (\) seguido del carácter "prohibido".

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

```
/home/fotos/arbol.jpg
```

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.

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

Las principales herramientas de gestión de archivos son:

- **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 ícono de carpeta. Para cambiar al padre pulsamos dos veces sobre el ícono de padre, que suele ser el primer ícono del listado.
 - **Ejecutar un programa o abrir un documento.** Pulsamos dos veces el botón principal del ratón con la flecha sobre el ícono del archivo.
 - **Copiar y pegar un archivo.** Con la flecha sobre el ícono del archivo a copiar, seleccionamos la opción *Copiar*, después cambiamos a otro directorio activo y seleccionamos la opción *Pegar*.
 - **Cortar y pegar un archivo.** Análogamente, seleccionamos la opción *Cortar* con la flecha sobre un ícono, 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 (Figura 3.10).

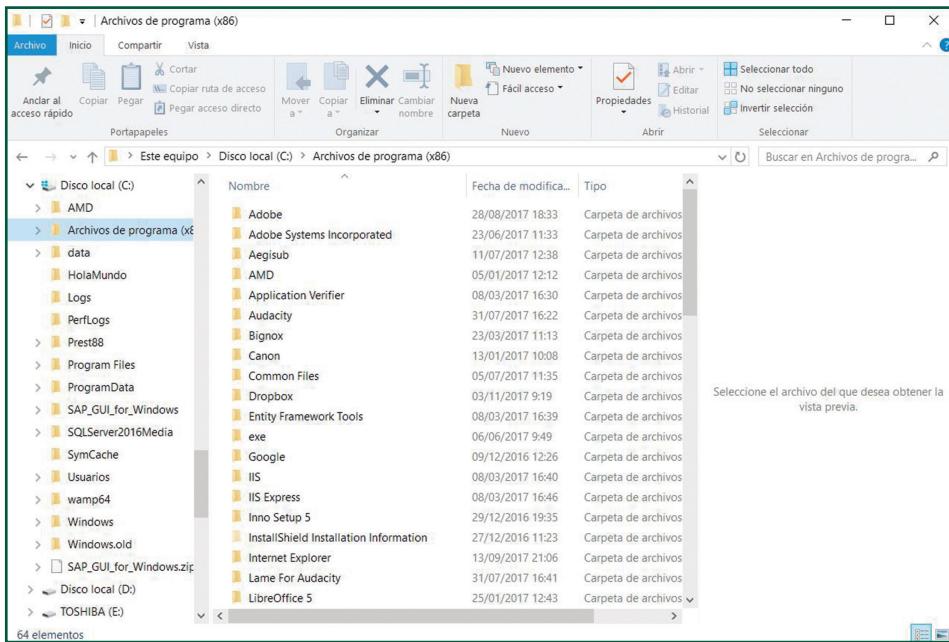


Figura 3.10

Un gestor de archivos permite administrar fácilmente los archivos de un ordenador.

- **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

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 ícono 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 por controlar que la información no se pierda por errores de escritura en el hardware del equipo y que, en caso de perderse la información pueda recuperarse.

La manera de conseguirlo es únicamente creando diferentes soportes que almacenen la misma información. Esto puede conseguirse de varias formas y utilizar todas ellas es una manera de aumentar las posibilidades de poder recuperar la información perdida:

- **Backups.** Una copia de seguridad o *backup* es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de que se pierdan. Hay que prestar mucha atención al proceso de copia de seguridad, pues la pérdida de datos es muy común, como demuestra la cifra de que el 66% de los usuarios de Internet han sufrido una seria pérdida de datos en algún momento.

Las copias de seguridad son útiles ante las situaciones que presentamos a continuación:

- Recuperar los datos de una catástrofe informática, natural o ataque.
- Restaurar una pequeña cantidad de archivos que pueden haberse eliminado accidentalmente, corrompido, infectado por un virus informático u otras causas.
- Guardar información histórica de forma más económica que los discos duros activos, lo que permite, además, trasladar esta copia a ubicaciones distintas de las de los datos originales.

A la hora de dimensionar nuestros dispositivos de copia de seguridad, deben tenerse en cuenta los requerimientos de almacenamiento, la organización del espacio de almacenamiento y la administración del proceso de efectuar la copia de seguridad.

Actualmente, existen muchos tipos diferentes de dispositivos para almacenar datos, que son útiles para hacer copias de seguridad, cada uno de ellos con las ventajas y los inconvenientes que hay que tener en cuenta para elegirlos, como duplicidad, seguridad en los datos y facilidad de traslado. Antes de que los datos sean enviados a su lugar de almacenamiento, deben seleccionarse, extraerse y manipularse. Se han desarrollado muchas técnicas diferentes para optimizar el procedimiento de efectuar backups.

Estos procedimientos incluyen optimizaciones para trabajar con archivos abiertos y fuentes de datos en uso, y también incluyen procesos de compresión, cifrado, y procesos de deduplicación, entendiéndose por esto último una forma específica de compresión donde los datos superfluos son eliminados.

- **RAID.** Este tipo de discos duros también pueden considerarse sistemas de tolerancia de fallos, puesto que, al permitir la escritura paralela en un servidor, podemos duplicar los datos para que en el mismo momento se almacenen en dos discos RAID diferentes.

La ventaja que esto tiene es que, a diferencia de los *backups*, los datos son actuales a partir del momento de guardado y, en caso de error, en uno de los soportes físicos se pueden recuperar los datos totalmente actualizados el momento.

3.12 Tareas automáticas

El mantenimiento de los sistemas de archivos requiere a menudo abordar tareas demasiado tediosas para tener que hacerlas una a una. Por ello, para poder evitarlas, se utilizan los *scripts*, que son pequeños programas que ejecuta el intérprete de comandos del sistema operativo.

Algunas tareas deben realizarse periódicamente y pueden interferir en el trabajo normal de los usuarios. Por ello es conveniente dejar programados *scripts* que se ejecuten en unos días y horas determinados. De todas formas, los sistemas operativos prevén este tipo de mantenimiento: en Windows se usa el **Administrador de Tareas**; en Mac OS X, la aplicación genérica de calendario iCal; y en Unix, el servicio **Crontab** (Figura 3.11).

```

1744 tty7 00:00:45 Xorg
chas@charlie:~$ cd /etc/cron.
cron.d/ cron.daily/ cron.hourly/ cron.monthly/ cron.weekly/
chas@charlie:~$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the 'crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )

#
chas@charlie:~$ cat /etc/crontab

```

Figura 3.11

Ejemplo de uso del fichero de configuración Crontab para planificar tareas periódicas en un sistema Unix.

Por lo que respecta a este tipo de tareas, merecen una atención especial las de **copia de seguridad** o *backup*, que suelen realizarse con programas especializados como rsync, Bacula o Backup Exec.

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 gráfico 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 gráfica**. 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 gráficas.

Ejercicios de autocomprobación

Indica si las siguientes afirmaciones son verdaderas (V) o falsas (F):

1. La unidad fundamental de un sistema de archivos es el archivo o fichero. Un fichero es una agrupación de datos que forma 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.
2. 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.
3. Generalmente, 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.
4. 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.
5. Se entiende por montar un dispositivo la acción de crear un acceso desde un directorio a un dispositivo conectado a nuestro sistema operativo. Significa crear un enlace entre el directorio y el dispositivo conectado, como a un escáner o a una impresora que se accede desde el panel de control.
6. Una copia de seguridad o *backup* es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de que se pierdan.
7. Para instalar periféricos en un ordenador no es necesario realizar la instalación de los controladores, que son los que permitirán al sistema operativo que accione los nuevos dispositivos.

Completa las siguientes afirmaciones:

8. Un sistema de _____ es el conjunto de las normas y los procedimientos que debe seguir un sistema para poder ubicar información en un soporte

físico _____, como puede ser un disco duro, un _____ o un _____, y para que el mismo sistema u otro que siga las mismas normas y procedimientos pueda recuperar dicha información.

9. 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 _____; el establecimiento de _____ y _____ RAID; el reconocimiento por parte del sistema operativo de los volúmenes (particiones) durante el proceso de arranque; el montaje inicial de los sistemas de _____ de dichos volúmenes en el árbol o arboles de directorios; el formateado de los sistemas de archivos, y las operaciones de reparticionado y copia de _____.
10. Una unidad montada es una unidad asignada a una _____ vacía de un _____ que utiliza el sistema de _____ NTFS. Las unidades montadas son rutas de acceso de unidad asignadas en lugar de letras de unidad. Cuando vemos una unidad montada, en el _____ de Windows, aparece como un _____ de unidad en la ruta de acceso en la que está montada.

Las soluciones a los ejercicios de autocomprobación se encuentran al final de este módulo. En caso de que no los hayas contestado correctamente, repasa la parte de la lección correspondiente.

4. CONFIGURACIÓN DE SISTEMAS OPERATIVOS

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 estos 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.

4.1 Configuración de usuarios y grupos locales

La condición más importante para poder crear usuarios y grupos locales en un sistema es ingresar en éste 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 se realiza inicializando el panel de control y accediendo a la opción *Cuentas de usuario*. En este panel se pueden administrar nuevos usuarios, permisos y otra serie de configuraciones.

Figura 4.1
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 de tipo Unix, la administración de grupos, usuarios y privilegios puede realizarse desde el intérprete de comandos. Se utilizan 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.

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 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.

4.2 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.

4.2.1 Usuarios y grupos predeterminados en entornos Windows

Los sistemas operativos y controladores de dominio Windows tienen predefinido el superusuario, cuyo nombre de cuenta es **Administrator** si la versión del sistema operativo es en lengua inglesa o **Administrador** cuando es una versión en lengua española. También está presente una cuenta de usuario invitado, cuyo nombre es **Guest**. Originalmente, la cuenta de usuario invitado no tiene derechos sobre el sistema y su función es facilitar la rápida asignación de unos derechos mínimos sobre recursos muy concretos a un usuario ocasional del sistema. Los sistemas Windows incluyen también una colección de grupos predefinidos. Estos grupos sirven para asignar derechos a los usuarios de forma rápida y segura; por ejemplo, basta con asignar una cuenta de usuario al grupo *Administradores locales* para que el usuario tenga todos los privilegios de un superusuario; o asignarla al grupo *Usuarios* para que la cuenta pueda acceder a los recursos que necesita un usuario genérico.

4.2.2 Usuarios y grupos predeterminados en entornos Unix

Los sistemas operativos que cumplen con el estándar Posix (los basados en Unix) crean, en el momento de su instalación, un superusuario (*root*) y un grupo para el superusuario (grupo *root*). Los sistemas operativos Posix tienen un diseño de seguridad que obliga a cada programa a operar en nombre del usuario que lo ha iniciado. El sistema crea en el momento de su instalación varias cuentas de usuario y grupos que son necesarios para que sus propios programas puedan acceder a los recursos que necesitan (Figura 4.2).

```
chas@charlie:/etc$ cat 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:
mant:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:chas
fax:x:21:
voice:x:22:
cdrom:x:24:chas
floppy:x:25:chas
tape:x:26:
sudo:x:27:
audio:x:29:chas
dip:x:30:
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
src:x:40:
gnats:x:41:
```

Figura 4.2

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

4.3 Seguridad de cuentas de usuario

El **usuario** de un sistema informático es aquella persona o programa que accede a un sistema informático para que éste 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: Equipos locales y dominios.

- **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 usuario pueden incorporarse a grupos con privilegios comunes (Figura 4.3).

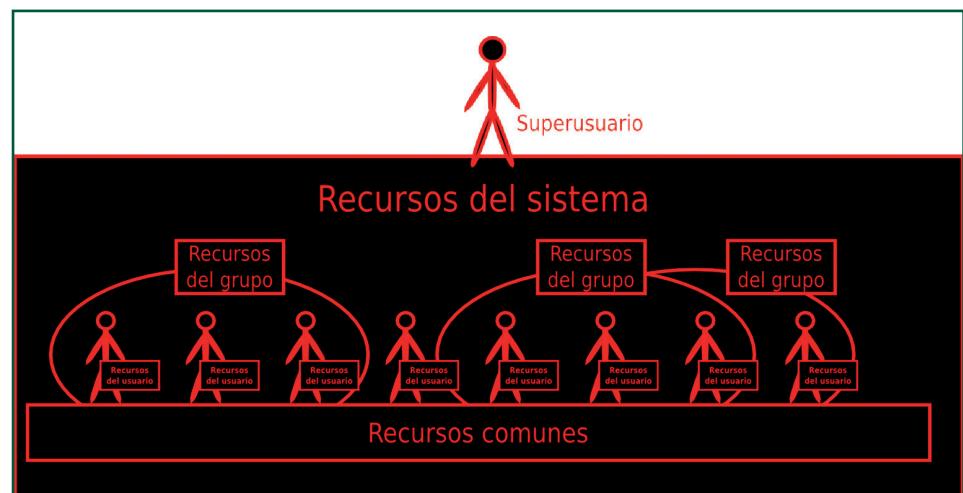


Figura 4.3

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.

4.4 Seguridad de contraseñas

La mayoría de los ataques contra la seguridad informática de las empresas e instituciones provienen de empleados o empleados 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 éste. 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 (Figura 4.4).

Recuerda

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

```
chas@charlie:/etc$ cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
chas@charlie:/etc$ cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
```

Figura 4.4

Listado del archivo de contraseñas `passwd` en Linux. Las contraseñas aparecen sustituidas por la letra `x`.

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. 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.

Una buena contraseña debe tener una longitud mínima de 6 caracteres alfanuméricos, los cuales incluirán al menos una mayúscula, una minúscula, un número y un símbolo. No deben contener nombres ni palabras que estén en el diccionario, ni fechas, ni frases que puedan asociarse con el usuario.

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.

4.4.1 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.

4.4.2 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 fichero 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 (ya que podría estar en varios grupos) 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**.

Los atributos de los archivos pueden visualizarse con la orden *ls -l*. La primera letra es una *d* si el archivo es un directorio o – (menos) si es un archivo, 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 de el 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 (Figura 4.5).

```
drwxr-xr-x  4 chas chas  4096 dic  3 03:22 tmp
drwxr--r--  9 chas chas  4096 jul 19 23:51 trabajo
-rw-r--r--  1 chas chas  86899 nov 16 13:58 Troquelado-experimento.jpg
-rw-r--r--  1 chas chas 572392 nov 16 13:47 Troquelado-experimento.xcf
drwxr-xr-x  2 chas chas  4096 may  9  2011 Video Projects
drwxr-xr-x  5 chas chas  4096 jun  8  2011 Yozo_Office
chas@charlie:~$
```

Recuerda

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

Figura 4.5

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

4.4.3 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 ícono 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 íconos 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 (Figura 4.6). En Windows no hay límite sobre la cantidad de usuarios y grupos que pueden tener acceso a un fichero.

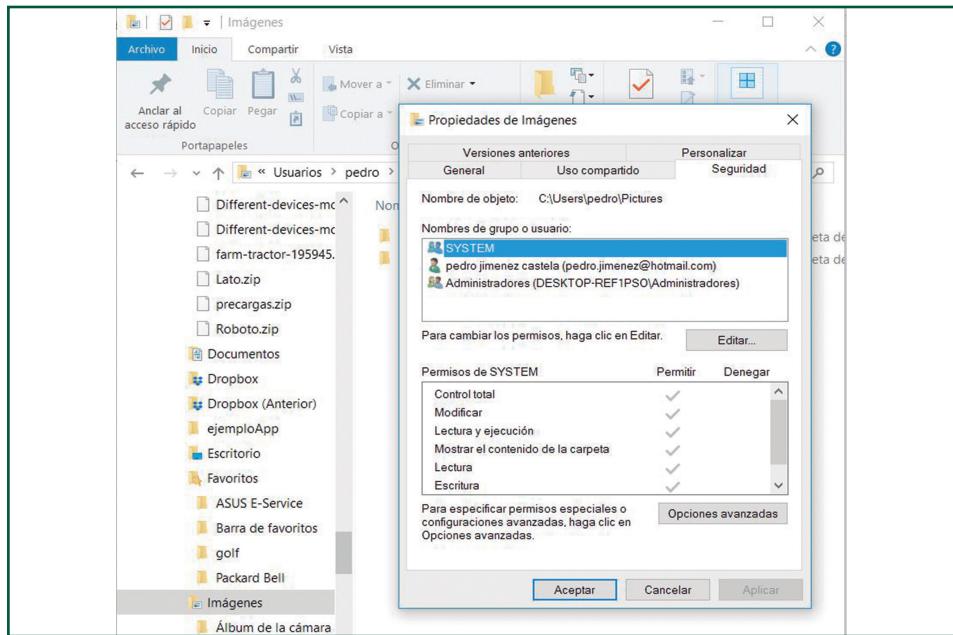


Figura 4.6

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

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.

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.

4.5 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* (Figura 4.7).

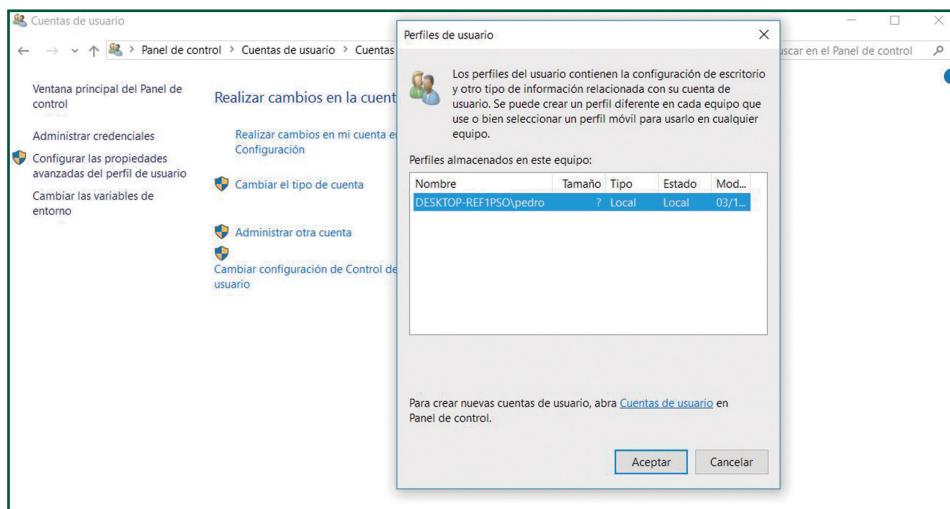


Figura 4.7

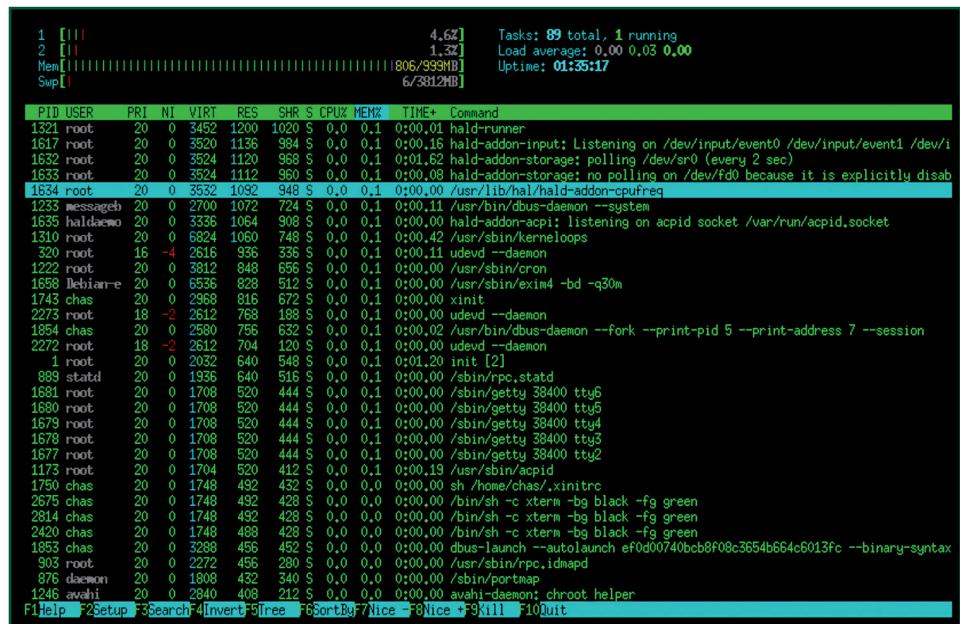
La consola de administración de Microsoft permite diseñar un perfil local para cada usuario.

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 los entornos 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.

4.6 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 (Figura 4.8).



```

1 [!!]          Tasks: 89 total, 1 running
2 [!!]          Load average: 0.00 0.03 0.00
Mem[!!!!]       Uptime: 01:35:17
Swap[!]

PID USER      PRI NI VIRT   RES   SHR S CPU% MEM% TIME+ Command
1321 root      20  0 3452 1200 1020 S 0.0  0.1 0:00,01 hald-runner
1617 root      20  0 3520 1136 984 S 0.0  0.1 0:00,16 hald-addon-input; Listening on /dev/input/event0 /dev/input/event1 /dev/
1632 root      20  0 3524 1120 968 S 0.0  0.1 0:01,62 hald-addon-storage; polling /dev/sr0 (every 2 sec)
1633 root      20  0 3524 1112 960 S 0.0  0.1 0:00,08 hald-addon-storage; no polling on /dev/fd0 because it is explicitly disabled
1634 root      20  0 3532 1092 948 S 0.0  0.1 0:00,00 /usr/lib/hal/hald-addon-cpufreq
1233 messagebus 20  0 2700 1072 724 S 0.0  0.1 0:00,11 /usr/bin/dbus-daemon --system
1635 haldaemon 20  0 3336 1064 908 S 0.0  0.1 0:00,00 hald-addon-acpi; listening on acpid socket /var/run/acpid.socket
1310 root      20  0 5824 1060 748 S 0.0  0.1 0:00,42 /usr/sbin/kerneloops
320 root      16 -4 2616  936 336 S 0.0  0.1 0:00,11 udevd --daemon
1222 root      20  0 3812  848 656 S 0.0  0.1 0:00,00 /usr/sbin/cron
1658 libblueme 20  0 5536  828 512 S 0.0  0.1 0:00,00 /usr/sbin/exim4 -bd -q30m
1743 chas      20  0 2968  816 672 S 0.0  0.1 0:00,00 xinit
2273 root      18 -2 2612  768 188 S 0.0  0.1 0:00,00 udevd --daemon
1854 chas      20  0 2580  756 632 S 0.0  0.1 0:00,02 /usr/bin/dbus-daemon --fork --print-pid 5 --print-address 7 --session
2272 root      18 -2 2612  704 120 S 0.0  0.1 0:00,00 udevd --daemon
1 root      20  0 2032  640 548 S 0.0  0.1 0:01,20 init [2]
889 statd     20  0 1936  640 516 S 0.0  0.1 0:00,00 /sbin/rpc.statd
1681 root      20  0 1708  520 444 S 0.0  0.1 0:00,00 /sbin/getty 38400 ttys0
1680 root      20  0 1708  520 444 S 0.0  0.1 0:00,00 /sbin/getty 38400 ttys5
1679 root      20  0 1708  520 444 S 0.0  0.1 0:00,00 /sbin/getty 38400 ttys4
1678 root      20  0 1708  520 444 S 0.0  0.1 0:00,00 /sbin/getty 38400 ttys3
1677 root      20  0 1708  520 444 S 0.0  0.1 0:00,00 /sbin/getty 38400 ttys2
1173 root      20  0 1704  520 412 S 0.0  0.1 0:00,13 /usr/sbin/acpid
1750 chas      20  0 1748  492 432 S 0.0  0.0 0:00,00 sh /home/chas/.xinitrc
2675 chas      20  0 1748  492 428 S 0.0  0.0 0:00,00 /bin/sh -x term -bg black -fg green
2814 chas      20  0 1748  492 428 S 0.0  0.0 0:00,00 /bin/sh -x term -bg black -fg green
2420 chas      20  0 1748  488 428 S 0.0  0.0 0:00,00 /bin/sh -x term -bg black -fg green
1853 chas      20  0 3288  456 452 S 0.0  0.0 0:00,00 dbus-launch --autolaunch ef0d00740bcbbf08c3b54b664c6013fc --binary-syntax
903 root      20  0 2272  456 280 S 0.0  0.0 0:00,00 /usr/sbin/rpc.idmapd
876 daemon    20  0 1808  432 340 S 0.0  0.0 0:00,00 /sbin/portmap
1246 avahi     20  0 2840  408 212 S 0.0  0.0 0:00,00 avahi-daemon: chroot helper
F1Help F2Setup F3Search F4Invert F5Tree F6SortBy F7Nice -7Nice +7Kill F10Quit

```

Figura 4.8

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

Otra características 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.

4.6.1 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.

Los *pipes* soportan una comunicación unidireccional y FIFO (en inglés, *First In First Out*); esto quiere decir que los mensajes enviados a través de la tubería se van almacenando y van siendo procesados por el receptor en orden de llegada.

- **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.

Recuerda

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

Recuerda

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

- **Cierre de un 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.

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

- **Escritura en un pipe.** El servicio de escritura a través de un *pipe* es el siguiente:

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, ésta 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.

4.6.2 Semáforos

Los semáforos son mecanismos de sincronización que permiten al sistema bloquear servicios para ordenar la capacidad de procesamiento del hardware. Un semáforo es inicializado con un número entero no negativo que representará el número de procesos a ser ejecutados en un mismo momento. Los semáforos están definidos 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 es puesto en espera si el número absoluto del semáforo es negativo; por el contrario, se desbloqueará uno de los procesos que están esperando. La estructura de las funciones *wait* y *signal* son las siguientes:

```
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;
}
```

4.6.3 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.** Intenta bloquear el mutex. Si el mutex ya está bloqueado por otro proceso, el proceso que realiza la operación se bloquea. En caso contrario, se bloquea el mutex sin bloquear el proceso.
- **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.

4.7 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 (Figura 4.9).

Intérprete de comandos de los sistemas basados en Unix	
su	Cambia la cuenta de usuario.
man	Solicita información sobre los comandos del intérprete.
ls	Lista el contenido de un directorio.
cd	Cambia el directorio de trabajo.
touch	Crea un archivo vacío.
cp	Copia un archivo.
mv	Mueve o renombra un archivo.
mkdir	Crea un directorio.
rm	Borra un archivo.
rmdir	Borra un directorio vacío.
find	Busca un fichero.
cat	Muestra el contenido de un fichero.

Intérprete de comandos de los sistemas Windows	
help	Solicita información sobre los comandos del intérprete.
dir	Lista el contenido de un directorio.
cd	Cambia el directorio de trabajo.
copy	Copia un archivo.
move	Mueve o renombra un archivo.
mkdir	Crea un directorio.
del	Borra un archivo.
rd	Borra un directorio vacío.
type	Muestra el contenido de un fichero.

Figura 4.9

El intérprete de línea de comandos proporciona herramientas para administrar el sistema de forma directa y eficiente. En la tabla se muestran algunos comandos básicos.

4.8 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.

4.8.1 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 "Configuración

del equipo\Directivas\Configuración de Windows\Configuración de seguridad\Directivas locales\Directiva de auditoría”.

En 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 “Configuración del equipo\Directivas\Configuración de Windows\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.

4.8.2 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.

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.

Ejercicios de autocomprobación

Indica si las siguientes afirmaciones son verdaderas (V) o falsas (F):

1. 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 es la cuenta del usuario llamado Administrador.
2. La cuenta de usuario invitado, cuyo nombre es Guest, no tiene derechos sobre el sistema y su función es dificultar la rápida asignación de unos derechos mínimos sobre recursos muy concretos a un usuario ocasional del sistema.
3. El acceso a un recurso se controla mediante sus propiedades, que pueden ser cambiadas exclusivamente por el propietario, el cual decide que privilegios otorga a que usuarios o grupos. En Windows hay límite sobre la cantidad de usuarios y grupos que pueden tener acceso a un fichero.
4. Los pipes realizan funciones de sincronización entre las partes y son capaces de administrar multitud de procesos.
5. Los servicios o *daemons* son programas que se ejecutan en el ordenador de forma transparente al usuario para dar servicio a otros programas.
6. Los semáforos son mecanismos de sincronización que permiten al sistema bloquear servicios para ordenar la capacidad de procesamiento del software. Un semáforo es inicializado con un número entero no negativo que representara el número de procesos a ser ejecutados en un mismo momento.
7. 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.

Completa las siguientes afirmaciones:

8. El usuario es aquella persona o _____ que accede a un sistema informático. El sistema asigna a cada usuario unas credenciales, formadas por un nombre único y una _____ (u otro sistema de _____) y el derecho a utilizar ciertos recursos. Esta asignación se llama _____ de usuario.

9. Las políticas de _____ se basan fundamentalmente en las acciones que el _____ puede realizar sobre los archivos y carpetas del sistema operativo. De esta manera, entre las políticas más comunes existen las de _____, ejecución o _____ de los archivos.

10. Las _____ pueden ser descifradas por _____ que analiza las posibles combinaciones de letras o el propio sistema. Una política recomendable a los _____ es la utilización de combinaciones de letras, números y símbolos que no formen ninguna palabra que este en el diccionario, pues son estas las primeras que se utilizan para intentar romper la _____ de un sistema.

Las soluciones a los ejercicios de autocomprobación se encuentran al final de este módulo. En caso de que no los hayas contestado correctamente, repasa la parte de la lección correspondiente.

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.

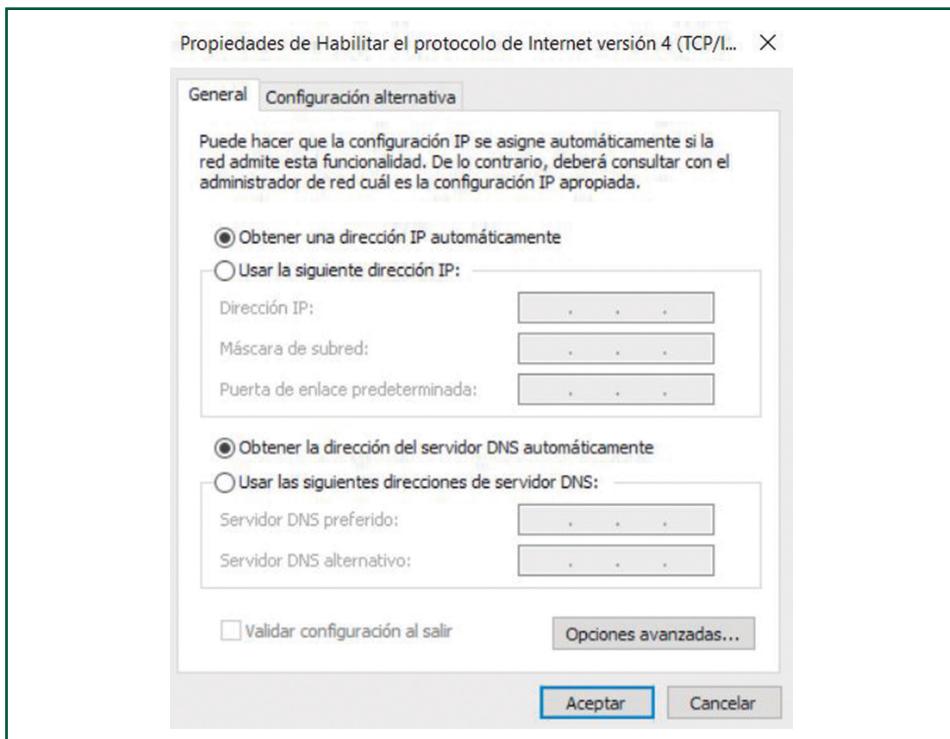
Por último, daremos algunas pautas a seguir, sobre todo en empresas, para minimizar los riesgos de sufrir un ataque. Estas pautas deberán de ser seguidas no solo por el administrador del sistema, sino por todos los usuarios de la red, implicando la necesidad de concienciar a los usuarios para evitar 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 32 bits, aunque generalmente se representa de manera decimal, separando cada octeto de bits por un punto (Figura 5.1).

**Figura 5.1**

Asignación manual de la dirección IP de un equipo.

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 modificuemos 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 11000000.10101000.01100100.000000110, 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 1100000.10101000.01100100.00000100.

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 $6,7 \times 10^{17}$ (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:

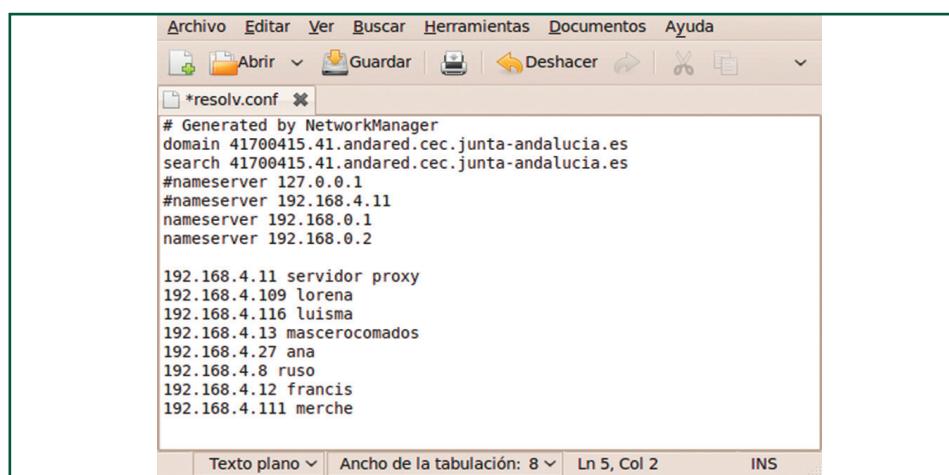
- **Primarios.** Guardan los datos de un espacio de nombres en sus ficheros en formato de lectura/escritura.

- **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:

- **/etc/hosts.** La 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).



```

Archivo Editar Ver Buscar Herramientas Documentos Ayuda
Abrir Guardar Deshacer
*resolv.conf
# Generated by NetworkManager
domain 41700415.41.andared.cec.junta-andalucia.es
search 41700415.41.andared.cec.junta-andalucia.es
#nameserver 127.0.0.1
#nameserver 192.168.4.11
nameserver 192.168.0.1
nameserver 192.168.0.2

192.168.4.11 servidor proxy
192.168.4.109 lorena
192.168.4.116 luisma
192.168.4.13 masecerocomados
192.168.4.27 ana
192.168.4.8 ruso
192.168.4.12 francis
192.168.4.111 merche

Texto plano Ancho de la tabulación: 8 Ln 5, Col 2 INS

```

Figura 5.3

Ejemplo de un archivo resolv.conf.

- **/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

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).

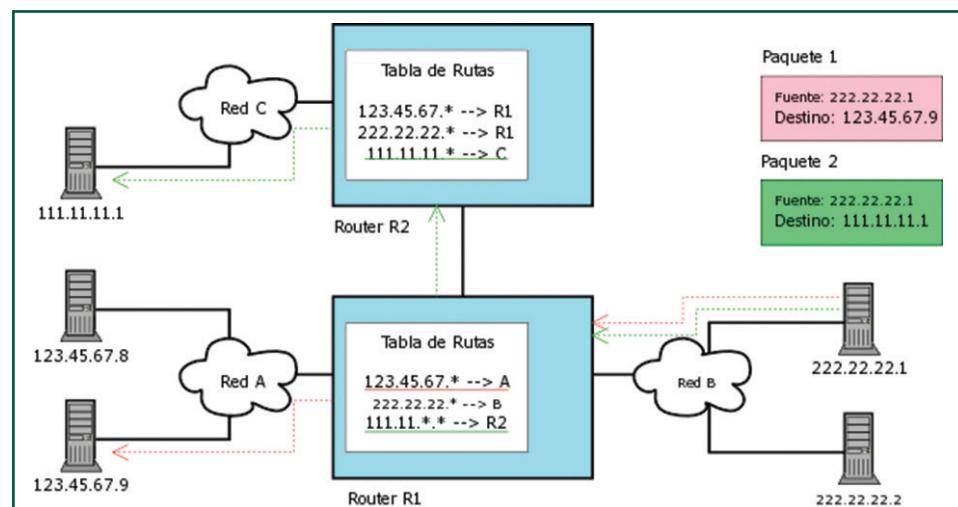


Figura 5.4

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

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 entran 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.

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 5.5

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.

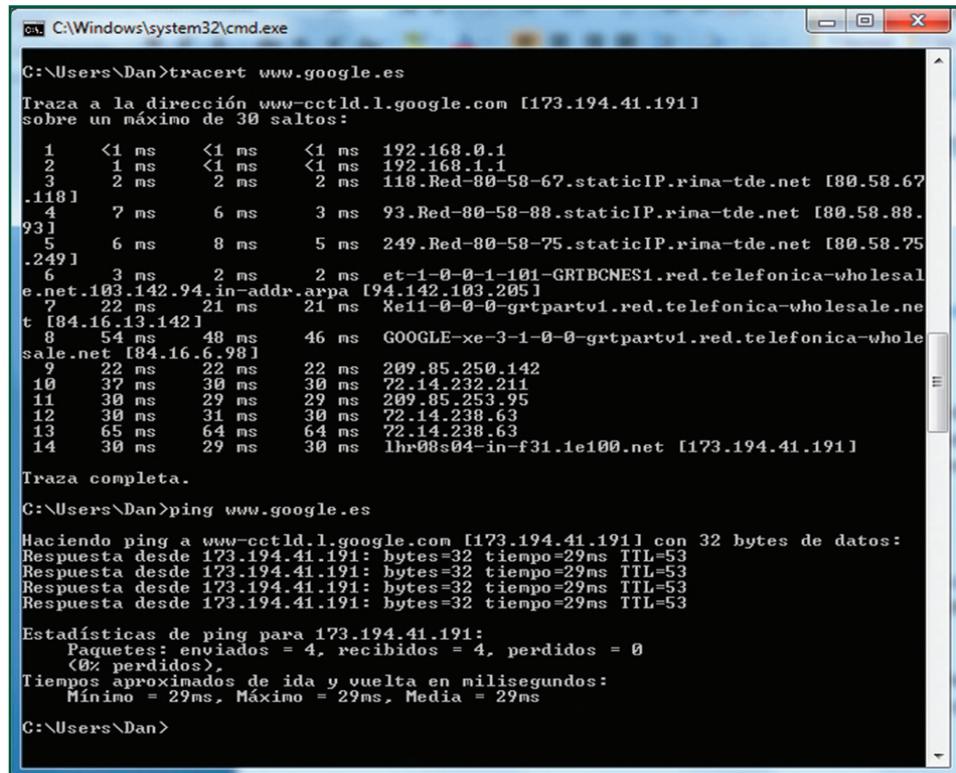
NAT - Edit SUA/NAT Server Set			
	Start Port No.	End Port No.	IP Address
1	All ports	All ports	0.0.0.0
2	6881	6900	192.168.1.33
3	4500	4503	192.168.1.33
4	59	59	192.168.1.33
5	4662	4662	192.168.1.33
6	4672	4672	192.168.1.33
7	0	0	0.0.0.0

Para saber más

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

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):



```
C:\Windows\system32\cmd.exe
C:\Users\Dan>tracert www.google.es
Traza a la dirección www-cctld.l.google.com [173.194.41.191]
sobre un máximo de 30 saltos:
 1  <1 ms    <1 ms    <1 ms  192.168.0.1
 2  1 ms    <1 ms    <1 ms  192.168.1.1
 3  2 ms    2 ms    2 ms  118.Red-80-58-67.staticIP.rima-tde.net [80.58.67.118]
 4  7 ms    6 ms    3 ms  93.Red-80-58-88.staticIP.rima-tde.net [80.58.88.93]
 5  6 ms    8 ms    5 ms  249.Red-80-58-75.staticIP.rima-tde.net [80.58.75.249]
 6  3 ms    2 ms    2 ms  et-1-0-0-1-101-GRTBCNES1.red.telefonica-wholesale.net [103.142.94.in-addr.arpa [94.142.103.205]
 7  22 ms   21 ms   21 ms  xe1-0-0-0-grtpartv1.red.telefonica-wholesale.net [84.16.13.142]
 8  54 ms   48 ms   46 ms  GOOGLE-xe-3-1-0-0-grtpartv1.red.telefonica-wholesale.net [84.16.6.98]
 9  22 ms   22 ms   22 ms  209.85.250.142
10  37 ms   30 ms   30 ms  72.14.232.211
11  30 ms   29 ms   29 ms  209.85.253.95
12  30 ms   31 ms   30 ms  72.14.238.63
13  65 ms   64 ms   64 ms  72.14.238.63
14  30 ms   29 ms   30 ms  lhr08s04-in-f31.1e100.net [173.194.41.191]

Traza completa.

C:\Users\Dan>ping www.google.es
Haciendo ping a www-cctld.l.google.com [173.194.41.191] con 32 bytes de datos:
Respueta desde 173.194.41.191: bytes=32 tiempo=29ms TTL=53

Estadísticas de ping para 173.194.41.191:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
<0% perdidos>
Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 29ms, Máximo = 29ms, Media = 29ms
C:\Users\Dan>
```

Figura 5.6

Comandos *ping* y *tracert* de la dirección de Google.

- **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 un listado de todas las máquinas por las 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, switches, routers, etc.

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 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):

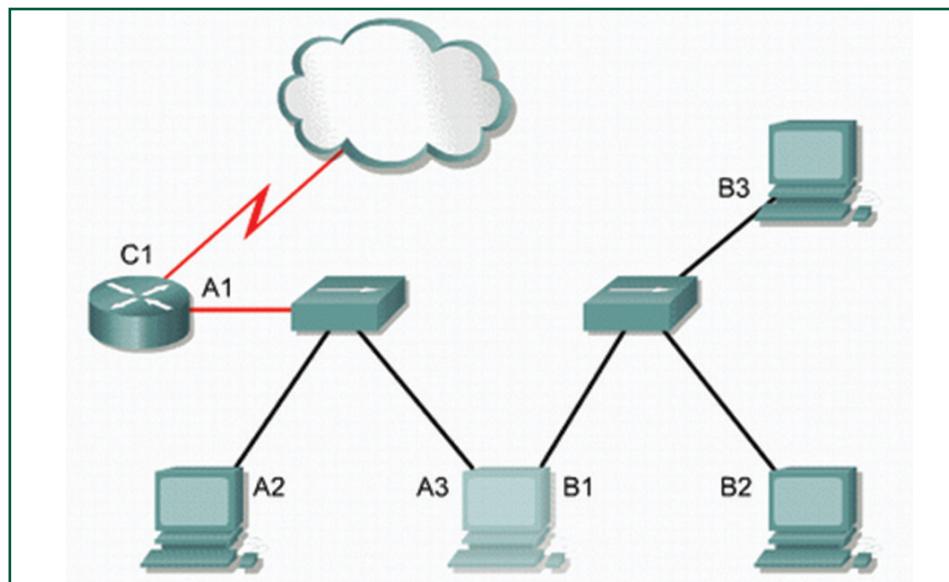


Figura 5.7
Estructura de una red donde intervienen varios nodos de conexión.

- **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:

- **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.
- **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 conexión 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 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).

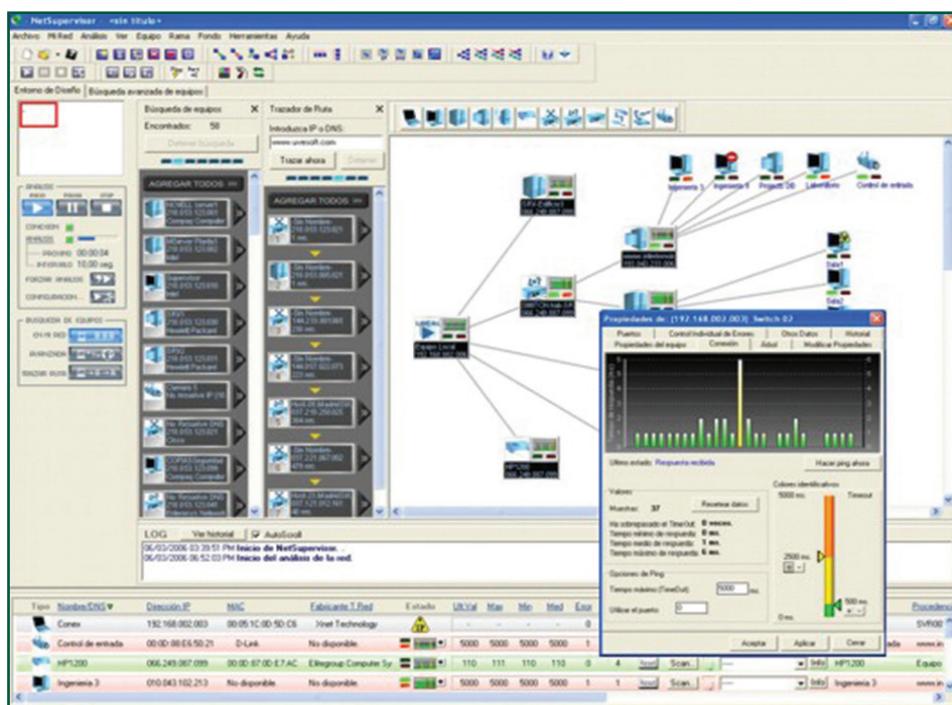


Figura 5.8
Software netSupervisor de monitorización de una red.

Para saber más

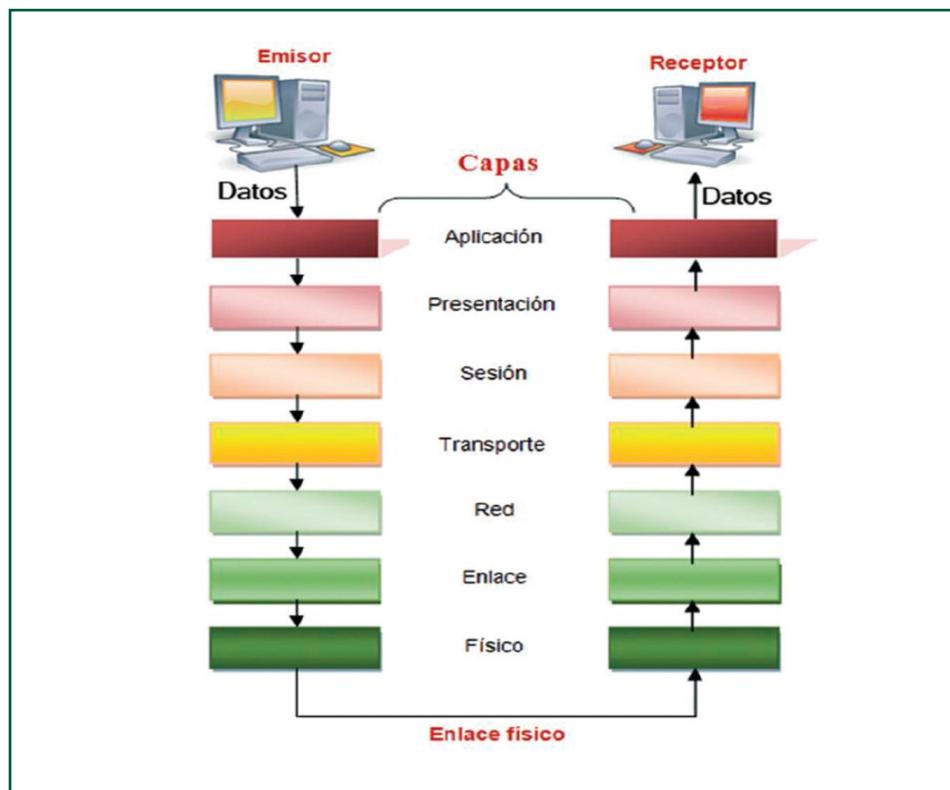
Un software multiplataforma para monitorizar redes es OverLook (<http://overlooksoft.com/>)

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.

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.
- **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).

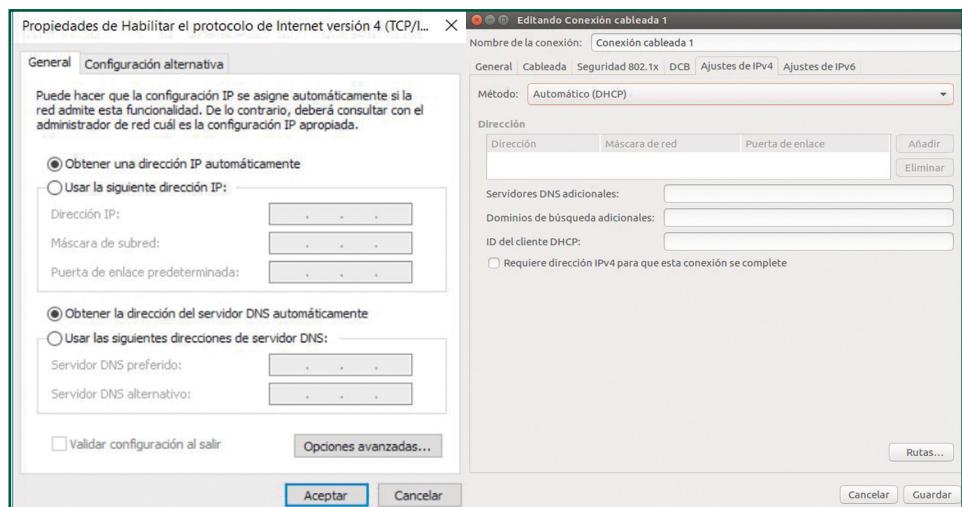


Figura 5.10

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

5.13 Software de configuración de los dispositivos de red

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, fue necesario un software de configuración proporcionado por el fabricante para poder utilizarlos puesto que los sistemas operativos no permitían en un principio la configuración de redes inalámbricas de forma nativa (Figura 5.11).

**Figura 5.11**

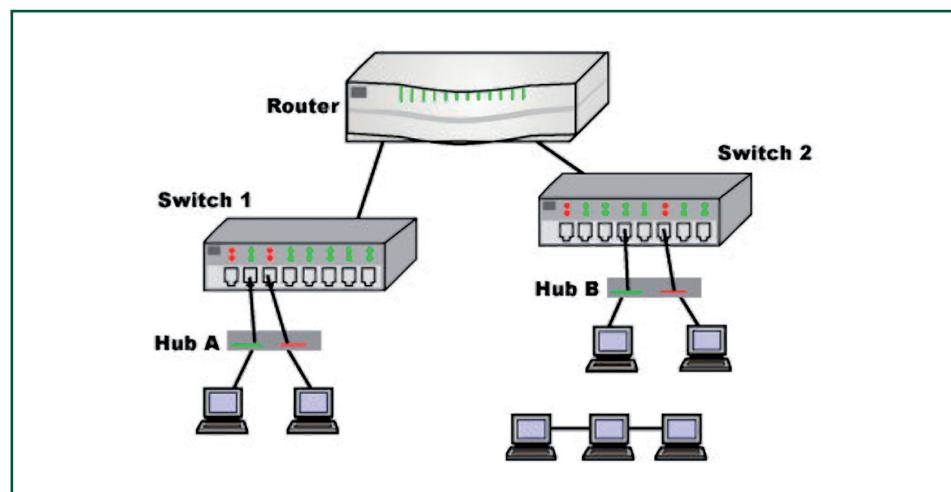
Pantalla del software de configuración de un dispositivo Wi-Fi.

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:

Para saber más

Cada adaptador de red que se vende en el mercado es identificado por un número 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.

- **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.
- **Switch (comutador).** 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. Comutadores, enrutadores, entre otros

Las redes cableadas se pueden dividir según su estructura física y su estructura lógica.

Las topologías físicas representan la manera en la que se realizan las conexiones físicas entre los diferentes nodos de una red. Dentro de esta categoría existen diferentes topologías (Figura 5.13):

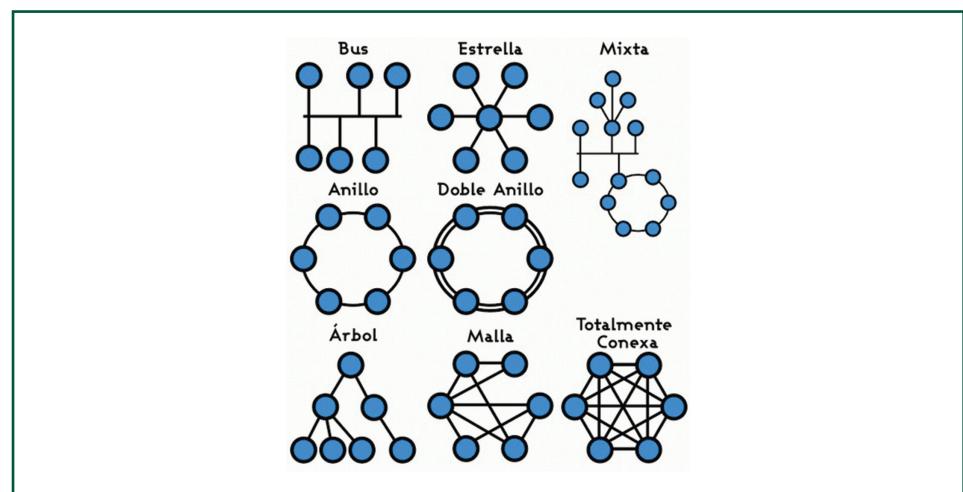


Figura 5.13

Tipologías físicas de una red de área local.

- 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 tráfico 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 existe 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*.

- 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.

Para saber más

Las redes Ethernet son el estándar de las redes de área local utilizadas actualmente en la mayoría de redes.

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).

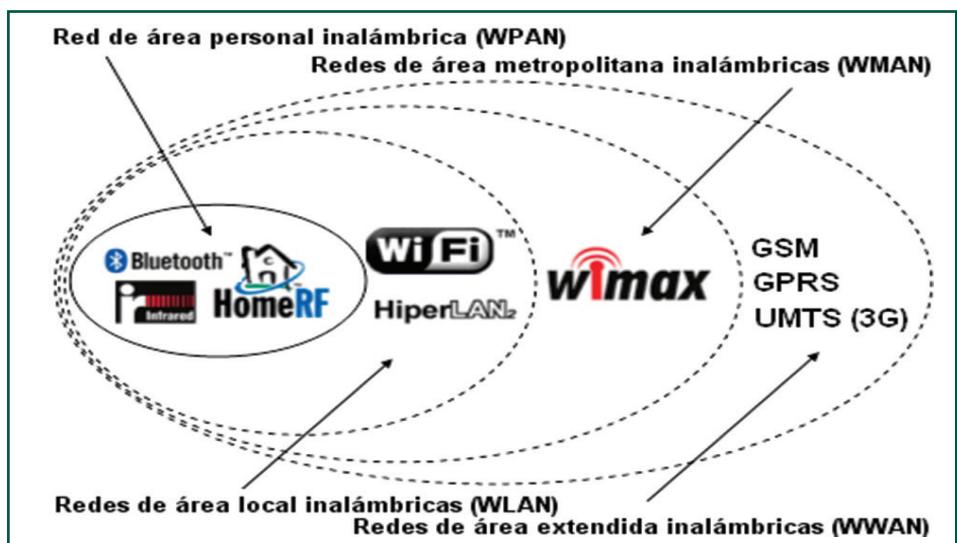


Figura 5.14

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. El listado de especificaciones más usados han sido **GPRS, GSM, 2G, 3G y 4G**.

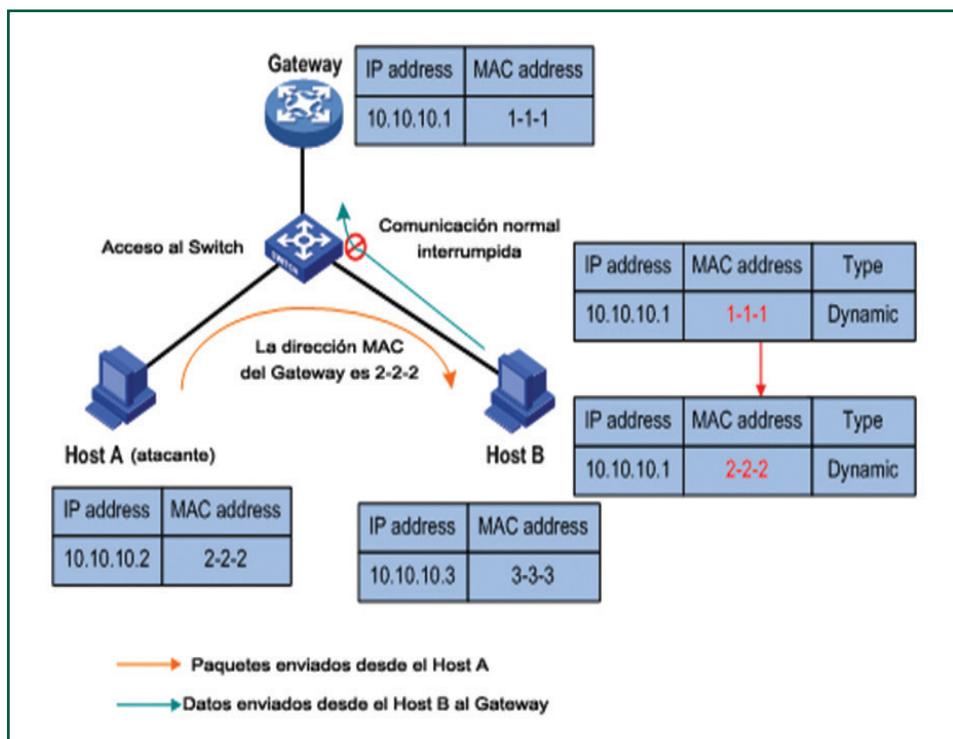
5.17 Seguridad básica en redes cableadas e inalámbricas

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 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

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).

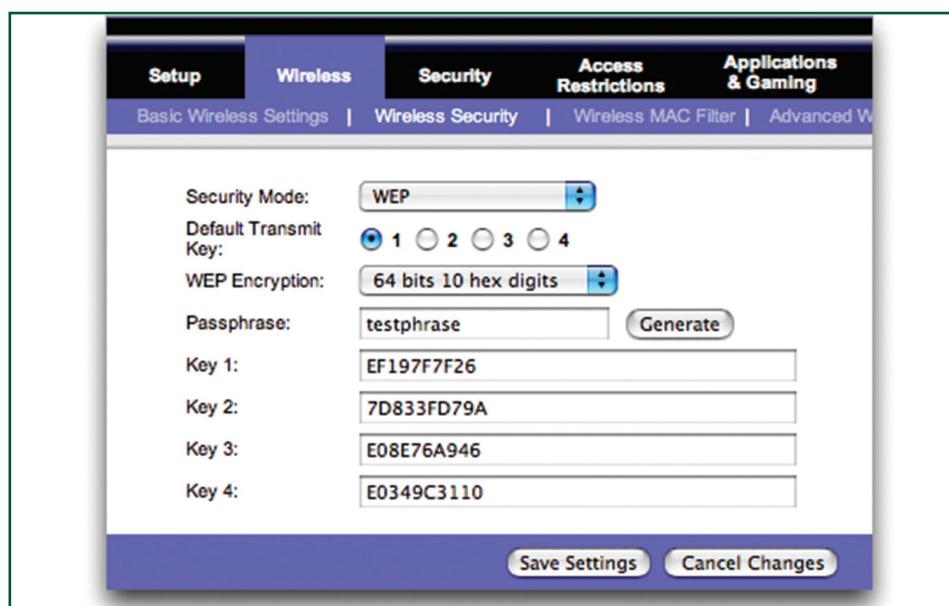


Figura 5.16

Definición de las claves de encriptación de un dispositivo Wi-Fi.

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** se refiere a 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 problema la utilización de este sistema, puesto que un empleado que no pertenezca 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 fiables 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 significativo de una red WAN. Normalmente, la WAN es una red punto a punto, es decir, red de paquetes conmutados. Las redes WAN pueden usar sistemas de comunicación vía satélite o de radio.

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 establecer 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).

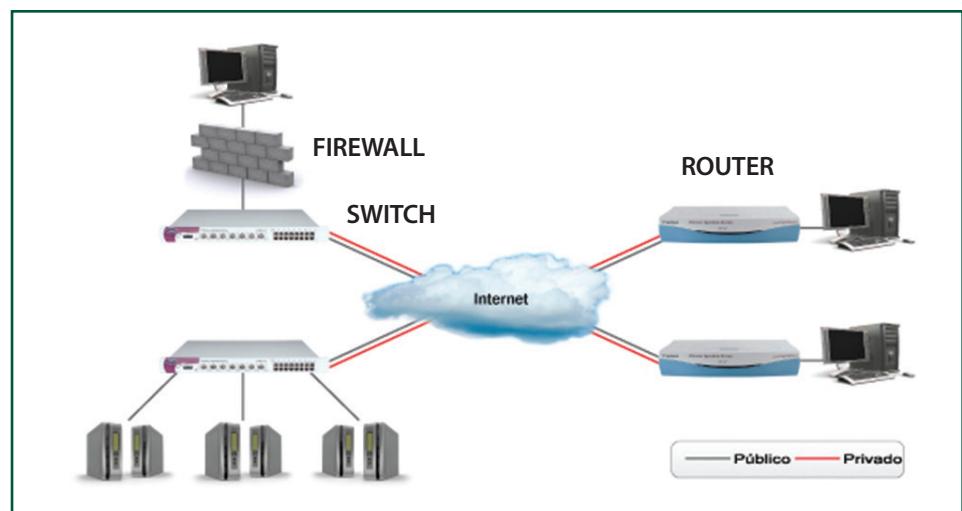


Figura 5.17

Esquema de Internet.

El ATM (en inglés *Asynchronous Transfer Mode* o Modo de Transferencia Asíncrona) es una tecnología de telecomunicación que se basa en la división de la información en cortos paquetes (celdas ATM) de longitud constante, que no son enviados por un mismo canal asignado, sino que son enrutados por canales virtuales hacia el destino. Este sistema permite hacer 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 indispensable una correcta configuración del sistema que dificulte los ataques de terceros que podrían afectar al funcionamiento de la red o poner en peligro la confidencialidad 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 modifiquen las configuraciones de cortafuegos o conexiones de Internet indispensables para evitar ataques a partir de los equipos clientes.

En cuanto al servidor, hay que identificar la información más sensible para almacenarla, si es necesario, en un dispositivo aislado de la red exterior y al que solo se pueda acceder desde los equipos conectados a la red previa autenticación de los usuarios.

El **cortafuegos** (en inglés, *firewall*) es el *software* o *hardware* mediante el cual se aislan 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.

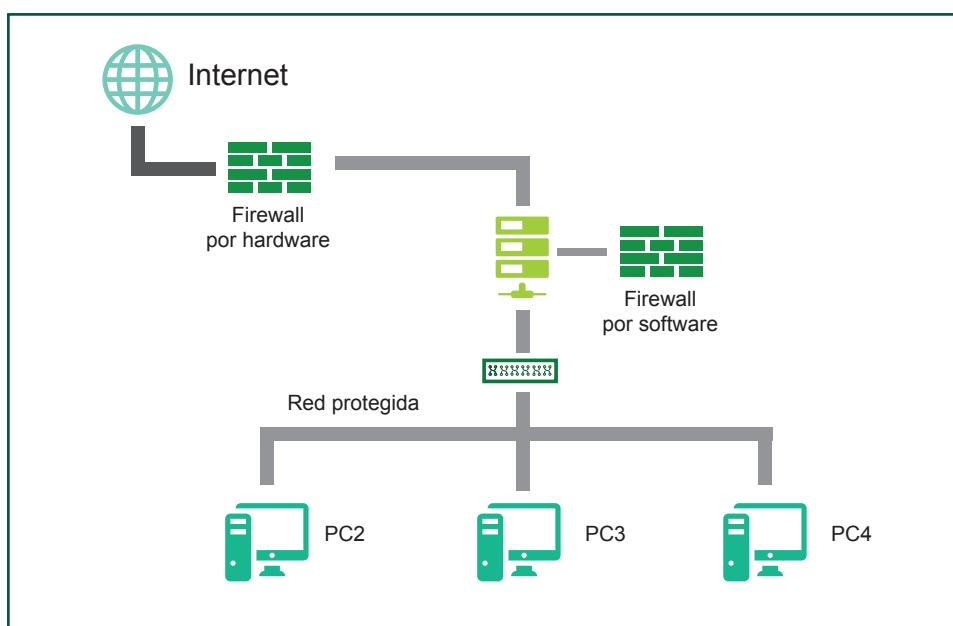


Figura 5.18

Esquema de una red con un dispositivo cortafuegos a la entrada de Internet y un software cortafuegos en el servidor central.

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.

Ejercicios de autocomprobación

Indica si las siguientes afirmaciones son verdaderas (V) o falsas (F):

1. A la hora de incorporar una máquina en una red, no es necesario tener consideraciones previas y basta configurar el nuevo equipo para que pueda comunicarse correctamente con el resto de nodos de la red, incluido el servidor.
2. IP es una combinación numérica de 32 bits, que generalmente se representa de manera decimal, separando cada octeto de bits por un punto.
3. 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 periodo 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.
4. La manera más rápida de comprobar el correcto funcionamiento de una red 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.
5. Duplicidad en la red es un error debido a una asignación repetida de la misma IP entre varios equipos de la misma red.
6. Las redes cableadas se pueden dividir según su estructura física y su estructura lógica.
7. El modelo TCP/IP es el conjunto de protocolos utilizados para poder realizar las conexiones de red.

Completa las siguientes afirmaciones:

8. El enrutamiento determinístico consiste en configurar los _____, que son los dispositivos encargados de dirigir los _____ dentro y fuera de la _____, de manera manual, definiendo en una tabla la _____ IP del router de las otras redes. Esto es una _____ debe realizarse únicamente en redes pequeñas, puesto que el mantenimiento para redes con muchos routers sería muy costoso.

9. Para comprobar el estado de nuestra _____ y detectar cualquier nodo que pudiera estar experimentando un mal funcionamiento, es necesario monitorizar todas las _____ y dispositivos de la red. Esto se realiza generalmente con _____ instalado en el _____ que 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 _____ del sistema en caso de encontrar cualquier error.
10. Los dispositivos de _____ son configurados mediante los propios sistemas operativos, pero es posible instalar _____ para configurarlos que añade nuevas funcionalidades como la creación de estadísticas, monitorización de _____ o simplemente una visualización más atractiva que la proporcionada por la del sistema operativo.

Las soluciones a los ejercicios de autocomprobación se encuentran al final de este módulo. En caso de que no los hayas contestado correctamente, repasa la parte de la lección correspondiente.

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).

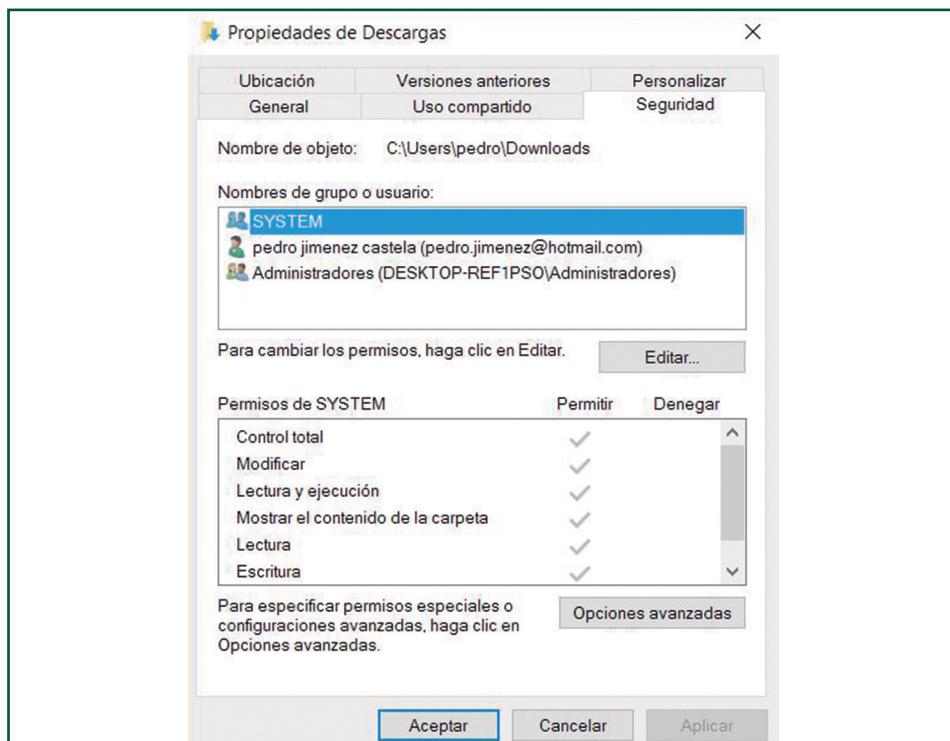


Figura 6.1

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.

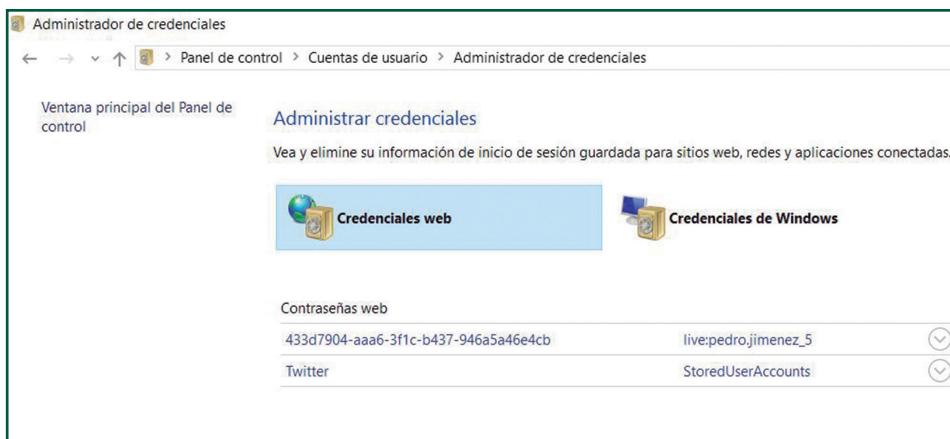
En cuanto a las instalaciones, una de las cosas más importantes es preparar el entorno para evitar que se puedan realizar intrusiones desde el exterior. Los dispositivos cortafuegos permiten que la comunicación fluya entre la red de área local y el exterior, al mismo tiempo que evita que entidades externas 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).

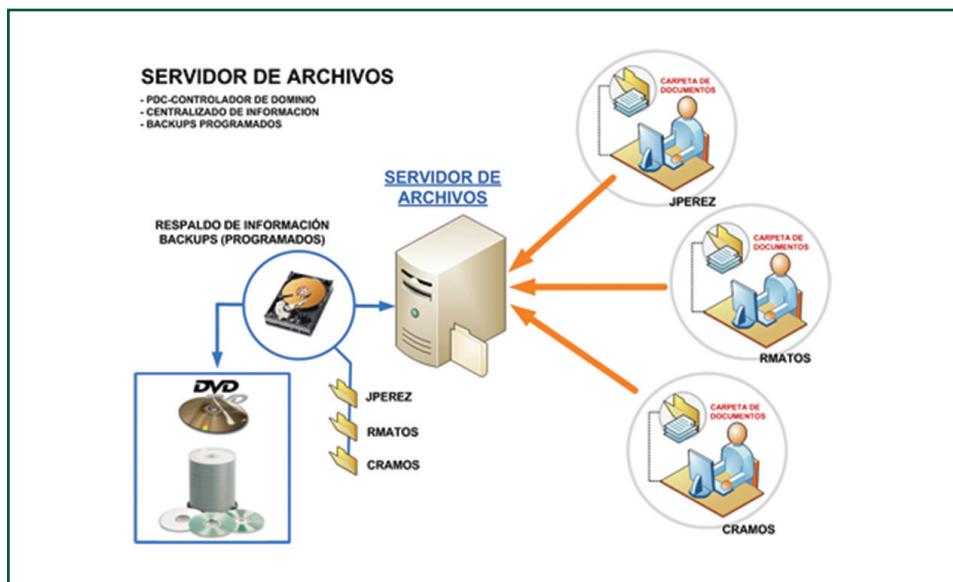


Figura 6.3

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/>).

Evidentemente, esta manera de almacenar archivos supone un problema cuando el mismo archivo es accedido y modificado por varias personas simultáneamente. El servidor deberá avisar a los editores que otras personas están accediendo al mismo archivo, por lo que existe la posibilidad de que las modificaciones que se realicen no queden registradas.

Las ventajas de utilizar un servidor de archivos son:

- **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:/directorio/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**

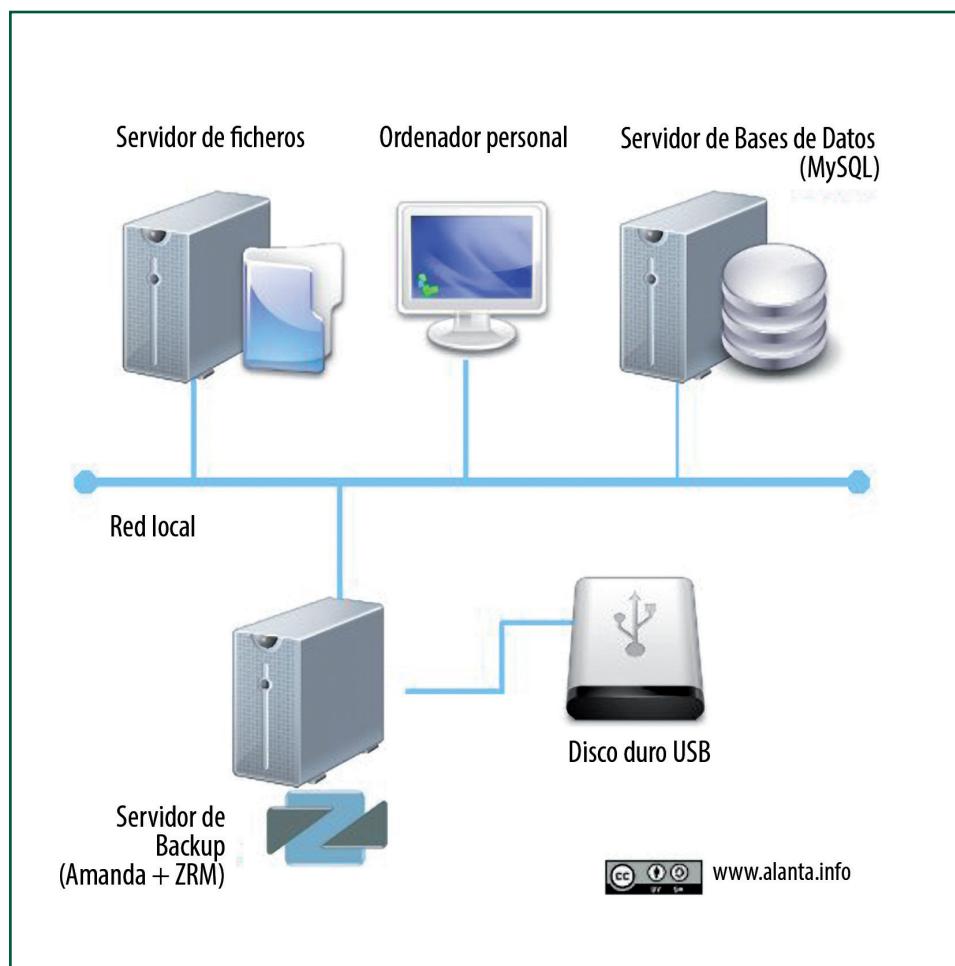
Dispositivo que conecta una impresora USB a la red mediante una conexión inalámbrica, creando un servidor de impresión accesible por el resto de usuarios.

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 las 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.

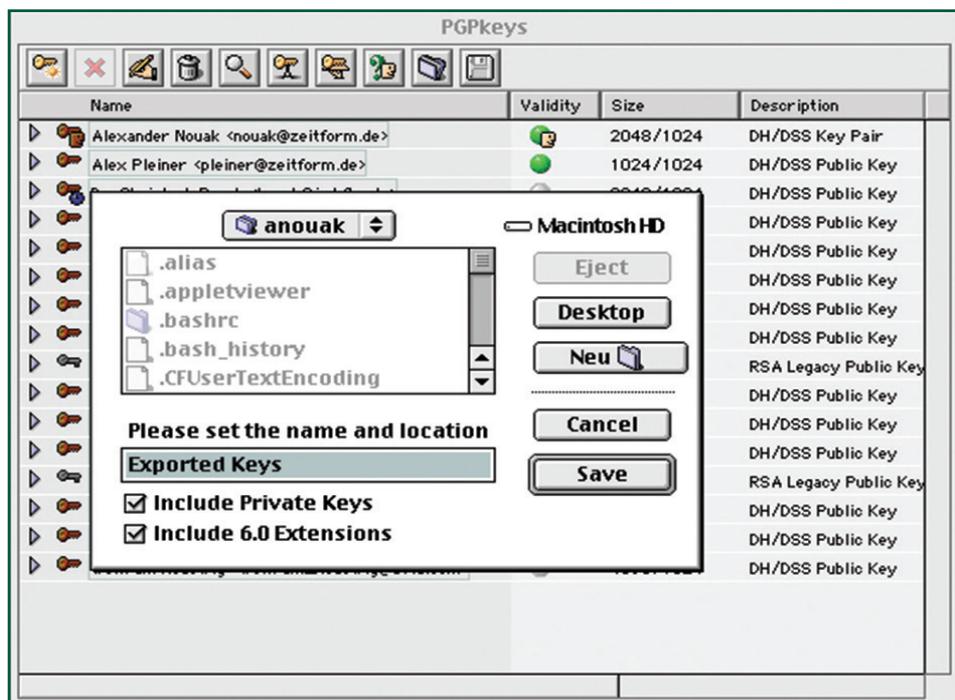
Las técnicas de conexión remota hay que utilizarlas con prudencia en equipos locales utilizados por los usuarios, puesto que hay que tener en cuenta temas como la privacidad o la protección de datos confidenciales. Es recomendable siempre avisar al usuario que se va a acceder a su equipo antes de hacerlo.

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 (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 autenticar y cifrar los datos.

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.

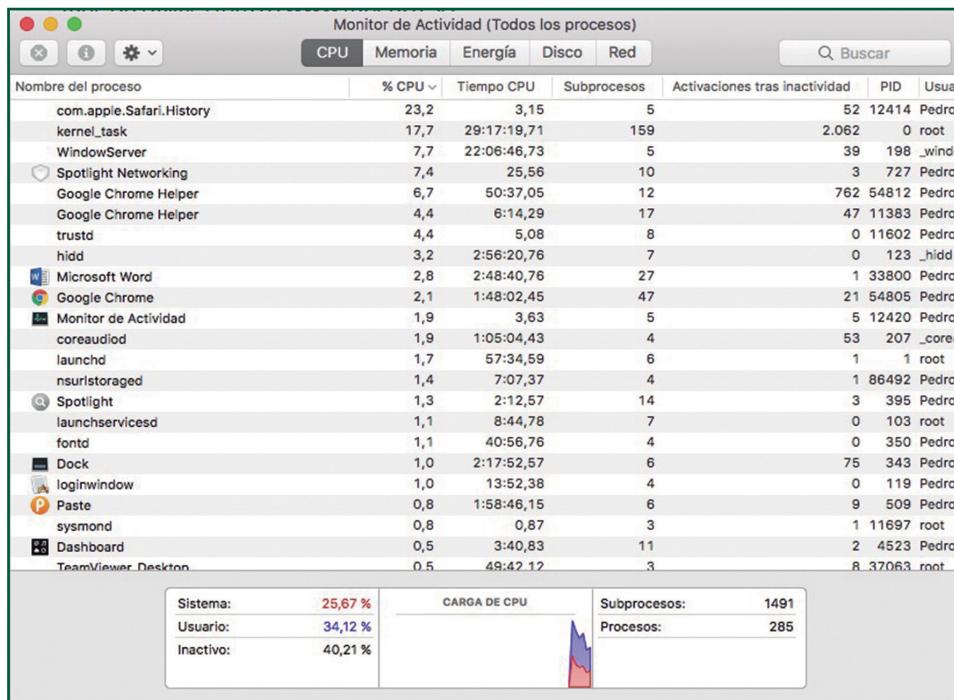
Hay numerosos tipos de cifrado dependiendo del algoritmo utilizado y la decisión de cuál escoge reside en el nivel de seguridad, el tiempo de codificación, la compatibilidad con el software utilizado, etc.

Las herramientas de cifrado son instaladas en los sistemas operativos servidores para encriptar 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 sistema y realizar un informe que detalle la forma en la que los equipos responden a las peticiones de servicio para comprobar el correcto funcionamiento de los sistemas. A pesar de existir herramientas nativas en los sistemas operativos (Figura 6.8), es habitual instalar software externo que realiza análisis mas precisos y exhaustivos, como *Tune Up Utilities* (<http://www.tuneup.es/>).

**Figura 6.8**

Análisis del monitor de actividad de MacOS X.

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 acceso, 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).

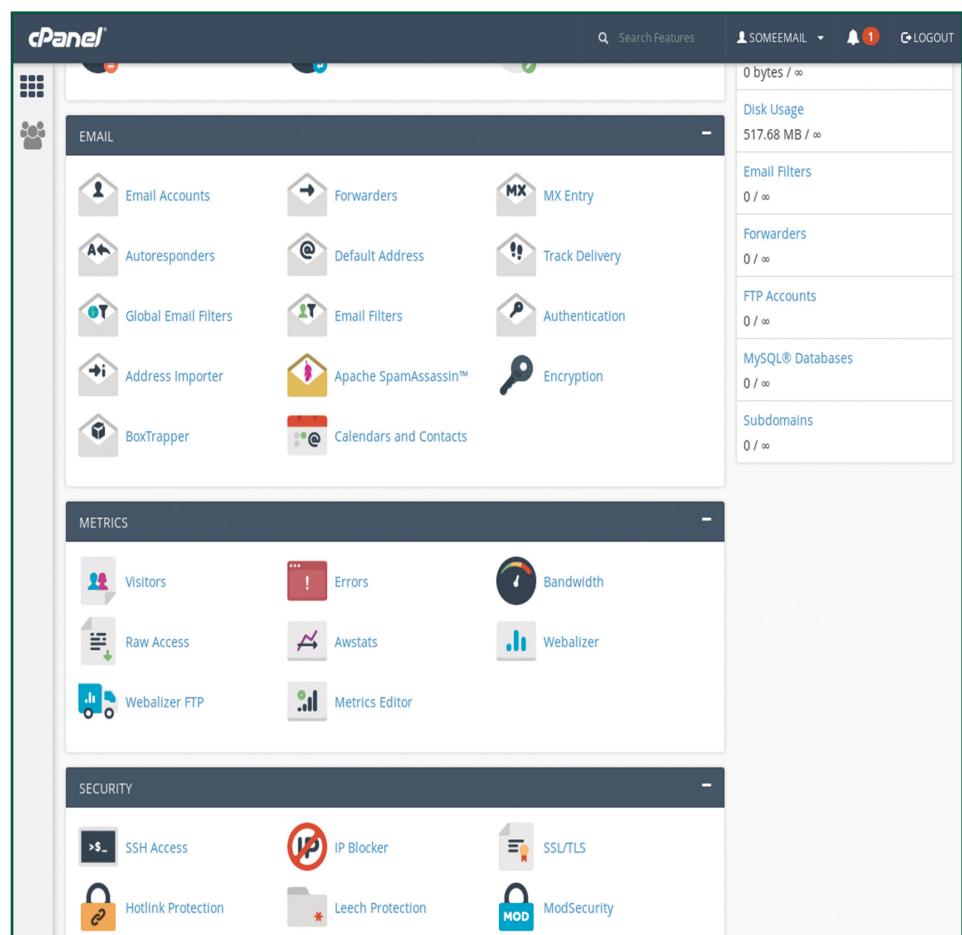


Figura 6.9

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 como último nodo antes de salir al exterior de una red. Por ejemplo, entre el *router* y el servidor.

Un cortafuego 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).

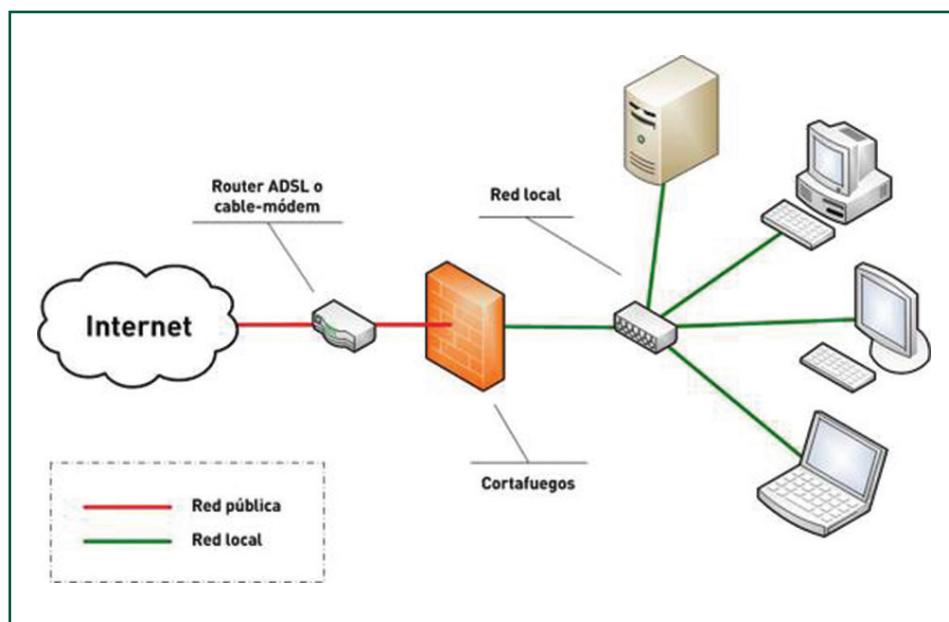


Figura 6.10
Esquema de una red aislada del exterior mediante un cortafuegos que filtra las conexiones entrantes.

Las diferencias entre los diferentes tipos de cortafuegos residen en las capas en que se aplican los filtros:

- **Nivel de aplicación de pasarela.** Aplica los mecanismos de filtrado para aplicaciones específicas, 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:

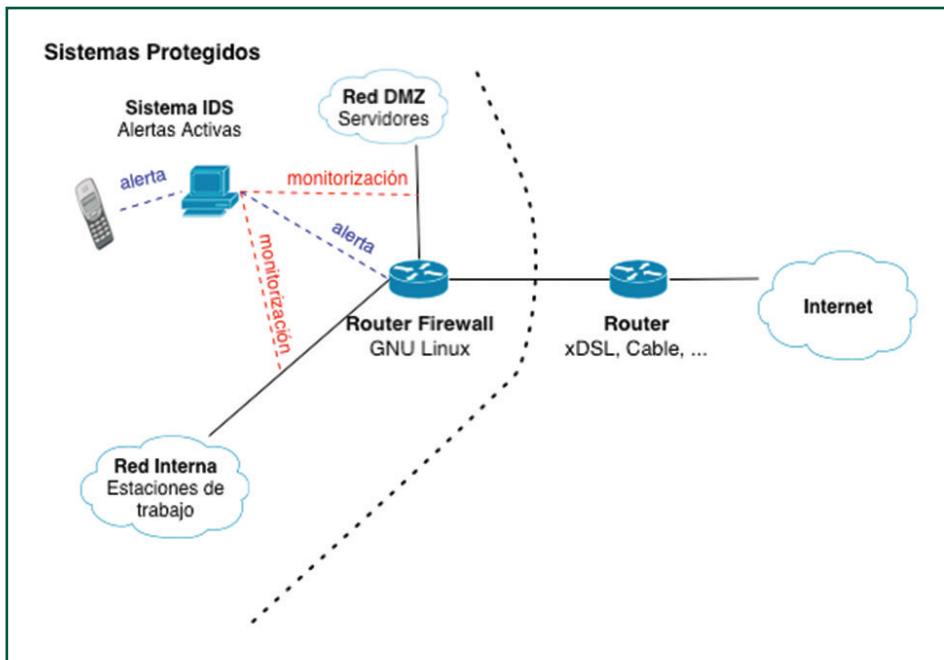
- **Política restrictiva.** Se niega el acceso a cualquier conexión externa excepto aquellas que han sido previamente definidas como permitidas por parte del administrador del sistema.
- **Política permisiva.** Se permite todo el tráfico excepto el que esté explícitamente denegado mediante una lista 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).

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.

**Figura 6.11**

El sistema IDS avisa a los usuarios administradores cuando detecta una intrusión mediante la monitorización del tráfico.

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 los 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 de nuestra organización.

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.

Las soluciones a los ejercicios de autocomprobación se encuentran al final de este módulo. En caso de que no los hayas contestado correctamente, repasa la parte de la lección correspondiente.

7. EXPLORACIÓN 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 específicas. La lista de este tipo de software es realmente larga, puesto que comprende la mayoría del software existente; como, por ejemplo, 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 término *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).

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.

Recuerda

Las licencias libres
pueden proporcionar
beneficios económicos
mediante otras vías.

re 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, la capacidad que tienen actualmente es muy limitada, siendo un requisito a muy tener en cuenta a la hora de utilizar un programa en nuestro sistema (Figura 7.1).

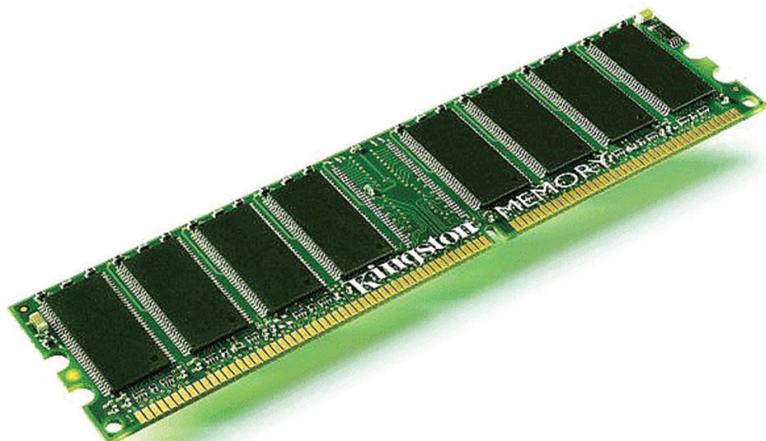


Figura 7.1

Memoria de un ordenador.

- **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 están fomentando almacenar la información en servidores externos, ya sea guardando archivos en servicios como DropBox o visualizando películas vía *streaming*.

- **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, debemos 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.

Para saber más

El término *streaming* es utilizado para definir la visualización de vídeos a través de Internet sin necesidad de descargarlos previamente. Youtube muestra videos vía streaming.

- **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.

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 (Figura 7.2).

Para saber más

La nube son los servidores accesibles desde Internet en los que podemos almacenar información y recuperarla en cualquier ordenador con conexión.



Figura 7.2
Un ejemplo de herramienta ofimática en la nube es Google Docs.

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:

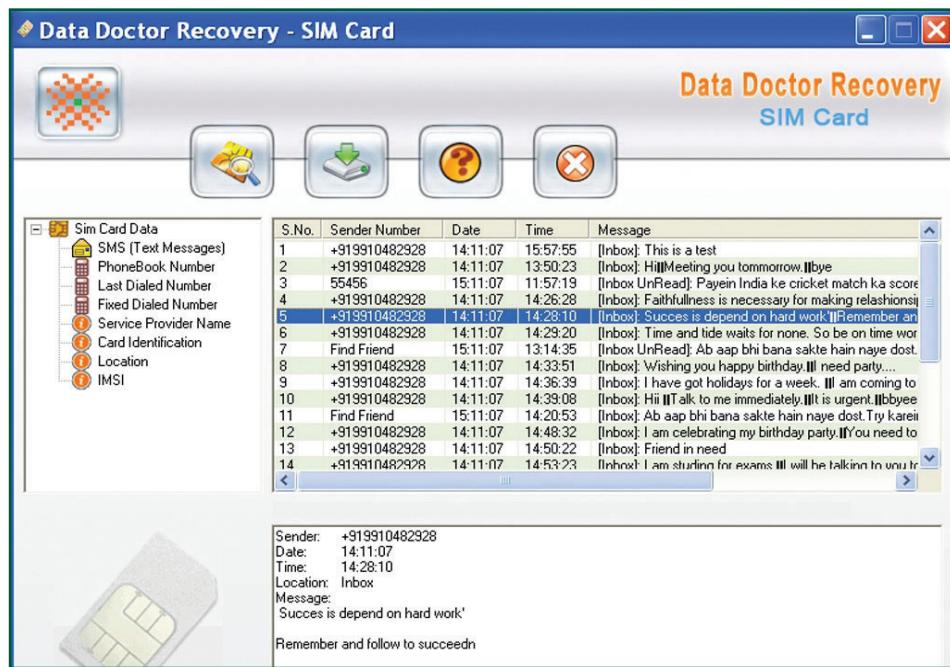
- **Redes sociales:** sistemas que actualmente están cambiando la manera en la que se relacionan las personas. Son plataformas que permiten a las personas compartir información con aquellos usuarios que tengan en sus listas de contacto o mantener el contacto con aquellos conocidos, hecho que, de manera 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 85% de los internautas, es www.google.es.
- **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

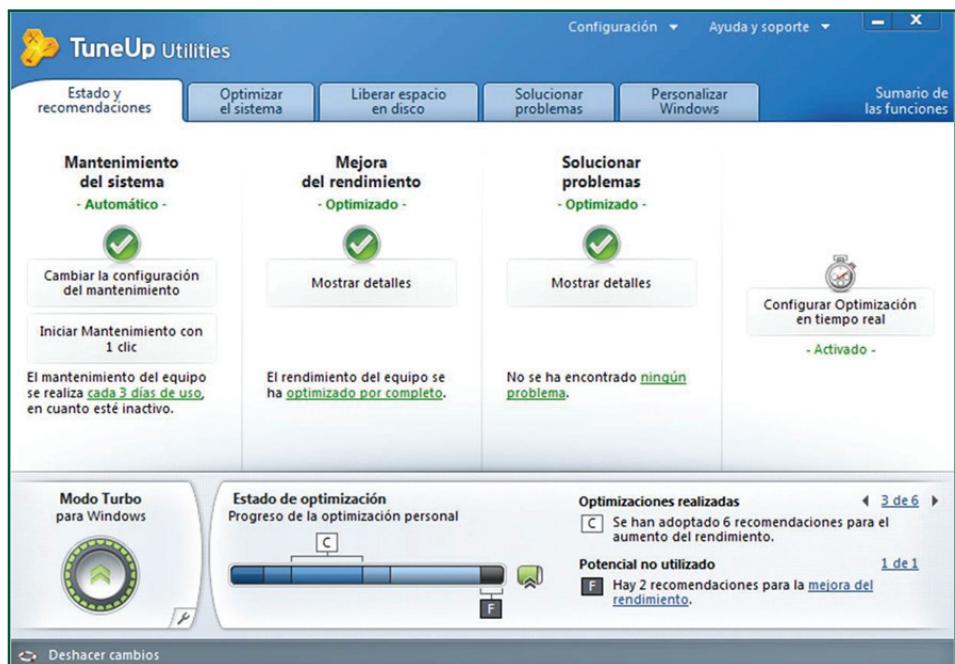
una empresa, sino que son desarrollados y comercializados o distribuidos para poder dar cobertura a las necesidades que pueden ser comunes a cualquier empresa o usuario. A continuación, podríamos definir algunas de las utilidades de propósito general más utilizadas generalmente:

- **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 especialmente 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 7.3).

**Figura 7.3**

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.



Software de recuperación de datos.

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 ma-

nera 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.

Las soluciones a los ejercicios de autocomprobación se encuentran al final de este módulo. En caso de que no los hayas contestado correctamente, repasa la parte de la lección correspondiente.

Soluciones de los ejercicios de autocomprobación

Unidad 1

1. V
2. V
3. F. Dada la rápida evolución del software y sus necesidades de rendimiento, no es habitual encontrar equipos que puedan soportar las necesidades de procesamiento de un programa, y que no tengan memoria RAM suficiente.
4. F. El hardware es el conjunto de máquinas que permite, directa o indirectamente, automatizar la resolución del problema siguiendo las instrucciones de los programadores.
5. V
6. V
7. trabajo, instrucciones, programas, operativo, datos.
8. representación, telecomunicación, nodos, dispositivos, enlaces.
9. redes, cables, tensiones, distancia, bits.
10. red, esquema, dirección, electrónica, servidores

Unidad 2

1. F. El sistema operativo es un conjunto de programas responsable de la gestión de los recursos que proporciona el hardware.
2. V
3. V
4. V
5. F. El paso más importante al virtualizar un sistema operativo es definir los parámetros, como la cantidad de memoria o el tamaño de disco duro que se dedicarán exclusivamente a ese sistema.
6. F. Cada sistema operativo se adapta solo a determinadas máquinas; por lo tanto, el sistema operativo y el hardware deben escogerse conjuntamente.
7. V
8. requisitos, versión, potencia, procesamiento, memoria.
9. utilidad, uso, persona, equipo, Microsoft.
10. instalación, versiones, software, actualización.

Unidad 3

1. V
2. V

3. F. 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.

4. V

5. V

6. V

7. F. 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.

8. archivos, informático, digital, USB, DVD.

9. BIOS, particiones, matrices, archivos, seguridad.

10. carpeta, volumen, archivos, Explorador, icono.

Unidad 4

1. V

2. F. La cuenta de usuario invitado, cuyo nombre es Guest, no tiene derechos sobre el sistema y su función es facilitar la rápida asignación de unos derechos mínimos sobre recursos muy concretos a un usuario ocasional del sistema.

3. F. El acceso a un recurso se controla mediante sus propiedades, que pueden ser cambiadas exclusivamente por el propietario, el cual decide que privilegios otorga a que usuarios o grupos. En Windows no hay límite sobre la cantidad de usuarios y grupos que pueden tener acceso a un fichero.

4. V

5. V

6. F. Los semáforos son mecanismos de sincronización que permiten al sistema bloquear servicios para ordenar la capacidad de procesamiento del hardware. Un semáforo es inicializado con un número entero no negativo que representa el número de procesos a ser ejecutados en un mismo momento.

7. V

8. programa, contraseña, autenticación, cuenta.

9. seguridad, usuario, lectura, modificación.

10. contraseñas, software, usuarios, seguridad.

Unidad 5

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

2. V

3. V

4. V
5. V
6. V
7. V
8. routers, paquetes, red, dirección, configuración.
9. red, conexión, software, servidor, administrador.
10. red, software, conexiones, interfaz.

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.
10. administradores, recurso, ordenadores, servidores.

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

Presentación del curso	3
Introducción al módulo	5
Esquema de contenido	7
1. Explotación de sistemas microinformáticos	11
1.1 Arquitectura de ordenadores	11
1.2 Componentes de un sistema informático	15
1.3 Periféricos. Adaptadores para la conexión de dispositivos.....	16
1.4 Chequeo y diagnóstico	18
1.5 Herramientas de monitorización	18
1.6 Normas de seguridad y prevención de riesgos laborales	19
1.7 Sistemas de comunicación	21
1.8 Características de una red: ventajas e inconvenientes	21
1.9 Tipos de redes	22
1.10 Componentes de una red informática	23
1.11 Topologías de red	24
1.12 Medios de transmisión	25
1.13 Tipos de cableado. Conectores	26
1.14 Mapa físico y mapa lógico de una red local	28
Resumen	29
Ejercicios de autocomprobación	30
2. Instalación de sistemas operativos	32
2.1 Estructura de un sistema informático	32
2.2 Arquitectura de un sistema operativo	34
2.3 Funciones de un sistema operativo	35
2.4 Tipos de sistemas operativos	37
2.5 Tipos de aplicaciones	38
2.6 Licencias y tipos de licencias	39

2.7 Gestores de arranque	40
2.8 Máquinas virtuales	41
2.9 Consideraciones previas a la instalación de sistemas operativos libres y propietarios	44
2.10 Instalación de sistemas operativos. Requisitos, versiones y licencias	45
2.11 Instalación y desinstalación de aplicaciones. Requisitos, versiones y licencias	47
2.12 Uso de instalaciones desatendidas	47
2.13 Actualización de sistemas operativos y aplicaciones	48
2.14 Ficheros de inicio de sistemas operativos	49
2.15 Controladores de dispositivos	50
Resumen	52
Ejercicios de autocomprobación	53

3. Gestión de información	55
3.1 Sistemas de archivos	55
3.1.1. FAT	56
3.1.2. NTFS	57
3.1.3. Otros sistemas	57
3.2 Gestión de sistemas de archivos mediante comandos y entornos gráficos	58
3.3 Estructura de directorios de sistemas operativos libres y propietarios	59
3.4 Búsqueda de información del sistema mediante comandos y herramientas gráficas	63
3.5 Identificación del software instalado mediante comandos y herramientas gráficas	65
3.6 Gestión de la información del sistema. Rendimiento. Estadísticas. Montaje y desmontaje de dispositivos en sistemas operativos	66
3.7 Herramientas de administración de discos	67
3.8 Sistemas de archivos de red y matrices de discos RAID	69
3.9 Gestión de archivos	71
3.9.1 Rutas	71
3.9.2 Herramientas de gestión de archivos	72
3.10 Montar volúmenes en carpetas	73
3.11 Tolerancia a fallos	74
3.12 Tareas automáticas	76
Resumen	78

Ejercicios de autocomprobación	79
	81
4. Configuración de sistemas operativos	81
4.1 Configuración de usuarios y grupos locales	82
4.2 Usuarios y grupos predeterminados	83
4.2.1 Usuarios y grupos predeterminados en entornos Windows	83
4.2.2 Usuarios y grupos predeterminados en entornos Unix	84
4.3 Seguridad de cuentas de usuario	85
4.4 Seguridad de contraseñas	86
4.4.1 Acceso a los recursos. Permisos locales	86
4.4.2 Acceso a los recursos del sistema en Unix	87
4.4.3 Acceso a los recursos del sistema en Windows	88
4.5 Directivas locales	90
4.6 Servicios y procesos	91
4.6.1 La comunicación de los procesos	93
4.6.2 Semáforos	94
4.6.3 Mutex	94
4.7 Comandos de sistemas libres y propietarios	95
4.8 Herramientas de monitorización del sistema	95
4.8.1 Monitorización en Windows	96
4.8.2 Monitorización en Unix	97
Resumen	98
Ejercicios de autocomprobación	100
5. Conexión de sistemas en red	100
5.1 Configuración del protocolo TCP/IP en un cliente de red	100
5.1.1 Configuración del protocolo TCP/IP en un cliente de red	101
5.1.2 Direcciones IPv	101
5.1.3 Máscaras de subred	102
5.1.4 IPv4. IPv6	102
5.1.5 Configuración estática	103
5.2 Configuración dinámica automática	103

5.2.1 Direcciones dinámicas	103
5.2.2. Direcciones fijas	104
5.3 Configuración de la resolución de nombres	105
5.4 Ficheros de configuración de red	106
5.5 Tablas de enrutamientos	106
5.5.1 Determinísticos o estáticos	107
5.5.2 Adaptativos o dinámicos	107
5.6 Gestión de puertos	108
5.7 Verificación del funcionamiento de una red mediante el uso de comandos	109
5.8 Resolución de problemas de conectividad en sistemas operativos en red	110
5.9 Comandos utilizados en sistemas operativos libres y propietarios	111
5.10 Monitorización de redes	112
5.11 Protocolos TCP/IP	113
5.12 Configuración de los adaptadores de red en sistemas operativos libres y propietarios	114
5.13 Software de configuración de los dispositivos de red	115
5.14 Interconexión de redes: adaptadores de red y dispositivos de interconexión	
5.15 Redes cableadas. Tipos y características. Adaptadores de red. Conmutadores, enrutadores, entre otros	116
5.16 Redes inalámbricas. Tipos y características	118
5.17 Seguridad básica en redes cableadas e inalámbricas	119
5.18 Seguridad en la comunicación de redes inalámbricas	121
5.19 Acceso a redes WAN. Tecnologías	122
5.20 Seguridad de comunicaciones	123
Resumen	125
Ejercicios de autocomprobación	126
	128

6. Gestión de recursos en una red

6.1 Diferencias entre permisos y derechos. Permisos de red. Permisos locales. Herencia. Permisos efectivos. Denegación de permisos	128
6.1.1 Diferencias entre permisos y derechos	128
6.1.2 Permisos de red	129
6.1.3 Permisos locales	130

6.1.4 Herencia	130
6.1.5 Permisos efectivos	130
6.1.6 Denegación de permisos	
6.2 Derechos de usuarios. Directivas de seguridad. Objetos de directiva. Ámbitos de las directivas.	131
Plantillas	131
6.3 Requisitos de seguridad del sistema y de los datos	132
6.4 Seguridad a nivel de usuarios y seguridad a nivel de equipos	133
6.5 Servidores de archivos	135
6.5.1 Tipos de servidores de archivos	136
6.5.2 Sistemas múltiples	136
6.5.3 Medidas de seguridad y problemas en el sistema de archivos	138
6.6 Servidores de impresión	139
6.7 Servidores de aplicaciones	140
6.8 Técnicas de conexión remota	141
6.9 Herramientas de cifrado	142
6.10 Herramientas de análisis y administración	145
6.11 Cortafuegos	146
6.12 Sistemas de detección de intrusión	148
Resumen	149
Ejercicios de autocomprobación	
	151
7. Explotación de aplicaciones informáticas de propósito general	151
7.1 Tipos de software	153
7.1.1 Desarrollo de software libre	153
7.2 Requisitos del software	155
7.3 Herramientas ofimáticas	157
7.4 Herramientas de Internet	158
7.5 Utilidades de propósito general	161
Resumen	162
Ejercicios de autocomprobación	164
Soluciones de los ejercicios de autocomprobación	

